KASPERSKY lab

Kaspersky Security для Windows Server

Руководство администратора

Версия программы: 10.1.0.622

Уважаемый пользователь!

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

Дата редакции документа: 18.04.2018

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

Содержание

Об этом руководстве

Руководство администратора Kaspersky Security 10.1.0.622 для Windows Server (далее также "Kaspersky Security 10.1 для Windows Server") адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security 10.1 для Windows Server на всех защищаемых устройствах, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security 10.1 для Windows Server.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Security 10.1 для Windows Server.

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

В этом разделе

В этом документе

Руководство администратора Kaspersky Security 10.1 для Windows Server содержит следующие разделы:

Источники информации о Kaspersky Security 10.1 для Windows Server

Этот раздел содержит описание источников информации о программе.

Kaspersky Security 10.1 для Windows Server

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Security 10.1 для Windows Server, перечень аппаратных и программных требований Kaspersky Security 10.1 для Windows Server.

Установка и удаление Kaspersky Security 10.1 для Windows Server

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Security 10.1 для Windows Server.

Интерфейс программы

Этот раздел содержит информацию об элементах интерфейса Kaspersky Security 10.1 для Windows Server.

Лицензирование программы

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

Запуск и остановка Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о запуске Плагина управления Kaspersky Security 10.1 для Windows Server (далее также "Плагин управления Kaspersky Security 10.1") и службы Kaspersky Security Service.

Права доступа к функциям Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о правах на управление Kaspersky Security 10.1 для Windows Server и службами Windows®, которые регистрирует программа, а также инструкции по настройке этих прав.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления задачами Kaspersky Security 10.1 для Windows Server на нескольких серверах.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Security 10.1 для Windows Server, их создании, настройке параметров выполнения, запуске и остановке.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center.

Постоянная защита сервера

Этот раздел содержит информацию о задачах постоянной защиты: Постоянная защита файлов, 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 Security 10.1 для Windows Server, которая позволяет контролировать запуски и программ подключения флеш-накопителей других внешних устройств по USB

Контроль активности в сети

Этот раздел содержит информацию об управлении сетевым экраном: о том, как работать с правилами сетевого экрана и как настраивать параметры задач.

Диагностика системы

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

Контроль производительности. Счетчики Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о счетчиках Kaspersky Security 10.1 для Windows Server: счетчиках производительности для программы Системный монитор, счетчиках и ловушках SNMP.

Работа с Kaspersky Security 10.1 для Windows Server из командной строки

Этот раздел содержит описание работы с Kaspersky Security 10.1 для Windows Server 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 о АО "Лаборатории Касперского".

Информация о стороннем коде

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

Уведомления о товарных знаках

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

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

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

Таблица 1. Условные обозначения

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

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

Источники информации о Kaspersky Security 10.1 для Windows Server

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

Информацию о Kaspersky Security 10.1 для Windows Server можно найти в следующих источниках:

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

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

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

Страница Kaspersky Security 10.1 для Windows Server на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security 10.1 для Windows Server (https://www.kaspersky.ru/small-to-medium-business-security/windows-server-security) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security 10.1 для Windows Server содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Security 10.1 для Windows Server в Базе знаний

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

На странице Kaspersky Security 10.1 для Windows Server в Базе знаний (https://support.kaspersky.ru/ksws10/) вы найдете статьи с полезной информацией, рекомендации и ответы на часто задаваемые вопросы о том, как купить, установить и использовать программу.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security 10.1 для Windows Server, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Документация Kaspersky Security 10.1 для Windows Server

Руководство администратора Kaspersky Security 10.1 для Windows Server содержит информацию об установке, удалении, настройке параметров и использовании программы.

Обсуждение программ "Лаборатории Касперского" на форуме

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

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

Kaspersky Security 10.1 для Windows Server

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Security 10.1 для Windows Server, перечень аппаратных и программных требований Kaspersky Security 10.1 для Windows Server.

В этом разделе

О Kaspersky Security 10.1 для Windows Server

Kaspersky Security 10.1 для Windows Server (ранее Антивирус Kaspersky для Windows Servers Enterprise Edition) защищает серверы,работающие под управлением операционных систем Microsoft® Windows®, и сетевые хранилища от вирусов и других угроз компьютерной безопасности, которым могут подвергаться серверы в результате обмена файлами. Kaspersky Security 10.1 для Windows Server предназначен для использования в локальных сетях организаций от среднего до крупного размера. Пользователями Kaspersky Security 10.1 для Windows Server являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Вы можете установить Консоль Kaspersky Security 10.1 для Windows Server на следующие типы серверов:

- на терминальных серверах;
- на серверах печати;
- на серверах приложений;
- на контроллерах доменов;
- на серверах, защищающих сетевые хранилища;
- на файловых серверах – они более других подвержены заражению, так как обмениваются файлами с рабочими станциями.

Вы можете управлять Kaspersky Security 10.1 для Windows Server следующими способами:

- через Консоль Kaspersky Security 10.1, установленную на одном сервере с Kaspersky Security 10.1 для Windows Server или на другом компьютере;
- с помощью команд командной строки;
- С помощью Консоли администрирования Kaspersky Security Center.

Вы можете использовать программу Kaspersky Security Center для централизованного управления защитой многих серверов, на каждом из которых установлен Kaspersky Security 10.1 для Windows Server.

Вы можете просматривать счетчики производительности Kaspersky Security 10.1 для Windows Server для программы "Системный монитор", а также счетчики и ловушки SNMP.

Компоненты и функции Kaspersky Security 10.1 для Windows Server

В состав программы входят следующие компоненты:

- **Постоянная защита** Kaspersky Security 10.1 для Windows Server проверяет объекты при обращении к ним. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память защищаемого устройства, а также объекты автозапуска.
- **Защита RPC-подключаемых сетевых хранилищ** и **Защита ICAP-подключаемых сетевых хранилищ.** Kaspersky Security 10.1 для Windows Server, установленный на сервере под управлением операционной системы Microsoft Windows, защищает сетевые хранилища от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.
- **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.
- **Защита от шифрования** и **Защита от шифрования для NetApp**. Компоненты выполняют защиту общих сетевых папок защищаемых серверов и сетевых хранилищ от вредоносного щифрования, путем блокировки компьютеров, проявляющих подозрительную активность.
- **Проверка скриптов**. Этот компонент контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies.
- **Защита трафика** Этот компонент перехватывает и проверяет объекты, передаваемые по веб-трафику (включая почтовый трафик), на наличие известных компьютерных и других угроз на защищаемом сервере.
- **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 Security 10.1 для Windows Server обнаруживает изменения в файлах, которые входят в область мониторинга, указанную в параметрах задачи. Эти изменения могут свидетельствовать о нарушении безопасности на защищаемом сервере.
- **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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server сохраняет зашифрованные копии объектов со статусом *Зараженный* или *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 Security 10.1 для Windows Server и состоянием антивирусной защиты компьютера.
- **Импорт и экспорт параметров** Вы можете экспортировать параметры Kaspersky Security 10.1 для Windows Server в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.
- **Управление правами доступа к функциям Kaspersky Security 10.1 для Windows Server**. Вы можете настраивать права на управление Kaspersky Security 10.1 для Windows Server и службами Windows, которые регистрирует программа, для пользователей и групп пользователей.
- **Запись событий в журнал событий программы** Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server, и информацию, необходимую для диагностики сбоев в работе программы.
- **Иерархическое хранилище** Kaspersky Security 10.1 для Windows Server может работать в режиме использования систем управления иерархическим хранилищем (HSM-систем). Использование HSM-системы позволяет перемещать данные между быстрыми локальными дисками и медленными устройствами долговременного хранения информации.
- **Доверенная зона** Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Security 10.1 для Windows Server будет применять в задачах проверки по требованию и постоянной защиты файлов.
- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.
- **Заблокированные узлы**. Вы можете заблокировать компьютеры, пытающиеся получить доступ к общим сетевым папкам сервера, при обнаружении вредоносной активности с их стороны.

Что нового

Kaspersky Security 10.1 для Windows Server - решение для защиты корпоративных серверов и систем хранения данных. Область защиты, доступная при использовании программы (сервера под управлением Windows, системы хранения данных), и набор функциональных компонентов зависит от типа приобретенной лицензии.

В версии Kaspersky Security 10.1 для Windows Server улучшена и в полном объеме сохранена функциональность предыдущей версии программы, а также добавлены новые компоненты защиты.

В Kaspersky Security 10.1 для Windows Server появились следующие возможности:

- Недавно добавленный компонент Защита трафика (см. раздел "Защита трафика" на стр. 207): теперь вы можете защитить свой сервер не только от угроз, проникающих по электронной почте, но и от угроз, поступающих через трафик HTTP или HTTPS. Новый компонент поддерживает следующие сценарии защиты:
  - антивирусная и антифишинговая защита почтового трафика с помощью расширения Kaspersky Security 10.1.0.622 Microsoft Outlook® (далее также "расширение Kaspersky Security 10.1 Microsoft Outlook");
  - антивирусная и антифишинговая защита веб-трафика;
  - проверка веб-ссылок по базам вредоносных веб-адресов;
  - проверка веб-ссылок по облачным базам вредоносных веб-адресов;
  - веб-контроль с помощью правил для веб-ссылок и сертификатов;
  - контроль веб-ресурсов по категориям;
  - проверка валидности сертификатов веб-серверов при подключении.

  Защита трафика выполняется с использованием ICAP-службы и может быть сконфигурирована в одном из трёх вариантов:
  - Внешний прокси-сервер: анализ перенаправленного трафика от внешнего прокси-сервера (без сетевого драйвера).
  - Перенаправление трафика: анализ перенаправленного трафика от браузеров, запущенных в терминальной сессии (без сетевого драйвера). Программа функционирует в режиме внутренней системной прокси.
  - Драйверный перехват: перехват трафика с помощью сетевого драйвера в терминальной сессии.
- Добавлен компонент Защита от шифрования для NetApp: теперь вы можете использовать сервер с установленной программой Kaspersky Security 10.1 для Windows Server для защиты подключаемого сетевого хранилища данных NetApp от вредоносного шифрования.

См. *Руководство по внедрению сетевых хранилищ.*

- Новый компонент Контроль устройств (см. раздел "Создание правил на основе данных системы о внешних устройствах, подключавшихся к компьютерам сети" на стр. 252): теперь вы можете формировать списки правил, которые программа сможет использовать для разрешения или запрещения обмена файлами с внешними устройствами хранения данных (запоминающие устройства USB и MTP, устройства CD/DVD).

- Новый компонент Защита от эксплойтов (см. раздел "Защита от эксплойтов" на стр. 198): теперь вы можете настраивать параметры для защиты от эксплойтов памяти процессов с помощью техник снижения рисков.
- Новый компонент Мониторинг файловых операций (см. раздел "Мониторинг файловых операций" на стр. 271): теперь вы можете выбирать объекты, целостность которых вы хотите контролировать.
- Новый компонент Анализ журналов (см. раздел "Анализ журналов" на стр. 279): теперь вы можете формировать правила для анализа журналов Windows и настраивать эвристический анализатор для их анализа.
- Новая возможность интеграции с внешними системами SIEM (см. раздел "Настройка параметров интеграции с SIEM" на стр. 172): теперь вы можете настраивать параметры экспорта журналов программы в сторонние системы агрегации событий по протоколу syslog.
- Добавлена функциональность отслеживания USB-подключений к защищаемому устройству (см. раздел "О задаче Контроль устройств" на стр.250): теперь вы можете настроить уведомления о фактах подключений различных типов устройств к защищаемому компьютеру через USB-интерфейс.
- Реализован Журнал нарушений безопасности(см. Стр. 172): теперь вы можете просматривать все события, фиксируемые компонентами программы и свидетельствующие о возможной компрометации защищаемой системы, в одном журнале.
- Новый компонент Управление сетевым экраном (см. раздел "Управление сетевым экраном" на стр. 258): теперь вы можете управлять правилами сетевого экрана Windows через графический пользовательский интерфейс Kaspersky Security 10.1 для Windows Server.
- Новая возможность проверять запоминающие устройства USB (см. раздел "Проверка съемных дисков" на стр. 162): теперь вы можете проверять запоминающие устройства, подключенные к защищаемому компьютеру.
- Новая возможность включать защиту паролем для управления программой (см. раздел "Защита доступа к функциям Kaspersky Security 10.1 для Windows Server с помощью пароля" на стр. 106): теперь вы также можете защитить Kaspersky Security 10.1 для Windows Server и использовать пароль для ограничения доступа к критическим операциям.
- Новая возможность автоматически разрешать запуск программ (см. раздел "Настройка контроля распространения программного обеспечения" на стр. 239) из доверенных пакетов установки: теперь вы можете добавлять исключения в параметрах задачи Контроль запуска программ для пакетов установки, чтобы упростить процесс разрешения запуска файлов при установке или обновлении программного обеспечения.
- Добавлена возможность проверки контейнеров Microsoft Windows Server (см.раздел "О задаче Постоянная защита файлов" на стр.178).
- Упрощенное Блокирование доступа к сетевым файловым ресурсам (см. раздел "Блокирование доступа к сетевым файловым ресурсам.Заблокированные узлы" на стр. 166): теперь компоненты Защита от шифрования и Постоянная защита файлов добавляют идентификаторы компьютеров, нарушающих безопасность защищаемого сервера, в хранилище заблокированных узлов. Вы можете выключить заполнение хранилища заблокированных узлов в параметрах задачи защиты. Кроме того, теперь вы можете просмотреть список заблокированных узлов в централизованном списке Консоли Сервера Администрирования.

- Оптимизированные возможности формировать список правил для доверенных процессов (см. раздел "Добавление доверенных процессов" на стр. 159) в доверенной зоне: теперь вы можете исключать процессы только по хэшу, только по пути или по тому и другому вместе.
- Упрощен и расширен механизм наполнения списков правил контроля запуска программ:

  (см.раздел "О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center" на стр.243): добавлена возможность совмещенного использования списков правил, настроенных на локальных компьютерах и в политике Kaspersky Security Center, а также возможность формирования правил на основе событий работы задачи в Kaspersky Security Center.

Комплект поставки

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

- запустить мастер установки Kaspersky Security 10.1 для Windows Server;
- запустить мастер установки Консоли Kaspersky Security 10.1;
- запустить мастер установки Плагина управления Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center;
- прочитать Руководство администратора;
- прочитать Руководство пользователя;
- прочитать Руководство по внедрению для защиты сетевых хранилищ;
- перейти на страницу Kaspersky Security 10.1 для Windows Server на веб-сайте "Лаборатории Касперского" https://www.kaspersky.ru/small-to-medium-business-security/windows-server-security;
- перейти на веб-сайт Службы технической поддержки http://support.kaspersky.ru/;
- прочитать информацию о текущем выпуске Kaspersky Security 10.1 для Windows Server.

Папка \client содержит файлы для установки Консоли Kaspersky Security 10.1 (набор компонентов "Средства Администрирования Kaspersky Security 10.1 для Windows Server").

Папка \server содержит:

- файлы для установки компонентов Kaspersky Security 10.1 для Windows Server на сервере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows;
- файл для установки плагина управления Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center;
- архив антивирусных баз, актуальных на момент выпуска программы;
- файл с текстом Лицензионного соглашения и Политики конфиденциальности;

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

Папка \email_plugin содержит установочный пакет расширения Kaspersky Security 10.1 для Microsoft Outlook.

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

Таблица 2. Файлы комплекта поставки Kaspersky Security 10.1 для Windows Server

Файл	Назначение
autorun.inf	Файл автозапуска мастера установки Kaspersky Security 10.1 для Windows Server при установке программы с переносных носителей.
ks4ws_admin_guide_en.pdf	Руководство администратора.
ks4ws_user_guide_en.pdf	Руководство пользователя.
release_notes.txt	Файл содержит информацию о выпуске.
setup.exe	Файл запуска программы приветствия (запускает setup.hta).
\client\ks4wstools_x86(x64).msi	Пакет установки службы Windows Installer; устанавливает на защищаемом сервере Консоль Kaspersky Security 10.1.
\client\setup.exe	Файл запуска мастера установки для набора компонентов "Средства администрирования" (в него входит Консоль Kaspersky Security 10.1); запускает файл пакета установки ks4wstools.msi с указанными в мастере параметрами установки.
\server\bases.cab	Архив антивирусных баз, актуальных на момент выпуска программы.
\server\setup.exe	Файл запуска мастера установки Kaspersky Security 10.1 для Windows Server на защищаемом сервере; запускает файл пакета ks4ws.msi с указанными в мастере параметрами установки.
\server\ks4ws_x86(x64).msi	Пакет установки службы Windows Installer; устанавливает Kaspersky Security 10.1 для Windows Server на защищаемом сервере.
\server\ks4ws.kud	Файл в формате Kaspersky Unicode Definition с описанием инсталляционного пакета для удаленной установки Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center.
\server\klcfginst.exe	Программа установки плагина управления Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center. Установите плагин на каждом сервере, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Security 10.1 для Windows Server через нее.
\server\license.txt	Текст Лицензионного соглашения и Политики конфиденциальности.
\setup\setup.hta	Файл запуска программы приветствия.
\email_plugin\ksmail_x86(x64).msi	Пакет установки службы Windows Installer; устанавливает расширение Kaspersky Security 10.1 для Microsoft Outlook на защищаемом сервере.

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

Аппаратные и программные требования

Этот раздел содержит перечень аппаратных и программных требований Kaspersky Security 10.1 для Windows Server.

В этом разделе

Требования к серверу, на который устанавливается Kaspersky Security 10.1 для Windows Server

Перед установкой Kaspersky Security 10.1 для Windows Server требуется удалить с сервера другие антивирусные программы.

Вы можете устанавливать Kaspersky Security 10.1 для Windows Server, не удаляя установленный Антивирус Касперского 8.0 для Windows Server Enterprise Edition или Kaspersky Security 10 для Windows Server.

Аппаратные требования к серверу

Общие требования:

- x86-64-совместимые системы в однопроцессорной и многопроцессорной конфигурации;
- объем дискового пространства:
  - для установки всех программных компонентов: 70 MB;
  - для загрузки и хранения антивирусных баз программы: 2 Гб (рекомендуется);
  - для хранения объектов на карантине и в резервном хранилище: 400 МБ (рекомендуется);
  - Для хранения журналов: 1 Гб (рекомендуется);

Минимальная конфигурация:

- процессор: однопроцессорный 1,4 ГГц.
- Объем оперативной памяти: 1GB.
- дисковая подсистема: 4 Гб доступного пространства.

Рекомендуемая конфигурация:

- процессор: четырехпроцессорный 2,4 ГГц.

- Объем оперативной памяти: 2 GB.
- дисковая подсистема: 4 Гб доступного пространства.

Программные требования к серверу

Вы можете установить Kaspersky Security 10.1 для Windows Server на сервере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и работы Kaspersky Security 10.1 для Windows Server требуется наличие на сервере Microsoft Windows Installer 3.1.

Вы можете установить Kaspersky Security 10.1 для Windows Server на сервер под управлением одной из следующих 32-разрядных операционных систем Microsoft Windows:

- Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

Вы можете установить Kaspersky Security 10.1 для Windows Server на сервер под управлением одной из следующих 64-разрядных операционных систем Microsoft Windows:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V® Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Server 2012 Core Standard / Datacenter;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Server 2016 Core Standard / Datacenter;

- Windows Storage Server 2016;
- Windows Hyper-V Server 2016.

Следующие операционные системы Windows более не поддерживаются производителем: Windows Server 2003 Standard / Enterprise / Datacenter SP2, Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 32-x, 64-x битая. Возможны ограничения технической поддержки Лаборатории Касперского серверов, работающих на данных операционных системах.

Вы можете установить Консоль Kaspersky Security 10.1 для Windows Server на следующие типы терминальных серверов:

- Microsoft Remote Desktop Services на базе Windows 2008 Server;
- Microsoft Remote Desktop Services на базе Windows 2008 R2 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server R2;
- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

Требования к защищаемому сетевому хранилищу

Kaspersky Security 10.1 для Windows Server может использоваться для защиты следующих сетевых хранилищ:

- NetApp с одной из следующих операционных систем:
  - Data ONTAP 7.x и Data ONTAP 8.x в режиме 7-mode;
  - Data ONTAP 8.2.1 или выше в режиме cluster-mode.
- Dell™ EMC™ Celerra™ / VNX™ со следующим программным обеспечением:
  - операционная система EMC DART 6.0.36 или выше;
  - Антивирусный агент Celerra (CAVA) 4.5.2.3 или выше.
- Dell EMC Isilon™ с операционной системой OneFS™ 7.0 или выше.
- Hitachi NAS на одной из следующих платформ:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080

- IBM NAS серии IBM System Storage® N series.
- Oracle® NAS Systems семейства Oracle ZFS Storage Appliance.
- Dell NAS на платформе Dell Compellent™ FS8600.

Требования к компьютеру, на который устанавливается Консоль Kaspersky Security 10.1

Аппаратные требования к компьютеру

Рекомендуемый объем оперативной памяти – 128 МБ или более.

Свободное дисковое пространство: 30 MB.

Программные требования к компьютеру

Вы можете установить Консоль Kaspersky Security 10.1 на сервере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и работы Консоли Kaspersky Security 10.1 требуется наличие на компьютере Microsoft Windows Installer 3.1.

Вы можете установить Консоль Kaspersky Security 10.1 на сервере под управлением одной из следующих 32-разрядных операционных систем Microsoft Windows:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Windows XP Professional с пакетом обновлений SP2 или выше;
- Microsoft Windows Vista®;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

Вы можете установить Консоль Kaspersky Security 10.1 на сервере под управлением одной из следующих 64-разрядных операционных систем Microsoft Windows:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Storage Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Storage Server 2016;
- Microsoft Windows XP Professional Edition с пакетом обновлений SP2 или выше;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

Ограничения и требования к среде

В этом разделе описаны дополнительные требования к среде и существующие ограничения для компонентов Kaspersky Security 10.1 для Windows Server.

В этом разделе

Установка и удаление

- Во время установки программы возникает предупреждение, если полный путь к папке установки Kaspersky Security 10.1 для Windows Server содержит более 150 символов. Предупреждение не влияет на процесс установки: Kaspersky Security 10.1 для Windows Server будет успешно установлен и запущен.
- Для установки компонента Поддержка протокола SNMP требуется перезапуск службы SNMP, если эта служба запущена.
- Для установки и работы Kaspersky Security 10.1 для Windows Server на устройстве под управлением встроенных операционных систем требуется наличие компонента Filter Manager.
- Недоступна установка Средств администрирования Kaspersky Security 10.1 для Windows Server через групповые политики Microsoft Active Directory®.
- При установке программы на компьютеры под управлением устаревших операционных систем, не имеющих возможности получать регулярные обновления, необходимо проверить наличие следующих корневых сертификатов: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Отсутствие указанных сертификатов может привести к некорректной работе программы. Рекомендуется установить указанные сертификаты любым доступным способом.
- Недоступно удаление Консоли Kaspersky Security 10.1 через меню Пуск. Вы можете удалить Консоль Kaspersky Security 10.1 в окне **Add / Remove Programs**.

Защита трафика

- Работа компонента возможна только на версиях операционных систем новее Microsoft Windows Server 2008 R2.
- Недоступна работа с правилами веб-контроля для веб-адресов.
- Недоступна проверка трафика при верификации веб-соединений с помощью криптографического токена.
- Не рекомендуется включать в область защиты задачи VPN-трафик (порт 1723).
- Веб-браузеры Mozilla™ Firefox™, Opera Presto Engine, Yandex Browser обнаруживают Kaspersky Security 10.1 для Windows Server при попытках подключения, если программа применяется для защиты HTTPS трафика.
- Недоступна работа с IP-адресами в формате IPv6.
- Программа расценивает самоподписанные сертификаты как невалидные и блокирует такие соединения, если в параметрах задачи установлен флажок **Не доверять веб-серверу с невалидным сертификатом**.
- Программа работает только с пакетами TCP.
- Защита от почтовых угроз не проверяет исходящий почтовый трафик.
- Сетевой Агент Сервера администрирования обнаруживает компонент защиты трафика при попытке соединения с программой, поэтому рекомендуется выполнять установку Плагина управления до разворачивания компонента Защита трафика. Если установка компонента и запуск задачи Защита трафика были выполнены до установки Плагина управления, перезапустите задачу Защита трафика.

- Компонент не работает с облачными хранилищами Yandex.Disk, Dropbox.
- Ограничения по VPN: возможны проблемы в работе с протоколами VPN-соединений от Microsoft.
- Если установка осуществлялась посредством KSC, при работе компонента в режиме Драйверный перехват, блокируются соединение MMC Консоли к Серверу администрирования KSC, так как при данном соединении используется недоверенный сертификат.
- Компонент блокирует соединение для сайтов, использующих устаревшие технологии формирования корневых сертификатов, например sha1.
- Опция **Не проверять объекты размером более** может принимать максимальное значение, равное 100Мб. Стоит учитывать, что при большом значении и низкой скорости доступа к сети Интернет, возможны трудности с получением больших файлов. Рекомендуемое значение данной опции 20Мб.
- Программа распознаёт соединения по протоколу HTTPS как небезопасные и блокирует их при выполнении следующих условий:
  - задача выполняется в режиме **Перенаправление трафика;**
  - перенаправление трафика выполняется с внешних устройств;
  - устройства, с которых выполняется перенаправление трафика, защищены с помощью KSWS 10.1 с установленным и хотя бы единожды запущенной задачей Защита Трафика.

Не рекомендуется использовать режим **Перенаправление трафика** для проверки трафика, перенаправленного с внешних компьютеров: помимо описанных выше ложных срабатываний, такая конфигурация может привести к высокой загрузке сервера и снижению производительности программы.

Мониторинг файловых операций

Компонент Мониторинг файловых операций по умолчанию не отслеживает изменения в системных каталогах и служебных каталогах файловой системы, чтобы в отчеты задачи не попадали данные о штатных изменениях файлов, выполняющихся постоянно в ходе работы ОС. Пользователь не может указать такие каталоги в области мониторинга вручную.

Следующие папки/файлы исключены из области мониторинга:

- Служебные файлы NTFS с file id от 0 до 33
- L"%SystemRoot%\\Prefetch\\",
- L"%SystemRoot%\\ServiceProfiles\\LocalService\\AppData\\Local\\",
- L"%SystemRoot%\\System32\\LogFiles\\Scm\\",
- L"%SystemRoot%\\Microsoft.NET\\Framework\\v4.0.30319\\",
- L"%SystemRoot%\\Microsoft.NET\\Framework64\\v4.0.30319\\",
- L"%SystemRoot%\\Microsoft.NET\\",
- L"%SystemRoot%\\System32\\config\\",
- L"%SystemRoot%\\Temp\\",

- L"%SystemRoot%\\ServiceProfiles\\LocalService\\",
- L"%SystemRoot%\\System32\\winevt\\Logs\\",
- L"%SystemRoot%\\System32\\wbem\\repository\\",
- L"%SystemRoot%\\System32\\wbem\\Logs\\",
- L"%ProgramData%\\Microsoft\\Windows\\WER\\ReportQueue\\",
- L"%SystemRoot%\\SoftwareDistribution\\DataStore\\",
- L"%SystemRoot%\\SoftwareDistribution\\DataStore\\Logs\\",
- L"%ProgramData%\\Microsoft\\Windows\\AppRepository\\",
- L"%ProgramData%\\Microsoft\\Search\\Data\\Applications\\Windows\\",
- L"%SystemRoot%\\Logs\\SystemRestore\\",
- L"%SystemRoot%\\System32\\Tasks\\Microsoft\\Windows\\TaskScheduler\\"

Программа исключает каталоги по первому уровню.

Компонент не контролирует изменения с фалами, выполненными в обход файловой системы ReFS/NTFS (сценарии файловых изменений через BIOS, LiveCD и т.п.).

Управление сетевым экраном

- Недоступна работа с IP-адресами в формате IPv6 при указании области применения правила, состоящей из одного адреса.
- Предзаданные правила политики Управление сетевым экраном обеспечивают выполнение основных сценариев взаимодействия локальных компьютеров с Сервером администрирования. Для полного использования функциональности Kaspersky Security Center требуется вручную задать правила для разрешения портов. Информация о номерах портов, протоколах и их функциях содержится в Базе Знаний Kaspersky Security Center (ID статьи: 9297).
- Программа не контролирует изменения правил и групп правил брандмауэра Windows при ежеминутном опросе задачи Управление сетевым экраном, если эти правила и группы были добавлены в параметры задачи при установке программы. Для обновления статуса и наличия таких правил требуется перезапуск задачи Управление сетевым экраном.
- Для ОС семейства Microsoft Windows Server 2008 и выше: перед установкой компонента Управление сетевым экраном требуется запустить сервис брандмауэра Windows (запущен по умолчанию).

Прочие ограничения

Проверка по требованию, Постоянная защита файлов:

- Недоступны MTP-устройства при проверке соединения.
- Недоступна проверка архивных объектов без проверки SFX-архивов: если в параметрах безопасности Kaspersky Security 10.1 для Windows Server применяется режим проверки архивов, программа автоматически проверяет объекты как в архивах, так и объекты в SFX-архивах. Проверка SFX-архивов без проверки архивов доступна.

Контроль компьютера и диагностика:

- Область действия задачи Контроль устройств распространяется на MTP-подключаемые запоминающие устройства, если защищаемый компьютер работает под управлением операционных систем Microsoft Windows Server 2008 R2 и выше.
- Задача Анализ журналов обнаруживает потенциальные паттерны атаки Kerberos (MS14-068) только на компьютерах под управлением операционных систем Windows Server 2008 и выше в роли доменного контроллера с установленными обновлениями.

Лицензирование:

- Недоступна активация программы с помощью ключа из мастера установки программы, если файл ключа расположен на диске, созданном с помощью команды SUBST, или если указан сетевой путь к файлу ключа.

Обновления:

- После установки критических обновлений модулей Kaspersky Security 10.1 для Windows Server, значок Kaspersky Security 10.1 для Windows Server по умолчанию скрыт;
- KLRAMDISK не поддерживается на компьютерах под управлением Windows XP или Windows 2003.

Интерфейс:

- В Консоли Kaspersky Security 10.1 для Windows Server при использовании фильтра в узлах Карантин, Резервное хранилище, Журнал системного аудита, Журналы выполнения задач требуется соблюдать регистр.
- При настройке области защиты и области проверки в Консоли Kaspersky Security 10.1 возможно использование только одной маски в пути и только в конце пути. Примеры правильного задания маски: "C:\Temp\Temp*", или "C:\Temp\Temp???.doc", или "C:\Temp\Temp*.doc". Ограничение не распространяется на параметры доверенной зоны.

Безопасность:

- При активированном контроле учетных записей (User Account Control) в параметрах операционной системы, для открытия Консоли Kaspersky Security 10.1 двойным щелчком мыши на значке программы в области уведомлений панели задач необходимо, чтобы учетная запись пользователя входила в группу KAVWSEE Administrators. В ином случае открывается окно "О программе".
- Удаление программы с помощью окна "Установка и удаление программ" Microsoft Windows недоступно при включенном контроле учетных записей пользователей (User Account Control).

Интеграция с Kaspersky Security Center:

- Сервер администрирования проверяет корректность обновлений баз программы по их получении и перед распространением на компьютеры сети. Проверка корректности полученных обновлений модулей программы на стороне Сервера администрирования не выполняется.
- При работе с компонентами, передающими динамически изменяющиеся данные в Kaspersky Security Center с помощью сетевых списков (Карантин, Резервное хранилище), убедитесь, что в параметрах взаимодействия с Сервером администрирования установлены соответствующие флажки.

Защита от эксплойтов

- Функциональность защиты памяти процессов от эксплойтов недоступна, если в текущей конфигурации среды не загружена библиотеки apphelp.dll.
- Компонент Защита от эксплойтов несовместим со служебной программой Microsoft EMET на компьютерах под управлением Microsoft Windows 10: Kaspersky Security 10.1 для Windows Server блокирует EMET, если на компьютер, где установлена программа EMET, устанавливается компонент Защита от эксплойтов.

Защита от шифрования для NetApp

- Защита от эксплойтов: защита от шифрования не может выполняться для СХД на новых ОС (ONTAP 9 и выше), если для таких серверов используются контейнеры типа FlexGroup.
- Ограничена функциональность по поиску файловых угроз на сетевых хранилищах NetApp в режиме 7 Mode.
- Защита от шифрования для сетевых хранилищ NetApp доступна только в кластерном режиме.
- На сервере может использоваться только один сетевой интерфейс и только один IP v4 адрес.

Хранилище заблокированных компьютеров: работает постоянно, когда включены компоненты Защита от шифрования или Постоянная защита файлов.

Защита ICAP-подключаемых сетевых хранилищ: Управление содержимым защищенного хранилища зависит от параметров хранилища. Например, невозможно удаление обнаруженных зараженных объектов, если действие не разрешено хранилищем. Хранилища типа HP 3Par работают только в режиме block access. Невозможно использовать доверенную зону.

Защита RPC-подключаемых сетевых хранилищ: для работы с кластерным режиомом необходим Active Directory.

Использование KSN: Для Windows Vista и ниже - не поддерживаются статистики для .

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Security 10.1 для Windows Server.

В этом разделе

Программные компоненты Kaspersky Security 10.1 для Windows Server и их коды для службы Windows Installer

По умолчанию файлы \server\ks4ws_x86(x64).msi устанавливают все программные компоненты Kaspersky Security 10.1 для Windows Server. Вы можете включить установку данного компонента при выборочной установке программы.

Файлы \client\ks4wstools_x86(x64).msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приводятся коды программных компонентов Kaspersky Security 10.1 для Windows Server для службы Windows Installer. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Security 10.1 для Windows Server из командной строки.

В этом разделе

Программные компоненты Kaspersky Security 10.1 для Windows Server

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Security 10.1 для Windows Server.

Таблица 3. Описание программных компонентов Kaspersky Security 10.1 для Windows Server

Компонент	Код	Выполняет функции
Основная функциональность	Core	Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.
Контроль запуска программ	AppCtrl	Этот компонент отслеживает попытки запуска программ пользователями и разрешает или Не разрешать запуск программ в соответствии с заданными правилами контроля запуска программ. Компонент реализуется в задаче Контроль запуска программ.
Контроль устройств	DevCtrl	Этот компонент отслеживает попытки подключения запоминающих USB устройств и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств. Компонент реализуется в задаче Контроль устройств.
Защита трафика	WebGW	Этот компонент обрабатывает сетевой трафик, включая трафик, поступающий через почтовые серверы, перехватывает и проверяет объекты, передаваемые по веб-трафику, на наличие известных компьютерных и других угроз на защищаемом сервере.
Антивирусная защита	AVProtection	Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: • Проверка по требованию • Постоянная защита файлов
Проверка по требованию	Ods	Этот компонент устанавливает системные файлы Kaspersky Security 10.1 для Windows Server и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого сервера, выполняемая по требованию). Если, устанавливая Kaspersky Security 10.1 для Windows Server из командной строки, вы укажете другие компоненты Kaspersky Security 10.1 для Windows Server, не указывая компонент Core, компонент Core будет установлен автоматически.

Компонент	Код	Выполняет функции
Постоянная защита файлов	Oas	Этот компонент обеспечивает антивирусную проверку файлов на защищаемом сервере при обращении к этим файлам. Компонент реализует задачу Постоянная защита файлов.
Использование Kaspersky Security Network	Ksn	Этот компонент реализует защиту на основе облачных технологий "Лаборатории Касперского". Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).
Мониторинг файловых операций	Fim	Этот компонент позволяет 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 сервера.
Управление сетевым экраном	Firewall	Этот компонент предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Security 10.1 для Windows Server. Компонент реализуется в задаче Управление сетевым экраном.
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Обеспечивает связь Kaspersky Security 10.1 для Windows Server с Агентом администрирования Kaspersky Security Center. Вы можете установить этот компонент на защищаемом сервере, если вы планируете управлять программой через Kaspersky Security Center.
Анализ журналов	LogInspector	Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.
Защита от шифрования	AntiCryptor	При обнаружении попытки вредоносного шифрования компонент добавляет атакующие комьютеры в список заблокированных компьютеров. Компонент реализуется в задаче Защита от шифрования.
Проверка скриптов	ScriptChecker	Этот компонент проверяет код скриптов, созданных с помощью технологии Microsoft Windows Script. Проверка осуществляется при попытке запуска скрипта. Компонент реализуется в задаче Проверка скриптов.

Компонент	Код	Выполняет функции
Защита RPC-подключаемых сетевых хранилищ.	RPCProt	Этот компонент защищает RPC-подключаемые сетевые хранилища (например, сетевые хранилища от NetApp) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.
Защита ICAP-подключаемых сетевых хранилищ.	ICAPProt	Этот компонент защищает ICAP-подключаемые сетевые хранилища (например, EMC Isilon) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.
Защита от шифрования для NetApp	AntiCryptorNAS	Этот компонент защищает папки сетевого хранилища от шифрования. Kaspersky Security 10.1 for Windows Server блокирует доступ к папкам доступа для скомпрометированных компьютеров при обнаружении попытки вредоносного шифрования.
Набор счетчиков производительности программы "Системный монитор"	PerfMonCounters	Компонент устанавливает набор счетчиков производительности программы "Системный монитор". Эти счетчики позволяют измерять производительность Kaspersky Security 10.1 для Windows Server и находить возможные узкие места при совместной работе Kaspersky Security 10.1 для Windows Server с другими программами.
Поддержка SNMP-протокола	SnmpSupport	Компонент публикует счетчики и ловушки Kaspersky Security 10.1 для Windows Server через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Вы можете установить этот компонент на защищаемом сервера только в случае, если служба Microsoft SNMP установлена на этом компьютере.
Значок Kaspersky Security 10.1 для Windows Server в области уведомлений	TrayApp	Компонент отображает значок Kaspersky Security 10.1 для Windows Server в области уведомлений панели задач защищаемого сервера. Значок Kaspersky Security 10.1 для Windows Server показывает состояние защиты компьютера, позволяет открыть Консоль Kaspersky Security 10.1 (если она установлена) и окно О программе.
Утилита командной строки	Shell	Позволяет управлять Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server	MmcSnapin	Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Security 10.1. Если, устанавливая набор "Средства администрирования" из командной строки, вы укажете другие компоненты набора, не указывая компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически.
Справка	Справка	Chm-файл справки; сохраняется в папке с файлами средств администрирования Kaspersky Security 10.1 для Windows Server. Вы можете открыть файл справки из меню **Пуск** или клавишей **F1** при открытом окне Консоли Kaspersky Security 10.1.
Документация	Docs	Kaspersky Security 10.1 для Windows Server сохраняет "Руководство администратора", "Руководство пользователя" в формате PDF на защищаемом компьютере. Вы можете открыть Руководство администратора" из меню **Пуск**.

Изменения в системе после установки Kaspersky Security 10.1 для Windows Server

При установке Kaspersky Security 10.1 для Windows Server и Консоли Kaspersky Security 10.1 (набора "Средства администрирования") служба Windows Installer выполняет на сервере следующие изменения:

- создает папки Kaspersky Security 10.1 для Windows Server на защищаемом сервере и сервере, где установлена Консоль Kaspersky Security 10.1;
- регистрирует службы Kaspersky Security 10.1 для Windows Server;
- создает группу пользователей Kaspersky Security 10.1 для Windows Server;
- регистрирует ключи Kaspersky Security 10.1 для Windows Server в системном реестре.

Эти изменения описаны в таблице ниже.

Папки Kaspersky Security 10.1 для Windows Server

Таблица 5. Папки Kaspersky Security 10.1 для Windows Server на защищаемом компьютере

Папка	Файлы Kaspersky Security 10.1 для Windows Server
Папка %Kaspersky Security 10.1 для Windows Server%; по умолчанию: В Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 для Windows Server\ В Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Security 10.1 for Windows Server\	Исполняемые файлы Kaspersky Security 10.1 для Windows Server (папка назначения, указанная при установке).
Папка %Kaspersky Security 10.1 for Windows Server%\mibs	Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Kaspersky Security 10.1 для Windows Server по протоколу SMNP.
Папка %Kaspersky Security 10.1 для Windows Server%\x64	64-разрядные версии исполняемых файлов Kaspersky Security 10.1 для Windows Server (папка создается только при установке Kaspersky Security 10.1 для Windows Server в Microsoft Windows 64-разрядной версии).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Security 10.1 for Windows Server\10.1\Dskm\	Служебные файлы Kaspersky Security 10.1 для Windows Server.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Update\	Файлы с параметрами источников обновлений.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\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 Security для Windows Server\10.1\Reports\	Журналы выполнения задач и журнал системного аудита.

Папка	Файлы Kaspersky Security 10.1 для Windows Server
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Bases\Current\	Набор баз, используемых в текущий момент.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Bases\Backup\	Резервная копия баз; перезаписывается при каждом обновлении баз.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Bases\Temp\	Временные файлы, создаваемые во время выполнения задач обновления.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Quarantine\	Объекты на карантине (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security для Windows Server\10.1\Backup\	Объекты в резервном хранилище (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored	Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию).

Таблица 6. Папки, создаваемые при установке Консоли Kaspersky Security 10.1

Папка	Файлы Kaspersky Security 10.1 для Windows Server
Папка %Kaspersky Security 10.1 для Windows Server%; по умолчанию: • В Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 для Windows Server\ в Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server\	Файлы набора «Средства администрирования» (папка назначения, указанная при установке Консоли Kaspersky Security 10.1)

Службы Kaspersky Security 10.1 для Windows Server

Службы Kaspersky Security 10.1 для Windows Server запускаются под системной учетной записью Локальная система (SYSTEM).

Таблица 7. Службы Kaspersky Security 10.1 для Windows Server

Служба	Назначение
Служба Kaspersky Security Service (KAVFS)	Основная служба Kaspersky Security 10.1 для Windows Server, которая управляет задачами и рабочими процессами Kaspersky Security 10.1 для Windows Server.
Служба Kaspersky Security Management Service (KAVFSGT)	Служба, предназначенная для управления программой через Консоль Kaspersky Security 10.1.
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 Security 10.1 для Windows Server

Таблица 8. Группы Kaspersky Security 10.1 для Windows Server

Группа	Назначение
KAVWSEE Administrators	Группа на защищаемом Server, пользователи которой имеют полный доступ к Службе Kaspersky Security Management Service, а также доступ ко всем функциям Kaspersky Security 10.1 для Windows Server.

Ключи системного реестра

Таблица 9. Ключи системного реестра

Ключ	Назначение
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Параметры службы Kaspersky Security 10.1 для Windows Server.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Параметры журнала событий Kaspersky Security 10.1 для Windows Server (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Параметры службы управления Kaspersky Security 10.1 для Windows Server.
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] В Microsoft Windows 64-разрядной версии: [[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Параметры счетчиков производительности.

Ключ	Назначение
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\SnmpAgent] В Microsoft Windows 64-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]	Параметры компонента "Поддержка SNMP-протокола".
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump\	Параметры записи файла дампа.
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\10.1\Trace\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\Trace\	Параметры журнала трассировки.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]	Параметры задач и фукнций программы.

Процессы Kaspersky Security 10.1 для Windows Server

Kaspersky Security 10.1 для Windows Server запускает процессы, описанные в таблице ниже.

Таблица 10. Процессы Kaspersky Security 10.1 для Windows Server

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Security 10.1 для Windows Server
kavtray.exe	Процесс компонента Значок Kaspersky Security 10.1 для Windows Server в области уведомлений
kavshell.exe	Процесс утилиты командной строки
kavfsrcn.exe	Процесс удаленного управления Kaspersky Security 10.1 для Windows Server.
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 Security 10.1 для Windows Server и их значения по умолчанию, указаны ключи для изменения значений параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды msiexec службы Windows Installer при установке Kaspersky Security 10.1 для Windows Server 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> 0 – вы отклоняете условия Лицензионного соглашения. 1 – вы принимаете условия Лицензионного соглашения.	Вам нужно принять условия Лицензионного соглашения для установки Kaspersky Security 10.1 для Windows Server.
Папка назначения	Kaspersky Security 10.1 для Windows Servers: %Program-Files%\Kaspersky Lab\Kaspersky Security 10,1 для Windows Server .1 Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10,1 для Windows Server .1 Admins Tools В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%.	INSTALLDIR=<полный путь к папке>	Папка, в которой будут сохранены файлы Kaspersky Security 10.1 для Windows Server при его установке. Вы можете указать другую папку.
Запуск постоянной защиты файлов при запуске Kaspersky Security 10.1 для Windows Server (**Включить постоянную защиту после установки программы**)	Запустить	RUNRTP=<значение> 1 – запустить; 0 – не запускать.	Включите этот параметр, чтобы запустить постоянную защиту файлов при запуске Kaspersky Security 10.1 для Windows Server (рекомендуется).

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Исключения из проверки, рекомендуемые корпорацией Microsoft (**Добавить к исключениям файлы, рекомендованные Microsoft**)	Исключать	ADDMSEXCLUSION=<значение> 1 – исключать; 0 – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на сервера, которые рекомендует исключать корпорация Microsoft. Некоторые программы на сервере 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" (**Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**)	Исключать	ADDKLEXCLUSION=<значение> 1 – исключать; 0 – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на сервера, которые рекомендует исключать "Лаборатория Касперского".
Разрешать удаленное подключение к Консоли Kaspersky Security 10.1.	Не разрешать	ALLOWREMOTECON=<значение> 1 – разрешать; 0 – не разрешать.	По умолчанию удаленное подключение к Консоли Kaspersky Security 10.1, установленной на защищенном сервере, не разрешено. Во время установки вы можете разрешить подключение. Kaspersky Security 10.1 для Windows Server создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Путь к файлу ключа (**Ключ**)	Папка комплекта поставки \server	LICENSEKEYPATH=< имя файла ключа>	По умолчанию программа установки пытается найти файл с расширением .key в папке \server комплекта поставки. Если в папке \сервера хранится несколько файлов ключа, программа установки выбирает файл ключа с самым поздней датой истечения срока действия. Вы можете предварительно сохранить файл ключа в папке \server или указать другой путь к файлу ключа с помощью параметра **Добавление ключа**. Вы можете добавить ключ после установки Kaspersky Security 10.1 для Windows Server с помощью выбранного вами средства администрирования, например, через Консоль Kaspersky Security 10.1. Если вы не добавите ключ программы во время его установки, после установки Kaspersky Security 10.1 для Windows Server не будет функционировать.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Путь к конфигурационному файлу	Не указан	CONFIGPATH=<имя конфигурационного файла>	Kaspersky Security 10.1 для Windows Server импортирует параметры из указанного конфигурационного файла, созданного в программе. Kaspersky Security 10.1 для Windows Server не импортирует из конфигурационного файла пароли, например, пароли учетных записей Запустить задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Разрешение сетевых соединений для Консоли	Выключена	ADDWFEXCLUSION=<значение> **1** – разрешать; **0** – не разрешать.	Используйте этот параметр, если вы устанавливаете Kaspersky Security 10.1 для Windows Server не на защищаемом компьютере. С помощью Консоли, установленной на другом сервера, вы сможете управлять защитой компьютера удаленно. В брандмауэре Microsoft Windows компьютера будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Security 10.1 для Windows Server kavfsrcn.exe и открыт доступ к программам DCOM. После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу KSWS Administrators на сервера и разрешите на нем сетевые соединения для службы Kaspersky Security Managment Service (файл kavfsgt.exe). В можете подробнее прочитать о дополнительной настройке при установке Консоли Kaspersky Security 10.1 на другом компьютере (см. раздел "Дополнительная настройка после установки Консоли Kaspersky Security 10.1 на другом компьютере" на стр. 56).

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 Security 10.1 для Windows Server, 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 резервного хранилища	Удалить	RESTOREBCK =<значение> **0** – удалить содержимое резервного хранилища; **1** – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH.
Ввод текущего пароля для подтверждения операции удаления (при активной функции применения пароля)	Не указан	UNLOCK_PASSWORD=<заданный пароль>
Папка для восстановленных объектов	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored	RESTOREPATH=<полный путь к папке> Восстановленные объекты будут сохранены в папке, указанной этим параметром: Объекты из карантина будут сохранены во вложенной папке \Quarantine. Объекты из резервного хранилища – во вложенной папке \Backup.

Журнал установки и удаления Kaspersky Security 10.1 для Windows Server

Если вы выполняете установку или удаление Kaspersky Security 10.1 для Windows Server с помощью мастера установки (удаления), служба Windows Installer создает журнал установки (удаления). Файл журнала с именем ks4ws_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 Security 10.1 для Windows Server из командной строки, по умолчанию журнал установки не создается.

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с созданием файла журнала ks4ws на диске C:\, выполните одну из следующих команд:*

- `msiexec /i ks4ws_x86.msi /l*v C:\log.txt /qn EULA=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\log.txt /qn EULA=1`

Планирование установки

Этот раздел содержит описание средств администрирования Kaspersky Security 10.1 для Windows Server, особенностей установки Kaspersky Security 10.1 для Windows Server с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. 51), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. 65), через Kaspersky Security Center (см. раздел "Установка и удаление программы через Kaspersky Security Center" на стр. 71) и через групповые политики Active Directory® (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 76).

Перед тем как начать установку Kaspersky Security 10.1 для Windows Server, спланируйте основные этапы ее проведения:

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Security 10.1 для Windows Server и его настройки.
2. Определите, какие программные компоненты требуется установить (см. раздел "Программные компоненты Kaspersky Security 10.1 для Windows Server и их коды для службы Windows Installer" на стр. 33).
3. Выберите способ установки.

В этом разделе

Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров Kaspersky Security 10.1 для Windows Server и управления им. В качестве средств администрирования Kaspersky Security 10.1 для Windows Server вы можете использовать Консоль Kaspersky Security 10.1, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Консоль Kaspersky Security 10.1

Консоль Kaspersky Security 10.1 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Security 10.1 для Windows Server через Консоль Kaspersky Security 10.1, установленную на защищаемом сервере или на другом компьютере в сети организации.

В одну Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток Kaspersky Security 10.1 для Windows Server, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Security 10.1 для Windows Server.

Консоль Kaspersky Security 10.1 входит в набор компонентов "Средства администрирования".

Утилита командной строки

Вы можете управлять Kaspersky Security 10.1 для Windows Server из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Security 10.1 для Windows Server.

Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации, вы можете управлять Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server. Он обеспечивает связь Kaspersky Security 10.1 для Windows Server с Агентом администрирования. Установите Модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемом сервере.
- **Агент администрирования Kaspersky Security Center**. Установите его на каждом защищаемом сервере. Этот компонент будет обеспечивать взаимодействие между Kaspersky Security 10.1 для Windows Server, установленным на компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин Kaspersky Security 10.1 для Windows Server**. Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Security 10.1 для Windows Server через Сервер администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки плагина, \Server\klcfginst.exe, входит в комплект поставки Kaspersky Security 10.1 для Windows Server.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Security 10.1 для Windows Server> (см. раздел "Программные компоненты Kaspersky Security 10.1 для Windows Server и их коды для службы Windows Installer Служба" на стр. 33), 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 Security 10.1 для Windows Server, или вы будете использовать параметры установки по умолчанию (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. 42);
- будут ли параметры установки едиными для всех серверу или индивидуальными для каждого компьютера.

Вы можете установить Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить Kaspersky Security 10.1 для Windows Server на одном компьютере, настроить его для работы и сохранить его параметры в конфигурационном файле, чтобы затем использовать созданный файл для установки Kaspersky Security 10.1 для Windows Server на других компьютерах (эта возможность не применяется при установке через групповые политики Active Directory).

Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Security 10.1 для Windows Server (см. раздел "Программные компоненты Kaspersky Security 10.1 для Windows Server" на стр. 34) на защищаемом сервере из файла \server\setup.exe включены в комплект поставки.
- Консоль Kaspersky Security 10.1 (см. раздел "Установка Консоли Kaspersky Security 10.1" на стр. 55) из файла \client\setup.exe, входящего в комплект поставки на защищаемом сервере или другом сервере в локальной сети.

Запуск из командной строки файла инсталляционного пакета с параметрами установки

Запустив файл инсталляционного пакета без командной строки ключей, вы установите Kaspersky Security 10.1 для Windows Server с параметрами установки по умолчанию. С помощью ключей Kaspersky Security 10.1 для Windows Server вы можете изменять параметры установки.

Вы можете установить Консоль Kaspersky Security 10.1 на защищаемом сервере и (или) рабочем месте администратора.

Примеры команд для установки Kaspersky Security 10.1 для Windows Server и Консоли Kaspersky Security 10.1 приведены в разделе "Об установке и удалении Kaspersky Security 10.1 для Windows Server из командной строки" (см. раздел "Установка и удаление программы из командной строки" на стр. 65).

Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой компьютеров сети, вы можете установить Kaspersky Security 10.1 для Windows Server на нескольких компьютерах с помощью задачи удаленной установки Kaspersky Security Center.

Серверы, на которых вы хотите установить Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center (см. раздел Установка и удаление программы с помощью Kaspersky Security Center на стр. 71), 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 Security 10.1 для Windows Server на защищаемом компьютере. Вы можете установить Консоль Kaspersky Security 10.1 на защищаемом сервере и (или) рабочем месте администратора.

Вы можете установить Kaspersky Security 10.1 для Windows Server только с параметрами установки по умолчанию.

Серверы, на которых Kaspersky Security 10.1 для Windows Server установлен с помощью групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 76), должны быть расположены в том же домене и в том же подразделении организации. Установка выполняется при запуске компьютера, перед входом в Microsoft Windows.

Установка и удаление программы с помощью мастера

Этот раздел содержит описание процедуры установки и удаления Kaspersky Security 10.1 для Windows Server и Консоли программы на защищаемом компьютере с помощью мастера установки, а также информацию о дополнительной настройке Kaspersky Security 10.1 для Windows Server и действиях после установки программы.

В этом разделе

Установка с помощью мастера установки

В следующих разделах содержится информация о том, как установить Kaspersky Security 10.1 для Windows Server и Консоль Kaspersky Security 10.1.

► *Чтобы установить и приступить к использованию Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. Установите Kaspersky Security 10.1 для Windows Server на защищаемом компьютере.
2. На компьютерах, с которых вы планируете управлять Kaspersky Security 10.1 для Windows Server, установите Консоль Kaspersky Security 10.1.
3. Если вы установили Консоль Kaspersky Security 10.1 не на защищаемом сервере, а на другом компьютере сети, выполните дополнительную настройку, чтобы пользователи Консоли могли через нее удаленно управлять Kaspersky Security 10.1 для Windows Server.
4. Выполните действия после установки Kaspersky Security 10.1 для Windows Server.

В этом разделе

Установка Kaspersky Security 10.1 для Windows Server

Перед установкой Kaspersky Security 10.1 для Windows Server выполните следующие действия:

- Убедитесь, что на сервере не установлены другие антивирусные программы. Вы можете устанавливать Kaspersky Security 10.1 для Windows Server, не удаляя установленный Антивирус Касперского 8.0 для Windows Server Enterprise Edition или Kaspersky Security 10 для Windows Server.
- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, зарегистрирована в группе администраторов на защищаемом сервере.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Security 10.1 для Windows Server. Вы можете прервать установку Kaspersky Security 10.1 для Windows Server на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Вы можете прочитать подробнее о параметрах установки (удаления) (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. 42).

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с помощью мастера установки, выполните следующие действия:*

1. На сервера запустите файл программы-приветствия setup.exe.
2. В открывшемся окне в блоке Установка перейдите по ссылке Установить **Kaspersky Security 10.1 для Windows Server**.
3. В открывшемся окне приветствия мастера установки Kaspersky Security 10.1 для Windows Server нажмите на кнопку **Далее**.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики 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.
6. Нажмите на кнопку **Далее**.

   Если на сервере есть совместимая версия установленной программы, откроется окно **Обнаружена предыдущая версия программы**.

   Если предыдущие версии программы не обнаружены, перейдите к шагу 8 этой инструкции.
7. Чтобы обновить программу предыдущей версии, нажмите на кнопку **Установить**. Мастер установки обновит программу до Kaspersky Security 10.1 для Windows Server и сохранит совместимые настройки в новой версии. По окончании обновления программы откроется окно **Завершение установки** (перейдите к шагу 15 этой инструкции).

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

   Вы можете просмотреть информацию о проверенных объектах Server: общее количество проверенных объектов, количество обнаруженных типов угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или подозрительных процессов, которые Kaspersky Security 10.1 для Windows Server удалил из памяти, и количество опасных или подозрительных процессов, которые программе не удалось удалить.

   Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.
9. В окне **Быстрая проверка перед началом установки** нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.
10. Выберите компоненты, которые вы хотите установить.

    По умолчанию в список устанавливаемых объектов включены все компоненты Kaspersky Security 10.1 для Windows Server, за исключением компонентов Управление сетевым экраном и Проверка скриптов.

    > Компонент Поддержка SNMP-протокола Kaspersky Security 10.1 для Windows Server отображается в списке устанавливаемых компонентов только в случае, если на компьютере установлена Служба SNMP Microsoft Windows.

11. Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.

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

    - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Security 10.1 для Windows Server.
    - Если требуется, просмотрите информацию о доступном пространстве на локальных жестких дисках по кнопке **Диск**.

    Нажмите на кнопку **Далее**.

13. 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**.

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

    a. Если вы хотите импортировать параметры Kaspersky Security 10.1 для Windows Server из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.

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

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

    - Если вы хотите активировать программу, укажите файл ключа Kaspersky Security 10.1 для Windows Server для активации программы.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
    - Если вы предварительно сохранили файл ключа в папке \server комплекта поставки, имя этого файла отобразится в поле **Ключ**.
    - Если вы хотите добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

    > 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 Security 10.1 для Windows Server 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.

16. В открывшемся окне **Готовность к установке** нажмите на кнопку Установить. Мастер приступит к установке компонентов Kaspersky Security 10.1 для Windows Server.
17. По завершении установки откроется окно **Установка завершена**.

18. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о выпуске после завершения работы мастера установки.
19. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. По завершении установки Kaspersky Security 10.1 для Windows Server будет готов к работе, если вы добавили ключ для активации программы..

Установка Консоли Kaspersky Security 10.1

Следуя инструкциям мастера установки, задайте параметры установки Консоли Kaspersky Security 10.1. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера нажмите на кнопку **Отмена**.

► *Чтобы установить Консоль Kaspersky Security 10.1, выполните следующие действия:*

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

   Откроется окно программы-приветствия.
3. Нажмите на ссылку **Установить Консоль Kaspersky Security 10.1**.

   Откроется окно приветствия мастера установки. Нажмите на кнопку **Далее**.
4. В открывшемся окне **Лицензионное соглашение** ознакомьтесь с условиями Лицензионного соглашения и установите флажок **Я принимаю условия Лицензионного соглашения**, чтобы продолжить установку. Нажмите на кнопку **Далее**.
5. В открывшемся окне **Дополнительные параметры установки** выполните следующие действия:
   - Если вы планируете с помощью Консоли Kaspersky Security 10.1 управлять Kaspersky Security 10.1 для Windows Server, установленным на удаленном компьютере, установите флажок **Разрешить удаленный доступ**.
   - Чтобы открыть окно **Пользовательская установка** и выбрать компоненты, выполните следующие действия:
     a. Нажмите на кнопку **Дополнительно**.

        Откроется окно **Выборочная установка**.
     b. Выберите компоненты набора средств администрирования из списка.

        По умолчанию устанавливаются все компоненты.
     c. Нажмите на кнопку **Далее**.

   Вы можете прочитать подробнее о программных компонентах Kaspersky Security 10.1 для Windows Server (см. раздел "Программные компоненты Kaspersky Security 10.1 для Windows Server и их коды для службы Windows Installer" на стр. 33).
6. В открывшемся окне **Выбор папки назначения** выполните следующие действия:
   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
   b. Нажмите на кнопку **Далее**.

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

   Мастер приступит к установке выбранных компонентов.

8. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. Консоль Kaspersky Security 10.1 будет установлена на защищаемом сервере.

Если вы установили набор "Средства администрирования" не на защищаемом сервере, а на другом компьютере сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли Kaspersky Security 10.1 на другом компьютере" на стр. 56).

Дополнительная настройка после установки Консоли Kaspersky Security 10.1 на другом компьютере

Если вы установили Консоль Kaspersky Security 10.1 не на защищаемом сервере, а на другом компьютере сети, выполните описанные ниже действия для того, чтобы пользователи могли удаленно управлять Kaspersky Security 10.1 для Windows Server:

- На защищаемом компьютере добавьте пользователей Kaspersky Security 10.1 для Windows Server в группу KAVWSEE Administrators.
- Разрешите сетевые соединения для службы Kaspersky Security Management Service (kavfsgt.exe), если на защищаемом сервера используется брандмауэр Windows или сторонний сетевой экран.
- Если при установке Консоли Kaspersky Security 10.1 на компьютере под управлением Microsoft Windows вы не установили флажок **Разрешить сетевые соединения для Консоли Kaspersky Security 10.1**, разрешите сетевые соединения для Консоли Kaspersky Security 10.1 вручную через брандмауэр на этом компьютере.

В этом разделе

О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Security 10.1 для Windows Server.

При установке Kaspersky Security 10.1 для Windows Server регистрирует службу управления программой Kaspersky Security 10.1 для Windows Server (KAVFSGT). Для управления программой через Консоль Kaspersky Security 10.1, установленную на другом компьютере требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Security 10.1 для Windows Server имела полный доступ к Kaspersky Security Management Service на защищаемом сервере.

По умолчанию доступ к управлению службой Kaspersky Security Management Service имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, и пользователи группы KAVWSEE Administrators, созданной на защищаемом сервере при установке Kaspersky Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server.

Вы можете соединиться с Kaspersky Security 10.1 для Windows Server под локальной учетной записью, если на защищаемом сервере зарегистрирована учетная запись с таким же именем и с таким же паролем.

Разрешать сетевые подключения к Консоли Kaspersky Security 10.1

Названия параметров могут отличаться в разных операционных системах Windows.

Консоль Kaspersky Security 10.1 на удаленном компьютере использует протокол DCOM, чтобы получать информацию о событиях Kaspersky Security 10.1 для Windows Server (например, проверенных объектах или завершении задач) от службы управления Kaspersky Security 10.1 для Windows Server на защищаемом сервере. Вам нужно разрешить сетевые соединения в брандмауэре Windows для Консоли Kaspersky Security 10.1, чтобы устанавливать соединения между Консолью программы и службой управления Kaspersky Security 10.1 для Windows Server.

Выполните следующие действия:

- убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный Запустить и активация программ COM);
- в брандмауэре Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Security 10.1 для Windows Server kavfsrcn.exe.

  Через порт TCP 135 клиентский компьютер, на котором установлена Консоль Kaspersky Security 10.1, обменивается информацией с защищаемым сервером.

Если Консоль Kaspersky Security 10.1 открыта во время настройки параметров соединения между защищаемым сервером и сервером, на котором установлена Консоль Kaspersky Security 10.1, вам нужно закрыть Консоль программы, дождаться завершения процесса удаленного управления Kaspersky Security 10.1 Server kavfsrcn.exe и снова запустить Консоль. Новые параметры соединения будут применены.

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

1. На сервере, на котором установлена Консоль Kaspersky Security 10.1, откройте консоль Службы компонентов.
2. Выберите **Пуск > Выполнить.**
3. Введите команду `dcomcnfg`.

4. Нажмите на кнопку **ОК**.
5. В консоли Службы компонентов сервера 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 Security 10.1 для Windows Server, выполните следующие действия:*

1. На удаленном компьютере закройте Консоль Kaspersky Security 10.1.
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 Security 10.1 для Windows Server, 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 пункт **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 kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Security 10.1.
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 Security 10.1 и службой Kaspersky Security Management Service, вам нужно разрешить сетевые соединения для службы через брандмауэр на защищаемом сервере.

Вам следует произвести настройку сетевых соединений, если Kaspersky Security работает под управлением операционных систем Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2.

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

1. На защищаемом сервера 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 kavfsgt.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Kaspersky Security 10.1 для Windows Server.
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 Security 10.1 для Windows Server

Kaspersky Security 10.1 для Windows Server запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если, устанавливая Kaspersky Security, вы выбрали пункт **Включить постоянную защиту после установки программы**, Kaspersky Security 10.1 для Windows Server проверяет объекты файловой системы сервера при доступе к ним, а также проверяет программный код запускаемых скриптов, если вы установили компонент проверки скриптов. Каждую пятницу в 20:00 Kaspersky Security 10.1 для Windows Server выполняет задачу Проверка важных областей.

После установки Kaspersky Security 10.1 для Windows Server рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Security 10.1 для Windows Server. После установки Kaspersky Security 10.1 для Windows Server проверяет объекты с использованием баз, которые входили в состав программы при поставке.

Рекомендуется сразу же обновить базы Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server на защищаемом Server не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Security 10.1 для Windows Server.

В этом разделе

Настройка и запуск задачи обновления баз Kaspersky Security 10.1 для Windows Server

► *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 Security 10.1 одним из следующих способов:
   - Откройте Консоль Kaspersky Security 10.1 на защищаемом сервере. Для этого выберите **Пуск → Программы → Kaspersky Security 10.1 для Windows Server → Средства администрирования → Консоль Kaspersky Security 10.1**.
   - Если вы запустили Консоль Kaspersky Security 10.1 не на защищаемом сервере, подключитесь к защищаемому серверу:
     a. Откройте контекстное меню узла **Kaspersky Security 10.1 для Windows Server** в дереве Консоли.
     b. Выберите пункт **Подключиться к другому компьютеру**.
     c. В диалоговом окне **Выбор компьютера** выберите вариант **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого сервера.

   Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management Service (см. раздел "О правах доступа к службе Kaspersky Security Management Service" на стр. 56), укажите учетную запись, которая обладает этими правами.

Откроется окно Консоли Kaspersky Security 10.1.

2. В дереве Консоли Kaspersky Security 10.1 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 Security 10.1 для Windows Server будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи (по умолчанию задача выполнится под учетной записью **Локальная система** (**SYSTEM**)).
      - **Использовать NTLM-аутентификацию с именем и паролем**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз программы** выберите пункт **Запустить**.

задачу Обновление баз программыЗапустить .

После того как задача успешно завершится, вы сможете посмотреть дату выпуска последних установленных обновлений баз в панели результатов узла Kaspersky Security 10.1 для Windows Server.

Проверка важных областей

После того как вы обновили базы Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 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 Security 10.1 для Windows Server

Вы можете добавлять или удалять компоненты Kaspersky Security 10.1 для Windows Server. 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 Security 10.1 для Windows Server запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге Мастера.

► *Чтобы изменить состав компонентов Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Security 10.1 для Windows Server > Изменение или удаление**.

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

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

   Откроется окно **Выборочная установка**.

3. В окне **Выборочная установка** в списке компонентов, доступных для использования, выберите компоненты, которые вы хотите добавить в Kaspersky Security 10.1 для Windows Server или удалить. Для этого выполните следующие действия:

   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента и в контекстном меню выберите:
     - пункт **Компонент будет установлен на локальный жесткий диск**, если хотите установить один компонент;

- пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если хотите установить группу компонентов.

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

Нажмите на кнопку **Установить**.

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

Состав компонентов Kaspersky Security 10.1 для Windows Server будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Security 10.1 для Windows Server возникли проблемы (Kaspersky Security 10.1 для Windows Server завершается аварийно; задачи завершаются аварийно или не запускаются), вы можете попробовать восстановить Kaspersky Security 10.1 для Windows Server. Вы можете выполнить восстановление, сохранив текущие значения параметров Kaspersky Security 10.1 для Windows Server или выбрать режим, при котором все параметры Kaspersky Security 10.1 для Windows Server примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Security 10.1 для Windows Server после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Security 10.1 для Windows Server > Изменение или удаление**.

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

   Откроется окно **Восстановление установленных компонентов**.
3. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если хотите сбросить настроенные параметры программы и восстановить Kaspersky Security 10.1 для Windows Server с предустановленными параметрами по умолчанию. Нажмите на кнопку **Установить**.
4. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
5. В окне, открывшемся по завершении восстановления, нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server будет восстановлен в соответствии с заданными параметрами.

Удаление с помощью мастера установки

Этот раздел содержит инструкции для удаления Kaspersky Security 10.1 для Windows Server и Консоли Kaspersky Security 10.1 с защищаемого сервера с помощью мастера установки.

В этом разделе

Удаление Kaspersky Security 10.1 для Windows Server

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Security 10.1 для Windows Server с защищаемого компьютера с помощью мастера установки / удаления.

После удаления Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге Мастера.

► *Чтобы удалить Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Security 10.1 для Windows Server > 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 карантине**, чтобы Kaspersky Security 10.1 для Windows Server экспортировал объекты, помещенные на карантин. По умолчанию флажок снят.

   b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server\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 Security 10.1 для Windows Server будет удален с защищаемого сервера.

Удаление Консоли Kaspersky Security 10.1

> Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль Kaspersky Security 10.1 с сервера с помощью мастера установки / удаления.

После удаления Консоли Kaspersky Security 10.1 перезагрузка сервера не требуется.

► *Чтобы удалить Консоль Kaspersky Security 10.1, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы → Kaspersky Security 10.1 для Windows Server → 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 Security 10.1 для Windows Server из командной строки, примеры команд для установки и удаления Kaspersky Security 10.1 для Windows Server из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Security 10.1 для Windows Server из командной строки.

В этом разделе

Об установке и удалении Kaspersky Security 10.1 для Windows Server из командной строки

Вы можете устанавливать и удалять Kaspersky Security 10.1 для Windows Server, добавлять или удалять его компоненты, запустив из командной строки файлы инсталляционного пакета \product\ks4ws_x86(x64).msi, указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом сервере или другом компьютере в сети, чтобы работать с Консолью Kaspersky Security 10.1 локально или удаленно. Для этого используйте инсталляционный пакет \client\ks4wstools.msi.

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

Если вы запустите на защищаемом компьютере один из файлов \product\ks4ws_x86(x64).msi без дополнительных ключей, Kaspersky Security 10.1 для Windows Server будет установлен с параметрами установки по умолчанию (см. стр.).

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

Примеры команд установки Kaspersky Security 10.1 для Windows Server

В этом разделе приводятся примеры команд для установки Kaspersky Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server: запуск файла setup.exe

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с параметрами установки по умолчанию в режиме без взаимодействия с пользователем, выполните следующую команду:*

\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1

► *Чтобы установить Kaspersky Security 10.1 для Windows Server со следующими параметрами:*

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать постоянную защиту при запуске Kaspersky Security 10.1 для Windows Server;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft;

выполните следующую команду:

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

Примеры команд для установки: запуск msi-файла инсталляционного пакета

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с параметрами установки по умолчанию в режиме без взаимодействия с пользователем, выполните следующую команду:*

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с параметрами установки по умолчанию; показать интерфейс установки, выполните следующую команду:*

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Security 10.1 для Windows Server с активацией с помощью файла ключа C:\0000000A.key:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Security 10.1 для Windows Server с предварительной проверкой активных процессов и загрузочных секторов локальных дисков компьютера, выполните следующую команду:*

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Security 10.1 для Windows Server, сохранив его файлы в папке назначения C:\WSEE, выполните следующую команду:*

```
msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Security 10.1 для Windows Server, сохраните файл журнала установки с именем ks4ws.log в папке, в которой хранится msi -файл инсталляционного пакета Kaspersky Security 10.1 для Windows Server, и выполните следующую команду:*

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Консоль Kaspersky Security 10.1, выполните следующую команду:*

```
msiexec /i ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Security 10.1 для Windows Server с активацией с помощью файла ключа C:\0000000A.key; настроить Kaspersky Security 10.1 для Windows Server в соответствии с параметрами, описанными в конфигурационном файле C:\settings.xml, выполните следующую команду:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Действия после установки Kaspersky Security 10.1 для Windows Server

Kaspersky Security 10.1 для Windows Server запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Security 10.1 для Windows Server был выбран пункт **Включить постоянную защиту после установки программы** (настройка по умолчанию), Kaspersky Security 10.1 for Windows Server проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 8 Kaspersky Security 10.1 для Windows Server выполняет задачу Проверка важных областей.

После установки Kaspersky Security 10.1 для Windows Server рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Security 10.1 для Windows Server. После установки Kaspersky Security 10.1 для Windows Server проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Security 10.1 для Windows Server. 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 Security 10.1 для Windows Server будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: 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 Security 10.1 для Windows Server на защищаемом Server 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 Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server.

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

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn EULA=1 PRIVACYPOLICY=1
```

или

```
\server\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 Security 10.1 для Windows Server переустановит указанные установленные компоненты.

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

```
msiexec /i ks4ws.msi REMOVE=AppCtrl,WiFiControl /qn EULA=1 PRIVACYPOLICY=1
```

Удаление Kaspersky Security 10.1 для Windows Server Примеры команд

► *Чтобы удалить Kaspersky Security 10.1 для Windows Server с защищаемого компьютера, выполните следующую команду:*

```
msiexec /x ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Чтобы удалить Консоль Kaspersky Security 10.1, выполните следующую команду:*

```
msiexec /x ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

или

- Для x32-разрядной операционной системы:

```
msiexec /x {232497F6-6572-4934-A6AF-24986952598B} /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {F96C7F1F-9B03-480D-A8F3-19D43CA89090} /qn
```

► *Чтобы удалить Kaspersky Security 10.1 для Windows Server с защищаемого сервера, на котором установлен пароль, выполните следующую команду:*

- Для x32-разрядной операционной системы:

```
msiexec /x {DD1532DD-387B-43C5-8968-7E8130CC8A5E} UNLOCK_PASSWORD=*** /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {D025308B-AA7E-42D6-8058-B2B79A3D71F5} UNLOCK_PASSWORD=*** /qn
```

► *Чтобы удалить плагин Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Kaspersky Security 10.1 для Windows Server не может быть установлен на компьютер под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows.

Код	Описание
25004	Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующие программы с защищаемого сервера: <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 работы информацию о настройке общих параметров Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security через Kaspersky Security Center, а также описание действий после установки Kaspersky Security 10.1 для Windows Server.

В этом разделе

Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки Kaspersky Security 10.1 для Windows Server будет установлен с одинаковыми параметрами на нескольких компьютерах.

Вы можете Server в одну группу администрирования и создать групповую задачу для установки Kaspersky Security 10.1 для Windows Server на Server этой группы.

Вы можете создать задачу удаленной установки Kaspersky Security 10.1 для Windows Server для набора компьютеров, не объединенных в одну группу администрирования. При ее создании вам нужно сформировать список отдельных Server, на которые требуется установить Kaspersky Security 10.1 для Windows Server.

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

Права для установки или удаления Kaspersky Security 10.1 для Windows Server

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

- На компьютерах, на которых вы хотите установить Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server 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 серверов.

- Все компьютеры, на которые вы хотите установить Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server через Kaspersky Security Center

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

Если вы планируете в дальнейшем управлять Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На Server с установленным Сервером администрирования Kaspersky Security Center установлен плагин управления Kaspersky Security 10.1 для Windows Server (файл \Server\klcfginst.exe комплекта поставки Kaspersky Security 10.1 для Windows Server).
- На защищаемых серверах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых компьютерах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Security 10.1 для Windows Server в задаче удаленной установки.

Вы также можете предварительно объединить серверы в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

► *Чтобы установить Kaspersky Security 10.1 для Windows Server с помощью задачи удаленной установки, выполните следующие действия:*

1. запустить утилиту Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** выберите вариант **Создать новый инсталляционный пакет для программы Лаборатории Касперского**.
3. Введите имя инсталляционного пакета.
4. Выберите файл ks4ws.kud из комплекта поставки Kaspersky Security 10.1 для Windows Server 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. Чтобы изменить набор устанавливаемых компонентов Kaspersky Security 10.1 для Windows Server (см.раздел "Изменение состава компонентов и восстановление Kaspersky Security 10.1 для Windows Server" на стр. 62) и настройки установки по умолчанию (см.раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. 42) в инсталяционном пакете:

   В Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** в рабочей области откройте контекстное меню созданного инсталляционного пакета Kaspersky Security 10.1 для Windows Server и выберите команду **Свойства**. В окне **Свойства: <название инсталляционного пакета>** в разделе **Настройка** выполните следующие действия:

   a. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Security 10.1 для Windows Server, 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 сервера перед началом установки.
- Включить постоянную защиту после установки программы.
- Добавить к исключениям файлы, рекомендованные Microsoft.
- Учесть исключения, рекомендованные "Лабораторией Касперского".

d. Если вы хотите импортировать конфигурационный файл, созданный в предыдущей версии Kaspersky Security для Windows Server, укажите требуемый файл.

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

7. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Security 10.1 для Windows Server на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

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

8. Запустите созданную задачу удаленной установки Kaspersky Security 10.1 для Windows Server.

Kaspersky Security 10.1 для Windows Server будет установлен на указанные в задаче компьютеры.

Действия после установки Kaspersky Security 10.1 для Windows Server

После установки Kaspersky Security 10.1 для Windows Server рекомендуется обновить базы Kaspersky Security 10.1 для Windows Server на компьютерах, а также выполнить проверку важных областей компьютеров, если до установки Kaspersky Security 10.1 для Windows Server на компьютерах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если Server, на которых вы установили Kaspersky Security 10.1 для Windows Server, объединены в одной группе администрирования Kaspersky Security Center, вы можете выполнить эти задачи следующими способами:

1. Создать задачу обновления баз программы для группы Server, на которых вы установили Kaspersky Security 10.1 для Windows Server. 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 серверов. В свойствах созданной политики на закладке **Системные задачи** отключить запуск по расписанию системных задач проверки по требованию и задач обновления баз программы на сервер группы администрирования.

Вы можете также настроить уведомления администратора о событиях Kaspersky Security 10.1 для Windows Server.

Установка Консоли Kaspersky Security 10.1 через Kaspersky Security Center

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

► *Чтобы установить Консоль Kaspersky Security 10.1 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 Security 10.1 для Windows Server 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 Security 10.1, не устанавливая файла справки и документации, выполните следующую команду:

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
     ```
2. В узле Инсталляционные пакеты создайте задачу удаленной установки Консоли Kaspersky Security 10.1 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

   Подробная информация о создании и настройке задачи удаленной установки содержится в *Руководстве администратора Kaspersky Security Center*.
3. Запустите созданную задачу удаленной установки.

Консоль Kaspersky Security 10.1 будет установлена на указанных в задаче компьютерах.

Удаление Kaspersky Security 10.1 для Windows Server через Kaspersky Security Center

Если доступ к управлению Kaspersky Security 10.1 для Windows Server на компьютерах сети защищен паролем, введите пароль при создании задачи группового удаления программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, Kaspersky Security 10.1 для Windows Server будет успешно удален на компьютерах, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Kaspersky Security 10.1 для Windows Server на других компьютерах удален не будет.

► *Чтобы удалить Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server только с параметрами удаления по умолчанию (см. раздел "установка и удаление и их ключи для службы Windows Installer" на стр. 42).

Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Security 10.1 для Windows Server через групповые политики Active Directory, а также информацию о действиях после установки Kaspersky Security 10.1 для Windows Server через групповые политики Active Directory.

В этом разделе

Установка Kaspersky Security 10.1 для Windows Server через групповые политики Active Directory

Вы можете установить Kaspersky Security 10.1 для Windows Server на нескольких компьютерах через групповую политику Active Directory. Таким же образом вы можете установить Консоль Kaspersky Security 10.1.

Серверы, на которых вы хотите установить Kaspersky Security 10.1 для Windows Server или Консоль Kaspersky Security 10.1 должны быть в одном домене и в одной организационной единице.

Операционные системы на Server, на которых вы хотите установить Kaspersky Security 10.1 для Windows Server с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Security 10.1 для Windows Server, используйте инсталляционные пакеты ks4ws_x86(x64).msi. Чтобы установить Консоль Kaspersky Security 10.1, используйте инсталляционные пакеты ks4wstools.msi.

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

► *Чтобы установить Kaspersky Security 10.1 для Windows Server (Консоль Kaspersky Security 10.1), 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 сервер.
3. С помощью **Group Policy Object Editor** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу инсталляционного пакета Kaspersky Security 10.1 для Windows Server (Консоли Kaspersky Security 10.1) 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 Security 10.1 для Windows Server будет установлен на компьютерах группы после их перезагрузки, перед входом в Microsoft Windows.

Действия после установки Kaspersky Security 10.1 для Windows Server

После установки Kaspersky Security 10.1 для Windows Server на защищаемых компьютерах рекомендуется сразу обновить базы программы и выполнить проверку важных областей компьютера. Вы можете выполнить эти действия из Консоли Kaspersky Security 10.1 (см. раздел "Действия после установки Kaspersky Security 10.1 для Windows Server" на стр. 59).

Вы можете также настроить уведомления администратора о событиях Kaspersky Security 10.1 для Windows Server.

Удаление Kaspersky Security 10.1 для Windows Server через групповые политики Active Directory

Если вы устанавливали Kaspersky Security 10.1 для Windows Server или Консоль программы на серверах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server через групповые политики Active Directory невозможно.

► *Чтобы удалить Kaspersky Security 10.1 для Windows Server (Консоль Kaspersky Security 10.1), выполните следующие действия:*

1. На контроллере домена выберите организационную единицу, с серверов которой вы хотите удалить Kaspersky Security 10.1 для Windows Server или Консоль Kaspersky Security 10.1.
2. Выберите политику, созданную для установки Kaspersky Security 10.1 для Windows Server, и в **Редакторе групповых политик**, в узле **Software Installation** (**Конфигурация компьютеров > Конфигурация программ > Software Installation**) откройте контекстное меню инсталляционного пакета (Консоли Kaspersky Security 10.1) и выберите команду **Все задачи→ Удалить** .
3. Выберите метод удаления **Немедленно удалить программу со всех сервер**.
4. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Security 10.1 для Windows Server будет удален с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

Проверка функций Kaspersky Security 10.1 для Windows Server. Использование тестового вируса EICAR

Этот раздел содержит описание тестового вируса EICAR и процедуру проверки функций Kaspersky Security 10.1 для Windows Server Постоянная защита и Проверка по требованию с помощью тестового вируса EICAR.

В этом разделе

О тестовом вирусе EICAR

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

Тестовый вирус не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

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

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Security 10.1 для Windows Server обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли Kaspersky Security 10.1, в журнале выполнении задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server обработал файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задач Kaspersky Security 10.1 для Windows Server Постоянная защита файлов и задач проверки по требованию.

Таблица 14. Префиксы в файлах EICAR

Префикс	Статус файла после проверки и действие Kaspersky Security 10.1 для Windows Server
Без префикса	Kaspersky Security 10.1 для Windows Server присваивает объекту статус **Зараженный** и удаляет его.
SUSP–	Kaspersky Security 10.1 для Windows Server присваивает объекту статус **Возможно зараженный** (обнаружен с помощью эвристического анализатора) и удаляет его (возможно зараженные объекты не подвергаются лечению).
WARN–	Kaspersky Security 10.1 для Windows Server присваивает объекту статус **Возможно зараженный** (код объекта частично совпадает с известным вредоносным кодом) и удаляет его (возможно зараженные объекты не подвергаются лечению).
CURE–	Kaspersky Security 10.1 для Windows Server присваивает объекту статус **Зараженный** и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".

Проверка функций Постоянная защита и Проверка по требованию

После установки Kaspersky Security 10.1 для Windows Server вы можете убедиться, что Kaspersky Security 10.1 для Windows Server обнаруживает объекты, содержащие вредоносный код. Для проверки вы можете использовать тестовый вирус EICAR (см. раздел "О тестовом вирусе EICAR" на стр. 78).

► *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. 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 серверу, и на компьютере, на котором вы сохранили файл eicar.com, включена Служба сообщений Microsoft Windows.
3. Откройте Консоль Kaspersky Security 10.1.
4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого сервера одним из следующих способов:
   - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на компьютер, подключившись к сервера 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 сервера.
- В Консоли Kaspersky Security 10.1 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 Security 10.1 разверните узел **Постоянная защита сервера**, выберите задачу Постоянная защита файлов и на панели результатов узла перейдите по ссылке **Открыть журнал выполнения**).
  - Появилось сообщение Службы сообщений Microsoft Windows на компьютере, с которого вы скопировали файл следующего содержания, следующие: `Kaspersky Security 10.1 для Windows Server 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. 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 Security 10.1.
3. Выполните следующие действия:
   a. В дереве Консоли Kaspersky Security 10.1 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).
   e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.
   f. Запустите задачу Проверка важных областей.

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

- Файл eicar.com удален с жестких компьютера.
- В Консоли Kaspersky Security 10.1 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 Security 10.1 для Windows Server разверните узел **Проверка по требованию**, выберите вложенный узел Проверка важных областей и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

Интерфейс программы

Вы можете управлять Kaspersky Security 10.1 для Windows Server через локальную Консоль и плагин управления Kaspersky Security Center. Действия с локальной Консолью описаны в *Руководстве пользователя Kaspersky Security 10.1 для Windows Server*. 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

Лицензионное соглашение

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 Security 10.1 для Windows Server.
- 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.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security 10.1 для Windows Server прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Security 10 для Windows Server). Чтобы продолжить использование Kaspersky Security 10.1 для Windows Server 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.

Kaspersky Security 10.1 для Windows Server не отслеживает дату окончания срока действия лицензии. Если вы еще раз активируете программу (пока первый код активации действителен) с истекшей лицензией, вам понадобится использовать действующую лицензию, чтобы снова добавить ключ активации.

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

- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или условия лицензии;
- Тип лицензии.

О типах лицензии

Kaspersky Security 10.1 для Windows Server является частью различных решений для корпоративной защиты. Доступная функциональность Kaspersky Security 10.1 для Windows Server зависит от выбранного решения. В таблице ниже вы можете просмотреть типы предлагаемых решений и функциональность программы, доступную для каждого из решений.

Kaspersky Endpoint Security Базовый	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном

Kaspersky Endpoint Security Стандартный	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном

Kaspersky Endpoint Security Расширенный	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль запуска программ Контроль устройств Защита трафика

Kaspersky Security для файловых серверов	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль запуска программ Контроль устройств Мониторинг файловых операций Анализ журналов Защита трафика (Режим Внешний прокси-сервер недоступен)

Kaspersky Endpoint Security Total	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль запуска программ Контроль устройств Защита трафика

Kaspersky Security для систем хранения данных	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль запуска программ Контроль устройств Мониторинг файловых операций Анализ журналов Защита трафика Защита сетевых хранилищ и Защита от шифрования для СХД

Kaspersky Security для гибридных облаков	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль устройств Защита трафика

Kaspersky Security Enterprise для гибридных облаков	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Мониторинг файловых операций Анализ журналов Контроль запуска программ Контроль устройств Защита трафика

Kaspersky Security для виртуальных сред	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Контроль устройств Защита трафика

Kaspersky Security для xSP	
Доступно по подписке	
Компоненты	Файловый антивирус Защита от эксплойтов Управление сетевым экраном Защита трафика

Подписка Amazon Web Services™	
Компоненты	Файловый антивирус Защита от эксплойтов Защита от шифрования (для папок с общим доступом) Управление сетевым экраном Мониторинг файловых операций Анализ журналов Контроль запуска программ Защита трафика Контроль устройств

Kaspersky Security Internet Gateway	
Компоненты	Файловый антивирус Защита от эксплойтов Управление сетевым экраном Защита трафика

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 Security 10.1 для Windows Server. 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 Security 10.1 для Windows Server 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".

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 Security 10.1 для Windows Server или после заказа пробной версии Kaspersky Security 10.1 для Windows Server.

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" на основе имеющегося кода активации.

О предоставлении данных

Лицензионное соглашение для Kaspersky Security 10.1 для Windows Server, 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: https://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 Security 10.1 для Windows Server локально обрабатывает и хранит ряд данных на защищаемом сервере:

- 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 сервере, 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 веб-активности, например, обработанные веб-адреса, присвоенные категории, данные о загружаемых объектах, атрибуты обработанных цифровых сертификатов, данные обработанных электронных писем, в том числе отправитель, получатель, тема, тело письма и его вложения;
- информация о сетевой активности, в том числе IP-адреса заблокированных клиентских компьютеров.

Kaspersky Security 10.1 для Windows Server 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 выполняются в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server, применив ключ.

Если в Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server с помощью ключа, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Лицензирование**.
2. На панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор** и выберите файл ключа с расширением key.

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

4. Нажмите на кнопку **ОК**.

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

Просмотр информации о действующей лицензии

Просмотр информации о лицензии

Информация о действующей лицензии отображается на панели результатов узла **Kaspersky Security** Консоли Kaspersky Security 10.1. Статус ключа может принимать следующие значения:

- **Выполняется проверка статуса лицензии** – Kaspersky Security 10.1 для Windows Server проверяет добавленный файл ключа или примененный код активации и ожидает ответа о текущем статусе ключа.
- **Действующая лицензия: до <дата и время окончания действия лицензии>** – Kaspersky Security 10.1 для Windows Server активирован до указанной даты. Статус ключа выделен желтым цветом в следующих случаях:
  - до истечения срока действия лицензии остается 14 дней, и не добавлен дополнительный ключ или код активации;
  - добавленный ключ помещен в черный список и скоро будет заблокирован.
- **Программа не активирована** – Kaspersky Security 10.1 для Windows Server не активирован, так как не добавлен ключ или код активации. Статус выделен красным цветом.
- **Срок действия лицензии истек** – Kaspersky Security 10.1 для Windows Server не активирован, так как истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – Kaspersky Security 10.1 для Windows Server не активирован, так как нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. 83). Статус выделен красным цветом.
- **Ключ помещен в черный список** – добавленный файл ключа заблокирован и помещен в черный список специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.
- **Подписка приостановлена** – подписка временно приостановлена. Статус выделен красным цветом. Вы можете восстановить действие подписки в любой момент.

Просмотр информации о действующей лицензии

► *Чтобы просмотреть информацию о действующей лицензии,*

В дереве Консоли Kaspersky Security 10.1 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
Код активации	Номер кода активации. Поле заполняется, если вы активируете программу с помощью кода активации.
Статус активации	Информация о статусе активации программы. Информация в графе Статус активации в панели управления узла Лицензирование может принимать следующие значения: • **Применено** – если вы активировали программу с помощью кода активации или ключа. • **Активация** – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус принимает значение Применено по завершении активации программы и после обновления содержимого панели результатов узла. • **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.
Ключ	Номер ключа, с помощью которого вы активировали программу.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Дата и время окончания срока действия	Дата окончания срока действия лицензии по активному ключу.
Статус кода активации или ключа	Статус кода активации или ключа: активный или дополнительный.

► *Чтобы просмотреть подробную информацию о лицензии,*

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

В открывшемся 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 Security 10.1 для Windows Server (см. таблицу ниже).

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

Поле	Описание
Закладка Общие	
Ключ	Номер ключа, с помощью которого вы активировали программу.
Дата добавления ключа	Дата добавления ключа в программу.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Истекает через (сут)	Число суток, оставшихся до даты окончания срока действия лицензии по активному ключу.

Поле	Описание
Дата окончания срока действия	Дата окончания срока действия лицензии по активному ключу. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если Kaspersky Security 10.1 для Windows Server не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*.
Программа	Название программы, для которой добавлен ключ или код активации.
Ограничение на использование ключа	Предусмотренное ограничение на использование ключа (если имеется).
Осуществление технической поддержки	Информация о том, оказывает ли "Лаборатория Касперского" или ее партнер техническую поддержку заказчику по условиям предоставления лицензии.
Закладка Дополнительно	
Информация о лицензии	Номер и тип действующей лицензии.
Информация о поддержке	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
Информация о владельце	Информация о заказчике лицензии: имя заказчика и название организации, для которой приобретена лицензия.

Функциональные ограничения даты окончания срока действия лицензии

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

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

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

Продление срока действия лицензии

По умолчанию программа уведомляет вас о скором окончании срока действия лицензии за 14 дней до даты окончания срока действия лицензии. При этом статус **Действующая лицензия: до <дата окончания действия лицензии>** в панели результатов узла **Kaspersky Security 10.1 для Windows Server** 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 Security 10.1 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:
     a. Перейдите по ссылке **Добавить ключ**.
     b. В открывшемся окне нажмите на кнопку **Обзор** и выберите новый файл ключа с расширением key.
     c. Установите флажок **Использовать в качестве дополнительного ключа**.
   - Если вы хотите продлить срок действия лицензии с помощью кода активации:
     a. Перейдите по ссылке **Добавить код активации**.
     b. В открывшемся окне введите приобретенный код активации.
     c. Установите флажок **Использовать в качестве дополнительного ключа**.

   Для применения кода активации необходимо подключение к интернету.
4. Нажмите на кнопку **ОК**.

Дополнительный ключ или код активации будет добавлен и автоматически станет активным по истечении срока действия используемого ключа или кода активации Kaspersky Security 10.1 для Windows Server.

Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Security 10.1 для Windows Server 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 Security 10.1 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 Security 10.1 для Windows Server

Этот раздел содержит информацию о запуске плагина управления Kaspersky Security 10.1 для Windows Server, а также запуске и остановке службы Kaspersky Security Service.

В этом разделе

Запуск плагина управления Kaspersky Security Center

Запуск плагина Kaspersky Security Center, в котором осуществляется работа с Kaspersky Security 10.1 для Windows Server, 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 *Руководстве администратора Kaspersky Security Center*.

Запуск и остановка службы Kaspersky Security

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 активности на компьютерах, Защиты сетевых хранилищ, Проверки по требованию и обновления.

По умолчанию при запуске службы Kaspersky Security Service 10.1 для Windows Server запускаются задачи Постоянная защита файлов, Проверка скриптов (если этот компонент установлен), 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 перезапустите 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 Security 10.1 для Windows Server** или с помощью оснастки **Службы** Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server откройте контекстное меню узла **Kaspersky Security 10 для Windows Server**.
2. Выберите одну из следующих команд:
   - **Остановить Kaspersky Security 10.1 для Windows Server**, чтобы остановить службу Kaspersky Security Service;
   - **Запустить Kaspersky Security 10.1 для Windows Server**, чтобы запустить службу Kaspersky Security Service.

Служба Kaspersky Security Service будет запущена или остановлена.

Права доступа к функциям Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о правах на управление Kaspersky Security 10.1 для Windows Server и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

В этом разделе

О правах на управление Kaspersky Security 10.1 для Windows Server

По умолчанию доступ ко всем функциям Kaspersky Security 10.1 для Windows Server имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, пользователи группы KAVWSEE Administrators, созданной на защищаемом сервере при установке Kaspersky Security 10.1 для Windows Server, а также группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Security 10.1 для Windows Server, могут предоставлять доступ к функциям Kaspersky Security 10.1 для Windows Server другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Security 10.1 для Windows Server, он не может открыть Консоль Kaspersky Security 10.1.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security 10.1 для Windows Server один из следующих предустановленных уровней доступа к функциям Kaspersky Security 10 для Windows Server:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Security 10.1 для Windows Server, параметры работы компонентов Kaspersky Security 10.1 для Windows Server, права пользователей Kaspersky Security 10.1 для Windows Server, а также просматривать статистику работы Kaspersky Security 10 для Windows Server.

- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Security 10.1 для Windows Server, параметры работы компонентов Kaspersky Security 10.1 для Windows Server.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Security 10.1 для Windows Server, параметры работы компонентов Kaspersky Security 10.1 для Windows Server, статистику работы Kaspersky Security 10.1 для Windows Server и права пользователей Kaspersky Security 10.1 для Windows Server.

Также вы можете выполнять расширенную настройку прав доступа (см. раздел "Настройка прав доступа на управление Kaspersky Security 10.1 для Windows Server и службой Kaspersky Security Service" на стр. 103): разрешать или запрещать доступ к отдельным функциям Kaspersky Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Security 10.1 для Windows Server.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать из конфигурационного файла параметры работы Kaspersky Security 10.1 для Windows Server. • Редактировать настройки программы.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Security 10.1 для Windows Server и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Security 10.1 для Windows Server; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Security 10.1 для Windows Server.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Security 10.1 для Windows Server.

Права доступа	Описание
Удаление программы	Возможность удалять Kaspersky Security 10.1 для Windows Server.
Чтение прав	Возможность просматривать список пользователей Kaspersky Security 10.1 для Windows Server и права доступа каждого пользователя.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Security 10.1 для Windows Server.

О правах на управление службой Kaspersky Security Service

При установке Kaspersky Security 10.1 для Windows Server 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 сервере через управление Kaspersky Security Service, вы можете ограничивать права на управление службой Kaspersky Security Service с помощью локальной Консоли Kaspersky Security 10.1 или плагина управления Kaspersky Security Center.

По умолчанию доступ к управлению службой Kaspersky Security Service имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

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

Пользователи, которые имеют доступ с правом на изменение к функциям (см. раздел "О правах на управление Kaspersky Security 10.1 для Windows Server" на стр. 99), могут предоставлять доступ к управлению службой Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security 10.1 для Windows Server один из следующих предустановленных уровней доступа на управление службой 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 10.1 для Windows Server (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 Security 10.1 для Windows Server

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: • добавлять и удалять пользователей Kaspersky Security Service; • изменять права доступа пользователей к Kaspersky Security Service.
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

Вы можете просмотреть список служб Kaspersky Security 10.1 для Windows Server.

При установке Kaspersky Security 10.1 для Windows Server регистрирует службу управления программой Kaspersky Security 10.1 для Windows Server (KAVFSGT). Для управления программой через Консоль Kaspersky Security 10.1, установленную на другом компьютере требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Security 10.1 для Windows Server имела полный доступ к Kaspersky Security Management Service на защищаемом сервере.

По умолчанию доступ к управлению службой Kaspersky Security Management Service имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, и пользователи группы KAVWSEE Administrators, созданной на защищаемом сервере при установке Kaspersky Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server.

Вы можете соединиться с Kaspersky Security 10.1 для Windows Server под локальной учетной записью, если на защищаемом сервере зарегистрирована учетная запись с таким же именем и с таким же паролем.

Настройка прав доступа на управление Kaspersky Security 10.1 для Windows Server и службой Kaspersky Security Service

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Security 10.1 для Windows Server 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 Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.

- Если вы хотите настроить параметры программы для одного сервера, 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. 124) 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 Security 10.1 для Windows Server.
   - 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 Security 10.1 для Windows Server"**.

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 Security 10.1 для Windows Server или службой Kaspersky Security Service, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server 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 серверов выберите закладку **Политики** и откройте **<Имя политики> > Параметры**.
   - Если вы хотите настроить параметры программы для одного сервера, 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. 124) 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 Security 10.1 для Windows Server.
   - 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 Security 10.1 для Windows Server"**.

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 Security 10.1 для Windows Server или службой Kaspersky Security Service.
   - **Чтение**:
     - следующие права на управление Kaspersky Security 10.1 для Windows Server: **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 Security 10.1 для Windows Server, кроме **Изменения 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 Security 10.1 для Windows Server** 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 Security 10.1 для Windows Server** нажмите на кнопку **ОК.**
7. В окне **Разрешения для группы "Kaspersky Security 10.1 для Windows Server"** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Security 10.1 для Windows Server или службой Kaspersky Security Service будут сохранены.

Защита доступа к функциям Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server" на стр. 99). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Security 10.1 для Windows Server.

Kaspersky Security 10.1 для Windows Server запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к локальной Консоли Kaspersky Security 10.1;
- удаление Kaspersky Security 10.1 для Windows Server;
- изменение компонентного состава Kaspersky Security 10.1 для Windows Server.

Kaspersky Security 10.1 для Windows Server не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
   - Если вы хотите настроить параметры программы для одного сервера, 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. 124) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В блоке **Настройки 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 Security 10.1 для Windows Server.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Security 10.1 для Windows Server будет запрашивать пароль при доступе к защищаемым операциям.

Установленный пароль невозможно восстановить. Утеря пароля приведет к полному потерю контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого сервера.

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 Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
   - Если вы хотите настроить параметры программы для одного сервера, 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. 124) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В блоке **Настройки пароля** снимите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** будут очищены и станут неактивны.
5. Нажмите на кнопку **ОК**.

Защита паролем будет отключена. Kaspersky Security 10.1 для Windows Server 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 сервере, выполните следующие действия:*

1. На защищаемом сервере под управлением Microsoft Windows Server выберите **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 Security 10.1.
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 сервере будут разрешены.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления задачами Kaspersky Security 10.1 для Windows Server на нескольких серверах.

В этом разделе

О политиках

Вы можете создавать единые политики Kaspersky Security Center для управления защитой нескольких серверов, на которых установлен Kaspersky Security 10.1 для Windows Server.

Политика применяет указанные в ней значения параметров Kaspersky Security 10.1 для Windows Server, его функций и задач на всех защищаемых серверах 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 Security 10.1 для Windows Server. Вы можете просмотреть ее в Консоли Kaspersky Security 10.1 в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на локальных компьютерах: *Запретить изменение параметров*. После применения политики Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не применяет значения параметров активной политики, рядом с которыми в свойствах политики установлен значок 🔓.

Если политика активна, то в Консоли Kaspersky Security 10.1 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 Security 10.1.

Параметры, настроенные в активной политике и помеченные значком 🔒, также блокируют изменение параметров в Kaspersky Security Center для одного сервера 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 или задач защиты сетевых хранилищ, 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 открывшемся окне **Свойства: <Имя политики>** созданной политики вы можете настроить параметры постоянной защиты, общие параметры Kaspersky Security 10.1 для Windows Server, параметры карантина и резервного хранилища, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Security 10.1 для Windows Server.

► *Чтобы создать политику для группы серверов, на которых установлен Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, а затем выберите группу администрирования, для серверов 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 Security 10.1 для Windows Server.
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 Security 10 для Windows Server**, чтобы использовать данную политикув качестве шаблона.

     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 кнопку 🔒, чтобы разблокировать настройку параметров задачи на компьютерах сети и запретить применение настроенных в политике параметров задачи.
   - Нажмите 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.
8. В окне мастера **Завершение работы** нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик на закладке **Политики** выбранной группы администрирования. В открывшемся окне **Свойства: <Имя политики>** вы можете настроить другие параметры, и задачи и функции Kaspersky Security 10.1 для Windows Server.

Настройка политики

В окне **Свойства: <Имя политики>** существующей политики вы можете настроить общие параметры Kaspersky Security 10.1 для Windows Server, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты, параметры контроля активности на компьютерах, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Security 10.1 для Windows Server, 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**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить, затем выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить и откройте окно **Свойства:<Имя политики>** одним из следующих способов:
   - Выберите параметр **Свойства** в контекстном меню политики.
   - В панели результатов выбранного узла перейдите по ссылке **настроить параметры политики**.
   - Дважды щелкните выбранную политику.
4. На закладке **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
   - **Активная политика**, если хотите, чтобы политика применялась на всех серверах, входящих в выбранную группу администрирования.
   - **Неактивная политика**, если не хотите, чтобы политика применялась на всех серверах, входящих в выбранную группу.

Параметр **Политика для автономных пользователей** недоступен при работе с Kaspersky Security 10.1 для Windows Server.

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 блоках **Постоянная защита**, **Контроль активности на компьютерах**, **Контроль активности в сети**, **Мониторинг целостности системы** настройте параметры выполнения задач программы, а также параметры их запуска (см. таблицу ниже).

   Вы можете включать и выключать выполнение любой задачи на всех серверах, 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.

Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

Разделы свойств политики Kaspersky Security 10.1 для Windows Server

Общие

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

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

Уведомления о событиях

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

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

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

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

Параметры программы

Таблица 19. Настройки раздела Параметры программы

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

Дополнительные возможности

Таблица 20. Настройки раздела Дополнительные возможности

Раздел	Параметры
Доверенная зона	В блоке **Доверенная зона** по кнопке **Настройка** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных дисков	В блоке **Менеджер устройств** по кнопке **Настройка** вы можете настроить параметры проверки съемных дисков, подключаемых по USB.
Права пользователей на управление программой	В блоке **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей к управлению Kaspersky Security 10.1 для Windows Server.
Права пользователей на управление службой	В блоке **Права пользователей на управление службой** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security Service.

Раздел	Параметры
Хранилища	В блоке **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить передачу на Сервер администрирования информации об объектах резервного хранилища и карантина. • Настройка периода блокировки узлов.

Постоянная защита сервера

Таблица 21. Настройки раздела Постоянная защита

Раздел	Параметры
Постоянная защита файлов	В блоке **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать предустановленный уровень безопасности или настроить параметры безопасности вручную; • Настройте параметры запуска задачи.
Использование KSN	В блоке **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • указать действия над объектами, недоверенными в KSN; • настроить производительность задачи; • настроить параметры использования Kaspersky Security Center в качестве прокси-сервера KSN; • принять Положение о KSN; • Настройте параметры запуска задачи.
Защита от эксплойтов	В блоке **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.

Раздел	Параметры
Проверка скриптов	В задаче **Проверка скриптов** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • разрешить или запретить выполнение предположительно опасных скриптов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • Настройте параметры запуска задачи.

Контроль активности на компьютерах

Таблица 22. Параметры в блоке Контроль активности на компьютерах

Раздел	Параметры
Контроль запуска программ	В блоке **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Выберите режим работы задачи. • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • Настройте параметры запуска задачи.
Контроль устройств	В блоке **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Выберите режим работы задачи. • Настройте параметры запуска задачи.

Контроль активности в сети

Таблица 23. Параметры в блоке Контроль активности в сети

Раздел	Параметры
Управление сетевым экраном	В блоке **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • настроить правила сетевого экрана; • Настройте параметры запуска задачи.
Защита от шифрования	В блоке **Защита от шифрования** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • настроить область защиты от вредоносного шифрования; • Настройте параметры запуска задачи.

Диагностика системы

Таблица 24. Настройки раздела Диагностика системы

Раздел	Параметры
Мониторинг файловых операций	В блоке **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.
Анализ журналов	В блоке **Анализ журналов** можно настроить контроль целостности защищаемого сервера на основе результатов анализа журналов событий Windows.

Журналы и уведомления

Таблица 25. Настройки раздела Журналы и уведомления

Раздел	Параметры
Журналы выполнения задач	В блоке **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач. • Укажите параметры интеграции SIEM с Kaspersky Security Center.
Уведомления о событиях	В блоке **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для события *Обнаружен объект*; • указать параметры уведомления администратора для любого выбранного события из списка событий в блоке **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В блоке **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, информацию о которых Kaspersky Security 10.1 для Windows Server будет передавать на Сервер администрирования.

Защита сетевых хранилищ

Таблица 26. Настройки раздела Защита сетевых хранилищ

Раздел	Параметры
Постоянная защита (RPC)	В блоке **Постоянная защита (RPC)** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Использование эвристического анализатора. • Параметры соединения с сетевым хранилищем. • Область защиты.
Постоянная защита (ICAP)	В блоке **Постоянная защита (ICAP)** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Параметры соединения с ICAP сервисом. • Интеграция с другими компонентами. • уровень безопасности.
Защита от шифрования для NetApp	В блоке **Защита от шифрования для NetApp** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Режим работы задачи • Использование эвристического анализатора. • Настройки соединения и аутентификации. • Укажите исключения из области защиты.

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 сервере 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 Security 10.1 для Windows Server 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 сервер из группы администрирования, расписание системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server на серверах группы, выберите команду **Свойства**.
3. В окне **Свойства: <Имя политики>** откройте блок **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.
4. Убедитесь, что политика (см. раздел "О политиках" на стр. 109), которую вы настраиваете, активна и применена к группе серверов администрирования.
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 Security 10.1 для Windows Server, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

О создании задач в Kaspersky Security Center

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

- Активация программы;
- Копирование обновлений;
- Обновление баз программы;
- обновление модулей программы;
- откат обновления баз программы;
- Проверка по требованию;
- проверка целостности программы;
- Автоматическое формирование разрешающих правил;
- генерация правил контроля устройств.

Вы можете создать локальные и групповые задачи следующими способами:

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

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 117) на всех защищаемых серверах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 сервер.
     b. В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом сервере 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 Security 10.1 для Windows Server** 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*:

     a. В окне **Область проверки** сформируйте область проверки.

        По умолчанию область проверки включает критические области сервера. Проверяемые области помечены в таблице 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 сервере 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 Security 10.1.

     - 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 сервера, папку, сетевой объект или файл на защищаемом сервере или другом компьютере в сети, а затем нажмите на кнопку **ОК**.

     - Области, являющиеся исключениями из проверки, помечены в таблице значком ☐.

     a. 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 Security 10.1 для Windows Server.

        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 сервера (серверов) 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 Security 10.1 для Windows Server, имеют приоритет **Средний** . Понижение приоритета процесса увеличивает время выполнения задачи, но оно также может положительно повлиять на скорость выполнения процессов других активных программ.

- *Если вы создаете одну из задач обновления*, установите параметры задачи в соответствии с вашими требованиями:

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

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

  c. На закладке **Настройка параметров соединения** выполните следующие действия:

     Укажите режим FTP-сервера для соединения с защищаемым сервером.

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

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

     Укажите местоположение защищаемого сервера (серверов), 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 сервера. Чтобы Kaspersky Security 10.1 для Windows Server автоматически запускал перезагрузку сервера 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 Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server**, в котором будет содержаться адрес страницы на нашем веб-сайте, откуда вы сможете загружать плановые обновления. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

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

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

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

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

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

  c. 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:

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

   b. Укажите частоту запуска задач: выберите одно из следующих значений из списка **Частота запуска**: **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**): задачи обновления баз и модулей программы;

      - если вы выбрали **Ежечасно**, укажите количество часов в поле **Раз в <количество> ч** в группе параметров **Параметры запуска задачи**;

      - если вы выбрали **Ежесуточно**, укажите количество дней в поле **Раз в <количество> сут** в группе параметров **Параметры запуска задачи**;

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

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

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

      - Укажите максимальную продолжительность выполнения задачи: в 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 распределения времени запуска: установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.

   e. Нажмите на кнопку **ОК**.

6. Если создаваемая задача является задачей для произвольного набора серверов, выберите серверы 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 создании. 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 сервера в окне Параметры программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый сервер.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя сервера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого сервера;
   - откройте контекстное меню на имени защищаемого сервера и выберите пункт **Свойства**.

   Откроется окно Откроется окно **<Имя Компьютера>**.
4. Чтобы настроить параметры локальной задачи, выполните следующие действия:
   a. Перейдите в раздел **Задачи**.
      - В списке задач выберите локальную задачу, параметры которой вы хотите настроить.
      - Дважды щелкните на имени задачи в списке задач.
      - Выберите имя задачи и нажмите на кнопку **Свойства**.
      - Затем выберите пункт **Свойства** в контекстном меню выбранной задачи.
5. Чтобы настроить параметры программы, выполните следующие действия:
   a. Перейдите в блок **Программы**.
      - В списке установленных программ выберите программу, которую хотите настроить.
      - двойным щелчком мыши на названии программы в списке установленных программ;
      - выделите название программы в списке установленных программ и нажмите на кнопку **Свойства**;
      - откройте контекстное меню на названии программы в списке установленных программ и выберите пункт **Свойства**.

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

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

Настройка групповых задач в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 *Руководстве администратора 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 блоке **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 сервера, в блоке **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу. Подробная информация о настройке параметров в этом разделе содержится в *Руководстве администратора 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 блоке содержится в *Руководстве администратора Kaspersky Security Center*.
9. В открывшемся 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 27. Параметры групповых задач Kaspersky Security 10.1 для Windows Server

Тип задачи Kaspersky Security 10.1 для Windows Server	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
Автоматическая генерация правил (задача Генерация правил контроля запуска программ и задача Генерация правил контроля устройств).	**Настройка**	При настройке параметров задачи Генерация правил контроля запуска программ вы можете: • 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.

	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. • **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. • **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. Этот вариант выбран по умолчанию. • **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 указанной 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 Security 10.1 для Windows Server создает по завершении задач.

	Расписание	Вы можете настроить параметры запуска задачи по расписанию.
Активация программы	**Параметры активации программы**	Вы можете добавить код активации или ключ для активации программы или для продления срока действия лицензии.
	Расписание	Вы можете настроить параметры запуска задачи по расписанию.
Копирование обновлений.	**Источник обновлений**	Вы можете указать сервер администрирования Kaspersky Security Center или Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Настройка параметров соединения** ► *Чтобы открыть окно **Настройка параметров соединения**,* нажмите на кнопку **Настройка параметров соединения** в разделе **Источник обновлений**.	В блоке **Параметры соединения с источниками обновлений** вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров копирования обновлений	Вы можете указать состав обновлений для копирования. В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Security 10.1 для Windows Server будет сохранять скопированные обновления.
	Расписание	Вы можете настроить параметры запуска задачи по расписанию.

<table>
<tr><td rowspan="2">Обновление баз программы</td><td>Источник обновлений</td><td>В блоке Источник обновлений вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.
Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:
• Снизить нагрузку на дисковую 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).</td></tr>
<tr><td>Объем оперативной памяти (в мегабайтах), который программа использует для размещения файлов обновлений.
По умолчанию установлен объем оперативной памяти 512 МБ.</td><td>Окно Настройка параметров соединения
► Чтобы открыть окно Настройка параметров соединения,
нажмите на кнопку Настройка параметров соединения в разделе Источник обновлений.</td><td>В блоке Параметры соединения с источниками обновлений вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.</td></tr>
<tr><td></td><td>Расписание</td><td>Вы можете настроить параметры запуска задачи по расписанию.</td></tr>
</table>

Обновление модулей программы	**Источник обновлений**	Вы можете указать сервер администрирования Kaspersky Security Center или Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Настройка параметров соединения** ► *Чтобы открыть окно **Настройка параметров соединения**,* нажмите на кнопку **Настройка параметров соединения** в разделе **Источник обновлений**.	В блоке Параметры соединения с источниками обновлений вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров обновления модулей программы	Вы можете указать действия, которые Kaspersky Security 10.1 для Windows Server будет совершать при наличии критических обновлений модулей программы, при наличии информации о доступных плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
	Расписание	Вы можете настроить параметры запуска задачи по расписанию.
Проверка по требованию	**Настройка**	Вы можете сформировать область проверки для задачи проверки по требованию, а также перейти к настройке уровня безопасности.

	Окно **Настройка проверки по требованию** ► *Чтобы открыть окно **Настройка проверки по требованию**,* нажмите на кнопку **Настройка параметров области защиты** в блоке **Настройка**.	Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную.
	Параметры	В блоке **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка. В блоке **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.
	Расписание	Вы можете настроить параметры запуска задачи по расписанию.
Проверка целостности модулей программы	**Расписание**	Вы можете настроить параметры запуска задачи по расписанию.

Для задачи типа Откат обновления баз программы вы можете настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этих разделах содержится в *Руководстве администратора Kaspersky Security Center.*

В этом разделе

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 **<Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.
5. Подробная информация о настройке параметров в этом разделе содержится в *Руководстве администратора Kaspersky Security Center.*
6. В разделе **Настройка** вы можете настроить следующие параметры:
   - изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами;
   - учитывать или не учитывать запущенные программы.
7. В разделе **Параметры** вы можете указать действия при формировании разрешающих правил контроля запуска программ:
   - **Использовать цифровой сертификат**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.
   - **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.

  Этот вариант выбран по умолчанию.

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

  Поле, в котором отображаются пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / или указанной 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 Security 10.1 для Windows Server создает по завершении задач.

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

10. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

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

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

   Подробная информация о настройке параметров в этих разделах содержится в *Руководстве администратора Kaspersky Security Center*.
10. В открывшемся 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 **<Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Руководстве администратора 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.

     c. Нажмите на кнопку **Настройка параметров соединения** и в открывшемся окне **Параметры соединения** настройте параметры использования прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского» и другими серверами.

- В блоке **Настройка параметров обновления модулей программы** для задачи Обновление модулей программы вы можете указать действия, которые Kaspersky Security 10.1 для Windows Server будет совершать при наличии критических обновлений модулей программы и при наличии информации о доступных плановых обновлениях. Вы также можете настроить действия Kaspersky Security 10.1 для Windows Server по завершении установки критических обновлений.
- В блоке **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.
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 этих разделах содержится в *Руководстве администратора Kaspersky Security Center*.

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

   Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы вы можете настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в блоках **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этих разделах содержится в *Руководстве администратора Kaspersky Security Center*.

Проверка целостности модулей программы

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. 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 **<Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

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

5. В разделе **Устройства**, выберите устройства для которых вы хотите настроить задачу проверки целостности модулей программы.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
8. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

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

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

   Настроенные параметры групповых задач будут сохранены.

Создание задачи проверки по требованию

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

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый сервер.
     b. В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом сервере 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 Security 10.1 для Windows Server** выберите задачу **Проверка по требованию** и нажмите на кнопку **Далее**.

4. В окне **Область проверки** сформируйте область проверки:

   По умолчанию область проверки включает критические области сервера. Проверяемые области помечены в таблице значком ☑. Области, являющиеся исключениями из проверки, помечены в таблице 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 предустановленную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
     a. Нажмите правой клавишей мыши в таблице **Область защиты** и выберите **Добавить область защиты**.
     b. В окне **Добавление в область проверки** выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом сервере или другом компьютере в сети и нажмите на кнопку **ОК**.
   - Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:
     a. Откройте контекстное меню и выберите параметр **Настроить**.
     b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
     c. На закладке **Общие** в окне параметров **Проверка по требованию** снимите флажок **Вложенные папки (вложенные файлы)** .
   - Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
     a. Откройте контекстное меню на области, параметры которой вы хотите изменить, и выберите **Настроить**.
     b. 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 Security 10.1.
   - Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:
     a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить исключение**.
     b. Укажите объекты, которые вы хотите исключить: выберите предустановленную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на сервере или другом компьютере сети.
     c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и дополнительные параметры:

   - Настройте использование эвристического анализатора (см. раздел "Использование эвристического анализатора" на стр. 181).
   - Установите флажок **Применять доверенную зону**, если в задаче вы хотите исключить из области проверки объекты, описанные в доверенной зоне Kaspersky Security 10.1 для Windows Server.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Security для Windows Server 10.1 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Security для Windows Server 10.1 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

     По умолчанию флажок установлен.

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

     Флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

     Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

     Если флажок снят, задача постоянной защиты файлов не использует службы KSN.

     По умолчанию флажок установлен.

   - Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый приоритет **Низкий** (Low), в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**.

     Флажок изменяет приоритет задачи.

     Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему сервера со стороны других задач Kaspersky Security 10.1 для Windows Server и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки и увеличивается при уменьшении нагрузки.

     Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Security 10.1 для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

     По умолчанию флажок снят.

     По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Security 10.1 для Windows Server, имеют приоритет **Средний** .

- Чтобы использовать создаваемую задачу в качестве задачи проверки важных областей сервера, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты сервера. Kaspersky Security Center оценивает безопасность сервера (серверов) по показателям производительности задачи и присваивает статус *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Security 10.1 для Windows Server. Вы можете изменять значение этого параметра на стороне Kaspersky Security Center.

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

  Если флажок снят, задача проверки выполняется с низким приоритетом.

  Флажок установлен по умолчанию для задачи Проверка важных областей.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** настройте расписание задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 146).
8. Укажите учетную запись пользователя, под которой вы хотите выполнять задачу, и укажите имя задачи.
9. Нажмите на кнопку **Готово**.

Будет создана новая задача проверки по требованию для выбранного сервера или группы серверов.

Настройка задач проверки по требованию

► *Чтобы настроить задачу Проверка по требованию, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. 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 **<Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

> Подробная информация о настройке параметров в этом разделе содержится в *Руководстве администратора Kaspersky Security Center.*

5. В блоке **Параметры** вы можете выполнить следующие действия:

   a. В блоке **Область проверки** установите флажки напротив тех, файловых ресурсов, которые вы хотите включить в область проверки.

   b. Нажмите на кнопку **Настройка параметров области защиты** и выберите уровень безопасности.

      Вы можете установить 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 блоке **Параметры** вы можете выполнить следующие действия:

   a. В блоке **Эвристический анализатор** включить или выключить использование эвристического анализатора и настроить уровень анализа с помощью ползунка.

   b. Настройте **Дополнительные параметры** (см. раздел "**Создание задачи проверки по требованию**" на стр. 138).

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

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

9. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

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

10. В открывшемся 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 серверу статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано параметром Kaspersky Security 10.1 для Windows Server **Порог формирования события Проверка важных областей не проводилась давно**.

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

1. Создайте групповую задачу проверки по требованию.
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей 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** как при создании задачи проверки по требованию для группы серверов или для набора серверов, так и позже, в окне **Свойства: <Название задачи>**.

3. С помощью новой или существующей политики отключите запуск по расписанию системных задач проверки по требованию на группе серверов (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 117).

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого сервера 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 Security 10.1 вы можете просмотреть, является ли задача проверки по требованию задачей проверки важных областей компьютера.

В Консоли Kaspersky Security 10.1 флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задач, но он не доступен для редактирования.

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Security 10.1 для Windows Server возникла проблема (например, Kaspersky Security 10.1 для Windows Server завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Security 10.1 для Windows Server и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Security 10.1 для Windows Server не отправляет файлы трейсов и дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Security 10.1 для Windows Server записывает информацию в файлы трассировки и файл дампа в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется настройками операционной системы и Kaspersky Security 10.1 для Windows Server. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Security 10.1 для Windows Server" на стр. 99) и разрешить доступ к журналам, файлам трейса и дампа только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. 124).
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 Security 10.1 для Windows Server будет сохранять файлы трассировки.
     - Настройте уровень детализации отладочной информации.

       В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки.

       Вы можете выбрать один из следующих уровней детализации:

       - **Критические события** – Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки только информацию о критических событиях.
       - **Ошибки** – Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки информацию о критических событиях и об ошибках.
       - **Важные события** – Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки информацию о критических событиях, об ошибках и о важных событиях.
       - **Информационные события** – Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки информацию о критических событиях, об ошибках, о важных событиях и об информационных событиях.
       - **Вся отладочная информация** – Kaspersky Security 10.1 для Windows Server сохраняет в файле трассировки всю отладочную информацию.

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

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

       Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.
     - Укажите максимальный размер файлов трассировки.
     - Укажите отлаживаемые компоненты. Коды компонентов следует вводить через точку с запятой И с учетом регистра (см. таблицу ниже).

Таблица 28. Коды подсистем Kaspersky Security 10.1 для Windows Server

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Security 10.1 для Windows Server в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.

bl	Управляющий процесс, реализует задачи управления Kaspersky Security 10.1 для Windows Server.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Security 10.1 для Windows Server.
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 Security 10.1 для Windows Server (gui) и плагина управления Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Security 10.1 для Windows Server сохраняет отладочную информацию о работе всех подсистем Kaspersky Security 10.1 для Windows Server (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 Security 10.1 для Windows Server будет сохранять файл дампа.

3. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут применены на защищаемом сервере.

Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Security 10.1 для Windows Server по расписанию, а также настраивать параметры запуска по расписанию.

В этом разделе

Настройка параметров расписания запуска задач

В Консоли Kaspersky Security 10.1 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 серверов выберите **Политика> <Имя политики> > <Раздел> > Настроить> Управление задачей**.
   - Если вы хотите настроить параметры задачи для одного сервера через Kaspersky Security Center, откройте окно **Параметры задачи** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. 124) в Kaspersky Security Center.

     Откроется окно **Параметры**.
2. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск задачи по расписанию запрещен действием политики Kaspersky Security Center.
3. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. В списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если 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 Security 10.1 для Windows Server;
- **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.

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

c. В поле **Начать с** укажите дату начала действия расписания.

> После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы откроете окно **Параметры задачи** на закладке **Расписание**.
> Значение **Запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики Kaspersky Security Center (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 117).

4. На закладке **Дополнительно** настройте в соответствии с вашими требованиями следующие параметры расписания.
   - В блоке **Параметры остановки задачи** выполните следующие действия:
     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**, чтобы сохранить параметры запуска задачи.

Включение и выключение запуска по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 откройте контекстное меню имени 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 будут применены 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 Security 10.1 для Windows Server в Kaspersky Security Center.

В этом разделе

О способах управления Kaspersky Security 10.1 для Windows Server из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленным Kaspersky Security 10.1 для Windows Server, включенными в группу администрирования, с помощью плагина Kaspersky Security Center.

Группа администрирования формируется на стороне Kaspersky Security Center вручную и включает в себя несколько серверов с установленным Kaspersky Security 10.1 для Windows Server, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Руководстве администратора Kaspersky Security Center*.

Параметры программы для одного сервера недоступны для настройки, если работа Kaspersky Security 10.1 для Windows Server на этом сервере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Security 10.1 для Windows Server из Kaspersky Security Center следующими способами:

- **Использование политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы серверов. Параметры задач, заданные в активной политике, имеют приоритет над параметрами задач, настроенными локально в Консоли Kaspersky Security 10.1 или удаленно в окне **Свойства: <Имя сервера>** Kaspersky Security Center.

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

- **Использование групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для группы серверов.

  С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления, параметры задачи автоматического формирования разрешающих правил.

- **Использование задач для набора устройств**. Задачи для набора устройств позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для серверов, которые не включены ни в одну из созданных групп администрирования.

- **Использование окна настройки параметров одного сервера**. В открывшемся окне **Свойства: <Имя сервера>** вы можете удаленно настроить параметры задачи для одного сервера, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Security 10.1 для Windows Server, если выбранный сервер не находится под управлением действующей 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 серверов, так и для одного сервера.

О настройке общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Security 10.1 для Windows Server из Kaspersky Security Center для группы серверов или для одного сервера.

В этом разделе

Настройка масштабируемости и интерфейса в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

   > Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Параметры программы** в блоке **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
4. В окне **Масштабируемость и интерфейс** на закладке **Общие** настройте следующие параметры:
   - В блоке **Параметры масштабируемости** настройте параметры, определяющие количество используемых Kaspersky Security 10.1 для Windows Server рабочих процессов:
     - **Определять параметры масштабируемости автоматически**.

       Kaspersky Security 10.1 для Windows Server регулирует количество используемых процессов автоматически.

       Это значение установлено по умолчанию.
     - **Указать количество рабочих процессов вручную**.

       Kaspersky Security 10.1 для Windows Server регулирует количество активных рабочих процессов в соответствии с указанными значениями.

       - **Максимальное количество активных процессов.**

         Максимальное количество процессов, которые использует Kaspersky Security 10.1 для Windows Server. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

       - **Число 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 Security 10.1 для Windows Server в области уведомлений панели задач: снимите или установите флажок **Показывать значок программы в панели задач**.

5. На закладке **Иерархическое хранилище** выберите один из следующих вариантов доступа к иерархическому хранилищу:

   - **Не HSM-система**

     Kaspersky Security 10.1 для Windows Server не использует параметры HSM-системы при выполнении задач проверки по требованию.

     Этот вариант выбран по умолчанию.

   - **HSM-система использует точки повторной обработки**

     Kaspersky Security 10.1 для Windows Server использует точки повторной обработки для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

   - **HSM-система использует расширенные атрибуты файла**

     Путь к папке, в которую восстанавливаются объекты в формате UNC (Universal Naming Convention).

     По умолчанию установлен путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\

   - **Неизвестная HSM-система**

     При выполнении задач проверки по требованию Kaspersky Security 10.1 для Windows Server проверяет все файлы как файлы, расположенные в удаленном хранилище.

     Не рекомендуется использовать этот вариант.

   Если вы не используете HSM-системы, оставьте значение параметра Параметры HSM-системы, установленное по умолчанию (Не HSM-система).

6. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 Security 10.1 для Windows Server в случае возникновения сбоев в работе программы или аварийного завершения работы программы.
     - **Выполнять восстановление задач**

       Флажок включает или выключает восстановление задач Kaspersky Security 10.1 для Windows Server после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок установлен, Kaspersky Security 10.1 для Windows Server автоматически восстанавливает задачи Kaspersky Security 10.1 для Windows Server после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок снят, Kaspersky Security 10.1 для Windows Server не восстанавливает задачи Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server. 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не запускает задачи проверки по расписанию при переходе на источник бесперебойного питания до восстановления стандартного режима питания.

Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server останавливает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

    Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.

1. Нажмите на кнопку **ОК**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

Настроенные параметры соединения используются для подключения Kaspersky Security 10.1 для Windows Server 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Настройка параметров соединения**.
4. В окне **Параметры соединения** настройте следующие параметры:
   - В блоке **Параметры прокси-сервера** задайте параметры использования прокси-сервера:
     - **Не использовать прокси-сервер**.

       Если выбран этот вариант, Kaspersky Security 10.1 для Windows Server не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
     - **Автоматически определять параметры прокси-сервера**.

       Если выбран этот вариант, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.

       Если флажок установлен, обращение к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Security 10.1 для Windows Server, выполняется напрямую. Прокси-сервер не используется.

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

По умолчанию флажок установлен.

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

5. Нажмите на кнопку **ОК**.

Настроенные параметры соединения будут сохранены.

О настройке дополнительных возможностей программы

Вы можете настроить дополнительные возможности Kaspersky Security 10.1 для Windows Server из Kaspersky Security Center для группы компьютеров или для одного компьютера.

В этом разделе

Настройка параметров доверенной зоны в Kaspersky Security Center

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

► *Чтобы настроить параметры доверенной зоны, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Доверенная зона**.
4. На закладке **Исключения** укажите объекты, которые Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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**

  Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server пропускает при проверке указанные обнаруживаемые объекты.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

- **Область применения исключения.**

  Название задачи Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server будет пропускать при проверке:

   - **Не проверять файловые операции резервного копирования**

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

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server пропускает при проверке операции чтения файлов, выполняемые установленными на сервере средствами резервного копирования.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server проверяет операции чтения файлов, выполняемые установленными на сервере 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 Security 10.1 для Windows Server пропускает при проверке файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server проверяет файловые операции доверенных процессов.

     По умолчанию флажок снят.

6. Если требуется, добавьте процессы, файловую активность которых вы не хотите проверять, нажав кнопку **Добавить** (см.раздел "Добавление доверенных процессов" на стр. 159).

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

Добавление доверенных процессов

► *Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Доверенная зона**.
4. На закладке **Доверенные процессы** установите флажок **Не проверять файловую активность указанных процессов**.
5. Нажмите на кнопку **Добавить**.
6. Выберите один из вариантов из контекстного меню кнопки:
   - **Несколько процессов.**

     В открывшемся окне **Добавление процессов в список доверенных** настройте следующее:

     a. **Использовать полный путь для определения доверенности процесса**.

        Если флажок установлен, Kaspersky Security 10.1 для Windows Server будет использовать полный путь к файлу для определения статуса доверенности процесса.

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

        По умолчанию флажок установлен.

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

Если флажок установлен, Kaspersky Security 10.1 для Windows Server 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.

c. Чтобы добавить данные на основе исполняемых файлов, нажмите на кнопку **Обзор**.

d. Выберите исполняемый файл в открывшемся окне.

Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

g. Нажмите на кнопку **ОК**.

Требуется, чтобы учетная запись, с правами которой запускается задача постоянной защиты файлов, имела права администратора на сервере с установленным Kaspersky Security 10.1 для Windows Server, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, PID или пути к исполняемому файлу процесса на локальном сервере. Обратите внимание, что вы можете выбрать процесс из списка запущенных процессов, нажав на кнопку **Процессы** только при работе через Консоль Kaspersky Security 10.1 на локальном сервере или в настройках локального компьютера в Kaspersky Security Center.

- **Процесс на основе имени и пути.**

В открывшемся окне **Добавление процессов в список доверенных** настройте следующее:

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

b. Нажмите на кнопку **ОК**.

- **Процесс на основе свойств объекта.**

В открывшемся окне **Добавление процессов в список доверенных** настройте следующее:

a. Нажмите на кнопку **Обзор** и выберите процесс.

b. **Использовать полный путь для определения доверенности процесса**.

Если флажок установлен, Kaspersky Security 10.1 для Windows Server будет использовать полный путь к файлу для определения статуса доверенности процесса.

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

По умолчанию флажок установлен.

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

Если флажок установлен, Kaspersky Security 10.1 для Windows Server 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.

d. Нажмите на кнопку **ОК**.

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

7. В окне **Добавление доверенного процесса** нажмите на кнопку **ОК**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать во время проверки легальное программное обеспечение и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.
- Проверка скриптов.
- Защита RPC-подключаемых сетевых хранилищ.
- Защита трафика.

Если маска не добавлена в список исключений, Kaspersky Security 10.1 для Windows Server применит действия указанные в настройках задачи для программ и ресурсов, которые входят в эту категорию.

► *Использование маски not-a-virus*

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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.

   Откроется окно **Доверенная зона**.

4. На закладке **Исключения**, прокрутите список и выберите строку со значением **not-a-virus:***, если флажок снят.

5. Нажмите на кнопку **ОК**.

Новые настройки будут применены.

Проверка съемных дисков

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

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server без антивирусных баз, проверка съёмных дисков будет недоступна.

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 29. 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 серверу.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 MB	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске. Kaspersky Security 10.1 для Windows Server не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • Максимальная защита • Рекомендуемый • Максимальное быстродействие Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют предустановленным уровням безопасности в задачах проверки по требованию.

Чтобы настроить параметры проверки съёмных дисков при подключении, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Дополнительные параметры** нажмите на кнопку **Настройка** в блоке **Проверка съемных дисков**.

   Откроется окно **Проверка съёмных дисков**.

4. В блоке **Параметры проверки при подключении** выполните следующие действия:

   - Установите флажок **Проверять съёмные диски при их подключении по USB**, если вы хотите, чтобы Kaspersky Security 10.1 для Windows Server 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.

5. Нажмите на кнопку **ОК**.

   Настроенные параметры будут сохранены и применены.

Настройка прав доступа в Kaspersky Security Center

Вы можете настроить права доступа к управлению программой и к управлению службой Kaspersky Security Service в Kaspersky Security Center для группы компьютеров и для одного компьютера.

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 Security 10.1 для Windows Server 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 (см. раздел "О правах доступа к функциям Kaspersky Security 10.1 для Windows Server" на стр. 99).

Настроенные параметры будут сохранены.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

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

   - Если вы хотите задать **папку-местоположение резервного хранилища**, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого сервера 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 сервера 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 сервера.
   - 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 сервера.

6. Нажмите на кнопку **ОК**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать недоверенные компьютеры и настроить параметры хранилища заблокированных компьютеров.

В этом разделе

О блокировании доступа к сетевым файловым ресурсам

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита, Защита от шифрования для NetApp, Защита от шифрования. Задачи отслеживают попытки удаленных компьютеров получить доступ к общим сетевым папкам защищаемого сервера или сетевого хранилища в соответствии со списком недоверенных узлов. Информация обо всех заблокированных компьютерах всех защищаемых серверов отправляется в Kaspersky Security Center. Kaspersky Security 10.1 для Windows Server блокирует доступ к общим сетевым папкам сервера или общим папкам сетевого хранилища для всех удаленных компьютеров в списке недоверенных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Если в ходе выполнения задачи Постоянная защита файлов со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена вредоносная активность и в параметрах задачи Постоянная защита файлов установлен флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных.**
- Если в ходе выполнения задачи Защита от шифрования со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена активность вредоносного шифрования.
- Если при активированной задаче Защита от шифрования для NetApp обнаружена атака с целью вымогательства на сетевое хранилище.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает критическое событие блокировки узла. Любая попытка такого компьютера получить доступ к защищаемым общим сетевым папкам будет заблокирована.

По умолчанию Kaspersky Security 10.1 для Windows Server удаляет недоверенные компьютеры из списка через 30 минут после добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка недоверенных. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

Включение блокирования доступа к сетевым файловым ресурсам

Чтобы добавить компьютеры, проявляющие вредоносную активность или попытки шифрования, в **хранилище заблокированных узлов** и заблокировать этим компьютерам доступ к сетевым файловым ресурсам, минимум одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от шифрования
- Защита от шифрования для NetApp

► *Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** → **Постоянная защита** → **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита сервера**.
3. В блоке **Интеграция с другими компонентами** установите флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных** если вы хотите, чтобы Kaspersky Security 10.1 для Windows Server блокировал доступ к сетевым файловым ресурсам для компьютеров, со стороны которых в ходе работы задачи Постоянная защита файлов обнаружена вредоносная активность.
4. Если задача не запустилась, откройте закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту **При запуске программы**.
5. В окне **Постоянная защита сервера** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** > **Контроль активности в сети** > **Настройка** в блоке **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.
3. Если задача не запустилась, откройте закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту **При запуске программы**.
4. В окне **Защита от шифрования** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу Защита от шифрования для NetApp, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** > **Защита сетевых хранилищ** > **Настройка** в блоке **Защита от шифрования для NetApp**.

   Откроется окно **Защита от шифрования для NetApp**.
3. Если задача не запустилась, откройте закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту **При запуске программы**.
4. В окне **Защита от шифрования для NetApp** нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server блокирует доступ к сетевым файловым ресурсам для компьютера, проявляющего вредоносную активность или попытки шифрования.

Настройка параметров хранилища заблокированных узлов

► *Чтобы настроить хранилище заблокированных компьютеров, 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. 124).
2. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке **Хранилища**.

   Откроется окно **Параметры хранилищ**.

   Вы можете настроить параметры блокирования компьютеров для группы управляемых серверов через параметры политики. Чтобы настроить период блокирования узлов, откройте **<Имя политики>** > **Дополнительные возможности** и нажмите кнопку **Настройка**. На закладке **Заблокированные узлы** настройте параметры блокирования компьютеров. Список заблокированных узлов недоступен в параметрах политики.
3. Откройте закладку **Заблокированные узлы**.
4. В блоке **Действия** укажите количество суток, часов и минут, через которые, с момента блокировки, заблокированные компьютеры получают доступ к сетевым файловым ресурсам.
5. Нажмите на кнопку **Список заблокированных узлов**.
6. Выполните одно из следующих действий:
   - В открывшемся окне **Список заблокированных узлов** выберите компьютеры, доступ которых вы хотите восстановить, и нажмите на кнопку **Удалить из списка**.
   - Нажмите на кнопку **Очистить весь список**, чтобы удалить компьютеры из списка недоверенных и восстановить доступ для всех заблокированных узлов.

7. Нажмите на кнопку **Закрыть**.

   Выбранные компьютеры будут разблокированы и удалены из списка заблокированных.

8. Нажмите на кнопку **ОК** в окне **Параметры хранилищ**.

Настроенные параметры заблокированных узлов 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 Security 10.1 для Windows Server и состоянием антивирусной защиты защищаемого сервера:

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

Вы можете настроить уведомления о событиях Kaspersky Security 10.1 для Windows Server как для одного сервера в окне **Свойства: <Имя сервера>**, так и для группы серверов 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 *Руководстве администратора Kaspersky Security Center*.
- В окне **Параметры уведомлений** вы можете настраивать уведомления как администратора, так и пользователей.

  Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

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

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

В этом разделе

Настройка параметров журналов

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *Чтобы настроить параметры журналов Kaspersky Security 10.1 для Windows Server, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

4. В окне **Параметры журналов** настройте следующие параметры Kaspersky Security 10.1 для Windows Server согласно вашим требованиям:
   - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
     a. В списке **Компонент** выберите функциональный компонент Kaspersky Security 10.1 для Windows Server, уровень детализации событий которого вы хотите указать.
     b. Чтобы задать уровень детализации в журналах выполнения задач и журнале системного аудита выбранного функционального компонента, выберите нужный уровень в списке **Уровень важности**.
   - Чтобы изменить местоположение журналов по умолчанию, укажите полный путь к папке или выберите папку с помощью кнопки **Обзор**.
   - Укажите, сколько дней будут храниться журналы выполнения задач.
   - Укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита**.
5. Нажмите на кнопку **ОК**.

Настроенные параметры журналов будут сохранены.

Журнал событий безопасности

Kaspersky Security 10.1 для Windows Server ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом сервере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить Журнал событий безопасности, так же, как и Журнал системного аудита. При этом Kaspersky Security 10.1 для Windows Server фиксирует событие системного аудита об очистке Журнала событий безопасности.

Настройка параметров интеграции с SIEM

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

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

Вы можете использовать интеграцию с SIEM в двух режимах:

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

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

- 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 Security 10.1 для Windows Server 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 30. Параметры интеграции с SIEM

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

Параметр	Значение по умолчанию	Описание
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

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

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

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

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

   По умолчанию флажок снят.

6. 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 следующие параметры подключения к зеркальному syslog-серверу: **IP-адрес** и **Порт**.

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

       Вы можете указать IP-адрес только в формате IPv4.

9. Нажмите на кнопку **ОК**.

Настроенные параметры интеграции с SIEM будут применены.

Настройка параметров уведомлений

► *Чтобы настроить параметры уведомления Kaspersky Security 10.1 для Windows Server, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server регистрирует события *Базы программы устарели, Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*.

     - **Базы устарели (сут).**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 7 дней.

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

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 14 дней.

     - **Проверка важных областей 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 Security 10.1 для Windows Server 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 Security 10.1 для Windows Server будет передавать на Сервер администрирования Kaspersky Security Center:
   - Данные об объектах карантина.
   - Данные об объектах резервного хранилища.
   - Данные о заблокированных узлах.
5. Нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server будет передавать информацию о выбранных типах объектов на Сервер администрирования.

Постоянная защита сервера

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

В этом разделе

Постоянная защита файлов

Этот раздел содержит информацию о задаче Постоянная защита файлов и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Security 10.1 для Windows Server проверяет следующие объекты защищаемого сервера при доступе к ним:

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

При записи или считывании записанного файла с сервера любой программой, Kaspersky Security 10.1 для Windows Server перехватывает этот файл, проверяет его на наличие угроз компьютерной безопасности и, при обнаружении угрозы, выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Kaspersky Security 10.1 для Windows Server возвращает файл программе, если он не заражен или успешно вылечен.

Kaspersky Security 10.1 для Windows Server перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016.

Контейнер– это изолированная среда, где программа может работать, не оказывая воздействия на операционную систему и не подвергаясь при этом воздействию с ее стороны. Если контейнер расположен в области защиты задачи, Kaspersky Security 10.1 для Windows Server проверяет файлы контейнера, к которому получают доступ пользователи, на наличие компьютерных угроз. При обнаружении угрозы, программа пытается вылечить контейнер. Если лечение успешно, контейнер продолжает работу. Если лечение невозможно, контейнер выключается.

Kaspersky Security 10.1 для Windows Server также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих настройках.

Настройка задачи Постоянная защита файлов

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

Таблица 31. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь компьютер, исключая виртуальные диски.	Вы можете ограничить область защиты.
Уровень безопасности	Единый для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для выбранных узлов в дереве файловых ресурсов компьютера вы можете: • применить другой предустановленный уровень безопасности; • вручную изменить уровень безопасности; • сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Режим защиты объектов	При открытии и изменении	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Security 10.1 для Windows Server проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Применять доверенную зону.	Применяется.	Единый список исключений, который вы можете применять в выбранных задачах.

Параметр	Значение по умолчанию	Описание
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 настроить параметры запуска задачи по расписанию.
Блокировать компьютеры, с которых ведется вредоносная активность	Не применяется	Вы можете включить добавление компьютеров, со стороны которых выявлена вредоносная активность, в список недоверенных узлов.

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Постоянная защита файлов**.
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим защиты объектов (см. раздел "Выбор режима защиты объектов" на стр. 182);
     - Применение эвристического анализатора (на стр. 181).
     - Параметры интеграции с другими компонентами Kaspersky Security 10.1 для Windows Server.
   - На закладке **Управление задачей**:
     - Запуск задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 146).

5. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Область защиты в задаче Постоянная защита файлов" на стр. 183).
     - 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 (см. раздел "Выбор предустановленных уровней безопасности" на стр. 184) или настройте параметры защиты объектов вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 187).

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

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

Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Применение эвристического анализатора;

Вы можете использовать эвристический аналихатор и выбрать уровень анализа для задач Kaspersky Security 10.1 для Windows Server.

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

1. Откройте параметры программы (см. раздел "О способах управления Kaspersky Security 10.1 для Windows Server из Kaspersky Security Center" на стр. 149) или настройки политики (см. раздел "Настройка политики" на стр. 111), для которой вы хотите настроить использование эвристического анализатора.
2. Снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами «Лаборатории Касперского».

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. Блок **Режим защиты объектов** позволяет определить, при каком типе доступа к объектам Kaspersky Security 10.1 для Windows Server их проверяет.

Параметр **Режим защиты объектов** имеет единое значение для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► *Чтобы выбрать режим защиты объектов, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Постоянная защита файлов** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

4. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:

   - **Интеллектуальный режим**

     Kaspersky Security 10.1 для Windows Server выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Kaspersky Security 10.1 для Windows Server повторно проверяет объект только после его последнего сохранения этим процессом.

   - **При открытии и изменении**

     Kaspersky Security 10.1 для Windows Server проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

     Этот вариант выбран по умолчанию.

   - **При открытии**

     Kaspersky Security 10.1 для Windows Server проверяет все объекты при их открытии как на чтение, так и на исполнение или изменение.

   - **При выполнении.**

     Kaspersky Security 10.1 для Windows Server проверяет файл только при открытии на выполнение.

5. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

Область защиты в задаче Постоянная защита файлов

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

В этом разделе

Предопределенные области защиты

Файловые ресурсы защищаемого сервера 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 Security 10.1 для Windows Server предусмотрены следующие предопределенные области защиты:

- **Локальные жесткие диски**. Kaspersky Security 10.1 для Windows Server защищает файлы на жестких дисках сервера.
- **Съемные диски**. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на сервере. Kaspersky Security 10.1 для Windows Server 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 сервер 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.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов сервера в Консоли Kaspersky Security 10.1. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на сервере, с которой этот псевдодиск связан.
Подключенные сетевые диски также не отображаются в дереве файловых ресурсов сервера. 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 сервера вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из этих уровней имеет свой набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Security 10.1 для Windows Server на серверах и рабочих станциях, принимаются дополнительные меры серверной безопасности, например, сетевые экраны и политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияние на производительность защищаемых серверов. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты серверов 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 32. Предустановленные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродей-ствие	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 не-возможно	Лечить, удалять, если лечение не-возможно	Лечить, удалять, если лечение не-возможно
Действие над возможно зараженными объектами	Помещать на карантин	Помещать на карантин	Помещать на карантин
Исключать объекты	нет	нет	нет
Не обнаруживать	нет	нет	нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять объекты размером бо-лее (МБ)	8 MB	8 MB	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	• Упакованные объекты* • Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* • Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* *Все объекты

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** 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 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

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

   Откроется окно **Настройка параметров постоянной защиты файлов**.
5. Выберите требуемый уровень безопасности в раскрывающемся списке:
   - **Максимальная защита**
   - **Рекомендуемый**
   - **Максимальное быстродействие**
6. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. этих параметров соответствуют значениям предустановленного уровня безопасности Рекомендуемый (см. раздел "Выбор предустановленных уровней безопасности" на стр. 184).

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 сервера.

При работе с деревом файловых ресурсов сервера параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Постоянная защита файлов**.
4. На закладке **Область защиты**, выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.
5. 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 Security 10.1 для Windows Server проверяет все объекты.
     - **Объекты, проверяемые по формату.**

       Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании формата файла.

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

  Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

  Kaspersky Security 10.1 для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

- **Проверять загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и главных загрузочных записей.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет загрузочные секторы и загрузочные надписи на жестких и съемных дисках сервера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server новыми или измененными с момента последней проверки.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет архивы.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые SFX-архивы.**

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет SFX-архивы.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять неизлечимый составной объект при обнаружении вложенного зараженного или другого объекта**.

    Флажок включает или выключает форсированное удаление составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта.

    Если флажок установлен и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Блокировать доступ и удалять**, Kaspersky Security 10.1 для Windows Server принудительно выполняет удаление всего составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

    Если флажок снят, и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Блокировать доступ и удалять**, Kaspersky Security 10.1 для Windows Server не выполняет указанное действие для родительского составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта в случае, если составной объект неизменяем.

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

- 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 Security 10.1 для Windows Server пропускает при проверке указанные объекты.

    Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server пропускает при проверке указанные обнаруживаемые объекты.

Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 объекты размером более (МБ)**

  Исключение из проверки объектов больше указанного размера.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server проверяет составные объекты, не учитывая размер.

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

- **Использовать технологию iChecker.**

  Проверка только новых или измененных с момента последней проверки файлов.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **ОК**.

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

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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server получает от Kaspersky Security Network только информацию о репутации программ и веб-адресов.

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 подробную информацию о передаче, обработке, хранении и уничтожении информации об использовании программы вы можете получить прочитав Положение 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 Security 10.1 для Windows Server. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network может использоваться в следующих задачах Kaspersky Security 10.1 для Windows Server:

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

- Защита трафика.
- Защита RPC-подключаемых сетевых хранилищ.
- Защита ICAP-подключаемых сетевых хранилищ.

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. 196) 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

Запуск задачи Использование KSN невозможен, если не принято Положение о KSN.

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

Таблица 33. Параметры по умолчанию задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	**Удалить**	Вы можете указывать действия, которые Kaspersky Security 10.1 для Windows Server будет выполнять над объектами, которые имеют 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 Security 10.1 для Windows Server рассчитывает хеш MD5 для файлов любого размера.

Параметр	Значение по умолчанию	Описание
Я принимаю Положение о KSN	Не принято	Решите, хотите ли вы использовать KSN после установки. Вы можете изменять свое решение в любой момент.
Отправлять статистику KSN	Не принято	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимите флажок.
Принять условия Положения о KMP	Не принято	Вы можете включать и выключать применение сервиса KMP. Сервис доступен, только если во время приобретения программы был подписан дополнительный договор.
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:

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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** нажмите на кнопку **Настройка** в блоке **Использование KSN**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Security 10.1 для Windows Server необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалить**

       Kaspersky Security 10.1 для Windows Server удаляет зараженный по данным KSN объект и помещает его копию в резервное хранилище.

       Этот вариант выбран по умолчанию.

- **Фиксировать информацию в отчете**

  Kaspersky Security 10.1 для Windows Server фиксирует в журнале выполнения задач информацию об обнаруженном зараженном по данным KSN объекте. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (МБ).

    Если флажок снят, Kaspersky Security 10.1 для Windows Server рассчитывает контрольную сумму для файлов любого размера.

    По умолчанию флажок установлен.

  a. Если требуется, в поле справа укажите максимальный размер файлов, для которых Kaspersky Security 10.1 для Windows Server будет рассчитывать контрольную сумму.

  b. Снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

     Флажок позволяет управлять передачей данных от защищаемых серверов в KSN.

     Если флажок снят, данные с сервера администрирования и защищаемых серверов не отправляются в KSN. Тем не менее, в зависимости от параметров сервер может отправлять данные в KSN напрямую (не через Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую.

     Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center.

     По умолчанию флажок установлен.

  Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Руководстве администратора Kaspersky Security Center* .

5. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**. Например, вы можете включить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если хотите, чтобы задача автоматически запускалась после перезагрузки сервера.

   Программа будет запускать задачу Использование KSN по расписанию.

6. Настройте обработку данных (см. раздел "Настройка обработки данных" на стр. 196) перед запуском задачи.
7. 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 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** нажмите на кнопку **Обработка данных** в блоке **Использование KSN**.

   Откроется окно **Обработка данных**.
4. На закладке **Службы** прочитайте Положение и установите флажок **Принять условия Положения о Kaspersky Security Network**.
5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:
   - **Отправлять данные о проверенных файлах**.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server отправляет контрольную сумму проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server не отправляет контрольную сумму файлов в KSN.

     По умолчанию флажок установлен.

- **Отправлять данные о запрашиваемых веб-адресах**.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server отправляет данные о запрашиваемых веб-ресурсах, включая веб-адреса, в "Лабораторию Касперского". Заключение о безопасности запрашиваемых веб-ресурсов основано на репутации, полученной от KSN.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server не проверяет репутацию веб-адресов в KSN.

  По умолчанию флажок установлен.

  Флажок влияет на настройку задачи Защита трафика.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

6. Откройте закладку **Статистики**. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы Kaspersky Security 10.1 для Windows Server отправлял дополнительную статистику в Лабораторию Касперского.

   Если флажок установлен, Kaspersky Security 10.1 для Windows Server отправляет статистику, включая персональные данные, обозначенные в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

   Если флажок снят, Kaspersky Security 10.1 для Windows Server не отправляет дополнительную статистику.

   По умолчанию флажок установлен.

7. На закладке **Kaspersky Managed Protection** прочитайте Положение о KMP и установите флажок **Я принимаю условия Положения о Kaspersky Managed Protection**.

   Если флажок установлен, программа может отправлять данные мониторинга активности на защищаемом сервере специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения инцидентов нарушения информационной безопасности.

   По умолчанию флажок снят.

Изменения параметра Я принимаю условия Положения о Kaspersky Managed Protection недостаточно, чтобы начать или остановить отправку данных. Для применения параметров перезапустите Kaspersky Security 10.1 для Windows Server.

Для использования сервиса Kaspersky Managed Protection требуется заключить договор на оказание услуг и запустить конфигурационные файлы на защищаемом сервере.

Для использования сервиса Kaspersky Managed Protection требуется согласие на обработку данных в рамках Положений о KSN на закладках Службы и Статистика.

8. Нажмите на кнопку **ОК**.

Конфигурация обработки данных будет сохранена.

Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

В этом разделе

О Защите от эксплойтов

Kaspersky Security 10.1 для Windows Server предоставляет возможность защиты памяти процессов от эксплуатации уязвимостей. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее также "Агент") в защищаемый процесс.

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Security 10.1 для Windows Server, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, необходимо завершить данный процесс. Может потребоваться перезагрузка сервера (например, если защищается системный процесс).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Security 10.1 для Windows Server выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;
- удалить процесс из списка защищаемых и перезапустить его.

Служба Kaspersky Security Broker Host

Для максимальной эффективности компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Broker Host на защищаемом сервере. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемый сервер создается и запускается процесс kavfswh. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

После остановки службы Kaspersky Security Broker Host Kaspersky Security 10.1 для Windows Server 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 компонента Защита 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).

- Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

  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 сервера** нажмите на кнопку **Настройка** в блоке **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

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

   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server не защищает процессы на сервере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Security 10.1 для Windows Server завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

   - **Только сообщать о компрометации процесса**.

     Если выбран данный режим, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать о компрометации процесса**.

5. В блоке **Действия по снижению рисков** настройте следующие параметры:

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

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server выводит на экран терминальное окно с описанием причины срабатывания защиты и указанием на процесс, где была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server 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.

- **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server будет снижать риски эксплуатации уязвимостей уже запущенных процессов не зависимо от статуса выполнения службы Kaspersky Security. Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

  По умолчанию флажок установлен.

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server не защищает процессы на сервере от эксплуатации уязвимостей.

  По умолчанию флажок снят.

6. Нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server сохранит и применит настроенные параметры защиты памяти процессов.

Добавление защищаемого процесса

Компонент Защита от эксплойтов защищает несколько процессов по умолчанию. Вы можете исключить какой-либо процесс из защиты, сняв флажок в соответствующей строке процесса.

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

   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 сервера** нажмите на кнопку **Настройка** в блоке **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

4. На закладке **Защищаемые процессы**, нажмите на кнопку **Обзор.**.

   Откроется стандартное окно Microsoft Windows **Открыть**.

5. 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 защиты от эксплойтов**.

9. Выберите один из вариантов применения техник снижения рисков:

   - **Применять все доступные техники защиты от эксплойта**.

     Если выбран этот вариант, редактирование списка недоступно, все техники применяются по умолчанию.

   - **Применять указанные техники защиты от эксплойта**.

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска:

     a. Установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

     b. Установите или снимите флажок **Применять технику 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**.

Процесс добавляется в область защиты задачи.

Техники снижения рисков

Таблица 34. 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 Exeption Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Export Adress 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.

Проверка скриптов

Этот раздел содержит информацию о задаче Проверка скриптов и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Проверка скриптов

В ходе выполнения задачи Проверка скриптов Kaspersky Security 10.1 для Windows Server контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), например, скриптов VBScript или JScript®. Kaspersky Security 10.1 для Windows Server разрешает выполнение скрипта, только если он признал этот скрипт безопасным. Kaspersky Security 10.1 для Windows Server запрещает выполнение скрипта, который он признал опасным. Если Kaspersky Security 10.1 для Windows Server признал скрипт предположительно опасным, он выполняет выбранное вами действие: запрещает или разрешает выполнение этого скрипта.

По умолчанию задача Проверка скриптов автоматически запускается при старте Kaspersky Security 10.1 для Windows Server.

По умолчанию компонент Проверка скриптов не устанавливается на сервер в составе программы.

Использование данного компонента может быть несовместима с работой некоторых сторонних программ на защищаемом сервере. В этом случае выполнение задачи проверки сторонних скриптов может приводить к ошибкам в работе данных скриптов. Рекомендуется либо отказаться от использования сторонней программы, либо остановить задачу Проверка скриптов. Если задача остановлена, риски связанные с контролем безопасности выполнения скриптов возрастают.

Если вы хотите использовать компонент Проверка скриптов, вам нужно выбрать его в списке устанавливаемых компонентов вручную во время инсталляции Kaspersky Security 10.1 для Windows Server.

Подробная информация о выборе компонентов программы при установке содержится в *разделе об установке Руководства администратора* Kaspersky Security 10.1 для Windows Server.

Вы можете настраивать параметры задачи Проверка скриптов.

Настройка параметров задачи Проверка скриптов

По умолчанию системная задача Проверка скриптов имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 35. Параметры задачи Проверка скриптов по умолчанию

Параметр	Значение по умолчанию	Описание
Выполнение опасных скриптов	Запрещено	Kaspersky Security 10.1 для Windows Server всегда запрещает выполнение скриптов, которые он признает опасными.
Выполнение предположительно опасных скриптов	Запрещено	Вы можете указывать действия, выполняемые при обнаружении предположительно опасных скриптов: запрещать или разрешать их выполнение.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Доверенная зона	Применяется	Единый список исключений, который вы можете применять в выбранных задачах.

► *Чтобы настроить задачу Проверка скриптов, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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**.

   Откроется окно **Свойства:** Откроется окно **Проверка скриптов**.
3. В блоке **Действия над предположительно опасными скриптами** выполните одно из следующих действий:
   - Если вы хотите разрешить выполнение предположительно опасных скриптов, выберите пункт **Разрешать выполнение**.

     Kaspersky Security 10.1 для Windows Server allows execution of a probably dangerous script.
   - Если вы хотите запретить выполнение предположительно опасных скриптов, выберите пункт **Блокировать выполнение**.

Kaspersky Security 10.1 для Windows Server запрещает выполнение возможно опасного скрипта.

Этот вариант выбран по умолчанию.

4. В блоке **Эвристический анализатор** выполните одно из следующих действий:

   - Снимите или установите флажок **Использовать эвристический анализатор**.

     Флажок включает или выключает использование эвристического анализатора при проверке объектов.

     Если флажок установлен, эвристический анализатор включен.

     Если флажок снят, эвристический анализатор выключен.

     По умолчанию флажок установлен.

   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

     Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни детализации проверки:

     - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
     - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами «Лаборатории Касперского».

       Этот уровень выбран по умолчанию.

     - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

5. В блоке **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.

   Флажок включает или выключает применение доверенной зоны в работе задачи.

   Если флажок установлен, Kaspersky Security для Windows Server 10.1 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

   Если флажок снят, Kaspersky Security для Windows Server 10.1 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

   По умолчанию флажок установлен.

6. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Защита трафика

Этот раздел содержит информацию о задаче Защита трафика и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Защита трафика

Компонент Защита трафика обрабатывает сетевой трафик, включая трафик, поступающий через почтовые серверы, перехватывает и проверяет объекты, передаваемые по веб-трафику, на наличие известных компьютерных и других угроз на защищаемом сервере. Служба ICAP проверяет входящий трафик на наличие угроз и блокирует или разрешает трафик в зависимости от результатов и настроенных параметров проверки.

Kaspersky Security 10.1 для Windows Server также обнаруживает и перехватывает скомпрометированный трафик, запрошенный с помощью процессов подсистемы Windows Subsystem for Linux. Для данных целей задача Защита трафика применяет действия, указанные в текущих настройках.

Компонент Защита трафика установлен по умолчанию. По завершении установки регистрируются и запускаются следующие службы:

- Служба Kaspersky Security Broker Host (KAVFSWH)
- Служба Kaspersky Traffic Security (KAVFSPROXY)

Компонент обеспечивает следующие типы защиты:

- Защита от почтовых угроз:
  - Антифишинг.
  - Защита от вредоносных программ, передающихся через почтовый трафик.
- Защита от угроз, передаваемых по сети:
  - Антифишинг.
  - Сигнатурный анализ.
  - Защита от вредоносных программ, передающихся через веб-трафик.

- Веб-контроль:
  - Контроль веб-адресов.
  - Контроль сертификатов.
  - Веб-контроль на основе категорий.

Настоятельно рекомендуется использовать службы KSN при запуске задачи Защита трафика для улучшения распознавания угроз. Облачные базы KSN содержат более актуальные данные о поступающих через трафик угрозах, чем локальные антивирусные базы. Анализ некоторых категорий веб-контроля проводится только по заключениям, полученным от служб KSN.

Режимы задачи Защита трафика

Защита трафика может работать в следующих режимах:

- **Драйверный перехват:** программа перехватывает трафик с помощью сетевого драйвера. Сетевой драйвер используется для перехвата и анализа входящего трафика, поступающего через указанные порты.
- **Перенаправление трафика:** Программа перенаправляет трафик путем настройки браузеров. Программа перенаправляет входящий трафик из браузеров в открытой терминальной сессии на внутренний прокси-сервер. В качестве внутреннего прокси-сервера указан Kaspersky Security 10.1 для Windows Server.
- **Внешний прокси-сервер:** программа обрабатывает трафик с внешнего прокси-сервера. Трафик передается с внешнего прокси-сервера в Kaspersky Security 10.1 для Windows Server. Программа анализирует трафик и рекомендует действие для внешнего прокси-сервера. Kaspersky Security 10.1 для Windows Server совместим только с решениями для прокси-сервера, которые передают трафик по протоколу ICAP.

О правилах веб-контроля

Kaspersky Security 10.1 для Windows Server позволяет добавлять и настраивать разрешающие или запрещающие правила для сертификатов и веб-адресов и использовать предустановленные правила для категорий, чтобы блокировать нежелательное содержимое. Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**.

Веб-контроль

Этот тип контроля реализуется путем применения разрешающих и запрещающих правил для веб-адресов и сертификатов. У разрешающих правил более высокий приоритет, чем у заключений KSN или сигнатурного анализа.

Веб-адрес или сертификат можно разрешить или заблокировать на основе заключения с приоритетом от высокого до низкого:

1. разрешающие и запрещающие правила;
2. антифишинговые и антивирусные базы;
3. KSN;
4. категории.

Веб-контроль на основе категорий.

Kaspersky Security 10.1 для Windows Server позволяет блокировать веб-адреса на основе категорий. Вы можете выбрать уровень эвристического анализа, используемого для категоризации. Контроль по веб-категориям использует для анализа предопределенный список категорий. Вы не можете изменять список, но можете выбрать категории ресурсов, которые будут разрешены или заблокированы, или выключить контроль категорий. Категория Прочие включает все веб-ресурсы, которые не попадают в другие категории из списка. Если этот флажок установлен, Kaspersky Security 10.1 для Windows Server разрешает все некатегоризированные веб-ресурсы. Если флажок снят, все веб-ресурсы блокируются.

> У категоризации самый низкий приоритет.

По умолчанию Kaspersky Security 10.1 для Windows Server применяет только одно правило – запрещающее правило для TOR-сертификатов. Вы можете отключить правило в параметрах правила, чтобы разрешить соединения TOR. Если правило применяется, все входящие и исходящие соединения TOR блокируются.

Защита трафика также учитывает заключения по маске `not-a-virus`, представляющие ресурсы или объекты, которые сами не являются вирусами, но могут быть использованы для нанесения вреда защищаемому серверу. По умолчанию Kaspersky Security 10.1 для Windows Server не применяет маску `not-a-virus` для категорий (см. раздел "Настройка контроля по веб-категориям" на стр. 227).

Защита от почтовых угроз

Задача Защита трафика проверяет электронную почту для версий Microsoft Outlook 2010, 2013 и 2016 (32-разрядных и 64-разрядных). Защита от почтовых угроз предоставляется через расширение Kaspersky Security 10.1 для Microsoft Outlook и устанавливается отдельно от компонентов Kaspersky Security 10.1 для Windows Server.

> Вы можете установить расширение Kaspersky Security 10.1 для Microsoft Outlook только если на защищаемом сервере установлены Kaspersky Security 10.1 для Windows Server и почтовый клиент Microsoft Outlook.

► *Чтобы установить расширение, запустите пакет ksmail_x86(x64).msi из папки \email_plugin.*

Защита от почтовых угроз включает:

- Проверку входящей электронной почты.
- Антивирусную проверку электронной почты.
- Антивирусную проверку вложений (включая упакованные объекты).
- Антифишинговую проверку электронной почты.
- Антифишинговую проверку вложений (включая упакованные объекты).

При обнаружении угрозы Kaspersky Security 10.1 для Windows Server выполняет следующие действия:

- удаляет вложения;

- изменяет тело зараженного письма;
- регистрирует событие *Обнаружена почтовая угроза*.

Kaspersky Security 10.1 для Windows Server проверяет сообщения при открытии, а не при получении сообщения на сервер. Проверка выполняется только один раз, когда вы открываете сообщение впервые. Проверенные сообщения и вложения хранятся в кеше до перезапуска Microsoft Outlook. После перезапуска все сообщения снова проверяются при открытии.

► *Расширение загружается в Microsoft Outlook при запуске почтового клиента. Если вы устанавливаете расширение, когда Outlook находится в рабочем состоянии, выполните следующее:*

1. Откройте **Файл > Параметры > Надстройки**.
2. Убедитесь, что расширение Kaspersky Security 10.1 для Microsoft Outlook добавлено в список (в статусе Активный или Неактивный).
3. Перезапустите Microsoft Outlook.
4. Проверьте статус расширения Kaspersky Security 10.1 для Microsoft Outlook (статус изменится на *Активно*).

Настройка задачи Защита трафика

Вы можете изменять параметры задачи Защита трафика, заданные по умолчанию (см.таблицу ниже).

Таблица 36. Параметры задачи Защита трафика по умолчанию

Таблица 37.

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Внешний прокси-сервер**	ICAP служба обрабатывает трафик с внешнего прокси-сервера.
Номер сетевого порта	1345	Порт ICAP службы по умолчанию.
Идентификатор службы	webscan	Идентификатор службы ICAP для адреса установленного антивирусного сервера.
Использовать базу вредоносных веб-адресов для проверки ссылок	Применяется	Включает или выключает сигнатурный анализ для каждого веб-адреса.
Использовать антифишинговую базу для проверки веб-страниц	Применяется	Включает или отключает антифишинговую проверку веб-адресов на основе эвристического анализа.
Использовать KSN для защиты	Применяется	Вы можете использовать данные KSN о репутации программ для защиты при выполнении задачи.

Параметр	Значение по умолчанию	Описание
Использование доверенной зоны	Применяется	При необходимости вы можете применить доверенную зону.
Уровень безопасности	Рекомендуемый	Выберите и настройте уровень безопасности для антивирусной защиты.
Расписание запуска задачи	Следующий запуск не определен	Задача Защита трафика не запускается автоматически. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить задачу Защита трафика, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.
4. На закладке **Режим работы** выберите и настройте режим работы задачи (см. раздел "Выбор режима работы задачи" на стр. 212).
5. На закладке **Обработка веб-адресов** настройте антифишинговую и антивирусную проверку веб-адресов и веб-контента (см. раздел "Настройка обработки веб-адресов и веб-контента" на стр. 221).
6. На закладке **Антивирусная защита** настройте эвристический анализ и уровень безопасности (см. раздел "Настройка защиты от вредоносных программ, передающихся через веб-трафик" на стр. 217).
7. На закладке **Управление задачей** запустите задачу на базе расписания (см. раздел "Работа с расписанием задач" на стр. 146).
8. Нажмите на кнопку **ОК**.

Параметры задачи будут сохранены.

Выбор режима работы задачи

► *Чтобы настроить режим работы задачи, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.
4. На закладке **Общие** выберите один из доступных режимов в раскрывающемся списке **Режим работы**:
   - **Драйверный перехват** (см. раздел "**Настройка режима Драйверный перехват**" на стр. 213)
   - **Перенаправление трафика** (см. раздел "**Настройка режима Перенаправление трафика**" на стр. 215)
   - **Внешний прокси-сервер**
5. Укажите параметры соединения службы ICAP (требуется для всех трех режимов):
   - **Номер сетевого порта**

     Номер порта службы ICAP Kaspersky Security 10.1 для Windows Server.
   - **Идентификатор службы**

     Идентификатор, который является частью параметра RESPMOD URI протокола ICAP (см. документ RFC 3507). RESPMOD URI обозначает адрес антивирусного ICAP-сервера, установленный для сетевого хранилища.

     Например, если IP-адрес защищаемого сервера – 192.168.10.10, номер порта – 1345, а идентификатор ICAP службы – webscan, эти параметры соответствуют адресу RESPMOD URI – icap://192.168.10.10/webscan:1345.
6. Настройте выбранный режим работы задачи.

   Для режима **Внешний прокси-сервер** дополнительная настройка не требуется. Настройка выполняется на стороне внешнего прокси-сервера.

7. Нажмите на кнопку **ОК**.

Параметры будут сохранены.

Настройка режима Драйверный перехват

► *В окне **Защита трафика** выполните следующие действия:*

1. Выберите закладку **Общие**.
2. Выберите режим работы задачи **Драйверный перехват**.
3. В блоке **Параметры режима работы** настройте следующие параметры:
   - **Проверять безопасные соединения по протоколу HTTPS**.

     Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

     Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

     По умолчанию флажок установлен.

     Проверка доступна, только если открыт HTTPS-порт.

   - Выберите версию протокола шифрования, которую вы хотите использовать:
     - **TLS 1.0;**
     - **TLS 1.1;**
     - **TLS 1.2.**

       По умолчанию установлен флажок **TLS 1.0**, и его нельзя снять.

   - **Не доверять веб-серверам с недействительными сертификатами**.

     Этот флажок доступен, только если установлен флажок **Проверять безопасные соединения по протоколу HTTPS**.

     Если этот флажок установлен, веб-страница с недействительным сертификатом блокируется (закончился срок действия сертификата, возникает ошибка проверки подписи, сертификат отозван и т. д.).

   - **Порт безопасности**.

     Укажите номер порта, который используется для перенаправления трафика из браузера или сетевого драйвера на внутренний порт, созданный Kaspersky Security 10.1 для Windows Server для обнаружения угроз, передаваемых по сети. Не рекомендуется изменять порт, установленный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если вы используете режим **Перенаправление трафика**, уже используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.
4. Чтобы добавить порты в область перехвата или исключить из нее, нажмите на кнопку **Настроить область перехвата**.

   Откроется окно **Область перехвата**.

5. На закладке **Перехватывать по портам** выберите один из следующих вариантов:
   - **Перехватывать все;**
   - **Перехватывать по указанным портам**:
     a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.
     b. Нажмите на кнопку **Добавить**.

        Порт будет включен в область перехвата.

     По умолчанию Kaspersky Security 10.1 для Windows Server перехватывает трафик, передаваемый через следующие порты: 80, 8080, 3128, 443.

6. Чтобы указать порт, который вы хотите исключить из области перехвата, на закладке **Исключать по портам** выполните следующие действия:
   a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.
   b. Нажмите на кнопку **Добавить**.

      Порт будет исключен из области перехвата.

   По умолчанию Kaspersky Security 10.1 для Windows Server исключает порты, которые используются другими программами и могут вызывать проблемы при попытке просмотра содержимого, передаваемого по зашифрованному соединению: 3389, 1723, 13291.

7. Чтобы исключить IP-адрес из области перехвата, на закладке **Исключить IP-адрес** выполните следующие действия:
   a. Нажмите на кнопку **Задать список исключений**.

      Откроется окно **Исключение IP-адресов**.
   b. Введите IP-адреса, используя формат IPv4 или маску.
   c. Нажмите на кнопку **Добавить**.
   d. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
8. Чтобы исключить процесс или исполняемый файл, который требует обмена трафиком, на закладке **Исключение процессов**:
   a. Установите флажок **Применять исключения для процессов**.
   b. Чтобы исключить файл, выполните следующие действия:
      1. Нажмите кнопку **Исполняемые файлы**.

         Отобразится стандартное окно **Открыть**.
      2. Выберите исполняемый файл, который хотите исключить, и нажмите **Открыть**.
   c. Чтобы исключить процесс, выполняемый на локальном компьютере, выполните следующие действия:
      1. Нажмите на кнопку **Выполняемые процессы**.

         Откроется окно **Активные процессы**.

2. Выберите выполняемый процесс и нажмите на кнопку **ОК**.

> Вы не можете выбрать процессы в Kaspersky Security Center.

9. В окне **Защита трафика** нажмите на кнопку **ОК**.

Параметры режима работы задачи будут сохранены.

Настройка режима Перенаправление трафика

► *В окне **Защита трафика** выполните следующие действия:*

1. Выберите закладку **Общие**.
2. Выберите режим работы **Перенаправление трафика**.
3. В блоке **Параметры режима работы** настройте следующие параметры:
   - **Проверять безопасные соединения по протоколу HTTPS**.

     Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

     Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

     По умолчанию флажок установлен.

   > Проверка доступна, только если открыт HTTPS-порт.

   - Выберите версию протокола шифрования, которую вы хотите использовать:
     - **TLS 1.0;**
     - **TLS 1.1;**
     - **TLS 1.2.**

     > По умолчанию установлен флажок **TLS 1.0**, и его нельзя снять.

   - **Перенаправлять трафик на внешний прокси-сервер после проверки**.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server перенаправляет уже проверенный трафик на внешний прокси-сервер, например, на корпоративный прокси-сервер, используемый в сети организации.

     Если флажок снят, трафик направляется на внутренний прокси-сервер.

     - **Адрес прокси-сервера.**

       Адрес внутреннего терминального прокси-сервера для перенаправления трафика. Введите адрес в формате IPv4.

     - **Порт**.

       Номер порта для внутреннего прокси-сервера.

   - **Порт безопасности**.

Укажите номер порта, который используется для перенаправления трафика из браузера или сетевого драйвера на внутренний порт, созданный Kaspersky Security 10.1 для Windows Server для обнаружения угроз, передаваемых по сети. Не рекомендуется изменять порт, установленный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если вы используете режим **Перенаправление трафика**, уже используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.

Для режима **Перенаправление трафика** в операционной системе должно быть настроено перенаправление зашифрованного трафика через Kaspersky Security 10.1 для Windows Server.

4. Нажмите на кнопку **ОК**.

Параметры режима работы задачи будут сохранены.

Параметры предустановленных уровней безопасности

Можно применить один из трех предустановленных уровней безопасности для узла, выбранного в дереве файловых ресурсов сервера: Максимальное быстродействие, Рекомендуемый и Максимальная защита. Каждый из этих уровней имеет свой набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Security 10.1 для Windows Server на серверах и рабочих станциях, принимаются дополнительные меры серверной безопасности, например, сетевые экраны и политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияние на производительность защищаемых серверов. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты серверов 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 38. Предустановленные уровни безопасности и соответствующие им параметры безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Проверка объектов.	Согласно списку расширений в базе данных.	По формату	Все объекты.
Действия над зараженными и другими обнаруженными объектами.	Блокировать	Блокировать	Блокировать
Не обнаруживать	нет	нет	нет

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять объекты размером более (МБ)	20 MB;	20 MB	нет
Проверять составные объекты.	• Упакованные объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* *Все объекты

Настройка защиты от вредоносных программ, передающихся через веб-трафик

Данные настройки защиты также применяются к почтовому трафику. Действия над зараженными и другими объектами применяются только к вложениям.

► *Чтобы настроить эвристический анализ для обнаружения вирусов и других угроз компьютерной безопасности, передаваемых через веб-трафик, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.

4. На закладке **Антивирусная защита** выполните следующие действия:

   - Установите флажок **Использовать эвристический анализатор**.
   - Выберите нужный уровень эвристического анализа для антивирусной проверки.
   - Выберите уровень безопасности (см. раздел "Параметры предустановленных уровней безопасности" на стр. 216) из раскрывающегося списка:
     - **Рекомендуемый**
     - **Максимальная защита**
     - **Максимальное быстродействие**
     - **Пользовательский**

5. На закладке **Описание** ниже вы можете просмотреть параметры выбранного уровня безопасности.

6. На закладке **Общие** в блоке **Защита объектов** укажите объекты, которые вы хотите включить в область проверки:

   - **Все объекты.**

     Kaspersky Security 10.1 для Windows Server проверяет все объекты.

   - **Объекты, проверяемые по формату.**

     Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

     Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании расширения файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

     Kaspersky Security 10.1 для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

     a. Нажмите на кнопку **Изменить**, чтобы изменить список расширений.

     b. В открывшемся окне укажите расширение.

     c. Нажмите на кнопку **Добавить**.

     Нажмите на кнопку **По умолчанию**, чтобы добавить предустановленный список исключенных расширений.

7. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Архивы**

     Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет архивы.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **SFX-архивы***

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет SFX-архивы.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

     Параметр активен, если снят флажок **Архивы**.

   - **Упакованные объекты***

     Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server пропускает исполняемые файлы, упакованные программами-упаковщиками, при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **Вложенные OLE-объекты**

     Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет встроенные в файл объекты.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server пропускает встроенные в файл объекты при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

8. На закладке **Действия** выберите действие над зараженными и другими обнаруживаемыми объектами:

   - **Блокировать**

     Kaspersky Security 10.1 для Windows Server блокирует загрузку веб-страницы при обнаружении вредоносного содержимого. Вместо запрашиваемой веб-страницы отображается причина блокирования.

   - **Разрешить**

     Kaspersky Security 10.1 для Windows Server не блокирует запрашиваемую веб-страницу, но регистрирует событие Обнаружено вредоносное содержимое.

9. На закладке **Производительность** настройте следующие параметры:
   - В блоке **Исключения** установите или снимите флажок **Не обнаруживать**. Чтобы настроить список исключенных объектов, выполните следующие действия:

     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 Security 10.1 для Windows Server пропускает при проверке указанные обнаруживаемые объекты.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

     a. Нажмите на кнопку **Изменить**.

     b. В открывшемся окне укажите имя объекта или маску.

     c. Нажмите на кнопку **Добавить**.

   - В блоке **Дополнительные параметры** ограничьте интервал проверки и размер объекта:
     - **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 объекты размером более (МБ)**

       Исключение из проверки объектов больше указанного размера.

       Если флажок установлен, Kaspersky Security 10.1 для Windows Server пропускает при антивирусной проверке объекты, чей размер превышает установленное значение.

       Если флажок снят, Kaspersky Security 10.1 для Windows Server проверяет объекты, не учитывая размер.

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

10. Нажмите на кнопку **ОК** в окне **Параметры антивирусной защиты**.

Параметры уровня безопасности будут сохранены.

Настройка защиты от почтовых угроз

Для использования защиты от почтовых угроз требуется установить расширение Kaspersky Security 10.1 для Microsoft Outlook и правильно настроить защищаемый сервер (см. раздел "Защита от почтовых угроз" на стр. 209).

► *Чтобы включить защиту от почтовых угроз, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.
4. На закладке **Защита от почтовых угроз**, установите флажок **Защищать сервер от почтовых угроз**.

   Если этот флажок установлен, Kaspersky Security 10.1 для Windows Server выполняет антивирусную и антифишинговую проверки всех входящих сообщений через расширение Kaspersky Security 10.1 для Microsoft Outlook.

   Если флажок не установлен, электронная почта не проверяется.

   По умолчанию флажок установлен.
5. Нажмите на кнопку **ОК**.

Изменения будут сохранены.

Настройка обработки веб-адресов

► *Чтобы проверять веб-ресурсы на наличие фишинга и обнаруживать вредоносные веб-адреса согласно антивирусной базе данных и репутации веб-адреса в KSN, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).

- Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

  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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.

4. На закладке **Режим работы** выберите и настройте режим работы задачи (см. раздел "Выбор режима работы задачи" на стр. 212).

5. На закладке **Обработка веб-адресов** выполните следующие действия:

   - Снимите или установите флажок **Использовать базу вредоносных веб-адресов для проверки веб-ссылок**.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server выполняет сигнатурный анализ каждого веб-адреса.

     Если флажок снят, антивирусные базы не используются для проверки веб-адресов.

     По умолчанию флажок установлен.

   - Снимите или установите флажок **Использовать антифишинговую базу для проверки веб-страниц**.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server проверяет каждый веб-адрес с помощью антифишинговой базы. Антифишинговая проверка основана на эвристическом анализе.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server не обнаруживает фишинговые атаки.

     По умолчанию флажок установлен.

     Обратите внимание, что когда вы настраиваете антифишинговую проверку ссылок, антифишинг автоматически применяется и к электронным сообщениям.

   - Снимите или установите флажок **Использование доверенной зоны**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Security для Windows Server 10.1 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Security для Windows Server 10.1 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

     По умолчанию флажок установлен.

   - Снимите или установите флажок **Использовать KSN для защиты**.

     Этот флажок включает или выключает использование служб KSN.

     Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

     Если флажок снят, задача не использует службы KSN.

     По умолчанию флажок установлен.

Репутация веб-адресов в KSN доступна, только если выполнены одновременно следующие условия:
a. В параметрах задачи Защита трафика установлен флажок **Использовать KSN для защиты**.
b. Принято Положение о KSN.
c. Установлен флажок **Отправлять данные о запрашиваемых веб-адресах** (см.раздел **Настройка параметров задачи Использование KSN** на стр.193).
d. Задача Использование KSN запущена.

6. Нажмите на кнопку **ОК**.

Параметры обработки веб-адресов будут сохранены.

Добавление контроля веб-адресов

Вы можете добавить правило контроля веб-адресов, чтобы запретить или разрешить конкретный веб-адрес. У правил самый высокий приоритет по сравнению с любыми другими заключениями.

► *Чтобы создать новое правило контроля веб-адресов, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

   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 блоке **Защита трафика** нажмите на кнопку **Правила**.

   Откроется окно **Правила веб-контроля**.
4. На закладке **Веб-контроль** установите флажок **Применить правила для веб-контроля**, чтобы применить правила.

   Если флажок установлен, Kaspersky Security 10.1 для Windows Server блокирует HTTPS-сертификаты с помощью пользовательских запрещающих правил для сертификатов.

   Если флажок снят, правила не применяются.

   По умолчанию флажок снят.

   Этот флажок доступен, только если установлен флажок **Сканировать HTTPS**.

5. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
6. В контекстном меню кнопки **Добавить** выберите пункт **Контроль веб-адресов**.
7. В открывшемся окне **Контроль веб-адресов** выполните следующие действия:
   a. Введите имя правила.
   b. Выберите **Тип** правила: **Запрещающее** или **Разрешающее**.
   c. Установите флажок **Применять правило**.
   d. Укажите **Веб-адрес** в поле ниже.
   e. Нажмите на кнопку **ОК**.
8. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
9. Нажмите на кнопку **ОК** в окне **Правила веб-контроля**.

Новые правила будут применены.

Настройка веб-контроля

Настройте использование правил, управляйте параметрами проверки сертификатов и контролем по веб-категориям.

В этом разделе

Настройка проверки сертификатов

Kaspersky Security 10.1 для Windows Server позволяет проверять и блокировать веб-ресурсы с недействительными сертификатами или сертификатами с истекшим сроком действия. Чтобы настроить проверку сертификатов, выполните следующие действия:

a. Выберите режим работы **Драйверный перехват** или **Перенаправление трафика**.
b. Настройте задачу Защита трафика (см. раздел "Выбор и настройка режима работы" на стр. 225).
c. Примените правила веб-контроля.
d. Добавьте и примените Правила для сертификатов (см. раздел "Добавление правил для сертификатов" на стр. 226).

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security 10.1 для Windows Server создает только запрещающие правила для сертификатов.

Выбор и настройка режима работы

► *Чтобы выбрать и настроить режим работы с сертификатами, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.
4. На закладке **Общие** из раскрывающегося списка **Режим работы** выберите режим, поддерживающий проверку сертификатов:
   - **Драйверный перехват** (см. раздел "**Настройка режима Драйверный перехват**" на стр. 213);
   - **Перенаправление трафика** (см. раздел "Настройка режима Перенаправление трафика" на стр. 215).
5. В блоке **Параметры режима работы** настройте следующие параметры:
   - **Проверять безопасные соединения по протоколу HTTPS**.

     Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

     Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

     По умолчанию флажок установлен.

     Проверка доступна, только если открыт HTTPS-порт.

- Выберите версию протокола шифрования, которую вы хотите использовать:
  - **TLS 1.0;**
  - **TLS 1.1;**
  - **TLS 1.2.**

    По умолчанию установлен флажок **TLS 1.0**, и его нельзя снять.

6. Нажмите на кнопку **ОК**.

Параметры задачи будут сохранены.

Добавление правил для сертификатов

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security 10.1 для Windows Server создает только запрещающие правила для сертификатов.

► *Чтобы добавить или настроить правило сертификата, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 блоке **Защита трафика** нажмите на кнопку **Правила**.

   Откроется окно **Правила веб-контроля**.
4. На закладке **Правила Веб-контроля** установите флажок **Применять правила на основе сертификатов**.

   Если флажок установлен, Kaspersky Security 10.1 для Windows Server блокирует HTTPS-сертификаты с помощью пользовательских запрещающих правил для сертификатов.

   Если флажок снят, программа не проверяется сертификаты.

   По умолчанию флажок снят.

   Этот флажок доступен, только если установлен флажок **Сканировать HTTPS**.

5. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
6. В контекстном меню кнопки **Добавить** выберите пункт **Правило контроля сертификатов**.
7. В открывшемся окне **Контроль сертификатов** выполните следующие действия:
   a. Введите имя правила.
   b. Установите флажок **Применять правило**.
   c. Выберите **Тип оператора**: **Маска** или **Регулярное выражение**.
   d. Укажите маску или выражение в поле **Оператор**.
   e. Нажмите на кнопку **ОК**.
8. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
9. Нажмите на кнопку **ОК** в окне **Правила веб-контроля**.

Новые правила будут применены.

Настройка веб-контроля на основе категорий

► *Чтобы добавить или изменить правило защиты трафика на основе категорий, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 блоке **Защита трафика** нажмите на кнопку **Правила**.

   Откроется окно **Правила веб-контроля**.
4. Откройте закладку **Категоризация**.
5. Установите флажок **Применять правила для веб-контроля на основе категорий**.

   Если флажок установлен, Kaspersky Security 10.1 для Windows Server категоризирует и блокирует веб-ресурсы, попадающие в выбранные категории.

   Если флажок снят, Kaspersky Security 10.1 для Windows Server не выполняет категоризацию.

   По умолчанию флажок снят.

Параметры контроля по веб-категориям становятся доступны.

6. Установите или снимите следующие флажки:
   - **Разрешать загрузку веб-страницы, если не удалось присвоить категорию**.
   - **Разрешать загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда серверу**.
   - **Разрешать загрузку легальных рекламных веб-ресурсов**.
7. В списке доступных категорий (см. раздел "Список категорий" на стр. 229):
   - Установите соответствующий флажок, чтобы разрешить категорию.

     Значение в графе **Тип** изменится на **Разрешающее**.
   - Снимите соответствующий флажок, чтобы запретить категорию.

     Значение в графе **Тип** изменится на **Запрещающее**.

   Список категорий предопределен, и его нельзя изменить (вы не можете добавлять или удалять категории).
8. Нажмите на кнопку **ОК**.

Параметры правил будут сохранены.

Использование маски not-a-virus

► *Чтобы использовать маску `not-a-virus` для анализа категорий, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте параметры задачи Использование KSN (см. раздел "Настройка задачи Использование KSN" на стр. 193).
2. Установите флажок **Разрешить отправку данных о запрашиваемых веб-адресах**, если флажок не установлен.
3. Запустите задачу Использование KSN.
4. В окне параметров задачи Защита трафика (см. раздел "Настройка задачи Защита трафика" на стр. 210) установите флажок **Использовать KSN для защиты**.
5. В окне **Правила веб-контроля**, на закладке **Категоризация**, установите флажок **Применять правила категоризации веб-ресурсов**.
6. В списке категорий выберите категории, к которым вы хотите применить маску `not-a-virus`.

   Задача Защита трафика не будет обнаруживать объекты из выбранных категорий, которые соответствуют заданной маске.

Использование маски `not-a-virus` можно настроить в параметрах компонента **Доверенная зона** (см. Раздел "Использование маски not-a-virus» на стр. 161).

Список категорий

Веб ресурсы анализируются и категоризируются по тегам. Теги принадлежат различным категориям (см.таблицу ниже).

Таблица 39. Теги категорий веб ресурсов

Тег	Описание	Список категорий
18+ (adult)	В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы для взрослых (18+), например описания насилия, порнографию или нецензурную брань.	Аборт, Знакомства для взрослых, Анорексия, Недовольство, Дискриминация, Эротика, Незаконные препараты, Незаконное скачивание, ЛГБТ, Нижнее белье, Сайты знакомств, Нудизм, Политическое решение, Порно, Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Половое воспитание, Секс-шопы, Социальные сети, Суицид, Нецензурная брань, Жестокость, Оружие.
children	В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы для детей. Например: образовательные сайты, развлекательные сайты для детей, форумы и блоги о воспитании.	Дети, Запрещено Федеральным законом 436 (РФ), Школы и университеты.
drug	В эти категории могут попадать веб-ресурсы, потенциально содержащие информацию о наркотических и других веществах, распространяемых легально или нелегально. Например, данные о распространении запрещенных препаратов, алкоголе или веб-страницы зарегистрированных фармокологических компаний.	Аборт, Алкоголь, Анорексия, Наркотики, Красота и здоровье, Незаконные препараты, Медицина, Фармакология, Табак.
education	В эти категории могут попадать веб-ресурсы, потенциально содержащие учебные материалы или посвященные обучению. Например: онлайн-энциклопедии, базы знаний, вики, веб-сраницы учебных заведений или страницы о половом воспитании.	Книги, Образование, Дети, Информационные технологии, Онлайн-энциклопедии, Школы и университеты, Поисковые системы, Половое воспитание.

Тег	Описание	Список категорий
hobby&entertainment	В эти категории могут попадать веб-ресурсы, потенциально относящиеся к развлечениям, хобби и свободному времяпрепровождению. Например: онлайн-игры разных типов, включая азартные, социальные сети, страницы о книгах или охоте, блоги о здоровье и красоте или новостные ленты.	Знакомства для взрослых, Хобби и развлечения, Онлайн общение, Астрология и эзотерика, Аудио, видео и дистрибутивы, Ставки, Блоги, Казино, Казуальные игры, Чаты и форумы, Компьютерные игры, Культура, Эротика, Мода, Файлообменники, Охота и рыбалка, Дети, Азартные игры, Красота и здоровье, Хобби и развлечения, Дом и семья, Юмор, ЛГБТ, Нижнее бельё, Лотереи, Потоковое вещание, Медицина, Музыка, Новости, Сайты знакомств, Нудизм, Онлайн-магазины, Онлайн шоппинг (собственные системы оплаты), Животные, Порно, Рестораны, кафе, еда, Секс-шопы, Социальные сети, Спорт, Торренты, Путешествия, Радио и телевидение, Wargaming.
gaming	В эти категории могут попадать веб-ресурсы, потенциально имеющие отношение к разным типам игр. Например: азартные игры и ставки, лотереи, сетевые или казуальные игры, а также веб-сайты и форумы на игровую тематику.	Казуальные игры, Компьютерные игры, Спорт, Военные игры.
hazard	В эту категорию входят веб-страницы, которые содержат: • Азартные игры в формате «плати и играй». • Ставки. • Лотереи с необходимостью приобретения билетов.	Ставки, Казино, карточные игры, Азартные игры, Лотереи.
health&medicine	Веб-страницы о здоровом образе жизни. Могут содержать страницы о фитнесе, здоровом питании, альтернативных практиках и методах лечения; страницы о медицине, фармацевтике, фармацевтических компаниях, аптеках, лекарствах.	Аборт, Анорексия, Наркотики, Незаконные препараты, Красота и здоровье, Медицина, Фармакология, Спорт.
illegal	В эти категории могут попадать потенциально нелегальные веб-ресурсы. Например: нелегальное распространение медиа-файлов или дистрибутивов или страницы, запрещенные официальным законодательством разных стран.	Алкоголь, Аудио, видео и дистрибутивы, Наркотики, Файлообменники, Незаконные препараты, Незаконное скачивание, Азартные игры, Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Табак.

Тег	Описание	Список категорий
IT	Веб-ресурсы, которые позволяют пользователям (имеющим и не имеющим аккаунт) обмениваться сообщениями (в том числе, почтовые сервисы, социальные сети, блоги и т.д.)	Анонимизация, Доменные и хостинговые сервисы, Нелегальные программы, Инфотмационные технологии, Поисковые системы, Почтовые веб-сервисы.
forbidden by law	В эти категории могут попадать веб-ресурсы, потенциально находящиеся под контролем федерального законодательства или имеющие отношение к государтсвенной или политической тематике.	Закон и политика, Упомянуто в Федеральном списке экстремистских материалов (РФ), Запрещено Федеральным законом 436 (РФ), Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ).
legal	В эти категории могут попадать потенциально легальные веб-ресурсы.	Алкоголь, Аудио, видео и дистрибутивы, Наркотики, Файлообменники, Легальные рекламные ресурсы, Лотереи, Армия, Фармакология, Религия, Половое воспитание, Реклама, Табак, Wargaming.
media sharing	В эти категории могут попадать веб-ресурсы, потенциально позволяющие совершать файловый обмен. Например: торренты, файлообменники, музыкальные и видео хостинги, как легальные, так и нелегальные.	Аудио, видео и дистрибутивы, Книги, Файлообменники, Дети, Онлайн-сервисы, Потоковое вещание, Музыка, Поисковые системы, Торренты, Радио и телевидение.
money&paying	В эти категории могут попадать веб-ресурсы, потенциально связанные с финансами и финансовыми операциями. Например: официальные сайты банков, онлайн-банки, онлайн-магазины, а также страницы для совершения денежных переводов.	Банки, Книги, Казуальные игры, Электронная торговля, Онлайн шоппинг (собственные системы оплаты), Онлайн оплата, Платёжные системы, Рестораны, кафе, еда, Путешествия.
online collaboration	В эти категории могут попадать веб-ресурсы, потенциально связанные с общением в интернете. Например: тематические блоги и форумы, приватные чаты, социальные сети или знакомства для взрослых.	Знакомства для взрослых, Блоги, Чаты и форумы, Дети, Красота и здоровье, Поиск работы, Медицина, Сайты знакомств, Социальные сети, Путешествия.
psychotropic&drug	Эти категории могут включать веб-ресурсы связанные с любыми типами наркотических веществ, психотропных препаратов или табаком.	Наркотики, Незаконные препараты, Красота и здоровье, Медицина, Фармакология, Табак.

Тег	Описание	Список категорий
sex&adult	В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы сексуального и эротического характера. Например: порнографические хостинги, страницы о половом воспитании или сайты, посвященные секс-меньшинствам.	Знакомства для взрослых, Эротика, ЛГБТ, Нижнее бельё, Нудизм, Порно, Половое воспитание, Секс-шопы.
society&law	Эта категория включает множество аспектов жизни общества и человека, включая религию, правительственные организации, законодательство; дом и семью; новости; армию и оружие.	Культура и общество, Закон и политика, Армия, Религия, Оружие.
shopping	В эти категории могут попадать веб-ресурсы, потенциально относящиеся к онлайн шоппингу.	Книги, Нижнее бельё, Онлайн-магазины, Онлайн шоппинг (собственные системы оплаты), Онлайн оплата, Рестораны, кафе, еда, Секс-шопы, Путешествия.
violence	В эти категории могут попадать веб-ресурсы, потенциально содержащие прямое выражение агресси, описания жестокого обращения, пропаганду экстремизма или суицида.	Недовольство, Дискриминация, Экстремизм и расизм, Охота и рыбалка, Ненависть и дискриминация, Упомянуто в Федеральном списке экстремистских материалов (РФ), Армия, Политическое решение (JP), Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Суицид, Жестокость, Wargaming, Оружие.
web services	В эти категории могут попадать веб-ресурсы, потенциально предоставляющие различные веб-сервисы. Например: анонимизация, веб-хостинги или сервисы электронной почты.	Анонимизация, Доменные и хостинговые сервисы, Онлайн-сервисы, Поисковые системы, Реклама, Почтовые веб-сервисы.

Контроль активности на компьютерах

Этот раздел содержит информацию о функциональности Kaspersky Security 10.1 для Windows Server, которая позволяет контролировать запуски и программ подключения флеш-накопителей других внешних устройств по USB

В этом разделе

Управление запуском программ из Kaspersky Security Center

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

В этом разделе

Настройка параметров задачи Контроль запуска программ

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

Таблица 40. Параметры задачи Контроль запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только статистика**. Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Применять правила контроля запуска программ** для защиты сервера после того, как будет сформирован окончательный список правил.
Правила	**Заменить правилами политики локальные правила**.	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 для программ и пакетов из списка.	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию разрешено только распространение программ с помощью службы Windows Installer.
Разрешение распространения программ через Windows Installer	Применяется.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются через Windows Installer.
Запретить запуск командных интерпретаторов без команд к исполнению	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.
Расписание запуска задачи	Следующий запуск не определен.	Задача Контроль запуска программ не запускается автоматически при запуске Kaspersky Security 10.1 для Windows Server. 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 кнопку **Настройка** в блоке **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
4. На закладке **Общие** в блоке **Режим работы** настройте следующие параметры:
   - В раскрывающемся списке **Режим работы** выберите режим работы задачи.

     В раскрывающемся списке вы можете выбрать один из режимов работы задачи Контроль запуска программ:

     - **Применять правила контроля запуска программ**. Kaspersky Security 10.1 для Windows Server контролирует запуск программ с помощью заданных правил.
     - **Только статистика**. Kaspersky Security 10.1 для Windows Server 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 **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

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

  Если флажок установлен, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server проверяет программу при каждом ее последующем запуске заново.

  По умолчанию флажок установлен.

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

  Если флажок установлен, Kaspersky Security 10 для Windows Server запрещает запуск интерпретатора командной строки, даже если запуск интерпретатора разрешен. Запуск командной строки без команд разрешается только при выполнении обоих условий:

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

  Если флажок снят, Kaspersky Security 10.1 для Windows Server учитывает только разрешающие правила для запуска командной строки. Запуск блокируется, если не применено разрешающее правило, или выполняемый процесс не имеет статуса доверенного в KSN. Если разрешающее правило применено, или у процесса есть статус доверенного в KSN, запуск командной строки разрешается как с командой, так и без нее.

  Kaspersky Security 10.1 для Windows Server работает со следующими интерпретаторами:

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

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

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

   Kaspersky Security 10.1 для Windows Server не распознает путь, включающий наклонную черту "/". Используйте обратную наклонную черту "\", чтобы правильно ввести путь.

b. Выберите режим применения правил:

- **Заменить правилами политики локальные правила.**

  Программа применяет список правил, заданный в политике, для централизованного контроля 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server разрешает или запрещает запуск исполняемых файлов программ с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server разрешает или запрещает загрузку DLL-модулей с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

  Если флажок снят, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

7. В блоке **Использование KSN** настройте следующие параметры запуска программ:

   - **Не разрешать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые подпадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

     По умолчанию флажок снят.

   - **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Security 10.1 для Windows Server разрешает запуск программ, имеющих статус доверенных в KSN. При этом запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

     Если флажок снят, Kaspersky Security 10.1 для Windows Server не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

     По умолчанию флажок снят.

   - Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ.

8. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка контроля пакетов установки" на стр. 239).

9. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 146).

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

Kaspersky Security 10.1 для Windows Server 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

Вы можете упростить процедуру установки или обновления программного обеспечения с помощью функции контроля пакетов установки. Контроль пакетов установки позволяет автоматически разрешать запуск программ, если он выполнен с помощью доверенной программы или доверенного пакета установки. После запуска доверенного пакета установки Kaspersky Security 10.1 для Windows Server автоматически рассчитывает контрольную сумму для каждого вложенного файла и в дальнейшем не применяет принцип блокировки по умолчанию к таким файлам. Kaspersky Security 10.1 для Windows Server разрешает распаковку доверенного пакета установки и запуск всех вложенных файлов, если их запуск не запрещен правилами задачи Контроль запуска программ или они не имеют статус недоверенных в KSN.

Изменение или перемещение вложенного файла может привести к блокированию запуска этого файла.

► *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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     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 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 Security 10.1 для Windows Server 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 сервер до факта установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки системы на сервер.

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 выберете 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.

        - **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.

          Этот вариант выбран по умолчанию.

   - **Добавить несколько по хешу**.

     Вы можете выбрать неограниченное число файлов запуска и пакетов установки и добавить их в список одновременно. Kaspersky Security 10.1 для Windows Server учитывает хеш и разрешает запуск при обращении операционный 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 Security 10.1 для Windows Server 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 сервера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

9. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Включение режима Разрешения по умолчанию

Режим Разрешение по умолчанию разрешает запуск всех программ, если они не запрещены правилами и имеют доверенный статус в KSN. Режим Разрешение по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить режим только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Правила контроля запуска программ**.
5. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите **Добавить одно правило**.

   Откроется окно **Параметры Правила**.
6. В поле **Название** введите название правила.
7. В раскрывающемся списке **Тип** выберите вариант **Разрешающее**.

8. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
9. В блоке **Критерий срабатывания правила** выберите **Путь к файлу**.
10. Введите следующую маску: **?:**
11. В окне **Параметры Правила** нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server применит режим разрешения по умолчанию.

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 серверов и групп серверов 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 автоматического формирования правил контроля запуска программ.

  При использовании этого сценария групповая задача формирует для каждого сервера 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. Вы также 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 запуска программ в сети убедитесь, что для всех защищаемых серверов 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 сервера 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 Security 10.1 для Windows Server не блокирует запуски программ, но фиксирует в разделе **События** Kaspersky Security Center все запуски и блокировки запусков программ на всех серверах 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 запуска программ.

Вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнялись все возможные сценарии работы защищаемых серверов и групп серверов 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 серверов разных типов (с различным набором установленных программ (см. раздел "Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center" на стр. 234)).

- На основе событий о блокировании программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на локальном компьютере должна находиться под управлением активной политики Kaspersky Security Center. Все события на локальном компьютере при этом передаются на Сервер администрирования.

Рекомендуется выполнять обновление списка правил при изменении состава программ, установленных на серверах сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется формировать обновленный список правил с помощью групповой задачи Автоматическое формирование разрешающих правил или с помощью политики Контроль запуска программ в режиме **Только статистика**, выполняемых на серверах тестовой группы администрирования. Тестовая группа администрирования включает серверы, необходимые для проверочного запуска новых программ перед их установкой на серверы сети.

Перед тем как добавить разрешающие правила, выберите один из доступных режимов применения правил (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 234). 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.

В этом разделе

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**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить и выберите в панели результатов закладку **Политики**.
3. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.

   Откроется окно **<Имя политики>**.
4. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.
5. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.
6. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
7. Выберите принцип добавления правил к списку уже заданных правил контроля запуска программ:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется окно **Формирование правил контроля запуска программ**.
8. Настройте следующие параметры запроса:
   - **адрес сервер администрирования;**
   - **порт;**
   - **пользователь;**
   - **пароль.**
9. Выберите типы событий, которые должны стать основой для задачи формирования:
   - **Режим Только статистика: запуск программы запрещен**.
   - **Запуск программы запрещен**.
10. Выберите период из раскрывающегося списка **Запрашивать события, созданные в течение периода**.
11. Нажмите на кнопку **Создать правила**.
12. Нажмите 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 сервера, на котором установлена Консоль администрирования Kaspersky Security Center.

Если список правил контроля запуска программ уже задан в политике, Kaspersky Security 10.1 для Windows Server добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с одинаковыми хешами не учитываются, так как каждое правило является уникальным.

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 сервере сети организации. Списки содержат разрешающие правила для запуска файлов и программ, тип которых соответствует параметрам, указанным в групповой задачи автоматического формирования правил.

Процедура настройки параметров функциональных компонентов Kaspersky Security 10.1 для Windows Server в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Security 10.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Security 10.1 для Windows Server содержатся в соответствующих разделах *Руководства пользователя Kaspersky Security 10.1 для Windows Server*.

► *Чтобы задать разрешающие правила запуска программ для группы серверов на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** в панели управления настраиваемой группы серверов создайте групповую задачу Автоматическое формирование разрешающих правил 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 блоке **Уведомления** настройте параметры сохранения отчета о выполнении задачи.

     Подробная инструкция по настройке параметров в этом блоке содержится в *Руководстве администратора Kaspersky Security Center*.

   - В блоке **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Также вы можете изменять состав папок, запуск программ из которых будет разрешен: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
   - В блоке **Параметры** укажите действия задачи во время ее выполнения и по ее завершении. Укажите критерий, на основе которого будут сформированы правила, и имя файла, в который будут экспортированы эти правила.

- В блоке **Расписание** настройте параметры запуска задачи по расписанию.
- В блоке **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
- В блоке **Исключения из области действия задачи** задайте группы серверов, которые требуется исключить из области действия задачи.

> Kaspersky Security 10.1 для Windows Server не будет создавать разрешающие правила по программам, запускаемым на исключенных серверах.

3. На закладке **Задачи** в панели управления настраиваемой группы серверов 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 запуска программ в сети убедитесь, что для всех защищаемых серверов 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 сервера 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:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

   c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:

      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи 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 запуска программ**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном сервере, будут применены для всех серверов в сети, для которых применяется настраиваемая политика. Для этих серверов 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 серверов 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.
   a. Для этого в свойствах задачи Контроль запуска программ разверните узел **Отчеты и уведомления**.
   b. Для этого 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.
   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных устройствах в файл формата TXT.

Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых вы хотите разрешить.

4. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля запуска программ:

      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

   e. Нажмите на кнопку **ОК** в окне Правила контроля запуска программ и в окне **Параметры задачи**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

Управление подключением устройств из Kaspersky Security Center

Вы можете запрещать или разрешать подключение флеш-накопителей и других запоминающих устройств ко всем серверам в сети, формируя единые списки правил контроля серверов на стороне Kaspersky Security Center для групп серверов.

В этом разделе

О задаче Контроль устройств

Kaspersky Security 10.1 для Windows Server контролирует регистрацию и использование запоминающих устройств и устройств чтения CD/DVD дисков в целях защиты сервера от угроз безопасности, которые могут возникнуть во время файлового обмена с подключаемым по USB флеш-накопителем или внешним устройством другого типа. Запоминающее устройство – это внешнее устройство, предназначенное для записи и хранения данных.

Kaspersky Security 10.1 для Windows Server контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители;
- устройства чтения компакт-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Security 10.1 для Windows Server сообщает обо всех устройствах, подключенных по USB, с помощью соответствующего события в журналах событий и выполнения задач. Описание события включает тип устройства и путь подключения При запуске задачи Контроль устройств Kaspersky Security 10.1 для Windows Server проверяет и перечисляет все устройства, подключенные по USB. Уведомления можно настроить в блоке параметров уведомлений Kaspersky Security Center.

Задача Контроль устройств отслеживает попытки подключения внешних устройств к защищаемому серверу и блокирует их подключение, если не находит разрешающих правил для этих устройств. После блокировки соединения устройство становится недоступно.

Программа присваивает каждому подключаемому внешнему устройству один из двух статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. Путь к экземпляру такого устройства подпадает под область применения хотя бы одного разрешающего правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область определения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Формирование правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Security 10.1 для Windows Server идентифицирует регистрируемое в системе внешнее устройство по значению *пути к экземпляру устройства*. Путь к экземпляру устройства является уникальным признаком для каждого устройства. Информация о пути к экземпляру устройства содержится в свойствах внешнего устройства в системе Windows и определяется Kaspersky Security 10.1 для Windows Server в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Security 10.1 для Windows Server контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом блокировки по умолчанию (Default Deny) и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

  Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому серверу в момент запуска задачи Контроль устройств в режиме **Активный**, то такое устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить сервер. В ином случае принцип блокирования по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Security 10.1 для Windows Server не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом сервере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

  Этот режим можно использовать для формирования правил на основе информации, зарегистрированной во время выполнения задачи.

О формировании правил контроля устройств для всей сети через Kaspersky Security Center

Вы можете создавать списки правил контроля устройств с помощью задач и политик Kaspersky Security Center сразу для всех серверов и групп серверов 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 сервера обо всех когда-либо подключавшихся флеш-накопителях и запоминающих устройствах. Задача также учитывает все запоминающие устройства, подключенные в момент выполнения групповой задачи. По завершении выполнения групповой задачи, Kaspersky Security 10.1 для Windows Server формирует списки разрешающих правил для всех зарегистрированных запоминающих устройств сети и сохраняет эти списки в XML-файл в указанной общей папке. Далее вы можете вручную импортировать сформированные списки правил в свойства политики Контроль устройств. В отличие от задачи на локальном компьютере, в политике вы не можете настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи автоматического генерации разрешающих правил.

  Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском политики Контроль устройств в режиме активного применения правил.

  При применении политики контроля устройств в сети убедитесь, что для всех защищаемых серверов 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 сервера 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил контроля устройств, основанных на применении данных системы о всех устройствах.

Создание правил на основе данных системы о внешних устройствах, подключавшихся к компьютерам сети

Вы можете создавать правила (см. раздел "О формировании правил контроля устройств для всей сети через Kaspersky Security Center" на стр. 251) на основании данных Windows обо всех хранилищах, подключаемых ранее или подключенных сейчас, с помощью трех сценариев:

- 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 серверу в данный момент.

Kaspersky Security 10.1 для Windows Server не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил контроля устройств, основанных на применении данных системы о всех устройствах.

В этом разделе

Формирование правил с помощью задачи Генерация правил контроля устройств

► *Чтобы задать разрешающие правила запуска программ для группы серверов с помощью задачи Генерация правил контроля устройств, выполните следующие действия:*

1. На закладке **Задачи** в панели управления настраиваемой группы компьютеров создайте групповую задачу Генератор правил контроля устройств 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.
   - 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 серверов в списке групповых задач выберите созданную задачу генерации правил контроля устройств и нажмите на кнопку **Запустить** для запуска задачи.

   По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в указанной общей сетевой папке в файлах формата XML.

При применении политики контроля устройств в сети убедитесь, что для всех защищаемых серверов 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 сервера 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 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 сервере, будут применены для всех серверов в сети, для которых применяется настраиваемая политика. Для этих серверов 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 **Создать 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**.

3. Разверните группу администрирования, параметры политики которой вы хотите настроить и выберите в панели результатов закладку **Политики**.
4. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
5. Откроется окно **<Имя политики>**.
6. В свойствах политики откройте окно настройки параметров задачи Контроль устройств и выполните следующие действия:
   a. На закладке **Общие** нажмите на кнопку Список правил.

      Откроется окно **Правила контроля устройств**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать правила на основе данных системы**.

   c. Выберите принцип добавления правил к списку уже заданных правил контроля устройств:

      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.
7. Нажмите на кнопку **ОК** в окне **Правила контроля устройств** и в окне **Параметры задачи**.

Список правил в политике Контроль устройств будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Формирование правил для подключенных устройств

► *Чтобы задать разрешающие правила с помощью опции **Создать правила на основе данных системы** в параметрах политики Контроль устройств, выполните следующие действия:*

1. В 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. Откроется окно **<Имя политики>**.
5. В разделе **Контроль активности на компьютерах** нажмите кнопку **Настройка** в блоке **Контроль устройств**.
6. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.

7. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.

8. В списке обнаруженных устройств, которые подключены к защищаемому серверу, выберите устройства, для которых вы хотите сформировать разрешающие правила.
9. Нажмите на кнопку **Добавить правила для выбранных устройств**.
10. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в политике Контроль устройств будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Импорт правил из файла отчета Kaspersky Security Center о заблокированных устройствах

Вы можете импортировать данные о заблокированных запоминающих устройствах из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил контроля устройств в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи 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 серверов 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:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля устройств**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных устройствах из отчета Kaspersky Security Center**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля устройств:

      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

   e. Нажмите на кнопку **ОК** в окне **Правила контроля устройств** и в окне **Параметры задачи**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

Контроль активности в сети

Этот раздел содержит информацию о задаче Управление сетевым экраном и задачи Защита от шифрования.

В этом разделе

Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Управление сетевым экраном

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server. В ходе выполнения задачи Управление сетевым экраном Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.

Если при установке Kaspersky Security 10.1 для Windows Server сетевой экран Windows отключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы сетевой экран Windows включен, задача Управление сетевым экраном выполняется по завершении установки и блокирует все сетевые подключения, на разрешенные заданными правилами.

Компонент Управление сетевым экраном не входит в набор компонентов Рекомендуемой установки и не устанавливается по умолчанию.

Задача Управление сетевым экраном форсирует блокирование всех входящих и исходящих подключений, если они не разрешены заданными правилами задачи.

Задача регулярно опрашивает сетевой экран Windows и контролирует его состояние. По умолчанию интервал опроса составляет 1 минуту и не может быть изменен. Если при совершении опроса Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server контролирует следующее:

- статус работы сетевого экрана Windows;
- статус правил, добавленных после установки Kaspersky Security 10.1 для Windows Server другими программами или инструментами (например, добавление нового правила программы для порта/приложения с помощью wf.msc).

После сообщения правил сетевому экрану Windows Kaspersky Security 10.1 для Windows Server создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.

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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server удаляет такое правило;
- если в параметрах сетевого экрана Windows удаляется существующее правило, Kaspersky Security 10.1 для Windows Server восстанавливает такое правило;
- если в параметрах сетевого экрана Windows изменяются параметры существующего правила, Kaspersky Security 10.1 для Windows Server отменяет изменения;
- если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Security 10.1 для Windows Server форсировано сообщает это правило сетевому крану Windows;
- если в параметрах задачи Управление сетевым экраном изменяются параметры существующего правила, Kaspersky Security 10.1 для Windows Server форсировано обновляет такое правило в параметрах сетевого экрана Windows.
- если в параметрах задачи Управление сетевым экраном изменяются параметры существующего правила, Kaspersky Security 10.1 для Windows Server форсировано обновляет такое правило в параметрах сетевого экрана Windows.

Kaspersky Security 10.1 для Windows Server не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server, контролируют только входящий трафик.

Вы можете работать с правилами сетевого экрана следующих типов:

- Правила для приложений
- Правила для портов

Правила для приложений

Правила этого типа выборочно разрешают сетевые подключения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу.

Вы можете управлять правилами для приложений:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- изменять параметры заданных правил: указывать имя правила, путь к исполняемому файлу и область применения правила.

Правила для портов

Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола.

Вы можете управлять правилами для портов:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- изменять параметры заданных правил: указывать имя правила, номер порта, тип протокола и область применения правила.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая подключения с помощью правил для портов, вы снижаете уровень безопасности защищаемого сервера.

Активация и деактивация правил сетевого экрана

► *Чтобы активировать или деактивровать существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Контроль активности в сети** нажмите кнопку **Настройка** в блоке **Управление сетевым экраном.**
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
6. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет деактивировано.
7. В окне Правила сетевого экрана нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Настроенные параметры задачи 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 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Контроль активности в сети** нажмите кнопку **Настройка** в блоке **Управление сетевым экраном**.
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или закладку **Порты** и выполните одно из следующих действий:

   - Чтобы изменить существующее правило, в списке правил выберите правило, параметры которого вы хотите настроить и нажмите на кнопку **Изменить**.
   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или окно **Настроить правило для порта**.
6. В открывшемся окне выполните следующие действия:

   - Если вы работаете с правилом для приложения, выполните следующие действия:

     a. В поле **Имя правила** укажите имя редактируемого правила.

     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью редактируемого правила.

        Вы можете задать путь вручную или с помощью кнопки **Обзор**.

     c. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

        > Допускается указание IP-адресов только в формате IPv4.

   - Если вы работаете с правилом для порта, выполните следующие действия:

     a. В поле **Имя правила** укажите имя редактируемого правила.

     b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.

     c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.

     d. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

        > Допускается указание IP-адресов только в формате IPv4.
7. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
8. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Настроенные параметры задачи 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 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности в сети** нажмите кнопку **Настройка** в блоке **Управление сетевым экраном.**
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
6. В списке правил выберите правило, которое вы хотите удалить.
7. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
8. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи Управление сетевым экраном будут сохранены. Настроенные параметры задачи будут сохранены; новые параметры правил будут сообщены сетевому экрану Windows.

Защита от шифрования

Этот раздел содержит информацию о задаче Защита от шифрования и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Защита от шифрования

Задача Защита от шифрования позволяет обнаруживать активность вредоносного шифрования сетевых файловых ресурсов защищаемого сервера со стороны удаленных компьютеров сети.

В ходе выполнения задачи Защита от шифрования, Kaspersky Security 10.1 для Windows Server проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых папках защищаемого сервера. Если программа расценивает действия удаленного компьютера над сетевыми файловыми ресурсами как активность вредоносного шифрования, такой компьютер вносится в список недоверенных и теряет доступ к общим сетевым папкам.

Kaspersky Security 10.1 для Windows Server не расценивает активность шифрования как вредоносную, если обнаруженная активность шифрования ведется в каталогах, исключенных из области действия задачи Защита от шифрования.

По умолчанию программа блокирует доступ недоверенных компьютеров к сетевым файловым ресурсам на 30 минут.

Задача Защита от шифрования не позволяет блокировать доступ удаленного компьютера к сетевым файловым ресурсам до тех пор, пока активность этого компьютера не признана вредоносной. Это может занять некоторое время, в течение которого программа-шифровальщик может вести вредоносную активность.

Если задача Защита от шифрования запущена в режиме Только статистика, Kaspersky Security 10.1 для Windows Server только фиксирует попытки вредоносного шифрования с удаленных компьютеров в журнале выполнения задачи.

Настройка параметров задачи Защита от шифрования

Задача Защита от шифрования имеет следующие параметры по умолчанию:

- **Режим работы задачи**. Задача Защита от шифрования может быть запущена в режиме **Активный** или **Только статистика** . **Активный** режим применяется по умолчанию.
- **Область защиты**. По умолчанию Kaspersky Security 10.1 для Windows Server применяет задачу Защита от шифрования ко всем общим сетевым папкам защищаемого сервера. Вы можете изменить область защиты, указав папки общего доступа, к которым должна применяться задача.

- **Эвристический анализатор**. По умолчанию Kaspersky Security 10.1 для Windows Server применяет уровень детализации проверки **Средний**. Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень детализации проверки.
- **Запуск задачи по расписанию**. По умолчанию первый запуск задачи не определен. Задача Защита от шифрования не запускается автоматически при старте Kaspersky Security 10.1 для Windows Server. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Защита от шифрования, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Защита от шифрования**.
4. В открывшемся окне настройте следующие параметры:
   - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. 267) на закладке **Общие**.
   - Область защиты (см. раздел "Формирование области защиты" на стр. 268) на закладке **Область защиты**.
   - Исключения (см.раздел "Добавление исключений" на стр. 269) на закладке **Исключения**.
   - Запуск задачи по расписанию (см. раздел "Настройка запуска задачи по расписанию" на стр. 146) на закладке **Управление задачей**.
5. Нажмите на кнопку **Закрыть**.

Kaspersky Security 10.1 для Windows Server 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.

Общие параметры задачи

► *Чтобы настроить общие параметры задачи, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Защита от шифрования**.
4. В блоке **Режим работы** укажите режим работы задачи:
   - **Только статистика**.

     Если выбран этот режим, все попытки вредоносного шифрования записываются в журнал событий задачи Защита от шифрования, и никакие действия не исключаются. Этот режим выбран по умолчанию.
   - **Активный**.

     Если выбран этот режим, Kaspersky Security 10.1 для Windows Server блокирует доступ к папкам общего доступа для скомпрометированных компьютеров при обнаружении попытки вредоносного шифрования.
5. Снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.
6. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами «Лаборатории Касперского».

  Этот уровень выбран по умолчанию.
- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

7. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Предустановленная**. Вы можете использовать область защиты, установленную по умолчанию и включающую в проверку все общие сетевые папки сервера. Применяется, если выбран параметр **Все общие сетевые папки сервера**.
- **Пользовательская**. Вы можете самостоятельно настроить область защиты, выбрав папки, которые требуется включить в область защиты от шифрования, вручную. Применяется, если выбран параметр **Только указанные общие папки**.

Для настройки области защиты задачи Защита от шифрования можно использовать только локальный путь.

► *Чтобы настроить область защиты для задачи Защита от шифрования, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).

- Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.

4. На закладке **Область защиты** выберите папки, которые Kaspersky Security 10.1 для Windows Server будет проверять при выполнении задачи Защита от шифрования:

   - **Все общие сетевые папки сервера**.

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security 10.1 для Windows Server проверяет все общие сетевые папки сервера

     Этот вариант выбран по умолчанию.

   - **Только указанные общие папки**.

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security 10.1 для Windows Server проверяет только те общие сетевые папки сервера, которые вы указали вручную.

5. Чтобы указать общую папку сервера, которую вы хотите включить в область защиты, используйте один из следующих способов:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Выберите папку для добавления**.

   b. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.

   c. Нажмите на кнопку **ОК**.

6. Нажмите на кнопку **ОК** в окне **Защита от шифрования**.

Настроенные параметры будут сохранены.

Добавление исключений

► *Чтобы добавить исключения из области защиты от шифрования, 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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).

- Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

3. В разделе **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.

4. На закладке **Исключения**, установите флажок **Учитывать исключенные области защиты**.

   Если флажок установлен, то во время работы задачи Защита от шифрования Kaspersky Security 10.1 для Windows Server не обнаруживает вредоносное шифрование, осуществляющееся в указанных областях.

   Если флажок снят, Kaspersky Security 10.1 для Windows Server обнаруживает попытки шифрования на всех сетевых папках сервера.

   По умолчанию флажок снят, список исключений пуст.

5. Нажмите на кнопку **Добавить**.

   Откроется окно **Выберите папку для добавления**.

6. Введите имя папки или нажмите кнопку **Обзор**, чтобы выбрать необходимую папку.

7. Нажмите на кнопку **ОК**.

Исключенные области добавлены в список.

Диагностика системы

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

В этом разделе

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Монитор целостности файлов.

В этом разделе

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу для выявления изменений файлов, которые могут свидетельствовать о нарушении безопасности на защищаемом сервере. 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 сервере. Kaspersky Security 10.1 для Windows Server 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 сервере установлено запоминающее устройство, поддерживающее файловые системы ReFS и NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN журнала компонент получает данные о файловых операциях.

  Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинга файловых операций, требуется перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга (см. раздел "Настройка правил мониторинга" на стр. 277). Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижнеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания задачи и регулировать уровень важности событий для обнаруженных файловых операций, фиксируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- Доверенные пользователи.
- Маркеры файловых операций

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Информационное событие в журнале выполнения задачи.

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не может получить данные о пользователе вследствие прерывания задачи или сбоя синхронизации данных драйвера и USN-журнала. Если Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 зафиксирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Security 10.1 для Windows Server учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 41. 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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS
INTEGRITY_CHANGE	изменен атрибут целостности для именованного файлового потока	только ReFS
NAMED_DATA_EXTEND	размер именованного файлового потока увеличен	NTFS, ReFS
NAMED_DATA_OVERWRITE	именованный файловый поток перезаписан	NTFS, ReFS
NAMED_DATA_TRUNCATION	именованный файловый поток усечен	NTFS, ReFS
OBJECT_ID_CHANGE	изменен идентификатор файла или папки	NTFS, ReFS
RENAME_NEW_NAME	присвоено новое имя для файла или папки	NTFS, ReFS
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять значения по умолчанию параметров задачи Мониторинг файловых операций (см.таблицу ниже).

Таблица 42. Параметры задачи Мониторинг файловых операций по умолчанию

Параметр	Значение	Как настроить
Области мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для каталогов и файлов заданной области мониторинга будут формироваться события мониторинга.
Список доверенных пользователей	Не задано	Вы можете задать пользователей и/или группы пользователей, действия которых в указанных каталогах будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или отключать учет файловых операций, которые были выполнены в указанных областях мониторинга в периоды, когда задача не выполнялась.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется мониторинг файловых операций. При выполнении задачи Мониторинг файловых операций Kaspersky Security 10.1 для Windows Server будет пропускать области мониторинга, заданные в качестве исключений.
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 Security 10.1 для Windows Server формирует событие мониторинга.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров для характеристики файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Security 10.1 для Windows Server формирует событие аудита.
Расписание запуска задачи	Первый запуск не определен	Вы можете настроить параметры запуска задачи по расписанию.

Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Мониторинг файловых операций**.
4. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте параметры области мониторинга:
   a. Снимите или установите флажок **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 Security 10.1 для Windows Server 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. 277), которые будет контролировать задача.
5. На закладке **Управление задачей** запустите задачу на базе расписания (см. раздел "Работа с расписанием задач" на стр. 146).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

По умолчанию область мониторинга не задана; задача не контролирует выполнение файловых операций ни в одной директории.

► *Чтобы добавить область мониторинга, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Мониторинг файловых операций**.
4. В 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: <volume letter>:\<mask>. При отсутствии указания тома Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 272), и формирует для них события с уровнем важности Критическое событие.

8. Выберите закладку **Маркеры файловых операций**.

9. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:

   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.

   b. В открывшемся списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 272) установите флажки напротив тех операций, которые вы хотите контролировать.

   По умолчанию Kaspersky Security 10.1 для Windows Server контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы Kaspersky Security 10.1 для Windows Server рассчитывал контрольную сумму файлов после изменений, выполните следующие действия:

    a. В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

       Если флажок установлен, Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не рассчитывает контрольную сумму измененных файлов.

       Программа не выполняет расчет контрольной суммы в следующих случаях:

       - если в результате файловой операции файл стал недоступен (например, изменены права доступа к файлу);
       - если файловая операция фиксируется для файла, который впоследствии был удален.

       По умолчанию флажок снят.

b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из вариантов:

- **Хеш MD5**
- **Хеш SHA256**

11. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 272) установите флажки напротив тех операций, которые вы хотите контролировать.
12. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
    a. Выберите закладку **Исключения**.
    b. Установите флажок **Учитывать исключенные области мониторинга**.

       Флажок включает или выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

       Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Security 10.1 для Windows Server будет пропускать области мониторинга, заданные в списке исключений.

       Если флажок снят, Kaspersky Security 10.1 для Windows Server будет фиксировать события для всех заданных областей мониторинга.

       По умолчанию флажок снят, список исключений пуст.
    c. Нажмите на кнопку **Добавить**.

       Откроется окно **Выберите папку для добавления**.
    d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.
    e. Нажмите на кнопку **ОК**.

       Указанная папка добавится в список исключенных областей.
13. В окне **Область мониторинга** нажмите на кнопку **ОК**.

    Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

В этом разделе

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Security 10.1 для Windows Server контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Security 10.1 для Windows Server считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами, заданными пользователем или параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Предзаданные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью предзаданных правил, осуществляющими анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом сервере, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь предзаданных правил. Вы можете включать и выключать применение любого правила. Вы не можете удалять существующие или создавать новые правила.

Вы можете настроить критерии срабатывания правил которые контролируют события для данных операций:

- Обработка подбора пароля
- Обработка сетевого входа

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

> Kaspersky Security 10.1 для Windows Server не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил задачи вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил задачи Анализ журналов содержит четыре правила. Вы можете включать и выключать применение данных правил, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при появлении новой записи в журнале событий Windows, если в параметрах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать поджурнал журнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал, указав его имя в поле выбора источника.

  > Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Security 10.1 для Windows Server фиксирует событие с уровнем важности Критическое в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает пользовательские правила.

> Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробную информацию о настройке вы можете найти в данной статье https://technet.microsoft.com/en-us/library/cc952128.aspx.

Настройка параметров предзаданных правил задачи

► *Чтобы настроить параметры предзаданных правил для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Параметры анализа журналов**.
4. Перейдите на закладку **Предзаданные правила**.

5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Security 10.1 для Windows Server применяет эвристический анализатор для обнаружения аномальной активности на защищаемом сервере.

   Если этот флажок не установлен, эвристический анализатор выключен, Kaspersky Security 10.1 для Windows Server использует предустановленные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок установлен.

   Для работы задачи должно быть выбрано хотя бы одно правило анализа журналов.

6. Из списка предзаданных правил, выберите правила, которые вы хотите применять для анализа журналов:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
7. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Параметры анализа журналов**.
8. В блоке **Обработка перебора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Security 10.1 для Windows Server расценивает данное действие как аномальную активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **ОК**.

       Указанный пользователь добавится в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.
13. Указанный IP-адрес добавится в список доверенных.

14. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 146).
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 политики для группы серверов, выберите закладку **Политики** и откройте окно **<Свойства>: <Имя политики>** (см. раздел "Настройка политики" на стр.111).
   - Если вы хотите настроить параметры программы для одного сервера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 124).

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

   Откроется окно **Анализ журналов**.
4. На закладке **Правила анализа журналов** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Security 10.1 для Windows Server применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, вы не можете добавлять или изменять пользовательские правила. Kaspersky Security 10.1 для Windows Server применяет параметры правил по умолчанию.

   По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

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

     Вы можете добавить новый пользовательский журнал, указав имя журнала в поле **Источник**.

7. В блоке **Параметры срабатывания** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

   a. Введите числовое значение идентификатора.

   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

   c. Нажмите на кнопку **ОК**.

   Правило анализа журналов добавится в общий список правил.

Работа с Kaspersky Security 10.1 для Windows Server из командной строки

Этот раздел содержит описание работы с Kaspersky Security 10.1 для Windows Server из командной строки.

В этом разделе

Команды командной строки

Вы можете выполнять основные команды управления Kaspersky Security 10.1 для Windows Server из командной строки защищаемого компьютера, если при установке Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server.

Некоторые из команд Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server (см. таблицу ниже).

Таблица 43. Команды Kaspersky Security 10.1 для Windows Server

Команда	Описание
KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ из файла KAVSHELL APPCONTROL" на стр. 298).	Дополняет список сформированных правил контроля запуска программ в соответствии с выбранным принципом добавления.
KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачей Контроль запуска программ KAVSHELL APPCONTROL /CONFIG" на стр. 295).	Управляет режимами работы задачи Контроль запуска программ.
KAVSHELL APPCONTROL /GENERATE (см. раздел "Автоматическое формирование разрешающих правил KAVSHELL APPCONTROL /GENERATE" на стр. 296).	Запускает задачу автоматического формирования разрешающих правил контроля запуска программ.
KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала Kaspersky Security 10.1 для Windows Server.KAVSHELL VACUUM" на стр. 307).	Дефрагментирует файлы журнала выполнения Kaspersky Security 10.1 для Windows Server.
KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Security 10.1 для Windows Server.KAVSHELL HELP" на стр. 288).	Вызывает справку о командах Kaspersky Security 10.1 для Windows Server.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" на стр. 288)	Запускает службу Kaspersky Security 10.1 для Windows Server.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" на стр. 288).	Останавливает службу Kaspersky Security 10.1 для Windows Server.
KAVSHELL SCAN (см. раздел "Проверка выбранной области.KAVSHELL SCAN" на стр. 288).	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды.

Команда	Описание
KAVSHELL SCANCRITICAL (см. раздел "Запуск задачи Проверка важных областей.KAVSHELL SCANCRITICAL" на стр. 293).	Запускает системную задачу Проверка важных областей.
KAVSHELL TASK (см. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK" на стр. 294).	Запускает / приостанавливает / возобновляет / останавливает указанную задачу в асинхронном режиме / возвращает текущее состояние задачи / статистику задачи.
KAVSHELL RTP (см. раздел "Запуск и остановка задачи Постоянная защита.KAVSHELL RTP" на стр. 295).	Запускает или останавливает все задачи постоянной защиты.
KAVSHELL UPDATE (см. раздел "Запуск задачи обновления баз Kaspersky Security 10.1 для Windows Server.KAVSHELL UPDATE" на стр. 300).	Запускает задачу обновления баз Kaspersky Security 10.1 для Windows Server с параметрами, указанными с помощью ключей команды.
KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Security 10.1 для Windows Server.KAVSHELL ROLLBACK" на стр. 304).	Откатывает базы до предыдущей версии.
KAVSHELL LICENSE (см. раздел "Активация программы KAVSHELL LICENSE" на стр. 304).	Управляет ключами и кодами активации.
KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журнала трассировки.KAVSHELL TRACE" на стр. 306).	Включает или выключает запись журнала трассировки, управляет параметрами журнала трассировки.
KAVSHELL DUMP (см. раздел "Включение и выключение файла дампа.KAVSHELL DUMP" на стр. 309).	Включает или выключает создание файлов дампов памяти процессов Kaspersky Security 10.1 для Windows Server при аварийном завершении процессов.
KAVSHELL IMPORT (см. раздел "Импорт параметров.KAVSHELL IMPORT" на стр. 310).	Импортирует общие параметры Kaspersky Security 10.1 для Windows Server, параметры его функций и задач из предварительно созданного конфигурационного файла.
KAVSHELL EXPORT (см. раздел "Экспорт параметров.KAVSHELL EXPORT" на стр. 311).	Экспортирует все параметры Kaspersky Security 10.1 для Windows Server и существующих задач в конфигурационный файл.
KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств.KAVSHELL DEVCONTROL" на стр. 299).	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

Вызов справки о командах Kaspersky Security 10.1 для Windows Server. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Security 10.1 для Windows Server, 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 сервера, используйте команду `KAVSHELL SCAN`. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная Запустить помощью команды KAVSHELL SCAN, является временной. Она отображается в Консоли Kaspersky Security 10.1 только во время ее выполнения (в Консоли Kaspersky Security 10.1 вы не можете просматривать параметры задачи). В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Security 10.1. 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. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK" на стр. 294).

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 44. Ключи команды KAVSHELL SCAN

Ключ	Описание
Область проверки. Обязательный ключ.	
<файлы> <папки> <сетевой путь>	Область проверки – список файлов, папок, сетевых путей и предопределенных областей. Указывайте сетевые пути в формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL: KAVSHELL SCAN Folder4 Если имя объекта, который вы хотите проверить, содержит пробелы, требуется заключить его в кавычки. Если вы выбрали папку, то Kaspersky Security 10.1 для Windows Server проверит также все вложенные подпапки для данной папки. Для проверки группы файлов вы можете использовать символы * или ?.
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на сервере.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.
/MYCOMP	Проверять все области защищаемого сервера.
/L: <имя файла со списком областей проверки>	Имя файла со списком областей проверки, включая полный путь к файлу. Разделяйте области проверки в файле символом перевода строки. Вы можете указывать предопределенные области проверки, как показано в следующем в примере файла со списком областей проверки: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Проверяемые объекты (File types). Если вы не укажете никаких значений этого ключа, Kaspersky Security 10.1 для Windows Server будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Security 10.1 для Windows Server проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Security 10.1 для Windows Server проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	Проверять только новые и измененные файлы. Если вы не укажете этот ключ, Kaspersky Security 10.1 для Windows Server будет проверять все объекты.

Ключ	Описание
/AI: **Действия над зараженными и другими обнаруженными объектами**. Если вы не зададите никаких значений этого ключа, Kaspersky Security 10.1 для Windows Server будет выполнять действие **Пропускать**.	
DISINFECT	Лечить, если невозможно, пропускать
DISINFDEL	Лечить, удалять, если лечение невозможно
DELETE	Удалять Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Security 10.1 для Windows Server для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI: и /AS:. В этом случае Kaspersky Security 10.1 для Windows Server не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
/AS: **Действия над возможно зараженными объектами**/ Если вы не зададите никаких значений этого ключа, Kaspersky Security 10.1 для Windows Server будет выполнять действие **Пропускать**.	
QUARANTINE	Помещать на карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
Исключения	
/E:ABMSPO	Ключ исключает составные объекты следующих типов: A – SFX-архивы; B – почтовые базы; M – файлы почтовых форматов; S – архивы (включая SFX-архивы); P – упакованные объекты; O – вложенные OLE-объекты.
/EM:<"маски">	Исключать файлы по маске Можно указать несколько задач, 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 Security 10.1 для Windows Server проверяет объекты любого размера.
/TZOFF	Отменить исключения доверенной зоны.
Дополнительные параметры (Options)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).

Ключ	Описание
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ANALYZERLEVEL: <уровень анализа>	Включить использование эвристического анализатора, настроить уровень анализа. Сюда входят следующие уровни эвристического анализа: 1 – поверхностный; 2 – средний; 3 – глубокий. Если вы опустите этот ключ, Kaspersky Security 10.1 для Windows Server не будет использовать эвристический анализатор.
/ALIAS:<альтернативное имя задачи>	Ключ позволяет присвоить задаче проверки по требованию временное имя, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Security 10.1 для Windows Server. Если этот ключ не задан, задаче присваивается альтернативное имя scan_<kavshell_pid>, например, scan_1234. В Консоли Kaspersky Security 10.1 задаче присваивается имя Проверка объектов.(<дата и время>), например, Проверка объектов 8/16/2007 5:13:14.
Параметры журналов выполнения задач (Report settings)	
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Security 10.1 для Windows Server сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Security 10.1 для Windows Server в консоли "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли Kaspersky Security 10.1. Если Kaspersky Security 10.1 для Windows Server не удается создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.
/ANSI	Ключ позволяет записывать события в журнал выполнения задач в кодировке ANSI. Ключ ANSI не будет применяться, если не задан ключ W. Если ключ ANSI не указан, то журнал выполнения задач ведется в кодировке UNICODE.

Запуск задачи Проверка важных областей. KAVSHELL SCANCRITICAL

Используйте команду `KAVSHELL SCANCRITICAL`, чтобы запустить системную задачу проверки по требованию Проверка важных областей с параметрами, заданными в Консоли Kaspersky Security 10.1.

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 45. Синтаксис ключа /W команды KAVSHELL SCANCRITICAL

Ключ	Описание
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Security 10.1 для Windows Server сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий программы в консоли "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Security 10.1. Если Kaspersky Security 10.1 для Windows Server не удается создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.

Управление указанной задачей в асинхронном режиме. KAVSHELL TASK

С помощью команды `KAVSHELL TASK` вы можете управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное 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 46. Ключи команды KAVSHELL TASK

Ключ	Описание
Без ключей	Команда возвращает список всех существующих задач Kaspersky Security 10.1 для Windows Server. Список содержит поля: альтернативное имя задачи, категория задачи (системная или пользовательская) и текущий статус задачи.
<альтернативное имя задачи>	Вместо имени задачи в команде SCAN TASK используйте ее альтернативное имя (Task alias) – дополнительное, краткое имя, которое Kaspersky Security 10.1 для Windows Server присваивает задачам. Чтобы просмотреть альтернативные имена задач Kaspersky Security 10.1 для Windows Server, введите команду KAVSHELL TASK без ключей.
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/PAUSE	Приостановить указанную задачу
/RESUME	Возобновить указанную задачу в асинхронном режиме
/STATE	Получить текущее состояние задачи (например, **Выполняется**, **Завершена**, **Приостановлена**, **Остановлена**, **Завершена с ошибкой**, **Запускается**, **Восстанавливается**)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

Команда "Коды возврата команды KAVSHELL TASK" (см. раздел "Коды возврата команды KAVSHELL TASK" на стр. 314).

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 47. 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 48. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
/mode:<applyrules|statistics>	Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: • active - Применять правила контроля запуска программ; • statistics - Только статистика.
/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.
/savetofile: <Полное имя xml-файла>	Сохранить список правил в файл.
/savetofile: <Полное имя xml-файла> /sdc	Сохранить список правил контроля распространения программного обеспечения в файл.
/clearsdc	Удалить все правила контроля распространения программного обеспечения.

Автоматическое формирование разрешающих правил 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 49. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
Область применения разрешающих правил	
<путь к папке>	Путь к папке, содержащей исполняемые файлы, для которых требуется автоматически создать разрешающие правила.
/source: <путь к файлу со списком папок>	Путь к файлу в формате TXT, содержащий список папок с исполняемыми файлами, для которых требуется автоматически создать разрешающие правила.
/masks: <edms>	Расширения исполняемых файлов, для которых требуется создать разрешающие правила контроля запуска программ. Вы можете включить в область срабатывания создаваемых правил файлы следующих расширений: • e - файлы с расширением exe; • d - файлы с расширением dll; • m - файлы с расширением msi; • s - скрипты.
/runapp	Учитывать при формировании разрешающих правил программы, запущенные на защищаемом сервера в момент выполнения задачи.
Действия при автоматическом формировании правил	
/rules: <ch|cp|h>	Указать действия, которые задача совершает во время формирования разрешающих правил контроля запуска программ: • ch - использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256. • cp - использовать цифровой сертификат. Если сертификат отсутствует, использовать значение пути к исполняемому файлу. • h - использовать хеш SHA256.
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании правил контроля запуска программ. Команда выполняется, если задано значение ключа /rules: <ch|cp>.
/user: <пользователь или группа пользователей>	Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или указанной группой.

Ключ	Описание
Действия по завершении автоматического формирования правил	
/export: <полный путь к XML файлу>	Сохранять сформированные правила в файл формата XML.
/unique	Добавлять информацию о сервера, по программам которого формируются разрешающие правила контроля запуска программ.
/prefix: < Префикс для названий правил>	Префикс для названий создаваемых правил контроля запуска программ.
/import: <a|r|m>	Импортировать сформированные правила в список заданных правил контроля запуска программ в соответствии с указанным принципом добавления новых правил: : • a - **Добавлять к существующим правилам** (одинаковые правила дублируются); • r - **Заменять существующие правила** (новые правила добавляются вместо заданных правил); • m - **Объединять с существующими правилами** (добавляются новые правила, параметры которых не совпадают с параметрами уже заданных правил).

Заполнение списка правил задачи Контроль запуска программ KAVSHELL APPCONTROL

С помощью команды `KAVSHELL APPCONTROL` вы можете добавлять правила в список правил задачи Контроль запуска программ из файла формата XML в соответствии с выбранным принципом, а также удалять все заданные правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL APPCONTROL

► *Чтобы добавить к заданным правилам контроля запуска программ правила из файла формата XML по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете выбирать принцип добавления новых правил из указанного файла формата XML в список заданных правил задачи Контроль запуска программ (см. таблицу ниже).

Таблица 50. Ключи команды KAVSHELL APPCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - **Добавить к существующим правилам** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - **Заменить существующие правила** (новые правила добавляются вместо заданных правил).
/merge <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - **Объединить правила с существующими** (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля запуска программ.

Наполнение списка правил контроля устройств из файла. KAVSHELL DEVCONTROL

С помощью команды `KAVSHELL DEVCONTROL` вы можете добавлять правила в список правил задачи Контроль устройств из файла формата XML в соответствии с выбранным принципом, а также удалять все заданные правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL DEVCONTROL

► *Чтобы добавить к заданным правилам контроля устройств правила из файла формата XML по принципу **Добавить к существующим правилам**, выполните команду:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете выбирать принцип добавления новых правил из указанного файла формата XML в список заданных правил задачи Контроль устройств (см. таблицу ниже).

Таблица 51. Ключи команды KAVSHELL DEVCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - **Добавить к существующим правилам** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - **Заменить существующие правила** (новые правила добавляются вместо заданных правил).
/merge <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - **Объединить правила с существующими** (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля устройств.

Запуск задач обновления баз Kaspersky Security 10.1 для Windows Server. KAVSHELL UPDATE

С помощью команды KAVSHELL UPDATE вы можете запускать задачу обновления баз Kaspersky Security 10.1 для Windows Server в синхронном режиме.

Задача обновления баз Kaspersky Security 10.1 для Windows Server, запущенная с помощью команды KAVSHELL UPDATE, является временной. Она отображается в Консоли Kaspersky Security 10.1 только во время ее выполнения. В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Security 10.1. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, как и к задачам обновления, созданным в Консоли Kaspersky Security 10.1, могут применяться политики программы Kaspersky Security Center. Об управлении Kaspersky Security 10.1 для Windows Server на компьютерах с помощью программы Kaspersky Security Center читайте в разделе "Управление Kaspersky Security 10.1 для Windows Server 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 \server\databases, 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 Security 10.1 для Windows Server с сервера обновлений «Лаборатории Касперского»; соединиться с источником обновлений через прокси-сервер (адрес прокси-сервера: 8080), для доступа к сервера использовать встроенную проверку подлинности Microsoft Windows (NTLM-authentication) под учетной записью (имя пользователя: 123456, выполните команду:*

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

Таблица 52. Ключи команды KAVSHELL UPDATE

Ключ	Описание
Источники обновления (обязательный ключ). Укажите один или несколько источников. Kaspersky Security 10.1 для Windows Server будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC.
<URL>	Пользовательские источники обновления. Пользовательский источник обновлений – адрес HTTP- или FTP-сервера, на котором помещается папка с обновлениями.
<Локальная папка>	Пользовательские источники обновления. Папка на защищаемом сервере.
/AK	Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
/KL	Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений
/NOUSEKL	Не использовать серверы обновлений "Лаборатории Касперского", если другие указанные источники обновлений недоступны (по умолчанию используются).

Ключ	Описание
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот ключ, Kaspersky Security 10.1 для Windows Server будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	Этот ключ задает метод проверки подлинности для доступа к прокси-серверу. Он может принимать следующие значения: **0** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Security 10.1 для Windows Server будет обращаться к прокси-серверу под учетной записью **Локальная система** (**SYSTEM**); **1** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Security 10.1 для Windows Server будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD; **2** – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication). Если для доступа к прокси-серверу не требуется проверка подлинности, указывать этот ключ нет необходимости.
/PROXYUSER:<имя пользователя>	Имя пользователя, которое будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.
/PROXYPWD:<пароль>	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. Если вы укажете ключ /PROXYUSER, а ключ /PROXYPWD опустите, считается что пароль пустой.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию используются)
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используются)
/USEPROXYFORLOCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать настройки прокси-сервера для соединения с локальными источниками обновления**.
Общие параметры FTP- и HTTP-сервера	
/NOFTPPASSIVE	Если вы укажете этот ключ, Kaspersky Security 10.1 для Windows Server будет использовать активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Security 10.1 для Windows Server будет использовать пассивный режим FTP-сервера, если возможно.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот ключ, Kaspersky Security 10.1 для Windows Server будет использовать значение по умолчанию: 10 с. В качестве значения ключа вы можете вводить только целые числа.

Ключ	Описание
/REG:<код iso3166>	Региональные параметры. Ключ "Региональные используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Security 10.1 для Windows Server оптимизирует загрузку обновлений на защищаемый компьютер, выбирая ближайший к нему сервер обновлений. В качестве значения ключа укажите буквенный код страны местоположения защищаемого сервера в соответствии со стандартом ISO 3166-1, например, /REG:gr или /REG:RU. Если вы опустите этот ключ или укажете несуществующий код страны, Kaspersky Security 10.1 для Windows Server будет распознавать местоположение защищаемого компьютера в соответствии с региональными настройками защищаемого компьютера.
/ALIAS:<альтернативное имя задачи>	Этот ключ позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Security 10.1 для Windows Server. Если этот ключ не задан, задаче присваивается альтернативное имя update_<kavshell_pid>, например, update_1234. В Консоли Kaspersky Security 10.1 задаче присваивается имя Обновление баз программы (<дата и время>), например: Обновление баз программы 8/16/2007 5:41:02.
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Security 10.1 для Windows Server сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Security 10.1 для Windows Server в консоли "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажите только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Security 10.1. Если Kaspersky Security 10.1 для Windows Server не удается создать файл журнала, он не прерывает выполнение команды и не отображает сообщение об ошибке.

Коды возврата команды KAVSHELL UPDATE (на стр. 315).

Откат обновления баз Kaspersky Security 10.1 для Windows Server. KAVSHELL ROLLBACK

С помощью команды `KAVSHELL ROLLBACK` вы можете выполнить системную задачу Откат обновления баз – откатить базы Kaspersky Security 10.1 для Windows Server до предыдущих установленных обновлений. Команда выполняется синхронно.

Синтаксис команды

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK (на стр. 315).

Управление анализом журналов. KAVSHELL LOG-INSPECTOR

Команда `KAVSHELL LOG-INSPECTOR` позволяет настроить контроль целостности среды сервера основываясь на анализе журнала событий Windows.

Синтаксис команды

```
KAVSHELL TASK LOG-INSPECTOR
```

Пример команды

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Таблица 53. Ключи команды KAVSHELL LOG-INSPECTOR

Ключ	Описание
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/STATE	Получить текущее состояние задачи (например, **Выполняется**, **Завершена**, **Приостановлена**, **Остановлена**, **Завершена с ошибкой**, **Запускается**, **Восстанавливается**)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

Команда "Коды возврата команды KAVSHELL TASK LOG-INSPECTOR" (см. раздел "Коды возврата команды KAVSHELL LOG-INSPECTOR" на стр. 313).

Активация программы KAVSHELL LICENSE

С помощью команды `KAVSHELL LICENSE` вы можете управлять ключами и кодами активации в Kaspersky Security 10.1 для Windows Server.

> 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 54. Ключи команды KAVSHELL LICENSE

Ключ	Описание
Без ключей	Команда возвращает следующую информацию о добавленных ключах: • Номер ключа. • Тип лицензии (коммерческая или пробная). • Срок действия связанной с ключом лицензии. • Статус ключа (активный или дополнительный). Если указано значение *, ключ добавлен в качестве дополнительного.
/ADD:<имя файла ключа или код активации>	Добавляет ключ с помощью указанного файла или кода активации. Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/R	Код активации или ключ /R является дополнительным к коду активации или ключу /ADD и указывает на то, что код активации или ключ добавляется в качестве дополнительного.
/DEL:<номер ключа или код активации>	Удаляет ключ с указанным номером или указанный код активации.

Коды возврата команды KAVSHELL LICENSE (см. раздел "Коды возврата команды KAVSHELL LICENSE" на стр. 316).

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 Security 10.1 для Windows Server, а также устанавливать уровень детализации информации в журнале.

Kaspersky Security 10.1 для Windows Server 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 55. Ключи команды KAVSHELL TRACE

Ключ	Описание
/ON	Включить ведение журнала трассировки.
/F:<папка с файлами журнала трассировки>	Этот ключ указывает полный путь к папке, в которой будут сохранены файлы журнала трассировки (обязательный ключ). Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Вы можете указывать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого сервера. 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”. /F:"C\Trace Folder". Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/S: <максимальный размер файла журнала в мегабайтах>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Security 10.1 для Windows Server начнет записывать информацию в новый файл; предыдущий файл журнала сохранится. Если вы не укажете этот ключ, максимальный размер одного файла журнала составит 50 МБ.

Ключ	Описание
/LVL:debug|info|warning|error|critical	Этот ключ устанавливает уровень детализации журнала от максимального (**Отладочная информация**), при котором в журнал записываются все события, до минимального (**Критические события**), при котором в журнал записывается только критические события. Если вы не укажете этот ключ, в журнал трассировки будут записываться события с уровнем детализации Отладочная информация.
/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 (см. раздел "Коды возврата команды KAVSHELL TRACE" на стр. 316).

Дефрагментация файлов журнала Kaspersky Security 10.1 для Windows Server. KAVSHELL VACUUM

С помощью команды `KAVSHELL VACUUM` вы можете провести дефрагментацию файлов журнала событий программы. Это позволяет избежать ошибок в работе системы или Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server\Reports. Если вы вручную указали другой путь для хранения файлов журналов, команда KAVSHELL VACUUM выполняет дефрагментацию файлов в папке, указанной в параметрах журналов Kaspersky Security 10.1 для Windows Server.

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 Сервера. Процедура дефрагментации блокирует доступ к журналам Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server, выполните команду:*

```
KAVSHELL VACUUM
```

Выполнение команды доступно при запуске с правами учетной записи локального администратора.

Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server создает файлы fidbox.dat и fidbox2.dat, которые содержат информацию об уже проверенных незараженных объектах. Чем больше различных файлов проверил Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server не приостанавливает защиту (в отличие от удаления файла fidbox.dat вручную).
- После очистки файла fidbox.dat Kaspersky Security 10.1 для Windows Server может увеличить нагрузку на компьютер. При этом антивирусная программа проверяет все файлы, к которым обращается впервые после очистки файла fidbox.dat. После проверки Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server при их аварийном завершении (см. таблицу ниже). Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Kaspersky Security 10.1 для Windows Server.

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 56. Ключи команды KAVSHELL DUMP

Ключ	Описание
/ON	Включает создание файла дампа процесса при его аварийном завершении.
/F:<папка с файлами дампов>	Это обязательный ключ. Обязательный ключ; указывает путь к папке, в которой будет сохранен файл дампа. Если вы укажете путь к несуществующей папке, файл дампа не будет создан. Вы можете использовать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого сервера. Указывая путь к папке с файлом дампа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Ключ	Описание
/SNAPSHOT	Снимает образ памяти указанного выполняющегося процесса Kaspersky Security 10.1 для Windows Server и сохраняет файл дампа в папке, путь к которой указан ключом /F.
/P	Идентификатор PID процесса; отображается в Диспетчере задач Microsoft Windows.
/OFF	Выключает создание файла дампа при аварийном завершении.

Коды возврата команды KAVSHELL DUMP (см. раздел "Коды возврата команды KAVSHELL DUMP" на стр. 317).

Импорт параметров. KAVSHELL IMPORT

С помощью команды `KAVSHELL IMPORT` вы можете импортировать параметры Kaspersky Security 10.1 для Windows Server, его функций и задач из конфигурационного файла в Kaspersky Security 10.1 для Windows Server 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 57. Ключи команды KAVSHELL IMPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL IMPORT (см. раздел "Коды возврата команды KAVSHELL IMPORT" на стр. 317).

Экспорт параметров. KAVSHELL EXPORT

С помощью команды `KAVSHELL EXPORT` вы можете экспортировать все параметры Kaspersky Security 10.1 для Windows Server и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Security 10.1 для Windows Server 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 58. Ключи команды KAVSHELL EXPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Вы можете присвоить конфигурационному файлу любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL EXPORT (см. раздел "Коды возврата команды KAVSHELL EXPORT" на стр. 318).

Интеграция с MS Operation Management Suite. KAVSHELL OMSINFO

С помощью команды KAVSHELL OMSINFO можно просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами и службой KSN. Данные об угрозах поступают из доступных журналов событий.

Синтаксис команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <полный путь к сгенерированному файлу с именем файла>
```

Примеры команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Таблица 59. Ключи команды KAVSHELL OMSINFO

Ключ	Описание
<путь к сгенерированному файлу с именем файла>	Имя сгенерированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах.

Коды возврата командной строки

В этом разделе

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Таблица 60. 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server работает под учетной записью Локальная система).
-99	Неизвестная ошибка

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Таблица 61. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден файл со списком областей проверки)
-5	Неверный синтаксис команды или не определена область проверки
-80	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 LOG-INSPECTOR

Таблица 62. Коды возврата команды KAVSHELL LOG-INSPECTOR

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
-6	Неверная операция (например, служба Kaspersky Security 10.1 для Windows Server уже запущена или уже остановлена)
402	Задача уже запущена (для ключа /STATE)

Коды возврата команды KAVSHELL TASK

Таблица 63. Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для ключа /STATE)
402	Задача уже запущена (для ключа /STATE)
403	Задача уже приостановлена (для ключа /STATE)
-404	Ошибка выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL RTP

Таблица 64. 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 65. Коды возврата команды KAVSHELL UPDATE

Код возврата	Описание
0	Операция выполнена успешно
200	Все объекты актуальны (базы или программные компоненты в актуальном состоянии)
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Ошибка аутентификации при подключении к прокси-серверу
-234	Ошибка подключения к программе Kaspersky Security Center
-235	Kaspersky Security 10.1 для Windows Server не прошел проверку подлинности при соединении с источником обновлений
-236	Базы Kaspersky Embedded Systems Security повреждены
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Таблица 66. 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 67. 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 68. 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 69. Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL DUMP

Таблица 70. 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 71. 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 Security 10.1 для Windows Server 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 Security 10.1 для Windows Server более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Таблица 72. 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 Security 10.1 для Windows Server не экспортировал параметры какого-либо из функциональных компонентов

Контроль производительности. Счетчики Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о счетчиках Kaspersky Security 10.1 для Windows Server: счетчиках производительности для программы Системный монитор, счетчиках и ловушках SNMP.

В этом разделе

Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы "Системный монитор" Microsoft Windows, которые регистрирует Kaspersky Security 10.1 для Windows Server во время установки.

В этом разделе

О счетчиках производительности Kaspersky Security 10.1 для Windows Server

В состав устанавливаемых компонентов Kaspersky Security 10.1 для Windows Server по умолчанию включен компонент **Счетчики производительности**. Во время установки Kaspersky Security 10.1 для Windows Server регистрирует свои счетчики производительности для программы "Системный монитор" Microsoft Windows.

С помощью счетчиков Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server и сбои в его работе.

Вы можете просматривать счетчики производительности Kaspersky Security 10.1 для Windows Server, 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 Security 10.1 для Windows Server в случае, если значения счетчиков их превышают.

Общее количество отвергнутых запросов

Таблица 73. Общее количество отвергнутых запросов

Имя	Общее количество отвергнутых запросов (Total number of requests denied)
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были принятых рабочими процессами Kaspersky Security 10.1 для Windows Server; рассчитывается с момента последнего запуска Kaspersky Security 10 для Windows Server. Программа пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Kaspersky Security 10.1 для Windows Server.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • снижение качества постоянной защиты из-за полной загрузки рабочих процессов Kaspersky Security 10.1 для Windows Server; • прерывание постоянной защиты из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч

Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: • счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Kaspersky Security 10.1 для Windows Server были полностью загружены, поэтому Kaspersky Security 10.1 для Windows Server не удалось проверить объекты. Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты. Вы можете использовать параметры Kaspersky Security 10.1 для Windows Server **Максимальное количество активных процессов** и **Число процессов для постоянной защиты**; • количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Security 10.1 для Windows Server не проверяет объекты при доступе. Перезапустите Kaspersky Security 10.1 для Windows Server.

Общее количество пропущенных запросов

Таблица 74. Общее количество пропущенных запросов

Имя	Общее количество пропущенных запросов (Total number of requests skipped).
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Security 10.1 для Windows Server, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Security 10.1 для Windows Server пропускает такой объект и на 1 увеличивается значение счетчика **Общее количество отвергнутых запросов**.
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за простоя потоков диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Kaspersky Security 10.1 для Windows Server, чтобы восстановить простаивающие потоки.

Количество запросов, не обработанных из-за нехватки системных ресурсов

Таблица 75. Количество запросов, не обработанных из-за нехватки системных ресурсов

Имя	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
Определение	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Security 10.1 для Windows Server. Kaspersky Security 10.1 для Windows Server пропускает объекты, запросы на проверку которых не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, рабочие процессы Kaspersky Security 10.1 для Windows Server нуждаются в увеличении объема оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

Количество запросов, отданных на обработку

Таблица 76. Количество запросов, отданных на обработку

Имя	Количество запросов, отданных на обработку (Number of requests sent to be processed).
Определение	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Security 10.1 для Windows Server и общий уровень файловой активности на сервере.
Нормальное / пороговое значение	Значение счетчика может колебаться в зависимости от уровня файловой активности на сервере.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	нет

Среднее количество потоков диспетчера файловых перехватов

Таблица 77. Среднее количество потоков диспетчера файловых перехватов

Имя	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, среднее по всем процессам, занятым в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты из-за полной загрузки процессов Kaspersky Security 10.1 для Windows Server.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Kaspersky Security 10.1 для Windows Server пропустит объект. Увеличьте количество процессов Kaspersky Security 10.1 для Windows Server для задач постоянной защиты. Вы можете использовать параметры Kaspersky Security 10.1 для Windows Server **Максимальное количество активных процессов** и **Число процессов для постоянной защиты**.

Максимальное количество потоков диспетчера файловых перехватов

Таблица 78. Максимальное количество потоков диспетчера файловых перехватов

Имя	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, наибольшее из всех процессов, занятых в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Kaspersky Security 10.1 для Windows Server неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Kaspersky Security 10.1 для Windows Server.

Количество элементов в очереди зараженных объектов

Таблица 79. Количество элементов в очереди зараженных объектов

Имя	Количество элементов в очереди зараженных объектов (Number of items in the infected object queue).
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими программами и Kaspersky Security 10.1 для Windows Server; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Security 10.1 для Windows Server обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.

Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Kaspersky Security 10.1 для Windows Server не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов); Перезапустите Kaspersky Security 10.1 для Windows Server. • Недостаточно процессорного времени для обработки объектов; Обеспечьте выделение Kaspersky Security 10.1 для Windows Server дополнительного процессорного времени, например, снизив нагрузку на сервер другими программами. • Возникла вирусная эпидемия. О возникновении вирусной эпидемии говорит большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи.

Количество объектов, обрабатываемых за секунду

Таблица 80. Количество объектов, обрабатываемых за секунду

Имя	Количество объектов, обрабатываемых за секунду (Number of objects processed per second).
Определение	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.
Назначение	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности сервера, возникшее из-за недостаточности выделяемого рабочим процессам Kaspersky Security 10.1 для Windows Server процессорного времени или сбоя в работе Kaspersky Security 10.1 для Windows Server.
Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.

Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от установленных значений параметров Kaspersky Security 10.1 для Windows Server и загрузки сервера процессами других программ. Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился, то могла произойти одна из следующих ситуаций: • Рабочим процессам Kaspersky Security 10.1 для Windows Server не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Security 10.1 для Windows Server дополнительного процессорного времени, например, снизив нагрузку на сервер другими программами. • Возник сбой в работе Kaspersky Security 10.1 для Windows Server (простаивает несколько потоков). Перезапустите Kaspersky Security 10.1 для Windows Server.

Счетчики и ловушки SNMP Kaspersky Security 10.1 для Windows Server

Этот раздел содержит информацию о счетчиках и ловушках SNMP Kaspersky Security 10.1 для Windows Server.

В этом разделе

О счетчиках и ловушках SNMP Kaspersky Security 10.1 для Windows Server

Если вы включили в состав устанавливаемых компонентов программы компонент **Счетчики и ловушки SNMP**, вы можете просматривать счетчики и ловушки Kaspersky Security 10.1 для Windows Server по протоколам Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Security 10.1 для Windows Server на рабочем месте администратора, запустите на защищаемом сервере Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

Счетчики SNMP Kaspersky Security 10.1 для Windows Server

Этот раздел содержит таблицы с описанием параметров счетчиков SNMP Kaspersky Security 10.1 для Windows Server.

В этом разделе

Счетчики производительности

Таблица 81. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отданных на обработку (см. стр. 322).
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов (см. раздел "Количество элементов в очереди зараженных объектов" на стр. 324).
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (см. стр. 325).
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Security 10.1 для Windows Server в текущий момент

Счетчики карантина

Таблица 82. 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 83. Счетчики резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Объем данных в папке резервного хранилища (МБ)

Общие счетчики

Таблица 84. Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней проверки важных областей сервера (промежуток времени в секундах между датой завершения задачи, имеющей статус *Задача проверки важных областей*, и текущим моментом).
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлены активный и дополнительный ключи или коды активации, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом или кодом активации.
currentApplicationUptime	Время работы Kaspersky Security 10.1 для Windows Server с момента его последнего запуска, в сотых долях секунды
currentFileMonitorTaskStatus	Состояние задачи Постоянная защита файлов: **On** – выполняется; **Off** – остановлена или приостановлена

Счетчик обновления

Таблица 85. 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 86. 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

Счетчик	Определение
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 Security 10.1 для Windows Server поместил на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server вылечил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и других объектов, которые Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server удалил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Security 10.1 для Windows Server 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 Security 10.1 для Windows Server поместил в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotBackedUp	Общее количество зараженных и других объектов, которые Kaspersky Security 10.1 для Windows Server пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

Ловушки SNMP

Параметры ловушек SNMP Kaspersky Security 10.1 для Windows Server описаны в таблице ниже.

Таблица 87. Ловушки SNMP Kaspersky Security 10.1 для Windows Server

Ловушка	Описание	Параметры
eventThreatDetected	Обнаружен объект.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Превышен максимальный размер резервного хранилища. Общий объем данных в папке резервного хранилища превысил значение, указанное параметром **Максимальный размер резервного хранилища**. Kaspersky Security 10.1 для Windows Server продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Достигнут порог свободного места в резервном хранилище. Размер свободного пространства в папке резервного хранилища, заданный параметром **Порог доступного пространства**, уменьшился до указанного значения. Kaspersky Security 10.1 для Windows Server продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource

Ловушка	Описание	Параметры
eventQuarantineStorageSizeExceeds	Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром **Максимальный размер карантина**. Kaspersky Security 10.1 для Windows Server продолжает помещать возможно зараженные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Достигнут порог свободного места в карантине. Размер свободного пространства в папке карантина, заданный параметром **Порог доступного пространства в карантине**, уменьшился до указанного значения. Kaspersky Security 10.1 для Windows Server продолжает помещать возможно зараженные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Ошибка карантина.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Ошибка сохранения копии объекта в резервном хранилище.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Ошибка карантина.	eventSeverity eventDateAndTime eventSource eventReason

Ловушка	Описание	Параметры
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 Security 10.1 для Windows Server запущен.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security 10.1 для Windows Server остановлен.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Проверка важных областей не проводилась давно. Рассчитывается количество дней с момента последнего завершения задачи, имеющей статус *Задача проверки важных областей*.	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

Ловушка	Описание	Параметры
eventTaskInternalError	Ошибка выполнения задачи.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Ошибка выполнения задачи обновления.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

В таблице ниже описаны параметры ловушек и возможные значения параметров.

Таблица 88. Значения параметров ловушек SNMP

Параметр	Описание и возможные значения
eventDateAndTime	Время возникновения события.
eventSeverity	Уровень важности события. Параметр принимает следующие значения: • critical (1) – критический, • warning (2) – предупреждение, • info (3) – информационный.
userName	Имя пользователя (например, пользователя, который пытался получить доступ к зараженному файлу).
computerName	Имя сервера (например, сервера, с которого пользователь пытался получить доступ к зараженному файлу).
eventSource	Источник события: функциональный компонент, в работе которого возникло событие. Параметр принимает следующие значения: • unknown (0) – функциональный компонент не определен; • quarantine (1) – Карантин; • backup (2) – Резервное хранилище; • reporting (3) – Журналы выполнения задач; • updates (4)– Обновление; • realTimeProtection (5) – Постоянная защита файлов; • onDemandScanning (6) – Проверка по требованию; • product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Security 10.1 для Windows Server в целом; • systemAudit (8) – Журнал системного аудита.

Параметр	Описание и возможные значения
eventReason	Причина возникновения события. Параметр принимает следующие значения: • reasonUnknown (0) – причина не определена, • reasonInvalidSettings (1) – только для событий резервного хранилища и карантина; отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав для доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Security 10.1 для Windows Server будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
objectName	Имя объекта (например, имя файла, в котором обнаружена угроза).
threatName	Имя обнаруженного объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Security 10.1 для Windows Server возвращает при обнаружении объекта. Полное имя обнаруженного объекта можно просмотреть в журнале выполнения задач (см. раздел "Настройка параметров журналов" на стр. 171).
detectType	Тип обнаруженного объекта. Параметр принимает следующие значения: • undefined (0) – не определен; • virware – классические вирусы и сетевые черви; • trojware – троянские программы; • malware – прочие вредоносные программы; • adware – рекламные программы; • pornware – порнографические программы; • riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным.
detectCertainty	Степень уверенности обнаружения угрозы. Параметр принимает следующие значения: • Suspicion (возможно зараженный) – Kaspersky Security 10.1 для Windows Server обнаружил частичное совпадение участка кода объекта с известным вредоносным кодом. • Sure (зараженный) – Kaspersky Security 10.1 для Windows Server обнаружил полное совпадение участка кода объекта с известным вредоносным кодом.
days	Количество дней (например, количество дней до окончания срока действия лицензии).
errorCode	Код ошибки.

Параметр	Описание и возможные значения
knowledgeBaseId	Адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
taskName	Имя задачи.
updaterErrorEventReason	Причина, по которой обновление не было применено. Параметр принимает следующие значения: • reasonUnknown (0) – причина не определена, • reasonAccessDenied – доступ запрещен; • reasonUrlsExhausted – список источников обновлений исчерпан; • reasonInvalidConfig – неправильный файл конфигурации; • reasonInvalidSignature – неверная подпись; • reasonCantCreateFolder – невозможно создать папку; • reasonFileOperError – файловая ошибка; • reasonDataCorrupted – объект поврежден; • reasonConnectionReset – сброс соединения; • reasonTimeOut – истекло время ожидания при соединении; • reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере; • reasonServerAuthError – ошибка проверки подлинности на сервере; • reasonHostNotFound – компьютер не найден; • reasonServerBusy – сервер недоступен; • reasonConnectionError – ошибка соединения; • reasonModuleNotFound – объект не найден; • reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.

Параметр	Описание и возможные значения
storageObjectNotAddedEventReason	Причина непомещения объекта в резервное хранилище или на карантин. Параметр принимает следующие значения: • reasonUnknown (0) – причина не определена, • reasonStorageInternalError – ошибка базы данных; восстановите Kaspersky Security 10.1 для Windows Server. • reasonStorageReadOnly – база данных доступна только для чтения; восстановите Kaspersky Security 10.1 для Windows Server. • reasonStorageIOError – ошибка ввода-вывода: а) Kaspersky Security 10.1 для Windows Server поврежден, восстановите Kaspersky Security 10.1 для Windows Server; б) диск, на котором хранятся файлы Kaspersky Security 10.1 для Windows Server, поврежден. • reasonStorageCorrupted – хранилище повреждено; восстановите Kaspersky Security 10.1 для Windows Server. • reasonStorageFull – база данных полна; освободите место на диске. • reasonStorageOpenError – не удалось открыть файл базы данных; восстановите Kaspersky Security 10.1 для Windows Server. • reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Security 10.1 для Windows Server. • reasonObjectNotFound – помещаемый в хранилище объект отсутствует на диске. • reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator. • reasonDiskOutOfSpace – недостаточно места на диске.

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help.).

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Security 10.1 для Windows Server и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять компьютер на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки компьютера.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность обработки и сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем защиты компьютеров от цифровых угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня “Лаборатория Касперского” – это международная группа компаний с 38 офисами в 33 стране мира. В компании работает более 3 000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: 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, а количество организаций, являющихся ее клиентами, превышает 270 000.

Веб-сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru
Вирусная лаборатория:	http://newvirus.kaspersky.ru/ (для проверки подозрительных файлов и веб-сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.ru

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Citrix, XenApp и XenDesktop – товарные знаки Citrix Systems, Inc. и/или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Dell и Dell Compellent – товарные знаки Dell, Inc.

Celerra, EMC, Isilon, OneFS и VNX – товарные знаки или зарегистрированные в США и/или других странах товарные знаки EMC Corporation.

Hitachi – товарный знак Hitachi, Ltd.

IBM и System Storage – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Excel, Hyper-V, JScript, Microsoft, Outlook, PowerShell, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

NetApp и Data ONTAP товарные знаки или зарегистрированные в США и/или других странах товарные знаки NetApp, Inc.

Oracle – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Глоссарий

K

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

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.

S

SIEM

Решение для управления информацией и событиями в системе безопасности организации.

A

Активный ключ

Ключ, используемый программой в данный момент.

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.

З

Задача

Функции, выполняемые программой “Лаборатории Касперского», реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера, Обновление баз программы.

Зараженный объект

Объект, 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.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

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 нуля 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.

Подозрительные объекты

Объект внутри которого содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный “Лаборатории Касперского”. Обнаружение подозрительных объектов выполняется с помощью эвристического анализатора.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Помещать на 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.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или возможно зараженные, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве “контейнера” для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, 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.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

У

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют четыре уровня важности:

- Критические события.
- Отказ функционирования.
- Предупреждение.
- Информационное событие.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы “Лаборатории Касперского». Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

Предметный указатель

Д

П