Kaspersky Security 10.1.2 для Windows Server

643.46856491.00084-04 90 02

Руководство пользователя

Версия программы: 10.1.2.996

Уважаемый пользователь!

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

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

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

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

Документ может быть изменен без предварительного уведомления.

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

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

Дата редакции документа: 10.05.2019

Обозначение документа: 643.46856491.00084-04 90 02

© 2018 АО "Лаборатория Касперского" Все права защищены.

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

Содержание

Об этом документе 8
Источники информации о Kaspersky Security для Windows Server 9
О программе 10
Интерфейс Kaspersky Security для Windows Server 11
Интерфейс Консоли программы 11
Значок Kaspersky Security для Windows Server в области уведомлений панели задач 15
Диагностическое окно 16
О диагностическом окне 16
Просмотр статуса Kaspersky Security для Windows Server через диагностическое окно 17
Текущая активность программы 18
Настройка записи файлов дампа и трассировки 20
Запуск и остановка Kaspersky Security для Windows Server 21
Запуск Консоли программы из меню Пуск 21
Запуск и остановка службы Kaspersky Security 22
Просмотр состояния защиты и информации о Kaspersky Security для Windows Server 23
Права доступа к функциям Kaspersky Security для Windows Server 29
О правах на управление Kaspersky Security для Windows Server 29
О правах на управление регистрируемыми службами 31
Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security для Windows Server 31
Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля 34
Работа с Консолью программы 35
О Консоли программы 35
Параметры работы Kaspersky Security для Windows Server в Консоли 36
Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере 43
Лицензирование 44
Настройка доверенной зоны 45
О доверенной зоне Kaspersky Security для Windows Server 45
Включение и выключение применения доверенной зоны в задачах Kaspersky Security для Windows Server 47
Добавление исключений в доверенную зону 47
Доверенные процессы 48
Удаление процесса из списка доверенных 50
Выключение постоянной защиты файлов на время резервного копирования 50
Управление задачами Kaspersky Security для Windows Server 51
Категории задач Kaspersky Security для Windows Server 51
Сохранение задачи после изменения ее параметров 52
Запуск / приостановка / возобновление / остановка задачи вручную 52
Работа с расписанием задач 53

Настройка параметров расписания запуска задач 53
Включение и выключение запуска по расписанию 54
Использование учетных записей для запуска задач 55
Об использовании учетных записей для запуска задач 55
Указание учетной записи для запуска задачи 56
Импорт и экспорт параметров 56
Об импорте и экспорте параметров 57
Экспорт параметров 58
Импорт параметров 59
Использование шаблонов параметров безопасности 60
О шаблонах параметров безопасности 60
Создание шаблона параметров безопасности 61
Просмотр параметров безопасности в шаблоне 61
Применение шаблона параметров безопасности 62
Удаление шаблона параметров безопасности 63
Постоянная защита сервера 64
Постоянная защита файлов. 64
О задаче Постоянная защита файлов 64
Статистика задачи Постоянная защита файлов 65
Настройка параметров задачи Постоянная защита файлов 68
Область защиты в задаче Постоянная защита файлов 76
Использование KSN 88
О задаче Использование KSN 88
Настройка параметров задачи Использование KSN 90
Настройка обработки данных 92
Статистика задачи Использование KSN 94
Защита от эксплойтов 95
О Защите от эксплойтов 96
Настройка параметров защиты памяти процессов 97
Добавление защищаемого процесса 98
Техника снижения рисков 100
Проверка скриптов 101
О задаче Проверка скриптов 101
Настройка параметров задачи Проверка скриптов 101
Статистика задачи Проверка скриптов 103
Защита трафика 104
О задаче Защита трафика 104
О правилах веб-контроля 106
Защита от почтовых угроз 106
Настройка задачи Защита трафика 107
Настройка защиты от вредоносных программ, передающихся через веб-трафик 114

Настройка защиты от почтовых угроз 117
Настройка обработки веб-адресов 118
Настройка веб-контроля 120
Контроль сервера 128
Контроль запуска программ 128
О задаче Контроль запуска программ 128
Настройка параметров задачи Контроль запуска программ 130
О правилах контроля запуска программ 140
О формировании списка правил контроля запуска программ 144
О задаче Формирование правил контроля запуска программ 149
Защита от шифрования 155
О задаче Защита от шифрования 156
Статистика задачи Защита от шифрования 156
Настройка параметров задачи Защита от шифрования 157
Диагностика системы 161
Мониторинг файловых операций 161
О задаче Мониторинг файловых операций 161
О правилах мониторинга файловых операций 162
Настройка параметров задачи Мониторинг файловых операций 166
Настройка правил мониторинга 167
Анализ журналов 170
О задаче Анализ журналов 170
Настройка параметров предзаданных правил задачи 172
Настройка правил анализа журналов 173
Проверка по требованию 175
О задачах проверки по требованию 175
Статистика задач проверки по требованию 176
Настройка параметров задач проверки по требованию 179
Применение эвристического анализатора 184
Выполнение задачи проверки по требованию в фоновом режиме 185
Использование KSN 185
Регистрация выполнения проверки важных областей 186
Область проверки в задачах проверки по требованию 186
Об области проверки 187
Настройка параметров отображения файловых ресурсов области проверки 187
Предопределенные области проверки 188
Формирование области проверки 189
Включение в область проверки сетевых объектов 191
Создание виртуальной области проверки 192
Параметры безопасности выбранного узла в задачах проверки по требованию 193
Выбор предустановленных уровней безопасности в задачах проверки по требованию 194

Настройка параметров безопасности вручную 196
Проверка съёмных дисков 201
Создание задачи проверки по требованию 202
Удаление задачи 205
Переименование задачи 205
Обновление баз и модулей Kaspersky Security для Windows Server 206
О задачах обновления 206
Об обновлении модулей Kaspersky Security для Windows Server 207
Об обновлении баз Kaspersky Security для Windows Server 208
Схемы обновления баз и модулей антивирусных программ в организации 208
Настройка задачи Обновление 212
Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server 212
Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы 215
Настройка параметров задачи Копирование обновлений 216
Настройка параметров задачи Обновление модулей программы 217
Откат обновления баз Kaspersky Security для Windows Server 218
Откат обновления программных модулей 218
Статистика задач обновления 219
Изолирование и резервное копирование объектов 220
Изолирование возможно зараженных объектов. Карантин 220
Об изолировании возможно зараженных объектов 220
Просмотр объектов на карантине 221
Проверка карантина 222
Восстановление содержимого карантина 224
Помещение объектов на карантин 226
Удаление объектов из карантина 226
Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" 226
Настройка параметров карантина 228
Статистика карантина 229
Резервное копирование объектов. Резервное хранилище: 229
О резервном копировании объектов перед лечением / удалением 230
Просмотр объектов в резервном хранилище 230
Восстановление файлов из резервного хранилища 232
Удаление файлов из резервного хранилища 234
Настройка параметров резервного хранилища 234
Статистика резервного хранилища 236
Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы 236
О блокировании доступа к сетевым файловым ресурсам 236
Включение блокирования доступа к сетевым файловым ресурсам 237
Настройка параметров заблокированных компьютеров 238

Регистрация событий. Журналы Kaspersky Security для Windows Server 240
Способы записи событий Kaspersky Security для Windows Server 240
Журнал системного аудита 241
Сортировка событий в журнале системного аудита 241
Фильтрация событий в журнале системного аудита 241
Удаление событий из журнала системного аудита 242
Журналы выполнения задач 243
О журналах выполнения задач 243
Просмотр списка событий в журналах выполнения задач 244
Сортировка событий в журналах выполнения задач 244
Фильтрация событий в журналах выполнения задач 244
Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач 245
Экспорт информации из журнала выполнения задачи 246
Удаление событий из журналов выполнения задач 246
Журнал событий безопасности 247
Просмотр журнала событий Kaspersky Security для Windows Server в консоли Просмотр событий 247
Настройка параметров журналов в Консоли программы 248
Об интеграции с SIEM 250
Настройка параметров интеграции с SIEM 251
Настройка уведомлений 254
Способы уведомления администратора и пользователей 254
Настройка уведомлений администратора и пользователей 255
Управление Иерархическим хранилищем 258
Об иерархическом хранилище 258
Настройка параметров HSM-системы 259
Обращение в Службу технической поддержки 260
Способы получения технической поддержки 260
Техническая поддержка через Kaspersky CompanyAccount 260
Использование файла трассировки и скрипта AVZ 261
АО "Лаборатория Касперского" 262
Информация о стороннем коде 264
Уведомления о товарных знаках 265
Глоссарий 266
Предметный указатель 271
Соответствие терминов 275
Приложение 276
Сертифицированное состояние программы: параметры и их значения 276

Об этом документе

Этот документ содержит руководство по эксплуатации программного изделия «Kaspersky Security 10.1.2 для Windows Server» (далее также «Kaspersky Security для Windows Server», «программа»).

Разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, которые осуществляют администрирование Консоли Kaspersky Security для Windows Server (далее также "Консоль программы") на защищаемом сервере.

Источники информации о Kaspersky Security для Windows Server

Приведенные ниже источники не являются эквивалентом настоящего документа и могут отличаться. Для корректной работы с программой рекомендуется использовать настоящее руководство.

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

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

Страница Kaspersky Security для Windows Server в Базе знаний

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

На странице Kaspersky Security 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 для Windows Server, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" на форуме

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

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

Документация Kaspersky Security для Windows Server

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

О программе

Программное изделие «Kaspersky Security для Windows Server», представляющее собой средство антивирусной защиты типа «Б» второго класса защиты, предназначенное для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Security для Windows Server, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы;
- контроль запуска приложений;
- выполнение проверок сообщений электронной почты (антифишинг);
- контроль выполнения файловых операций;
- защита от эксплойтов;
- контроль загрузки веб-страниц.

Интерфейс Kaspersky Security для Windows Server

Этот раздел содержит информацию об основных элементах интерфейса программы.

В этом разделе

Интерфейс Консоли программы 11

Значок Kaspersky Security для Windows Server в области уведомлений панели задач 15

Диагностическое окно 16

Интерфейс Консоли программы

Консоль программы отображается в дереве Microsoft Management Console в виде узла с именем **Kaspersky Security**.

После подключения к Kaspersky Security для Windows Server, установленному на другом сервере, в название узла добавляется имя сервера, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Security <имя компьютера> как <имя учетной записи>**. При подключении к Kaspersky Security для Windows Server, установленному на том же сервере, что и Консоль программы, название узла имеет вид: **Kaspersky Security**.

По умолчанию окно Консоли программы содержит следующие элементы:

- Дерево Консоли;
- панель результатов;
- панель быстрого доступа;
- панель инструментов.

Также вы можете включить отображение в окне Консоли программы области описания и панели действия.

Дерево Консоли

В дереве Консоли отображается узел Kaspersky Security и вложенные в него узлы функциональных компонентов программы.

В состав узла **Kaspersky Security** входят следующие вложенные узлы:

- **Постоянная защита**: управление постоянной защитой файлов и параметрами использования служб KSN. Узел Постоянная защита позволяет управлять следующими задачами:
  - **Постоянная защита файлов**
  - **Проверка скриптов**
  - **Использование KSN**
  - **Защита трафика**

- **Контроль сервера**: контроль подключаемых устройств, а также контроль программ, запускаемых на защищаемом сервере. Узел Контроль сервера позволяет управлять следующими задачами:
  - **Защита от шифрования**
  - **Контроль запуска программ**
- **Автоматическая генерация правил**: настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ и Контроль устройств.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имя задач>** (если есть).

    Групповые задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. 51) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль программы.
- **Диагностика системы**: настройка контроля файловых операций и анализа системного журнала операционной системы.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Защита сетевых хранилищ:** настройка задач, контролирующих безопасность сетевых хранилищ.
  - **Защита RPC-подключаемых сетевых хранилищ**
  - **Защита ICAP-подключаемых сетевых хранилищ**
  - **Защита от шифрования для NetApp**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка объектов на карантине**
  - **проверка целостности программы**
  - Пользовательские задачи **<Имя задач>** (если есть).

    В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. 51), созданные при установке программы, добавленные пользовательские задачи, а также групповые задачи проверки по требованию, сформированные и переданные на компьютер с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Security для Windows Server, а также копированием обновлений для сохранения их в папке локального источника обновлений. Узел содержит вложенные узлы для управления каждой задачей обновления и задачей отката последнего обновления баз программы:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

В узле отображаются все пользовательские и групповые задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. 51) обновления, сформированные и переданные на компьютер с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами карантина, резервного хранилища и заблокированных компьютеров.
  - **Карантин**
  - **Резервное хранилище**
  - **Заблокированные узлы**
- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом событий безопасности и журналом системного аудита Kaspersky Security для Windows Server.
  - **Журнал событий безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование**: добавление и удаление ключей и кодов активации Kaspersky Security для Windows Server, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел Kaspersky Security, в панели отображается информация о текущем состоянии защиты сервера (см. раздел "Просмотр состояния защиты и информации о Kaspersky Security для Windows Server" на стр. 23), информация о Kaspersky Security для Windows Server, состоянии его функциональных компонентов и статусе лицензии или ключа.

Контекстное меню узла Kaspersky Security

С помощью пунктов контекстного меню узла **Kaspersky Security** вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключитесь к другому компьютеру (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере" на стр. 43), чтобы управлять установленным на нем Kaspersky Security для Windows Server. Для выполнения этой операции вы также можете воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Security**.
- **Запустить программу** / **Остановить программу**. Запустить или остановить программу или выбранную задачу (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 52). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Параметры проверки съёмных дисков**. Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. 201), подключенных к защищаемому компьютеру через USB-порт.
- **Защита от эксплойтов: общие параметры**. Настроить режим защиты от эксплойтов и профилактические действия (см. раздел "Настройка параметров защиты памяти процессов" на стр. 97).
- **Защита от эксплойтов: параметры защиты процессов**. Добавить процессы, которые нужно защитить (см. раздел "Добавление процессов для защиты" на стр. 98) и выбрать техники снижения рисков (см. раздел "Техники снижения рисков" на стр. 100).
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны (см. раздел "О доверенной зоне Kaspersky Security для Windows Server" на стр. 45).

- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Security для Windows Server (см. раздел "Права доступа к функциям Kaspersky Security для Windows Server" на стр. 29).
- **Изменить права пользователей на управление службой Kaspersky Security**. Просмотреть и настроить права пользователя на управление Kaspersky Security Service (см. раздел "Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service" на стр. 31).
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел "Экспорт параметров" на стр. 58). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла в формате XML (см. раздел "Импорт параметров" на стр. 59). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Security для Windows Server и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Security для Windows Server или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Security** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Security для Windows Server. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель быстрого доступа и контекстное меню задач Kaspersky Security для Windows Server

Вы можете управлять задачами Kaspersky Security для Windows Server с помощью пунктов контекстного меню каждой задачи в дереве Консоли.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Возобновить / Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 52). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты и задач проверки по требованию.
- **Добавить задачу**. Создать новую пользовательскую задачу (см. раздел "Создание задачи проверки по требованию" на стр. 202). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. 243). Операция доступна для всех задач.
- **Сохранить задачу**. Сохранить и применить измененные параметры задачи (см. раздел "Сохранение задачи после изменения ее параметров" на стр. 52). Операция доступна для задач постоянной защиты файлов и задач проверки по требованию.
- **Удалить задачу**. Удалить пользовательскую задачу (см. раздел "Удаление задачи" на стр. 205). Операция доступна для задач проверки по требованию.

- **Статистика**. Перейти к просмотру статистики задачи. Операция доступна для задачи проверки целостности программы.
- **Шаблоны параметров**. Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. 60). Операция доступна для задач постоянной защиты файлов и проверки по требованию.

Значок Kaspersky Security для Windows Server в области уведомлений панели задач

Каждый раз, когда Kaspersky Security для Windows Server автоматически запускается после перезагрузки защищаемого компьютера, в области уведомлений панели задач отображается значок Kaspersky Security для Windows Server . Он отображается по умолчанию, если при установке программы вы установили компонент **Значок области уведомлений Kaspersky Security для Windows Server**.

Внешний вид значка области уведомлений Kaspersky Security для Windows Server является индикатором текущего состояния защиты сервера. Значок Kaspersky Security для Windows Server может иметь одно из следующих состояний:

- активное (цветной значок), если в текущий момент выполняется хотя бы одна из задач: Постоянная защита файлов, Контроль запуска программ, Проверка скриптов.
- неактивное (черно-белый значок), если в текущий момент не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ, Проверка скриптов.

Вы можете открыть контекстное меню значка Kaspersky Security для Windows Server по правой клавише мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон программы (см. таблицу ниже).

Таблица 1. Команды контекстного меню значка области уведомлений Kaspersky Security для Windows Server

Команда	Описание
Запустить Консоль программы	Открывает Консоль программы (если она установлена).
Посмотреть статус сервера	Откройте диагностическое окно.
О программе	Открывает окно О программе с информацией о Kaspersky Security для Windows Server. Если вы зарегистрированы в качестве пользователя Kaspersky Security для Windows Server, окно О программе содержит информацию об установленных срочных обновлениях.
Скрыть	Скрывает значок Kaspersky Security для Windows Server в области уведомлений панели задач.

Вы можете снова отобразить скрытый значок Kaspersky Security для Windows Server в любой момент.

► *Чтобы снова отобразить значок программы,*

в меню **Пуск** Microsoft Windows выберите Программы → Kaspersky Security для Windows Server → **Значок Kaspersky Security**.

Названия параметров могут отличаться в разных операционных системах Windows.

В параметрах программы вы можете включать и выключать отображение значка Kaspersky Security для Windows Server в области уведомлений при автоматическом запуске программы после перезагрузки сервера.

Диагностическое окно

В этом разделе описано, как использовать диагностическое окно для просмотра статуса или текущей активности сервера и как настраивать запись файла дампа и файла трассировки.

В этом разделе

О диагностическом окне 16
Просмотр статуса Kaspersky Security для Windows Server через диагностическое окно 17
Текущая активность программы 18
Настройка записи файлов дампа и трассировки 20

О диагностическом окне

Компонент Диагностическое окно устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы, и может быть использован, даже если Консоль программы не установлена на защищаемом сервере. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на сервере.

В диагностическом окне можно выполнять следующие действия:

- Просматривать информацию об общем статусе программы (см. раздел "Просмотр статуса Kaspersky Security для Windows Server через диагностическое окно" на стр. 17).
- Просматривать текущую активность (см. раздел "Текущая активность программы" на стр. 18) на защищаемом сервере.
- Запускать и останавливать запись файлов дампа и трассировки (см. раздел "Настройка записи файлов дампа и трассировки" на стр. 20).
- Открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Если доступ к функциям Kaspersky Security для Windows Server защищен паролем, диагностическое окно предложит вам ввести пароль.

Диагностическое окно нельзя настроить через Kaspersky Security Center.

Просмотр статуса Kaspersky Security для Windows Server через диагностическое окно

► *Чтобы открыть диагностическое окно, выполните следующие действия:*

1. Щелкните правой кнопкой мыши значок Kaspersky Security для Windows Server в области уведомлений панели задач.
2. Выберите пункт **Посмотреть статус сервера**.

   Откроется **диагностическое окно**.
3. Вы можете просмотреть текущий статус лицензии и задач Постоянная защита и Обновление на закладке **Статус защиты**. Каждый из блоков на панели статуса может принимать следующие значения:

Таблица 2. Значения панели статуса диагностического окна.

Блок	Статус

Постоянная защита	*Зеленый цвет* панели отображается в следующих ситуациях (при выполнении любого количества условий):
	• Рекомендуемая конфигурация:
	  • Задача Постоянная защита файлов запущена с параметрами по умолчанию.
	  • Задача Контроль запуска программ запущена в режиме **Применять правила контроля запуска программ** и с параметрами по умолчанию.
	• Приемлемая конфигурация:
	  • Задача Постоянная защита файлов настроена пользователем.
	  • Параметры задачи Контроль запуска программ изменены.

	Желтый цвет панели отображается в следующих случаях (выполнено одно или несколько условий): • Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию). • Задача Контроль запуска программ запущена в режиме **Только статистика**. • Задачи Защита от эксплойтов и Контроль запуска программ запущены в режиме **Только статистика**.
	Красный цвет панели отображается в следующем случае (выполнены оба условия): • Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена. • Компонент Контроль запуска программ не установлен или задача запущена в режиме **Только статистика**.
Лицензирование	*Зеленый цвет* панели отображается, если текущая лицензия действительна.

Блок	Статус
	Желтый цвет панели отображается, если возникло одно из следующих событий: • **Выполняется проверка статуса лицензии**. • **До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации**. • **Добавленный ключ помещен в черный список и скоро будет заблокирован**. • **Подписка приостановлена**.
	Красный цвет отображается, если возникло одно из следующих событий: • **Программа не активирована.** • **Срок действия лицензии истек.** • **Нарушено Лицензионное соглашение.** • **Ключ помещен в черный список.**
Обновление	*Зеленый цвет* панели отображается в следующем случае: • Базы обновлены.
	Желтый цвет панели отображается в следующем случае: • Базы устарели.
	Красный цвет панели отображается в следующем случае: • Базы сильно устарели.

Текущая активность программы

На этой закладке вы можете просматривать статус текущих задач и процессов программы, а также получать динамические сообщения о происходящих критических событиях.

Для отображения статуса активности программы используется цветовая индикация:

- В блоке **Задачи**:
  - *Зеленый цвет*. Не выполнены условия для желтого или красного цветов.
  - *Желтый цвет*. Проверка важных областей давно не выполнялась.
  - *Красный цвет*. Выполнено какое-либо из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В блоке **Службы Kaspersky Security Network**:
  - *Зеленый цвет*. Задача запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

► *Чтобы просмотреть текущую активность программы на сервере, выполните следующие действия:*

1. Щелкните правой кнопкой мыши значок Kaspersky Security для Windows Server в области уведомлений панели задач.
2. Выберите пункт **Посмотреть статус сервера**.

   Откроется **диагностическое окно**.
3. Откройте закладку **Текущая активность программы**.
4. В блоке **Задачи** можно просмотреть следующую информацию:
   - **Проверка важных областей давно не выполнялась**.

     Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
   - **Выполняются сейчас.**
   - **Завершены с ошибкой.**
   - **Следующий запуск определен по расписанию.**
5. В блоке **Службы Kaspersky Security Network** можно просмотреть следующую информацию:
   - **Используется / Не используется / Используется с заключениями для файлов и веб-адресов.**
   - **Статистика программы отправляется в KSN.**

     Программа отправляет данные об обнаружениях вредоносных программ, в том числе ложных, в ходе выполнения задач постоянной защиты и проверки по требованию, а также отладочную информацию о сбоях при проверке.

     Поле отображается, если в параметрах задачи Использование KSN установлен флажок **Отправлять статистику по событиям работы программы**.
   - **Служба Kaspersky Managed Protection включена.**

     Если флажок установлен, служба KMP включена.

     Если флажок снят, служба KMP выключена.

     Служба доступна пользователям Kaspersky Security for Business и Kaspersky Anti Targeted Attack Platform, которые приняли дополнительное соглашение об использовании службы KMP.

     Служба обнаруживает и предотвращает направленные атаки на сервер. Служба включает круглосуточное наблюдение экспертов "Лаборатории Касперского" и непрерывный анализ данных о киберугрозах для постоянного обнаружения как известных, так и новых кампаний кибершпионов и киберпреступников, направленных на критические информационные системы.
6. В блоке **Интеграция с Kaspersky Security Center** можно просмотреть следующую информацию:
   - Локальное управление разрешено.
   - Применяется политика: <имя сервера Kaspersky Security Center>.
7. Закройте **диагностическое окно**.

Настройка записи файлов дампа и трассировки

В диагностическом окне можно настроить запись файлов дампа и трассировки.

Вы также можете настроить запись диагностики сбоев (см. раздел "Параметры работы Kaspersky Security для Windows Server в Консоли» на стр. 36) в Консоли программы.

► *Чтобы запустить запись файлов дампа и трассировки, выполните следующие действия:*

1. Щелкните правой кнопкой мыши значок Kaspersky Security для Windows Server в области уведомлений панели задач.
2. Выберите пункт **Посмотреть статус сервера**.

   Откроется **диагностическое окно**.
3. Откройте закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
   a. Установите флажок **Записывать отладочную информацию в файл трассировки**.
   b. Нажмите кнопку **Обзор** и укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы трассировки.
5. Если требуется, настройте следующие параметры дампа:
   a. Установите флажок **Создавать во время сбоя файл дампа**.
   b. Нажмите кнопку **Обзор** и укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы дампа.
6. Нажмите кнопку **Применить**.

   Новая конфигурация будет применена.

Запуск и остановка Kaspersky Security для Windows Server

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security Service.

В этом разделе

Запуск Консоли программы из меню Пуск 21

Запуск и остановка службы Kaspersky Security Service 22

Запуск Консоли программы из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль программы из меню Пуск:*

в меню **Пуск** выберите **Программы** → **Kaspersky Security для Windows Server** → **Средства администрирования** → **Консоль программы**.

Если вы планируете добавлять в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► *Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы** → **Kaspersky Security для Windows Server** → **Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.

Консоль программы будет запущена в авторском режиме.

Если вы запустили Консоль на защищаемом сервере, откроется окно Консоли (см. раздел "Интерфейс Kaspersky Security для Windows Server" на стр. 8).

Если вы запустили Консоль программы не на защищаемом сервере, а на другом компьютере, подключитесь к защищаемому серверу.

► *Чтобы подключиться к защищаемому серверу, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите команду **Подключиться к другому компьютеру**.

   Откроется окно **Выбор компьютера**.
3. В открывшемся окне выберите **Другой компьютер**.

4. В поле ввода справа укажите сетевое имя защищаемого сервера.
5. Нажмите на кнопку **OK**.

Консоль программы будет подключена к защищаемому серверу.

Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management Service на сервере, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

Запуск и остановка службы Kaspersky Security

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

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

Если вы остановите службу Kaspersky Security Service, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security Service, программа автоматически запустит только задачи, в расписании которых указана частота запуска При запуске программы, остальные задачи требуется запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security Service с помощью контекстного меню узла Kaspersky Security или с помощью оснастки Службы Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Security для Windows Server, если вы входите в группу "Администраторы" на защищаемом сервере.

► *Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите одну из следующих команд:
   - **Остановить программу**, чтобы остановить службу Kaspersky Security Service;
   - **Запустить программу**, чтобы запустить службу Kaspersky Security Service.

Служба Kaspersky Security Service будет запущена или остановлена.

Просмотр состояния защиты и информации о Kaspersky Security для Windows Server

► *Чтобы просмотреть информацию о состоянии защиты сервера и информацию о Kaspersky Security для Windows Server,*

выберите узел **Kaspersky Security** в дереве Консоли программы.

По умолчанию информация в панели результатов Консоли программы обновляется автоматически:

- каждые 10 сек. при локальном подключении;
- каждые 15 сек. при удаленном подключении.

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле Kaspersky Security,*

в контекстном меню узла **Kaspersky Security** выберите пункт **Обновить**.

В панели результатов Консоли отображается следующая информация о программе:

- Статус использования Kaspersky Security Network;
- состояние защиты сервера;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля сервера;
- данные о лицензии;
- статус интеграции с Kaspersky Security Center: данные компьютера с установленным Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В блоке **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется, Остановлена* или *Не выполнялась*. Индикатор может принимать следующие значения:

- Зеленый цвет панели означает, что задача Использование KSN выполняется, и запросы репутации веб-адресов отправляются в KSN.
- Желтый цвет панели означает, что принятой одной из Положений, но задача не выполняется, или запросы репутации веб-адресов не отправляются в KSN.

Закладка Защита сервера

Блок **Защита сервера** (см. таблицу ниже) отображает информацию о текущем состоянии защиты сервера.

Таблица 3. Информация о состоянии защиты сервера

Блок Защита сервера	Информация
Индикатор статуса защиты сервера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что задачи постоянной защиты выполняются, а задача проверки важных областей завершилась не более 30 дней назад (по умолчанию). • Желтый цвет панели – одна или несколько задач постоянной защиты не запущены или остановлены, а задача проверки важных областей давно не выполнялась. • Красный цвет панели – задачи постоянной защиты файлов не выполняются.
Постоянная защита файлов	**Статус задачи** – текущее состояние задачи, например, Выполняется или Остановлена. **Обнаружено** – количество объектов, которые обнаружил Kaspersky Security для Windows Server. Например, если Kaspersky Security для Windows Server обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ превышает 0, значение выделяется красным цветом.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз компьютерной безопасности. *Не проводилась* – событие, которое возникает, если задача проверки важных областей выполнялась 30 и более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.
Резервные копии объектов	*Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если порог доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Security для Windows Server при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом. *Превышен максимальный размер резервного хранилища* – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Security для Windows Server при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом. **Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище в текущий момент. **Используемое пространство** – объем используемого пространства в резервном хранилище.
Защита от эксплойтов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: • Завершать скомпрометированные процессы. • Только сообщать об эксплойте. **Процессов защищено** – общее количество процессов, которые находятся под защитой и обрабатываются в соответствие с выбранным режимом.

Блок **Обновление** (см. таблицу ниже) отображает информацию об актуальности антивирусных баз и модулей программы.

Таблица 4. Информация о состоянии баз и модулей Kaspersky Security для Windows Server

Блок Обновление	Информация
Индикатор состояния баз и модулей программы	Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что базы программы актуальны, а также отсутствуют доступные критические обновления модулей программы. • Желтый цвет панели – означает, что базы устарели, или последняя задача обновления баз программы завершена с ошибкой. • Красный цвет панели – возникло событие *Базы программы сильно устарели* или *Базы повреждены*.
Обновление баз и модулей программы	**Актуальность баз программы** – оценка актуальности баз программы. Параметр может принимать следующие значения: • **Базы программы актуальны** – базы программы обновлены не более чем 7 дней назад (по умолчанию); • **Базы программы устарели** – базы программы обновлены 7–14 дней назад (по умолчанию); • **Базы программы сильно устарели** – базы программы обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий Базы программы устарели и *Базы программы сильно устарели*. **Дата выпуска баз программы** – дата и время выпуска последнего установленного обновления баз программы. Дата и время указаны в UTC. **Статус последней запущенной задачи обновления баз программы** – дата и время последнего обновления базы программы. Дата и время указаны по местному времени защищаемого сервера. Значение в поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*. **Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Security для Windows Server, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Security для Windows Server.

Блок **Контроль** (см. таблицу ниже) отображает информацию о состоянии задач Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

Таблица 5. Информация о состоянии контроля сервера

Блок Контроль	Информация
Сервер Индикатор состояния контроля сервера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что все задачи контроля сервера выполняются. • Желтый цвет панели – задача Защита от шифрования выполняется в режиме Только статистика, или не выполняется любая другая задача контроля сервера. • Красный цвет панели – не выполняется задача Контроль запуска программ или Защита от шифрования.
Контроль запуска программ	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Контроль запуска программ: Активна, Только статистика. **Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Security для Windows Server в ходе выполнения задачи контроля запуск программ. Если количество заблокированных запусков программ превышает 0, значение поля окрашивается в красный цвет. **Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Security для Windows Server для обработки попытки запуска программ на сервере.
Защита от шифрования	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Защита от шифрования. **Компьютеров заблокировано** – количество скомпрометированных компьютеров, заблокированных при попытке подключения к защищаемому серверу.

Блок **Диагностика** (см. таблицу ниже) отображает информацию о состоянии задач Мониторинг файловых операций и Анализ журналов.

Таблица 6. Информация о состоянии диагностики системы

Блок Диагностика	Информация
Индикатор статуса диагностики	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что все задачи функции Мониторинг целостности системы. • Желтый цвет панели – не выполняется одна из задач функции Мониторинг целостности системы; возникает событие *Не выполняется*. • Красный цвет панели – е выполняются обе задачи функции Мониторинг целостности системы.
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированные операции** – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого устройства.
Анализ журналов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Возможных нарушений** – количество зафиксированных нарушений по данным журнала событий Windows, выявленных на основе заданных правил задачи или применения эвристического анализатора.

Информация о лицензии Kaspersky Security для Windows Server (см. раздел "Лицензирование" на стр. 44) отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Security**.

Вы можете настроить свойства Kaspersky Security для Windows Server, перейдя по ссылке Свойства программы (см. раздел "Параметры работы Kaspersky Security для Windows Server в Консоли " на стр. 36).

Вы можете выполнить подключение к другому компьютеру, перейдя по ссылке Подключиться к другому компьютеру (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере" на стр. 43).

Чтобы получить подробные сведения о закладке Защита сетевых хранилищ, см. Руководство по внедрению Kaspersky Security для Windows Server для защиты сетевых хранилищ.

Права доступа к функциям Kaspersky Security для Windows Server

Этот раздел содержит информацию о правах на управление Kaspersky Security 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 для Windows Server 29

О правах на управление регистрируемыми службами 31

Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service 31

Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля 34

О правах на управление Kaspersky Security для Windows Server

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

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

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

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

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

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Security 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 7. Права доступа к функциям Kaspersky Security для Windows Server

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Security для Windows Server.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Возможность импортировать из конфигурационного файла параметры работы Kaspersky Security для Windows Server. • Редактировать настройки программы.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Security для Windows Server и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Security 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 для Windows Server.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Security для Windows Server.
Удаление программы	Возможность удалять Kaspersky Security для Windows Server.
Чтение прав	Возможность просматривать список пользователей Kaspersky Security 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 для Windows Server.

О правах на управление регистрируемыми службами

Подробная информация о регистрируемых службах Windows и настройке доступа к регистрируемым службам содержится в *Руководстве администратора Kaspersky Security для Windows Server.*

При установке Kaspersky Security для Windows Server регистрирует в Windows службу Kaspersky Security Service (KAVFS) и службу управления программой Kaspersky Security Management Service (KAVFSGT).

Служба Kaspersky Security Service

По умолчанию доступ к управлению 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.

Пользователи, которые имеют доступ к функции уровня Изменение прав (см. раздел "Защищенный паролем доступ к функциям Kaspersky Security для Windows Server" на стр. 34), могут предоставлять доступ к управлению Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Служба Kaspersky Security Management Service

Для управления программой через Консоль программы, установленную на другом сервере требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Security для Windows Server, имела полный доступ к Kaspersky Security Management Service на защищаемом сервере.

По умолчанию доступ к управлению 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 для Windows Server.

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

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

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Security 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 программы откройте контекстное меню узла **Kaspersky Security** и 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 для Windows Server.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Security для Windows Server"**.
2. 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**.
3. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security** и выполните одно из следующих действий:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите настроить права доступа к функциям Kaspersky Security для Windows Server.
   - Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите настроить права доступа к службе Kaspersky Security Service.

     Откроется окно **Разрешения для группы "Kaspersky Security для Windows Server"**.
2. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.
3. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Security 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 для Windows Server или службой Kaspersky Security Service.
   - **Чтение**:
     - следующие права на управление Kaspersky Security 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 для Windows Server, кроме **Изменение прав**;
     - следующие права на управление службой Kaspersky Security Service: **Изменение параметров службы, Чтение прав**.
   - **Исполнение**: следующие права на управление службой Kaspersky Security Service: **Запуск службы**, **Остановка службы**, **Приостановка / Возобновление службы**, **Чтение прав**, **Пользовательские запросы к службе**.
6. Если вы хотите выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Security 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 **OK**.
   g. В окне **Дополнительные параметры безопасности для Kaspersky Security для Windows Server** нажмите на кнопку **OK.**
7. В окне **Разрешения для** группы **"Kaspersky Security для Windows Server"** нажмите на кнопку **Применить**.

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

Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля

Более подробную информацию о защите паролем см. в разделе "Защищенный паролем доступ к функциям Kaspersky Security для Windows Server" *Руководства администратора*.

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей (см. раздел "Права доступа к функциям Kaspersky Security для Windows Server" на стр. 29). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Security для Windows Server.

► *Чтобы защитить доступ к функциям Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Security** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. На закладке **Безопасность и надежность** в блоке **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.
3. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям Kaspersky Security для Windows Server.
4. В поле **Подтверждение пароля** введите пароль повторно.
5. Нажмите на кнопку **OK**.

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

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет отключена, и контрольная сумма старого пароля будет удалена. Повторите процесс ввода пароля с новым паролем.

Работа с Консолью программы

Этот раздел содержит информацию о Консоли программы (далее "Консоль") и об управлении программой через Консоль программы, установленную на защищаемом сервере или другом компьютере.

В этом разделе

О Консоли программы 35

Параметры работы Kaspersky Security для Windows Server в Консоли..... 36

Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере 43

О Консоли программы

Консоль программы представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом сервере или на другом компьютере в сети организации. После того как вы установили Консоль программы на другом компьютере (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере" на стр. 43), вам нужно выполнить дополнительную настройку.

Если Консоль программы и программа установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в доставке информации от Kaspersky Security для Windows Server в Консоль программы. Например, после старта какой-либо задачи Kaspersky Security для Windows Server статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы программа установки сохраняет файл kavfs.msc в папке установки и добавляет оснастку Kaspersky Security для Windows Server в список изолированных оснасток Microsoft Windows.

Вы можете открыть Консоль программы из меню **Пуск**. На защищаемом сервере вы также можете открыть Консоль программы с помощью значка Kaspersky Security для Windows Server в области уведомлений панели задач.

Вы можете запустить msc-файл оснастки Kaspersky Security для Windows Server или добавить оснастку программы в существующую консоль Microsoft Management Console как новый элемент в ее дереве (см. раздел "Интерфейс окна Консоли программы" на стр. 11).

В 64-битной версии Microsoft Windows вы можете добавить оснастку Kaspersky Security для Windows Server только в Microsoft Management Console 32-битной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

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

Параметры работы Kaspersky Security для Windows Server в Консоли

Общие параметры и параметры диагностики сбоев Kaspersky Security для Windows Server определяют общие условия работы программы. Эти параметры позволяют регулировать количество рабочих процессов, используемых Kaspersky Security для Windows Server, включать восстановление задач Kaspersky Security для Windows Server после их аварийного завершения, вести журнал трассировки, включать создание файла дампа процессов Kaspersky Security для Windows Server при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров работы программы в Консоли программы недоступна, если в активной политике Kaspersky Security Center установлен запрет на изменение данных параметров.

► *Чтобы настроить параметры работы Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Security** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. В открывшемся окне настройте общие параметры работы Kaspersky Security для Windows Server согласно вашим требованиям:
   - На закладке **Масштабируемость и интерфейс** вы можете настроить следующие параметры:
     - В блоке **Параметры масштабируемости**:
       - Максимальное количество активных процессов, которые Kaspersky Security для Windows Server может запустить.

Таблица 8. Максимальное количество активных процессов.

Параметр	Максимальное количество активных процессов.
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Security для Windows Server. Он устанавливает максимальное количество рабочих процессов, которые программа может запустить одновременно. Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Kaspersky Security для Windows Server к сбоям. Однако, высокое значение этого параметра может снизить общую производительность компьютера и повысить потребление оперативной памяти. В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр **Максимальное количество активных процессов** только для Kaspersky Security для Windows Server на отдельном компьютере (в диалоговом окне **Параметры программы**); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.
Возможные значения:	1 – 8
Значение по умолчанию	Kaspersky Security для Windows Server выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:

Количество процессоров	**Максимальное количество активных процессов.**
1	1
1 < кол-во процессоров < 4	2
4 и более	4

- Количество процессов для постоянной защиты.

Таблица 9. Количество процессов для постоянной защиты.

Параметр	**Количество процессов для постоянной защиты.**
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Security для Windows Server. С помощью этого параметра вы можете устанавливать фиксированное количество процессов, в которых Kaspersky Security для Windows Server будет выполнять задачи постоянной защиты. Более высокое значение этого параметра повысит скорость проверки объектов в задачах постоянной защиты. Однако чем больше рабочих процессов задействует Kaspersky Security для Windows Server, тем больше будет его влияние на общую производительность защищаемого компьютера и его потребление оперативной памяти. В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр **Количество процессов для постоянной защиты** только для Kaspersky Security для Windows Server на отдельном компьютере (в окне **Параметры программы**); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.
Возможные значения:	Возможные значения: 1-N, где N – значение, заданное параметром **Максимальное количество активных процессов**. Если вы установите значение параметра **Количество процессов для постоянной защиты** равным максимальному числу активных процессов, вы снизите влияние Kaspersky Security для Windows Server на скорость файлового обмена компьютеров с компьютером, еще повысив его быстродействие во время постоянной защиты. Однако задачи обновления и задачи проверки по требованию с базовым приоритетом **Средний** (Normal) будут выполняться в уже запущенных рабочих процессах Kaspersky Security для Windows Server. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени. Задачи проверки по требованию с базовым приоритетом **Низкий** (Low) всегда выполняются в отдельном процессе или процессах.
Значение по умолчанию	Kaspersky Security для Windows Server выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере: **Количество процессоров** — **Количество процессов для постоянной защиты.** =1 — 1 >1 — 2

- Количество рабочих процессов для фоновых задач проверки по требованию.

Таблица 10. Количество процессов для фоновых задач проверки по требованию.

Параметр	Количество процессов для фоновых задач проверки по требованию.
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Security для Windows Server. С помощью этого параметра вы можете указывать максимальное количество процессов, в которых Kaspersky Security для Windows Server будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, которое вы устанавливаете этим параметром, не входит в общее количество рабочих процессов Kaspersky Security для Windows Server, заданное параметром **Максимальное количество активных процессов**. Например, если вы установите следующие значения параметров: • максимальное количество активных процессов – 3; • количество процессов для задач постоянной защиты – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты и одну задачу проверки по требованию в фоновом режиме, общее количество рабочих процессов kavfswp.exe Kaspersky Security для Windows Server составит 4. В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию. Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.
Возможные значения:	1-4
Значение по умолчанию	1

- В блоке **Взаимодействие с пользователем** настройте отображение значка Kaspersky Security для Windows Server в области уведомлений панели задач (см. раздел "Значок Kaspersky Security для Windows Server в области уведомлений панели задач" на стр. 15) при каждом запуске программы.

- На закладке **Безопасность и надежность** вы можете настроить следующие параметры:
  - В блоке **Параметры надежности** укажите количество попыток восстановления задач проверки по требованию после их аварийного завершения.

Таблица 11. Восстановление задач

Параметр	Восстановление задач (**Выполнять восстановление задач**).
Описание	Этот параметр относится к группе **Параметры надежности** Kaspersky Security для Windows Server. Он включает восстановление задач, если они завершаются аварийно, и устанавливает количество попыток восстановления задач проверки по требованию. Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Security для Windows Server пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения. Если восстановление задач выключено, Kaspersky Security для Windows Server не восстанавливает задачи постоянной защиты и проверки по требованию. Если восстановление задач включено, Kaspersky Security для Windows Server пытается восстановить задачи постоянной защиты, пока они не будут успешно запущены, и пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.
Возможные значения:	Включено / выключено. Количество попыток восстановления задач проверки по требованию: 1-10.
Значение по умолчанию	Восстановление задач включено. Количество попыток восстановления задач проверки по требованию: 2.

- В блоке **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Security для Windows Server при работе от источника бесперебойного питания.

Таблица 12. Использование источника бесперебойного питания

Параметр	Действия при переходе на источник бесперебойного питания.
Описание	Этот параметр определяет действия, которые Kaspersky Security для Windows Server выполнит, когда компьютер перейдет на питание от источника бесперебойного питания.
Возможные значения:	Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию. Выполнять или останавливать все выполняемые задачи проверки по требованию.
Значение по умолчанию	По умолчанию при работе компьютера от источника бесперебойного питания Kaspersky Security для Windows Server работает в следующем режиме: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию; • автоматически останавливает все выполняемые задачи проверки по требованию.

- В блоке **Настройки пароля** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля" на стр. 34).

- На закладке **Параметры соединения**:
  - В блоке **Параметры прокси-сервера** укажите параметры использования прокси-сервера.
  - В блоке **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и необходимые данные для аутентификации на прокси-сервере.

- В блоке **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.

- На закладке **Диагностика сбоев**:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
    - В поле ниже укажите папку, в которую Kaspersky Security 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 для Windows Server сохраняет в файле трассировки.

      Вы можете выбрать один из следующих уровней детализации:

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

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

Таблица 13. Коды подсистем Kaspersky Security для Windows Server

Код подси-стемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Security 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 для Windows Server.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Security 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 для Windows Server (gui) и плагина управления Kaspersky Security 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 для Windows Server применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Security для Windows Server сохраняет отладочную информацию о работе всех подсистем Kaspersky Security 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**.

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

- В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файл дампа.

Kaspersky Security 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 для Windows Server. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Security для Windows Server" на стр. 29) и разрешить доступ к журналам, файлам трейса и дампа только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Security для Windows Server будут сохранены.

Управление Kaspersky Security для Windows Server через Консоль программы на другом компьютере

Вы можете управлять Kaspersky Security для Windows Server через Консоль, которая установлена на удаленном компьютере.

Чтобы управление программой с помощью Консоли программы на удаленном компьютере было доступно, убедитесь в следующем:

- Пользователи Консоли программы на удаленном компьютере добавлены в группу KAVWSEE Administrators на защищаемом сервере.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management Service kavfsgt.exe, если на защищаемом сервере включен брандмауэр Windows.
- Во время установки Kaspersky Security для Windows Server был установлен флажок **Разрешить удаленный доступ** в окне Мастера установки.

Если Kaspersky Security для Windows Server на удаленном компьютере защищен паролем, вам нужно ввести пароль для получения доступа к управлению программой через Консоль.

Лицензирование

Подробнее о типах лицензионных сертификатов, способах активации продуктов и Лицензионном соглашении см. в разделе "Лицензирование программы" *Руководства администратора Kaspersky Security для Windows Server*.

► *Чтобы добавить активный ключ, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Лицензирование**.
2. В зависимости от способа, которым вы хотите активировать Kaspersky Security для Windows Server,выберите один из следующих вариантов в панели результатов узла **Лицензирование**:
   - Чтобы добавить файл ключа:
     a. Перейдите по ссылке **Добавить ключ**.
     b. В открывшемся окне **Добавление ключа** нажмите на кнопку **Обзор**.
     c. Выберите файл ключа на своем компьютере и нажмите на кнопку **Открыть**.

     Также можно пометить ключ как дополнительный, установив флажок **Использовать дополнительный ключ**.
   - Чтобы добавить код активации:
     a. Перейдите по ссылке **Добавить код активации**.
     b. Введите полученный от "Лаборатории Касперского" код активации в открывшееся окно **Активировать кодом**.
     c. Нажмите на кнопку **Показать информацию о лицензии**, чтобы просмотреть данные лицензии.

     Также можно пометить код как дополнительный, установив флажок **Использовать дополнительный код активации**.
3. Нажмите на кнопку **ОК**, чтобы применить добавленный файл ключа или код активации.

Настройка доверенной зоны

Этот раздел содержит информацию о доверенной зоне Kaspersky Security для Windows Server, инструкции по добавлению объектов в доверенную зону и по применению доверенной зоны в задачах Kaspersky Security для Windows Server.

В этом разделе

О доверенной зоне Kaspersky Security для Windows Server 45

Включение и выключение применения доверенной зоны в задачах Kaspersky Security для Windows Server 47

Добавление исключений в доверенную зону 47

О доверенной зоне Kaspersky Security для Windows Server

Доверенная зона – это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах Проверка по требованию и Постоянная защита файлов, Проверка скриптов и Защита RPC-подключаемых сетевых хранилищ.

Если при установке Kaspersky Security для Windows Server вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**, Kaspersky Security для Windows Server добавляет в доверенную зону файлы, рекомендованные Microsoft и "Лабораторией Касперского", для задач постоянной защиты.

Вы можете формировать доверенную зону Kaspersky Security для Windows Server по следующим правилам:

- Доверенные процессы. В доверенную зону помещаются объекты, к которым обращаются процессы программ, чувствительных к файловым перехватам.
- Операции резервного копирования. В доверенную зону помещаются объекты, доступ к которым выполняется в операциях систем резервного копирования жестких дисков на внешние устройства.
- Исключения. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задачах постоянной защиты файлов, проверки скриптов, защиты RPC-подключаемых сетевых хранилищ, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи проверки объектов на карантине.

По умолчанию доверенная зона применяется в задачах постоянной защиты файлов, проверки скриптов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный файл в формате XML, чтобы затем импортировать его в Kaspersky Security для Windows Server на другом компьютере.

Доверенные процессы

Применяется в задаче постоянной защиты файлов.

Некоторые программы на сервере могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Security для Windows Server. К таким программам относятся, например, системные программы домен-контроллеров.

Чтобы не нарушать работу таких программ, вы можете выключить функцию постоянной защиты объектов, к которым обращаются выполняющиеся процессы этих программ, сформировав в доверенной зоне список доверенных процессов.

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Имена некоторых из них приводятся на веб-сайте корпорации Microsoft (https://www.microsoft.com/ru-ru/ (код статьи: KB822158)).

Вы можете включать и выключать применение доверенных процессов в доверенной зоне.

Если исполняемый файл процесса изменяется, например, обновляется, Kaspersky Security для Windows Server исключает его из списка доверенных процессов.

Kaspersky Security для Windows Server не использует значение пути к файлу на защищаемом сервере для идентификации процесса как доверенного. Путь к файлу на защищаемом сервере применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

Операции резервного копирования

Применяется в задачах постоянной защиты.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства вы можете выключить функцию постоянной защиты объектов, доступ к которым осуществляется в операциях резервного копирования. Kaspersky Security для Windows Server не проверяет объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Исключения

Применяется в задачах постоянной защиты файлов, защиты RPC-подключаемых сетевых хранилищ и проверки по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в настройках параметров уровня безопасности каждой задачи Kaspersky Security для Windows Server по отдельности.

Вы можете добавлять в доверенную зону объекты по их местоположению на сервере, по имени или маске имени обнаруженного в них объекта или использовать оба параметра.

На основании исключения Kaspersky Security для Windows Server может пропускать в указанных задачах объекты согласно следующим параметрам:

- указанные обнаруживаемые объекты по имени или маске имени в указанных областях сервера или сетевого хранилища;
- все обнаруживаемые объекты в указанных областях сервера или сетевого хранилища;
- указанные обнаруживаемые объекты по имени или маске имени во всей области защиты или проверки..

Включение и выключение применения доверенной зоны в задачах Kaspersky Security для Windows Server

По умолчанию доверенная зона применяется в задачах Постоянная защита файлов, Защита RPC-подключаемых сетевых хранилищ и Проверка скриптов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

После того как вы включите или выключите доверенную зону, заданные в ней исключения начнут или перестанут действовать в выполняющихся задачах немедленно.

► *Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой хотите настроить применение доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**
3. В открывшемся окне на закладке Общие в соответствующем блоке выполните одно из следующих действий:
   - Если вы хотите применять доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Если вы хотите выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Если вы хотите настроить параметры доверенной зоны, перейдите по ссылке, расположенной в названии флажка **Применять доверенную зону** (см. раздел "Добавление исключений в доверенную зону" на стр. 47).
5. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Добавление исключений в доверенную зону

Этот раздел содержит инструкции по добавлению единых исключений в доверенную зону Kaspersky Security для Windows Server.

В этом разделе

Доверенные процессы 48
Удаление процесса из списка доверенных 50
Выключение постоянной защиты файлов на время резервного копирования 50

Доверенные процессы

Вы можете добавить процесс в список доверенных процессов одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом сервере.
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

Если исполняемый файл процесса изменится, Kaspersky Security для Windows Server исключит этот процесс из списка доверенных процессов.

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

1. В дереве Консоли Kaspersky Security для Windows Server откройте контекстное меню узла **Kaspersky Security для Windows Server**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. На закладке **Доверенные процессы** установите флажок **Не проверять файловую активность указанных процессов**.
4. Нажмите кнопку **Добавить**.
5. 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 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 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 **OK**.

> Требуется, чтобы учетная запись, с правами которой запускается задача постоянной защиты файлов, имела права администратора на сервере с установленным Kaspersky Security 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 программы 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 **OK**.

- **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 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 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 **OK**.

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

6. В окне **Добавление доверенного процесса** нажмите на кнопку **OK**.

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

Удаление процесса из списка доверенных

► *Чтобы выключить применение доверенного процесса в доверенной зоне, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security для Windows Server откройте контекстное меню узла **Kaspersky Security для Windows Server**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. В окне **Доверенная зона** на закладке **Доверенные процессы** в списке доверенных процессов снимите флажок рядом с именем исполняемого файла процесса, который вы хотите временно не применять в доверенной зоне.
4. Нажмите на кнопку **OK**.

Окно **Доверенная зона** будет закрыто; выбранные процессы будут удалены из списка доверенных.

Выключение постоянной защиты файлов на время резервного копирования

► *Чтобы выключить постоянную защиту файлов на время резервного копирования данных с жестких дисков, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security для Windows Server откройте контекстное меню узла **Kaspersky Security для Windows Server**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. В окне **Доверенная зона**, на закладке **Доверенные процессы** установите флажок **Не проверять файловые операции резервного копирования**.
4. Нажмите на кнопку **OK**.

Окно **Доверенная зона** будет закрыто; постоянная защита файлов будет приостановлена на время резервного копирования.

Управление задачами Kaspersky Security для Windows Server

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

В этом разделе

Категории задач Kaspersky Security для Windows Server 51

Сохранение задачи после изменения ее параметров 52

Запуск / приостановка / возобновление / остановка задачи вручную 52

Работа с расписанием задач 53

Использование учетных записей для запуска задач 55

Импорт и экспорт параметров 56

Использование шаблонов параметров безопасности 60

Категории задач Kaspersky Security для Windows Server

Функции постоянной защиты, контроля сервера, проверки по требованию и обновления Kaspersky Security для Windows Server реализованы в виде задач.

Вы можете управлять задачей с помощью пунктов контекстного меню названия задачи в дереве Консоли, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Security для Windows Server: *локальные* и *групповые*.

Локальные задачи

Локальные задачи выполняются только на том защищаемом сервере, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи**. Создаются автоматически при установке Kaspersky Security для Windows Server. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.
- **Локальные пользовательские задачи**. В Консоли программы вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые задачи и задачи для наборов компьютеров, созданные через Kaspersky Security Center, отображаются в Консоли программы. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли программы вы можете только просматривать состояние групповых задач.

Сохранение задачи после изменения ее параметров

Вы можете изменять параметры как выполняемой, так и остановленной (приостановленной) задачи. Новые значения параметров вступят в силу при следующих условиях:

- если вы изменили параметры выполняемой задачи: новые значения параметров применяются сразу после сохранения задачи;.
- если вы изменили параметры остановленной (приостановленной) задачи: новые значения параметров применяются при следующем запуске задачи.

► *Чтобы сохранить измененные параметры задачи,*

в контекстном меню названия задачи выберите пункт **Сохранить задачу**.

Если после изменения параметров задачи вы выберете другой узел дерева Консоли, не выбрав предварительно команду **Сохранить задачу**, появится окно сохранения параметров.

► *Чтобы сохранить измененные параметры при переходе к другому узлу Консоли,*

в окне сохранения параметров нажмите на кнопку **Да**.

Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты и проверки по требованию.

► *Чтобы запустить / приостановить / возобновить / остановить задачу, выполните следующие действия:*

1. Откройте контекстное меню названия задачи в Консоли программы.
2. Выберите одну из следующих команд: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (на стр. 241).

После возобновления задачи проверки по требованию Kaspersky Security для Windows Server продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

Работа с расписанием задач

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

В этом разделе

Настройка параметров расписания запуска задач 53

Включение и выключение запуска по расписанию 54

Настройка параметров расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить параметры расписания запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**
3. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

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

   - **Ежечасно**, если 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 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**.
В поле **Следующий запуск** отображается значение **Определено политикой**, если запуск системных задач по расписанию определен параметрами действующей политики Kaspersky Security Center.

5. На закладке **Дополнительно** настройте в соответствии с вашими требованиями следующие параметры расписания.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.
     b. Установите флажок **Приостановить с … до** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **Применить**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Включение и выключение запуска по расписанию

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

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

1. В дереве Консоли программы 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 применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

В этом разделе

Об использовании учетных записей для запуска задач 55

Указание учетной записи для запуска задачи 56

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Security для Windows Server:

- Задачи генерации правил контроля устройств и контроля запуска программ
- задачи проверки по требованию;
- задачи обновления;

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом компьютере в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной проверкой подлинности Microsoft Windows (NTLM-authentication);
- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к каким-либо из проверяемых объектов (например, к файлам в общих сетевых папках компьютера);
- в задаче автоматической генерации правил, если после окончания выполнения задачи сформированные правила импортируются в конфигурационный файл, который расположен по недоступному для системной учетной записи пути (например, в одной из общих сетевых папок сервера).

Вы можете запускать задачи обновления, проверки по требованию и автоматической генерации правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Security for Windows Server обращается к папкам общего доступа на другом компьютере в сети, если этот компьютер зарегистрирован в одном домене с защищаемым сервером. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Security для Windows Server будет обращаться к компьютеру с правами учетной записи **<имя домена \ имя компьютера>**.

Указание учетной записи для запуска задачи

► *Чтобы указать учетную запись для запуска задачи, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню названия задачи, для которой хотите настроить запуск с правами учетной записи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**
3. В открывшемся окне на закладке Запуск с правами выполните следующие действия:
   a. Выберите пункт **Имя пользователя**.
   b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

   Выбранный вами пользователь должен быть зарегистрирован на защищаемом сервере или в одном домене с ним.

   c. Подтвердите введенный пароль.
4. Нажмите на кнопку **Применить**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

Этот раздел содержит информацию об экспорте параметров работы Kaspersky Security для Windows Server или параметров работы отдельных компонентов программы в конфигурационный файл в формате XML и импорте этих параметров из конфигурационного файла в программу.

В этом разделе

Об импорте и экспорте параметров 57
Экспорт параметров 58
Импорт параметров 59

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Security для Windows Server в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Security для Windows Server из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Security для Windows Server, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Security для Windows Server:

- Постоянная защита файлов.
- Использование KSN
- Контроль устройств
- Контроль запуска программ.
- Формирование правил контроля устройств.
- Формирование правил контроля запуска программ.
- Проверка по требованию
- Обновление баз и модулей Kaspersky Security для Windows Server.
- Карантин
- Резервное хранилище:
- Журналы.
- Уведомления администратора и пользователей.
- Доверенная зона

Также вы можете сохранять в файле общие параметры Kaspersky Security для Windows Server и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Security для Windows Server экспортирует все пароли, которые используются для работы программы, например, учетные данные для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Вы можете импортировать пароли только с помощью Kaspersky Security для Windows Server, установленного на этом же сервере, если он не был переустановлен или обновлен.

Вы не можете импортировать ранее сохраненные пароли с помощью Kaspersky Security для Windows Server, установленного на другом компьютере. После импорта параметров на другом компьютере вам нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения, применяемые политикой.

Вы можете импортировать параметры из конфигурационного файла, содержащего параметры только некоторых компонентов Kaspersky Security для Windows Server (например, созданного в Kaspersky Security для Windows Server, который был установлен с неполным набором компонентов). После импорта параметров в Kaspersky Security для Windows Server изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

Импортируемые параметры задач не применяются во время выполнения задачи. Для применения импортированных параметров необходимо перезапустить задачу.

Заблокированные параметры активной политики Kaspersky Security Center при импорте параметров не изменяются.

Экспорт параметров

► *Чтобы экспортировать параметры в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Security** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Security для Windows Server.
   - В контекстном меню названия задачи, параметры которой вы хотите экспортировать, и выберите пункт **Экспортировать параметры**, чтобы экспортировать параметры отдельного функционального компонента программы.
   - Чтобы экспортировать параметры компонента Доверенная зона:
     a. В дереве Консоли откройте контекстное меню узла **Kaspersky Security**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

     Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Экспорт**.

     Откроется окно приветствия мастера экспорта параметров.
2. Выполните инструкции в окнах **мастера**: задайте имя конфигурационного файла, в котором вы хотите сохранить параметры, и путь к файлу.

   Указывая путь, вы можете использовать системные переменные окружения, но не можете использовать пользовательские переменные окружения.

   Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения параметров в политике.
3. В окне **Экспорт параметров программы завершен** нажмите на кнопку **OK**.

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

Импорт параметров

► *Чтобы импортировать параметры из конфигурационного файла, выполните следующие действия:*

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Security** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Security для Windows Server.
   - В контекстном меню названия задачи, параметры которой вы хотите импортировать, и выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.
   - Чтобы импортировать параметры компонента Доверенная зона:
     a. В дереве Консоли откройте контекстное меню узла **Kaspersky Security**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

     Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Импорт**.

     Откроется окно приветствия мастера импорта параметров.
2. Выполните инструкции в окнах мастера: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После того как вы импортируете общие параметры Kaspersky Security for Windows Server или его функциональных компонентов на сервере, вы не сможете вернуть их прежние значения.
3. В окне **Импорт параметров программы завершен** нажмите на кнопку **OK**.

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.
4. В панели инструментов Консоли программы нажмите кнопку **Обновить**,

Импортированные параметры отобразятся в окне Консоли.

Kaspersky Security для Windows Server не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом сервере или на том же сервере, после того как на нем переустановили или обновили Kaspersky Security для Windows Server. После завершения импорта вам нужно ввести пароли вручную.

Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Security для Windows Server.

В этом разделе

О шаблонах параметров безопасности 60

Создание шаблона параметров безопасности 61

Просмотр параметров безопасности в шаблоне 61

Применение шаблона параметров безопасности 62

Удаление шаблона параметров безопасности 63

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Security для Windows Server.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Security для Windows Server:

- Постоянная защита файлов.
- Защита RPC-подключаемых сетевых хранилищ.
- Проверка при старте операционной системы;
- Проверка важных областей;
- пользовательские задачи проверки по требованию.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов компьютера, устанавливаются на все вложенные узлы. Шаблон родительского узла не применяется к вложенным узлам в следующих случаях:

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел "Применение шаблона параметров безопасности" на стр. 62).
- Если вложенные узлы являются виртуальными. Вам нужно применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

► *Чтобы сохранить параметры безопасности узла вручную и сохранить эти параметры в шаблон, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов сервера выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите любую дополнительную информацию о шаблоне.
7. Нажмите на кнопку **OK**.

Шаблон с набором значений параметров безопасности будет сохранен.

Вы также можете перейти к созданию шаблона параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

Просмотр параметров безопасности в шаблоне

► *Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, шаблон безопасности которой хотите просмотреть.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Имя шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приводится список значений параметров безопасности, сохраненных в шаблоне.

Применение шаблона параметров безопасности

► *Чтобы применить параметры безопасности из шаблона для выбранного узла, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов сервера откройте контекстное меню узла, для которого вы хотите применить шаблон.
4. Выберите Применить шаблон → **<Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню настраиваемой задачи.
6. Выберите пункт **Сохранить задачу**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов сервера. На закладке **Уровень безопасности выбранного узла будет установлено значение** Другой.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов сервера, устанавливаются на все вложенные узлы.

Если область защиты или проверки вложенных узлов в дереве файловых ресурсов сервера настраивалась отдельно, параметры безопасности из шаблона, примененного к родительскому узлу, не установятся автоматически для таких вложенных узлов.

► *Чтобы установить параметры безопасности из шаблона для всех вложенных узлов, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов сервера выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем вложенным узлам.
4. Выберите Применить шаблон → **<Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню настраиваемой задачи.
6. Выберите пункт **Сохранить задачу**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов сервера. На закладке **Уровень безопасности выбранного узла будет установлено значение** Другой.

Удаление шаблона параметров безопасности

► *Чтобы удалить шаблон параметров безопасности, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для настройки которой больше не хотите использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Вы можете перейти к созданию шаблона параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения операции удаления.
5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов файловых ресурсов сервера, настроенные параметры безопасности для этих узлов сохраняются после удаления шаблона.

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 64
Использование KSN 88
Защита от эксплойтов 95
Проверка скриптов 101
Защита трафика 104

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 64
Статистика задачи Постоянная защита файлов 65
Настройка параметров задачи Постоянная защита файлов 68
Область защиты в задаче Постоянная защита файлов 76

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Security for 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.

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

Kaspersky Security 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 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 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.

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Security для Windows Server обработал с момента запуска задачи по текущий момент.

► *Чтобы просмотреть статистику задачи Постоянная защита файлов, выполните следующие действия:*

1. В дереве Консоли разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть следующую информацию об объектах, которые Kaspersky Security для Windows Server обработал с момента запуска задачи по текущий момент (см. таблицу ниже).

Таблица 14. Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Security для Windows Server. Например, если Kaspersky Security для Windows Server обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруженных объектов	Количество объектов, которые Kaspersky Security для Windows Server признал зараженными, или обнаруженных объектов, являющихся легальными программами, которые не были исключены из области действия задач постоянной защиты или проверки, и были определены как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
Возможно зараженных объектов	Количество объектов, которые Kaspersky Security для Windows Server признал возможно зараженными.
Объектов не вылечено	Количество объектов, которые Kaspersky Security для Windows Server не вылечил по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые Kaspersky Security для Windows Server попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые Kaspersky Security для Windows Server попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server попытался сохранить в резервном хранилище, но это ему не удалось, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые Kaspersky Security для Windows Server вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Security для Windows Server поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Security для Windows Server удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Security для Windows Server пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые Kaspersky Security для Windows Server пропустил, так как их формат искажен.

Поле	Описание
Обработано объектов	Общее количество объектов, которые Kaspersky Security для Windows Server обработал.

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

Если значение в поле **Всего событий** в окне журнала выполнения задачи постоянной защиты файлов больше 0, рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Настройка параметров задачи Постоянная защита файлов

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

Таблица 15. 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 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.
Использование служб KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Расписание запуска задачи	При запуске программы	Вы можете настраивать параметры запуска задачи по расписанию.
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 программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Использовать эвристический анализатор** (см. раздел "**Использование эвристического анализатора**" на стр. 71)
     - **Режим защиты объектов** (см. раздел "**Выбор режима защиты объектов**" на стр. 70);

- **Интеграция с другими компонентами** (см. раздел "**Интеграция задачи с другими компонентами Kaspersky Security для Windows Server**" на стр. 72).

- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53)

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

   Изменения параметров задачи будут сохранены.

6. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

7. Выполните следующие действия:
   - В дереве или списке файловых ресурсов сервера выберите узлы, которые хотите включить в область защиты задачи (см. раздел "Об области защиты в задаче Постоянная защита файлов" на стр. 76).
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности" на стр. 82) или настройте параметры защиты объектов вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 83).

8. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Kaspersky Security 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.

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 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 программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**

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

     Kaspersky Security 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 для Windows Server повторно проверяет объект только после его последнего сохранения этим процессом.

- **При открытии и изменении.**

  Kaspersky Security для Windows Server проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

  Данный вариант выбран по умолчанию.

- **При открытии**

  Kaspersky Security для Windows Server проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.

- **При выполнении.**

  Kaspersky Security для Windows Server проверяет файл только при открытии на выполнение.

5. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Применение эвристического анализатора

Вы можете использовать эвристический анализатор и настроить уровень анализа для задач Проверка по требованию и Постоянная защита файлов.

► *Чтобы настроить применение эвристического анализатора, выполните следующие действия:*

1. В зависимости от задачи:
   - Для задачи Проверка по требованию:
     a. В дереве Консоли программы разверните узел **Проверка по требованию**.
     b. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
     c. В панели результатов перейдите по ссылке **Свойства**.
   - Для задачи Постоянная защита файлов:
     a. В Консоли программы разверните узел **Постоянная защита файлов**.
     b. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
2. Снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории

Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены. немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Интеграция задачи с другими компонентами Kaspersky Security для Windows Server

В задаче Постоянная защита файлов вы можете настроить параметры интеграции задачи с другими функциональными компонентами Kaspersky Security для Windows Server.

Чтобы запустить задачу Использование KSN, необходимо принять хотя бы одно из двух Положений: Положение о Kaspersky Security Network или Положение о статистике Kaspersky Security Network.

► *Чтобы настроить взаимодействие задачи Постоянная защита файлов с другими компонентами программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Интеграция с другими компонентами** настройте следующие параметры:
   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

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

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

     По умолчанию флажок установлен.
   - Установите или снимите флажок **Использовать KSN для защиты**.

     Этот флажок включает или выключает использование служб KSN.

     Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы

и снижает вероятность ложных срабатываний.

Если флажок снят, задача не использует службы KSN.

По умолчанию флажок установлен.

Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Список расширений файлов, проверяемых по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Security для Windows Server проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*

- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*

- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

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

Об области защиты в задаче Постоянная защита файлов 76

Предопределенные области защиты 77

Настройка параметров отображения файловых ресурсов области проверки 77

Формирование области защиты 78

О виртуальной области защиты 80

Создание виртуальной области защиты 80

Параметры безопасности выбранного узла в задаче Постоянная защита файлов 81

Выбор предустановленных уровней безопасности 82

Настройка параметров безопасности вручную 83

Об области защиты в задаче Постоянная защита файлов

По умолчанию задача Постоянная защита файлов защищает все объекты файловой системы сервера. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов сервера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого сервера отображаются в виде списка.

► *Чтобы включить отображение файловых ресурсов компьютера в виде дерева,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области защиты**, выберите пункт **Показывать в виде дерева**.

Узлы в списке или дереве файловых ресурсов сервера отображаются следующим образом:

Узел включен в область защиты.

Узел исключен из области защиты.

По крайней мере один из узлов, вложенных в этот узел, исключен из области защиты или параметры безопасности вложенного узла (узлов) отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области защиты для выбранного вложенного узла.

Имена виртуальных узлов области защиты отображаются шрифтом синего цвета.

Предопределенные области защиты

Файловые ресурсы защищаемого компьютера отображается в панели результатов узла **Постоянная защита файлов** по ссылке **Настройка области защиты**. Вы можете настроить отображение файловых ресурсов в виде списка или дерева.

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 для Windows Server предусмотрены следующие предопределенные области защиты:

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

Настройка параметров отображения файловых ресурсов области проверки

► *Чтобы выбрать способ отображения файловых ресурсов компьютера при настройке параметров области проверки, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.

3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:

   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.
   - Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

   По умолчанию файловые ресурсы защищаемого сервера отображаются в виде списка.

5. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут применены.

Формирование области защиты

Процедура формирования области защиты в задаче Постоянная защита файлов зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 187). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

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

► *Чтобы сформировать область защиты, работая с деревом файловых ресурсов, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

4. В левой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:

   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
     - если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на сервере, установите флажок **Съемные диски**);

- если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
- если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.

6. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область защиты, работая со списком файловых ресурсов, выполните следующие действия*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В открывшемся окне **Добавление области защиты** выберите тип объекта, который вы хотите добавить в область защиты:
      - **Предопределенная область**, если вы хотите включить в область защиты одну из предопределенный областей на защищаемом сервере. Затем в раскрывающемся списке выберите необходимую область.
      - **Диск, папка или сетевой объект**, если вы хотите включить в область защиты отдельный диск, папку или сетевой объект нужного типа. Затем выберите необходимый файл по кнопке **Обзор**.
      - **Файл**, если вы хотите включить в область защиты только отдельный файл на диске. Затем выберите необходимый файл по кнопке **Обзор**.

   Вы не можете добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.
5. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
6. Чтобы изменить добавленную область защиты или исключение, в контекстном меню области, которую хотите изменить, выберите пункт **Изменить область**.

7. Чтобы скрыть отображение ранее добавленной области защиты или исключения в списке файловых ресурсов, в контекстном меню области, которую хотите скрыть, выберите пункт **Удалить из списка**.

   Область защиты исключается из области действия задачи Постоянная защита файлов при ее удалении из списка файловых ресурсов.

8. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Вы можете запустить задачу **Постоянная защита файлов**, если по крайней мере один узел файловых ресурсов компьютера включен в область защиты.
Если вы укажете сложную область защиты, например, установите различные значения параметров безопасности для многих отдельных узлов в дереве файловых ресурсов сервера, это может привести к замедлению проверки объектов при доступе.

О виртуальной области защиты

Kaspersky Security для Windows Server может проверять не только существующие папки и файлы на жестких и съемных дисках, но и диски, которые монтируются на сервер временно, например, общие диски кластера, которые динамически создаются на сервере различными программами и службами.

Если вы включили в область защиты все объекты сервера, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для этих динамических узлов или вы выбрали для постоянной защиты не весь сервер, а отдельные области, то, для того чтобы включить в область защиты динамические диски, файлы или папки, вам нужно предварительно создать их в Консоли программы – задать виртуальную область защиты. Созданные вами диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого сервера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, динамические папки или файлы, которые появятся в ней, не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

Создание виртуальной области защиты

Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 187).

► *Чтобы добавить в область защиты виртуальный диск, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

Откроется окно **Настройка области защиты**.

4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. Откройте контекстное меню узла **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.

   Установите флажок рядом с добавленным диском, чтобы включить этот диск в область защиты.
6. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

► *Чтобы добавить в область защиты виртуальную папку или виртуальный файл, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если хотите добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, если хотите добавить виртуальный файл в область защиты.
6. В поле ввода задайте имя для папки или файла.
7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
8. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задаче Постоянная защита файлов

В задаче Постоянная защита файлов вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты или проверки, так и различными для разных узлов в дереве или списке 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.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех предустановленных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов в дереве или списке файловых ресурсов сервера (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

Выбор предустановленных уровней безопасности

Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из предустановленных уровней безопасности 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 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 влияния 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 16. Предустановленные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	По расширению	По формату	По формату
Оптимизация	Включена	Включена	Выключено
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Карантин	Карантин	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 составные объекты размером более (МБ).	8 MB	8 MB	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Проверять загрузочные секторы дисков и MBR	Да	Да	Да

Параметры	Уровень безопасности		
	Максимальное быстродей-ствие	Рекомендуе-мый	Максимальная защита
Защита составных объектов	• упакованные объекты* • только новые и измененные объекты	• SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* • только новые и измененные объекты	• 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 Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. Выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.
5. Убедитесь, что этот узел включен в область защиты.
6. В правой части окна на закладке **Уровень безопасности** в списке выберите уровень безопасности, который вы хотите применить.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному вами уровню безопасности.
7. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Kaspersky Security 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 задачах постоянной защиты применяются единые параметры безопасности для всей области проверки. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый** (см. раздел "Выбор предустановленных уровней безопасности" на стр. 82).

Вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области проверки, 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, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному узлу в области защиты можно применить предустановленный шаблон с параметрами безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 60).
5. Настройте 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 для Windows Server проверяет все объекты.
     - **Объекты, проверяемые по формату.**

       Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

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

       Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
     - **Объекты, проверяемые по указанному списку расширений.**

       Kaspersky Security 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 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 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 для Windows Server новыми или измененными с момента последней проверки.

  Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.
  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет архивы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет SFX-архивы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Security 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 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 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 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 для Windows Server пропускает при проверке указанные объекты.

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

    Если флажок снят, Kaspersky Security 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 составные объекты размером более (МБ).**

    Исключение из проверки составных объектов больше указанного размера.

    Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, чей размер превышает

установленное значение.

Если флажок снят, Kaspersky Security 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 для Windows Server проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Security для Windows Server проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **OK**.

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 88
Настройка параметров задачи Использование KSN 90
Настройка обработки данных 92

О задаче Использование KSN

Использование Глобального KSN предполагает передачу данных, описанных в Положении о KSN, на серверы Лаборатории Касперского, и влечет к выходу программы из сертифицированного состояния.

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 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 для Windows Server получает от Kaspersky Security Network только информацию о репутации программ и запрашиваемых URL.

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" (https://kaspersky.ru/Products-and-Services-Privacy-Policy).

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Security 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 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.) задачи Использование KSN вы можете прочитать Положение о KPSN и включить или выключить использование компонента в любой момент с помощью флажка Я принимаю условия участия в Kaspersky Private Security Network. Принимая условия, вы соглашаетесь отправлять все типы данных (запросы безопасности, статистические данные), предусмотренные в Положении о KPSN, в службы KSN.

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

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

Настройка параметров задачи Использование KSN

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

Таблица 17. Параметры задачи Использование KSN по умолчанию

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	**Удалить**	Вы можете указывать действия, которые Kaspersky Security 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 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	Первый 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 программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Security для Windows Server необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалить**

       Kaspersky Security для Windows Server удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

       Данный вариант выбран по умолчанию.
     - **Фиксировать информацию в отчете.**

       Kaspersky Security для Windows Server фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Security 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 для Windows Server не рассчитывает

контрольную сумму для файлов, размер которых превышает установленное значение (МБ).

Если флажок снят, Kaspersky Security для Windows Server рассчитывает контрольную сумму для файлов любого размера.

По умолчанию флажок установлен.

- Если требуется, в поле справа укажите максимальный размер файлов, для которых Kaspersky Security для Windows Server будет рассчитывать контрольную сумму.

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. 92) перед запуском задачи.
7. Нажмите на кнопку **OK**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка обработки данных

► *Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.

   Откроется окно **Обработка данных**.

4. На закладке **Службы** прочитайте Положение и установите флажок **Прининять условия Положения о Kaspersky Security Network**.
5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**.

     Если флажок установлен, Kaspersky Security 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 для Windows Server не отправляет контрольную сумму файлов в KSN.

     По умолчанию флажок установлен.

   - **Разрешить отправку данных о запрашиваемых веб-адресах**.

     Если флажок установлен, Kaspersky Security 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 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 **Статистика**. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы Kaspersky Security для Windows Server отправлял дополнительную статистику в Лабораторию Касперского.

   Если флажок установлен, Kaspersky Security для Windows Server отправляет дополнительную 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 для Windows Server не отправляет дополнительную статистику.

   По умолчанию флажок установлен.

7. На закладке **Kaspersky Managed Protection** прочитайте Положение о KMP и установите флажок **Прининять 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 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 **OK**.

Конфигурация обработки данных будет сохранена.

Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Security для Windows Server обработал с момента ее запуска по текущий момент. Информация обо всех событиях, возникающих во время работы задачи, записывается в журнал выполнения задачи (см. раздел "О журналах выполнения задач" на стр. 243).

► *Чтобы просмотреть статистику задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые Kaspersky Security для Windows Server обработал за время работы задачи (см. таблицу ниже).

Таблица 18. Статистика задачи Использование KSN

Поле	Описание
Отправлено файловых запросов	Количество запросов о репутации файлов, которые Kaspersky Security для Windows Server отправил для проверки в службы KSN.
Отправлено запросов для веб-ссылок	Количество запросов о репутации веб-адреса, которые Kaspersky Security для Windows Server отправил для проверки в службы KSN.
Недоверенных заключений по файлам	Количество объектов, признанных недоверенными службами KSN.
Недоверенных заключений по веб-адресам	Количество веб-адресов, признанных недоверенными службами KSN.
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Пакетов статистики сформировано	Количество пакетов с данными, которые были сформированы в процессе работы задачи.
Удалено объектов	Количество объектов, которые Kaspersky Security для Windows Server удалил в результате работы задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server сохранил в резервном хранилище.
Объектов не удалено	Количество объектов, которые Kaspersky Security для Windows Server попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server попытался сохранить в резервном хранилище, но это ему не удалось, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи.

Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

В этом разделе

О задаче Защита от эксплойтов 96
Настройка параметров защиты памяти процессов 97
Добавление защищаемого процесса 98
Техники снижения рисков 100

О Защите от эксплойтов

Kaspersky Security для Windows Server предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее Агент) в защищаемый процесс.

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Security 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 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 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 защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из двух режимов:

- Завершать скомпрометированные процессы: применяйте данный режим, чтобы завершать процесс при попытке эксплуатации уязвимости.

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Security 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 для Windows Server фиксирует все попытки эксплуатации уязвимостей посредством создания событий.

Настройка параметров защиты памяти процессов

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. выберите узел Kaspersky Security в дереве Консоли.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: общие параметры защиты**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.
3. В блоке **Защита памяти процессов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Security для Windows Server не защищает процессы на сервере от эксплуатации уязвимостей.

     По умолчанию флажок снят.
   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Security 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 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 для Windows Server обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать о компрометации процесса**.

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

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

     Если флажок установлен, Kaspersky Security 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 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 Kspersky Security Broker Host. По умолчанию флажок установлен.

   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**.

     Если флажок установлен, Kaspersky Security для Windows Server будет снижать риски эксплуатации уязвимостей уже запущенных процессов не зависимо от статуса выполнения службы Kaspersky Security. Kaspersky Security 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 для Windows Server не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

     По умолчанию флажок установлен.

     Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Security для Windows Server не защищает процессы на сервере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

5. В окне **Параметры защиты от эксплойтов** нажмите на кнопку **ОК**.

   Kaspersky Security 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. выберите узел Kaspersky Security в дереве Консоли.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: общие параметры защиты**.

   Откроется окно **Параметры защиты процессов**.
3. Добавьте процесс в список защищаемых процессов, выполнив следующие действия:
   a. Нажмите на кнопку **Обзор**.

      Откроется стандартное окно Microsoft Windows **Открыть**.
   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.
   c. Нажмите на кнопку **Открыть**.
   d. Нажмите кнопку **Добавить**.

      Указанный процесс добавится в список защищаемых процессов.
4. Выберите добавленный процесс в списке.
5. На странице **Параметры защиты процесса** отображается текущая конфигурация:
   - **Имя процесса.**
   - **Выполняется сейчас.**
   - **Техники снижения рисков**.
6. Чтобы отредактировать применяемые к данному процессу техники снижения рисков, выберите закладку **Техники защиты**.
7. 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 снижения рисков Attack Surface Reduciton**.
8. 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®.

9. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

Техника снижения рисков

Таблица 19. Техника 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 101

Настройка параметров задачи Проверка скриптов 101

Статистика задачи Проверка скриптов 103

О задаче Проверка скриптов

В ходе выполнения задачи Проверка скриптов Kaspersky Security для Windows Server контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), например, скриптов VBScript или JScript®. Kaspersky Security для Windows Server разрешает выполнение скрипта, только если он признал этот скрипт безопасным. Kaspersky Security для Windows Server запрещает выполнение скрипта, который он признал опасным. Если Kaspersky Security для Windows Server признал скрипт предположительно опасным, он выполняет выбранное вами действие: запрещает или разрешает выполнение этого скрипта.

По умолчанию задача Проверка скриптов запускается автоматически при начале работы Kaspersky Security 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 для Windows Server.

Подробная информация о выборе компонентов программы при установке содержится в *разделе об установке Руководства администратора* Kaspersky Security для Windows Server.

Вы можете настраивать параметры задачи Проверка скриптов (см. раздел "Настройка параметров задачи Проверка скриптов" на стр. 101).

Настройка параметров задачи Проверка скриптов

По умолчанию системная задача Проверка скриптов имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 20. Параметры задачи Проверка скриптов по умолчанию

Параметр	Значение по умолчанию	Описание
Выполнение опасных скриптов	Запрещено	Kaspersky Security 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 программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Проверка скриптов**.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. 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 для Windows Server разрешает выполнение потенциально опасного скрипта.
   - Если вы хотите запретить выполнение предположительно опасных скриптов, выберите пункт **Блокировать выполнение**.

     Kaspersky Security для Windows Server блокирует выполнение возможно опасного скрипта.

     Данный вариант выбран по умолчанию.
5. 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 выполняется быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

  Этот уровень выбран по умолчанию.
- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

6. 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 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

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

   По умолчанию флажок установлен.

7. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Статистика задачи Проверка скриптов

В ходе выполнения задачи Проверка скриптов вы можете просматривать информацию о количестве скриптов, которые Kaspersky Security для Windows Server обработал с момента запуска задачи по текущий момент.

► *Чтобы просмотреть статистику задачи Проверка скриптов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Проверка скриптов**.

Текущая статистика задачи отобразится на закладке **Обзор и управление** панели результатов узла в блоке **Статистика**.

Вы можете просмотреть информацию об объектах, которые Kaspersky Security для Windows Server обработал за время работы задачи (см. таблицу ниже).

Таблица 21. Статистика задачи Проверка скриптов

Поле	Описание
Заблокировано скриптов	Количество скриптов, выполнение которых запретил Kaspersky Security для Windows Server.
Обнаружено опасных скриптов	Количество обнаруженных опасных скриптов.
Обнаружено предположительно опасных скриптов	Количество обнаруженных предположительно опасных скриптов.
Обработано скриптов	Общее количество обработанных скриптов.

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 104

О правилах защиты трафика 106

Защита от почтовых угроз 106

Настройка задачи Защита трафика 107

Настройка защиты от вредоносных программ, передающихся через веб-трафик 114

Настройка защиты от почтовых угроз 117

Настройка обработки веб-адресов и веб-контента 118

Настройка веб-контроля 120

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 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 угроз, передаваемых по электронной почте:
  - Антифишинг.
  - Защита от вредоносных программ, передающихся через почтовый трафик.
- Защита от веб-угроз:
  - 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 производится только по заключениям, полученным от KSN служб.

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 для Windows Server.
- **Внешний прокси-сервер:** программа обрабатывает трафик с внешнего прокси-сервера. Трафик передается с внешнего прокси-сервера в Kaspersky Security для Windows Server. Программа анализирует трафик и рекомендует действие для внешнего прокси-сервера. Kaspersky Security для Windows Server совместим только с программными решениями для прокси-сервера, которые передают трафик по протоколу ICAP.

О правилах веб-контроля

Kaspersky Security 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 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 для Windows Server разрешает все некатегоризированные веб-ресурсы. Если флажок снят, все веб-ресурсы блокируются.

У категоризации самый низкий приоритет.

По умолчанию Kaspersky Security для Windows Server применяет только одно правило – запрещающее правило для TOR-сертификатов. Вы можете снять флажок с правила в настройках правил, чтобы разрешить TOR соединения. Если правило применяется, все входящие и исходящие TOR соединения 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 для Windows Server не применяет маску `not-a-virus` к категориям.

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 для Microsoft Outlook (далее также "расширение Microsoft Outlook") и устанавливается отдельно от компонентов Kaspersky Security для Windows Server.

Вы можете установить расширение для Microsoft Outlook только если на защищаемом сервере установлены Kaspersky Security 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:

- Проверка входящей электронной почты.
- Антивирусная проверка электронной почты.
- Антивирусная проверка вложений (включая упакованные объекты);
- Антифишинговая проверка электронной почты.
- Антифишинговая проверка вложений (включая упакованные объекты).

При обнаружении угрозы Kaspersky Security для Windows Server выполняет следующие действия:

- Удаляет вложения.
- изменяет тело зараженного письма;
- Регистрирует событие *Обнаружена почтовая угроза*.

Kaspersky Security 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 для Microsoft Outlook добавлено в список (в статусе Активный или Неактивный).
3. Перезапустите Microsoft Outlook.
4. Проверьте статус расширения 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 22. Параметры задачи Защита трафика по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Внешний прокси-сервер**	ICAP служба обрабатывает трафик с внешнего прокси-сервера.

Параметр	Значение по умолчанию	Описание
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.
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	Первый 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 программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Режим работы** выберите и настройте режим работы задачи (см. раздел "Выбор режима работы задачи" на стр. 109).
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. 118).
6. На закладке **Антивирусная защита** настройте эвристический анализ и уровень безопасности (см. раздел "Настройка защиты от вредоносных программ, передающихся через веб-трафик" на стр. 114).
7. На закладке **Управление задачей** запустите задачу на базе расписания (см. раздел "Работа с расписанием задач" на стр. 53).
8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Выбор режима работы задачи

► *Чтобы настроить режим работы задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Общие** выберите один из доступных режимов в раскрывающемся списке **Режим работы**:
   - **Драйверный перехват** (см. раздел "**Настройка режима Драйверный перехват**" на стр. 110)
   - **Перенаправление трафика** (см. раздел "**Настройка режима Перенаправление трафика**" на стр. 109)
   - **Внешний прокси-сервер**
5. Укажите параметры соединения службы ICAP (требуется для всех трех режимов):
   - **Номер сетевого порта**

     Номер порта ICAP службы Kaspersky Security 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 **OK**.

Параметры будут сохранены.

Настройка режима Перенаправление трафика

► *В окне **Защита трафика** выполните следующие действия:*

1. Выберите закладку **Режим работы**.
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 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 Kaspersky Security для Windows Server для обнаружения угроз, передающихся через веб-трафик. 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 для Windows Server.

4. Нажмите на кнопку **OK**.

Параметры режима работы задачи будут сохранены.

Настройка режима Драйверный перехват

► *В окне **Защита трафика** выполните следующие действия:*

1. Выберите закладку **Режим работы**.
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 Kaspersky Security для Windows Server для обнаружения угроз, передающихся через веб-трафик. 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 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 для Windows Server исключает порты, которые используются другими программами и могут вызывать проблемы при попытке просмотра содержимого, передаваемого по зашифрованному соединению: 3389, 1723, 13291.1

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 **OK**, чтобы сохранить внесенные изменения.
8. Чтобы исключить процесс или исполняемый файл, который требует обмена трафиком, на закладке **Исключать по приложениям**:
   a. Установите флажок **Применять исключения по приложениям**.
   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 **Запущенные процессы**.

         Откроется окно **Активные процессы**.
      2. Выберите выполняемый процесс и нажмите на кнопку **OK**.

      Вы не можете выбрать процессы в Kaspersky Security Center.

9. В окне **Защита трафика** нажмите на кнопку **OK**.

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 предустановленных уровней безопасности 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 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 влияния 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 23. Предустановленные уровни безопасности и соответствующие им

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
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 программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**

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. 113) 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 для Windows Server проверяет все объекты.
   - **Объекты, проверяемые по формату.**

     Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

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

     Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
   - **Объекты, проверяемые по указанному списку расширений.**

     Kaspersky Security 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 для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security 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 для Windows Server проверяет SFX-архивы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Security 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 для Windows Server блокирует загрузку веб-страницы при обнаружении вредоносного содержимого. Вместо запрашиваемой веб-страницы отображается причина блокирования.

   - **Разрешить**

     Kaspersky Security 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 для Windows Server пропускает при проверке указанные обнаруживаемые объекты.

Если флажок снят, Kaspersky Security 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 для Windows Server пропускает при антивирусной проверке объекты, чей размер превышает установленное значение.

    Если флажок снят, Kaspersky Security для Windows Server проверяет объекты, не учитывая размер.

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

10. Нажмите на кнопку **OK** в окне **Параметры антивирусной защиты**.

Параметры уровня безопасности будут сохранены.

Настройка защиты от почтовых угроз

► *Чтобы включить защиту от почтовых угроз, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Защита от почтовых угроз**, установите флажок **Защищать сервер от почтовых угроз**.

   Если этот флажок установлен, Kaspersky Security для Windows Server выполняет антивирусную и антифишинговую проверки всех входящих сообщений через расширение для Microsoft Outlook.

   Если флажок не установлен, электронная почта не проверяется.

По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

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 программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Режим работы** выберите и настройте режим работы задачи (см. раздел "Выбор режима работы задачи" на стр. 109).
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 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 для Windows Server проверяет каждый веб-адрес с помощью антифишинговой базы. Антифишинговая проверка основана на эвристическом анализе.

     Если флажок снят, Kaspersky Security 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 **Использовать доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

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

     Если флажок снят, Kaspersky Security для Windows Server 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.90).
d. Задача Использование KSN запущена.

6. Нажмите на кнопку **OK**.

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 программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Правила контроля трафика**.

   Откроется окно **Правила контроля трафика**.
4. На закладке **Контроль веб-страниц** установите флажок **Применять правила контроля веб-страниц**, чтобы применить правила.
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 сертификатов** 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 **OK**.
8. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
9. Нажмите на кнопку **OK** 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.....120
Настройка веб-контроля на основе категорий.....122
Список категорий.....123

Настройка проверки сертификатов

Kaspersky Security 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.

c. Примените правила веб-контроля.

d. Добавьте и примените правила для сертификатов.

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security 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 разделе **Постоянная защита сервера** в блоке **Защита трафика** нажмите на кнопку **Параметры**.

   Откроется окно **Защита трафика**.

2. На закладке **Общие** из раскрывающегося списка **Режим работы** выберите режим, поддерживающий проверку сертификатов:

   - **Драйверный перехват** (см. раздел "**Настройка режима Драйверный перехват**" на стр. 110);
   - **Перенаправление трафика** (см. раздел "Настройка режима Перенаправление трафика" на стр. 109).

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.

4. Нажмите на кнопку **OK**.

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 для Windows Server создает только запрещающие правила для сертификатов.

► *Чтобы добавить или настроить правило сертификата, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Правила контроля трафика**.

   Откроется окно **Правила контроля трафика**.

4. На закладке **Контроль веб-страниц** установите флажок **Применять правила контроля сертификатов**, чтобы применить правила.

   Если флажок установлен, Kaspersky Security 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 **OK**.

8. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
9. Нажмите на кнопку **OK** 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 программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Правила контроля трафика**.

   Откроется окно **Правила контроля трафика**.
4. Откройте закладку **Категоризация**.
5. Установите флажок **Применять правила для веб-контроля на основе категорий**.

   Если флажок установлен, Kaspersky Security для Windows Server категоризирует и блокирует веб-ресурсы, попадающие в выбранные категории.

   Если флажок снят, Kaspersky Security 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. 123):
   - 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 не доступен для редактирования (вы не можете добавлять или удалять категории).
8. Нажмите на кнопку **OK**.

Параметры правил будут сохранены.

Использование маски not-a-virus

► *Чтобы использовать маску `not-a-virus` для анализа категорий, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security Center откройте параметры задачи Использование KSN (см. раздел "Настройка задачи Использование KSN" на стр. 90).
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 Обработка веб-адресов" на стр. 118) 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**.

Список категорий

Веб ресурсы анализируются и категоризируются по тегам. Каждая категория принадлежит к определенному количеству тегов (см.таблицу ниже).

Таблица 24. 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: об-	Дети, Запрещено Федеральным законом 436 (РФ), Школы и университеты.

Тег	Описание	Список категорий
	разовательные сайты, развлекательные сайты для детей, форумы и блоги о воспитании.	
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.
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.

Тег	Описание	Список категорий
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.
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.

Тег	Описание	Список категорий
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.
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.

Тег	Описание	Список категорий
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 сервера

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

В этом разделе

Контроль запуска программ 128
Контроль устройств 155
Управление сетевым экраном 155
Защита от шифрования 155

Контроль запуска программ

Этот раздел содержит информацию о задаче Контроль запуска программ и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Контроль запуска программ 128
Настройка параметров задачи Контроль запуска программ 130
О правилах контроля запуска программ 140
О формировании списка правил контроля запуска программ 144
О задаче Формирование правил контроля запуска программ 149

О задаче Контроль запуска программ

В ходе выполнения задачи Контроль запуска программ Kaspersky Security для Windows Server отслеживает попытки запуска программ пользователями и разрешает или запрещает их запуск. Основой работы задачи Контроль запуска программ является технология блокировки по умолчанию (Default Deny), которая предполагает автоматическое блокирование запуска любых программ, неразрешенных в параметрах задачи.

Вы можете разрешить запуск программ одним из следующих способов:

- задать разрешающие правила для доверенных программ;
- учитывать репутацию доверенных программ в KSN при их запуске.

Запрет запуска программы имеет абсолютный приоритет: если запуск программы заблокирован одним компонентом задачи Контроль запуска программ, то запуск такой программы будет запрещен вне зависимости от заключений других компонентов задачи. Например, если программа признана недоверенной службами KSN, но подпадает под область действия разрешающего правила, запуск такой программы будет запрещен.

Все попытки запуска программ фиксируются в журнале выполнения задач (см. раздел "О журналах выполнения задач" на стр. 243).

Задача Контроль запуска программ может выполняться в одном из двух режимов:

- **Применять правила контроля запуска программ**. Kaspersky Security для Windows Server контролирует с помощью заданных правил запуск программ, которые подпадают под область применения правил задачи Контроль запуска программ. Область применения правил задачи Контроль запуска программ указывается в параметрах этой задачи. Если программа подпадает под область применения правил задачи Контроль запуска программ, и ее параметры не удовлетворяют ни одному из правил контроля запуска программ, то запуск такой программы запрещен.

  Запуск программ, которые не подпадают под область применения правил, указанную в параметрах задачи Контроль запуска программ, разрешен вне зависимости от параметров правил контроля запуска программ.

  Запуск задачи **Контроль запуска программ** в режиме Применять правила контроля запуска программ невозможен, если не создано ни одно правило или количество созданных правил для одного сервера превышает порог в 65 535 правил.

- **Только статистика**. Kaspersky Security для Windows Server не контролирует запуск программ с помощью правил, а только фиксирует в журнале выполнения задач информацию о запусках программ, правилах контроля запуска программ, которым удовлетворяют запущенные программы, и о действиях, которые были бы предприняты, если бы задача работала в режиме **Применять правила контроля запуска программ**. Запуск всех программ разрешен. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования списка правил контроля запуска программ (см. раздел "Формирование списка правил по событиям задачи Контроль запуска программ" на стр. 148) на основе информации, зафиксированной в журнале выполнения задач.

Вы можете построить работу задачи Контроль запуска программ в соответствии с одним из следующих сценариев:

- Дополнительная настройка правил (см. раздел "О правилах Контроля запуска программ" на стр. 140) и их использование для контроля запуска программ.
- Минимальная настройка правил и использование KSN (см. раздел "Использование KSN в задаче Контроль запуска программ" на стр. 135) для контроля запуска программ.

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Kaspersky Security для Windows Server также перехватывает процессы, запущенные в рамках Windows Subsystem for Linux (за исключением скриптов, запущенных из оболочки UNIX® или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ распознает запуск программы и генерирует соответствующие правила для программ, работающих в рамках Windows Subsystem for Linux.

Настройка параметров задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 25. 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 **Активный** для защиты сервера после того, как будет сформирован окончательный список правил.
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	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически при запуске Kaspersky Security 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 программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.

3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**

4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 132).
     - Область применения правил в задаче (см. раздел "Формирование области применения задачи Контроль запуска программ" на стр. 134).
     - Использование KSN (см. раздел "Использование KSN в задаче Контроль запуска программ" на стр. 135).
   - На закладке **Контроль пакетов установки**:
     - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. 137).
   - На закладках **Расписание** и **Дополнительно**:
     - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53)
5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.

6. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.
7. При необходимости измените список правил контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 140).

Kaspersky Security 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.

Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В раскрывающемся списке **Режим работы** выберите режим работы задачи.

   В раскрывающемся списке вы можете выбрать один из режимов работы задачи Контроль запуска программ:

   - **Активный**. Kaspersky Security для Windows Server контролирует запуск программ с помощью заданных правил.
   - **Только статистика**. Kaspersky Security 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**.

5. 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 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 для Windows Server проверяет программу при каждом ее последующем запуске заново.

   По умолчанию флажок установлен.

   Kaspersky Security для Windows Server заводит новый список прецедентов в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом запуск программ контролируется в соответствии с актуальными настройками безопасности.

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

   Если флажок установлен, Kaspersky Security для Windows Server блокирует 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 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 для Windows Server поддерживает работу со следующими командными интерпретаторами:

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

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Формирование области применения задачи Контроль запуска программ

► *Чтобы сформировать область применения задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. 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 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 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 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 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 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 для Windows Server не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Использование KSN в задаче Контроль запуска программ

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

При использовании данных KSN о репутации программ в задаче Контроль запуска программ репутация программы в KSN является критерием разрешения или блокировки запуска этой программы. Если при попытке запуска программы Kaspersky Security для Windows Server получает недоверенное заключение KSN, запуск такой программы запрещен. Если при попытке запуска программы Kaspersky Security для Windows Server получает доверенное заключение KSN, запуск такой программы разрешен. Вы можете применять KSN совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом сервере без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Security для Windows Server вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

> При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом блокировки по умолчанию. Применение KSN, при отсутствии правил, позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании KSN совместно с правилами контроля запуска программ действуют следующие сценарии:

- Kaspersky Security для Windows Server всегда блокирует запуск программы, если программа подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет вам вручную расширять список нежелательных программ.
- Kaspersky Security для Windows Server всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для такой программы задано разрешающее правило, оно имеет меньший приоритет

и не учитывается; программа все равно будет заблокирована. Это позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу, но не были учтены при предварительной настройке правил.

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Использование KSN** задайте параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Security 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 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.
   - Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Security 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 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.
   - Если флажок **Разрешать запуск программ, доверенных в KSN** установлен, укажите пользователей и / или группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

     a. Нажмите на кнопку **Изменить**.

        Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

     b. Задайте список пользователей и / или групп пользователей.

     c. Нажмите на кнопку **OK**.

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

Настроенные параметры будут сохранены.

Формирование списка доверенных пакетов установки

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 для Windows Server автоматически рассчитывает хеш для каждого вложенного файла и в дальнейшем не применяет принцип блокировки по умолчанию к таким файлам. Kaspersky Security 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 программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла Контроль запуска программ перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
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 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.

  Данный 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 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 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 **OK**.

Настроенные параметры задачи будут сохранены.

О правилах контроля запуска программ

Принцип работы правил контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешать или запрещать запуск программ и называются *разрешающими* или *запрещающими*, соответственно. Для создания списков разрешающих правил контроля запуска программ вы можете использовать задачу для создания разрешающих правил или режим **Только статистика** в задаче Контроль запуска программ. Вы также можете добавлять разрешающие правила вручную (см. раздел "Добавление одного правила контроля запуска программ" на стр. 145).

  > Подробнее о работе с правилами контроля запуска программ можно прочитать в разделе "О формировании правил для задачи Контроль запуск программ" в *Руководстве администратора Kaspersky Security для Windows Server*.

- Пользователь и / или группа пользователей.

  Правила контроля запуска программ контролируют запуски программ указанными в правиле пользователем и / или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут быть применены к запускам *исполняемых файлов программ* или к запускам *скриптов* и *пакетов MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ контролируют запуск тех файлов, которые удовлетворяют указанному в параметрах правила критерию: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

  Если в качестве критерия срабатывания правила установлен параметр **Цифровой сертификат**, созданное правило контролирует запуск любых программ, доверенных в операционной системе. Вы можете задать более строгие условия для этого критерия, установив флажки:

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

  Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий Цифровой сертификат, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

  Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки Задать критерий срабатывания правила из свойств файла, расположенной над блоком Критерий срабатывания правила.

  По умолчанию флажок снят.

- **Использовать отпечаток**

Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий Цифровой сертификат, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки Задать критерий срабатывания правила из свойств файла, расположенной над блоком Критерий срабатывания правила.

По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывания правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для уточнения разрешающих правил: например, если вы хотите разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить выбранные**.
6. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
5. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
6. Нажмите на кнопку **Сохранить**.

Параметры правила будут экспортированы в указанный файл.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу на срабатывание правил, чтобы определить, какие правила контролируют запуск выбранной программы.

По умолчанию Kaspersky Security для Windows Server блокирует программы, запуск которых не контролируется ни одним правилом. Чтобы избежать блокировки запуска важных программ, вам нужно создать разрешающие правила для таких программ.

Если запуск программы контролируется несколькими правилами разных типов, приоритетными при запуске программы считаются запрещающие правила: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы протестировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.
4. Откроется окно **Правила контроля запуска программ**.
5. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
6. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все найденные правила, которые будут срабатывать при запуске указанного файла.

Переход в режим 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, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
6. В поле **Название** введите название правила.
7. В раскрывающемся списке **Тип** выберите вариант **Разрешающее**.
8. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
9. В блоке **Критерий срабатывания правила** выберите **Путь к файлу**.
10. Введите следующую маску: **?:**
11. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Security для Windows Server применит режим разрешения по умолчанию.

О формировании списка правил контроля запуска программ

Вы можете импортировать списки правил контроля запуска программ из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль запуска программ или задачи Формирование правил контроля запуска программ. Списки, содержащиеся в таких XML-файлах, могут использоваться для создания только разрешающих правил контроля запуска программ.

Запрещающие правила контроля запуска программ создаются вручную. Также запрещаются запуски программ, для которых не найдено никаких правил.

Использование задачи Формирование правил контроля запуска программ

XML-файл, сформированный по завершении задачи Формирование правил контроля запуска программ, содержит разрешающие правила для запуска программ, указанных при настройке параметров задачи во время ее запуска. Для программ, запуск которых не разрешен в заданных параметрах задачи, не будет создано ни одного правила и их запуск будет заблокирован по умолчанию.

Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Использование отчета задачи Контроль запуска программ в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль запуска программ в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Security для Windows Server фиксирует все запуски программ на защищаемом сервере в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные сценарии работы защищаемого сервера и хотя бы одна его перезагрузка.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом сервере. Запуск задач автоматического формирования разрешающих правил и контроля запуска программ в режиме **Только статистика** для формирования списков правил рекомендуется выполнять на эталонной машине организации, чтобы учесть все используемые программы в сети.

Перед формированием списка разрешающих правил по программам, запущенным на эталонной машине организации, убедитесь, что на эталонной машине нет вредоносных программ.

Вы можете использовать списки правил, полученные по результатам анализа запуска программ на эталонной машине, при настройке политики в Kaspersky Security Center и применении созданных разрешающих правил для всей сети.

Добавление одного правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется контекстное окно **Параметры правила**.
6. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило запрещало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь и / или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
      i. Нажмите на кнопку **Обзор**.
      ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
      iii. Задайте список пользователей и / или групп пользователей.
      iv. Нажмите на кнопку **OK**.
   e. Выполните следующие действия, если вы хотите взять значения для критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла:
      i. Нажмите на кнопку **Задать критерий срабатывания файла из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.
      ii. Выберите файл и нажмите на кнопку **OK**.

         Значения критериев из файла отобразятся в полях блока Критерий срабатывания правила. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным отпечатком.
- **Хеш SHA256**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, расположенных по указанному пути.

> Kaspersky Security для Windows Server не распознает путь, включающий наклонную черту "/". Используйте обратную наклонную черту "\", чтобы правильно ввести путь.

g. Выполните следующие действия, если хотите добавить исключения из правила:

i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения из правила.

iii. Укажите параметры исключения файлов запуска программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

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

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий Цифровой сертификат, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

    Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки Задать критерий срабатывания правила из свойств файла, расположенной над блоком Критерий

срабатывания правила.

По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий Цифровой сертификат, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки Задать критерий срабатывания правила из свойств файла, расположенной над блоком Критерий срабатывания правила.

  По умолчанию флажок снят.

- **Хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается 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.

  Данный вариант выбран по умолчанию.

- **Путь к файлу**

  Если флажок установлен, Kaspersky Security 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.

i. Нажмите на кнопку **OK**.

ii. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

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

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Формирование списка правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл со списком правил контроля запуска программ, сформированным по событиям задачи Контроль запуска программ, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 132), чтобы зафиксировать в журнале выполнения задачи все срабатывания правил на запуски программ на защищаемом сервере.
2. По завершении выполнения задачи в режиме **Только статистика**, откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Security для Windows Server создаст конфигурационный файл в формате XML со списком правил, сформированных по работе задачи Контроль запуска программ в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. 148) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что запуск критичных для работы компьютера программ (например, файлов операционной системы) разрешен заданными правилами.

Все события работы задачи фиксируются в журнале в ходе выполнения задачи в любом из двух режимов. Вы можете создать конфигурационный файл со списком правил по событиям задачи в режиме **Применять правила контроля запуска программ**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется формировать списки правил до запуска задачи в режиме применения правил контроля запуска программ.

Импорт правил контроля запуска программ из файла формата XML

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Импортировать правила из файла**.
6. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла**:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

Откроется стандартное окно Microsoft Windows **Открыть**.

7. В окне Microsoft Windows **Открыть** выберите XML-файл, который содержит параметры правил контроля запуска программ.
8. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

О задаче Формирование правил контроля запуска программ

Задача Формирование правил контроля запуска программ позволяет автоматически формировать список разрешающих правил контроля запуска программ на основе указанных типов файлов из указанных папок. Например, если вы укажете в качестве параметров задачи исполняемые файлы из папки C:\Program Files (x86), программа будет автоматически формировать правила, по которым разрешается запуск этих файлов. В дальнейшем программа будет разрешать запуск программ, для которых были автоматически сформированы разрешающие правила.

Сформированные правила отображаются по ссылке **Правила контроля запуска программ** в узле **Контроль запуска программ**.

Настройка параметров задачи Автоматическое формирование разрешающих правил

По умолчанию задача Формирование правил контроля запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 26. Параметры задачи Формирование правил контроля запуска программ

по умолчанию

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем сервера, на котором установлен Kaspersky Security для Windows Server.	Вы можете изменить префикс для названий разрешающих правил.
Область применения разрешающих правил	Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов: • файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files; • пакеты MSI, расположенные в папке C:\Windows; • скрипты, расположенные в папке C:\Windows. Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.	Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы.
Критерии формирования разрешающих правил	Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.	Вы можете использовать хеш SHA256 при формировании разрешающих правил. Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль запуска программ; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи автоматического формирования разрешающих правил с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Первый запуск не определен.	Задача Формирование правил контроля запуска программ не запускается автоматически при старте Kaspersky Security для Windows Server. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. В открывшемся окне настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите префикс для названий правил.

       Первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя сервера, на котором установлен Kaspersky Security для Windows Server. Вы можете изменить префикс для названий разрешающих правил.
     - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 152).
   - На закладке **Действия** укажите действия, которые Kaspersky Security для Windows Server должен совершать:
     - При формировании правил (см. раздел "Действия при автоматическом формировании правил контроля запуска программ" на стр. 152).
     - По завершении задачи (см. раздел "Действия по завершении автоматического формирования правил контроля запуска программ" на стр. 154).
   - На закладках **Расписание** и **Дополнительно**:
     - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53)
   - На закладке **Запуск с правами**:
     - Параметры запуска задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 56)
5. Нажмите на кнопку **OK**.

Kaspersky Security 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.

В этом разделе

Ограничение области применения задачи 152

Действия при автоматическом формировании правил контроля запуска программ 152

Действия по завершении автоматического формирования правил контроля запуска программ 154

Ограничение области действия задачи

► *Чтобы ограничить область применения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте следующие параметры задачи:
   - **Создавать разрешающие правила на основе запущенных программ.**

     Флажок включает или выключает автоматическое формирование разрешающих правил контроля запуска программ для уже запущенных программ. Этот вариант рекомендуется, если на компьютере запущен эталонный набор программ, по которому вы хотите построить разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются в соответствии с запущенными программами.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок установлен.

     Флажок не может быть снят, если не выбрана ни одна папка в таблице Создавать разрешающие правила для программ из папок.
   - **Создавать разрешающие правила для программ из папок.**

     В таблице вы можете выбрать или указать области сканирования задачи и типы исполняемых файлов, которые будут учитываются при формировании правил контроля запуска программ. Задача будут формировать разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил контроля запуска программ

► *Чтобы настроить действия, которые Kaspersky Security для Windows Server должен совершать во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Откройте закладку **Действия**.

5. В блоке **При формировании разрешающих правил** настройте следующие параметры:

- **Использовать цифровой сертификат**

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

- **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 Kaspersky Security для Windows Server 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.

Данный 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 группой.

  По умолчанию выбрана группа **Все**.

6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил контроля запуска программ

► *Чтобы настроить действия, которые Kaspersky Security для Windows Server должен совершать по завершении автоматического формирования правил, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Откройте закладку **Действия**.
5. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается по ссылке Правила контроля запуска программ в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Security для Windows Server добавляет правила, сформированные в ходе выполнения задачи Автоматическое формирование разрешающих правил, в список правил контроля запуска программ согласно установленному принципу добавления.

     Если флажок снят, Kaspersky Security для Windows Server не добавляет сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

     Флажок не может быть снят, если не установлен флажок **Экспортировать разрешающие правила в файл**.

   - **Принцип добавления**.

Раскрывающийся список, позволяющий указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

- **Добавлять к существующим правилам**. Правила дополняют список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Заменять существующие правила**. Правила добавляются вместо существующих правил.
- **Объединять с существующими правилами**. Правила дополняют список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

По умолчанию установлен способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт сформированных разрешающих правил контроля запуска программ в файл.

  Если флажок установлен, по завершении задачи автоматического формирования разрешающих правил Kaspersky Security для Windows Server экспортирует сформированные правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи автоматического формирования разрешающих правил Kaspersky Security для Windows Server не экспортирует сформированные правила в файл, а только добавляет их в список правил контроля запуска программ.

  По умолчанию флажок снят.

  Флажок не может быть снят, если не установлен флажок **Добавлять разрешающие правила в список правил контроля запуска программ.**

- **Добавлять информацию о компьютере в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом сервере в имя файла, в который экспортируются сформированные правила контроля запуска программ.

  Если флажок установлен, программа добавляет имя защищаемого сервера, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом сервере в имя файла экспорта.

  Флажок доступен, если установлен флажок **Экспортировать разрешающие правила в файл**.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

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 156
Статистика задачи Защита от шифрования 156
Настройка параметров задачи Защита от шифрования 157

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 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 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 для Windows Server только фиксирует попытки вредоносного шифрования с удаленных компьютеров в журнале выполнения задачи.

Статистика задачи Защита от шифрования

Если задача Защита от шифрования выполняется, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Security для Windows Server обработал с момента запуска этой задачи по текущий момент, то есть статистику задачи.

► *Статистика задачи Защита от шифрования:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел**Защита от шифрования**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые Kaspersky Security для Windows Server обработал за время работы задачи (см. таблицу ниже).

Таблица 27. Статистика задачи Защита от шифрования

Поле	Описание
Обнаружено попыток шифрования	Количество попыток доступа к сетевому хранилищу, при которых Kaspersky Security для Windows Server обнаружил активность шифрования.
Ошибок обработки	Количество запросов программы к области сетевого хранилища, которые закончились ошибкой.
Обработано объектов	Общее количество попыток доступа, которые обработал Kaspersky Security для Windows Server.

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 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**. Kaspersky Security для Windows Server применяет**Средний** уровень проверки. 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 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 программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. В открывшемся окне настройте следующие параметры:
   - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. 158) на закладке **Общие**.
   - Область защиты (см. раздел "Формирование области защиты" на стр. 159) на закладке **Область защиты**.
   - Исключения (см.раздел "Добавление исключений" на стр. 160) на закладке **Исключения**.
   - Запуск задачи по расписанию (см. раздел "Настройка запуска задачи по расписанию" на стр. 53) на закладках **Расписание** и **Дополнительно**.
5. Нажмите на кнопку **Закрыть**.

Kaspersky Security 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 программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
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 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 выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества

ложных срабатываний.

Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

7. Нажмите на кнопку **OK**, 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.

При использовании как предустановленной, так и пользовательской области защиты вы можете исключить выбранные папки из области защиты, например, если данные в этих папках шифруются программами, установленными на удаленных устройствах.

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Область защиты** выберите папки, которые Kaspersky Security для Windows Server будет проверять при выполнении задачи Защита от шифрования:
   - **Все общие сетевые папки сервера**.

     Если выбран данный вариант при работе задачи Защита от шифрования Kaspersky Security для Windows Server проверяет все общие сетевые папки сервера.

     Данный вариант выбран по умолчанию.
   - **Только указанные общие папки**.

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security 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:
   - Вручную:
     a. Введите имя папки общего доступа на защищаемом сервере.
     b. Нажмите кнопку **Добавить**.

     Путь к папке будет добавлен в список.

- Используя поиск:
  a. Нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows.

  b. Выберите папку, которую вы хотите добавить в область защиты задачи.

  c. Нажмите на кнопку **ОК**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Добавление исключений

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладке **Исключения** установите флажок **Учитывать исключенные области защиты**.

   Если флажок установлен, то во время работы задачи Защита от шифрования Kaspersky Security для Windows Server не обнаруживает вредоносное шифрование, осуществляющееся в указанных областях.

   Если флажок снят, Kaspersky Security для Windows Server обнаруживает активность шифрования во всех общих сетевых папках.

   По умолчанию флажок снят, список исключений пуст.
5. Укажите имя папки или маску.
6. Нажмите кнопку **Добавить**.
7. Если требуется, повторите пункты 5-6 для добавления дополнительных исключений.
8. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Исключения из области защиты будут добавлены и применены.

Диагностика системы

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

В этом разделе

Мониторинг файловых операций 161

Анализ журналов 170

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Монитор целостности файлов.

В этом разделе

О задаче Мониторинг файловых операций 161

О правилах мониторинга файловых операций 162

Настройка параметров задачи Мониторинг файловых операций 166

Настройка правил мониторинга 167

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 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. 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 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 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 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 для Windows Server не может получить данные о пользователе вследствие прерывания задачи или сбоя синхронизации данных драйвера и USN-журнала. Если Kaspersky Security 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 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 для Windows Server учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 28. Маркеры файловых операций

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
BASIC_INFO_CHANGE	изменены атрибуты или метки времени файла или папки	NTFS, ReFS
COMPRESSION_CHANGE	изменено сжатие файла или папки	NTFS, ReFS
DATA_EXTEND	размер файла или папки увеличен	NTFS, ReFS
DATA_OVERWRITE	перезаписаны данные в файле или папке	NTFS, ReFS
DATA_TRUNCATION	файл или папка усечены	NTFS, ReFS
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS
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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

Таблица 29. Параметры задачи Мониторинг файловых операций по умолчанию

Параметр	Значение	Как настроить
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список доверенных пользователей	Не задано	Вы можете задать пользователей и/или группы пользователей, действия которых в указанных каталогах будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Security 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 для Windows Server формирует событие мониторинга.

Параметр	Значение	Как настроить
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 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 программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. В открывшемся окне на закладке **Общие** снимите или установите флажок **Контролировать файловые операции во время простоя задачи**.

   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 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.
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 53).
6. Нажмите на кнопку **OK**, 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 программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга**.

   Откроется окно **Правила мониторинга**.
4. Добавьте область мониторинга одним из следующих способов:
   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Обзор папок**.

     b. В открывшемся окне выберите папку, операции в которой вы хотите контролировать, и нажмите кнопку **OK**.

     c. Нажмите на кнопку **Добавить**, чтобы Kaspersky Security для Windows Server начал контролировать файловые операции в указанной области мониторинга.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> - все файлы с расширением <ext> 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 для Windows Server не добавит указанную область мониторинга.

   В правой части окна на закладке **Параметры правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.
5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.
6. Выберите закладку **Пользователи**.
7. Нажмите кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.
8. Выберите пользователей или группы пользователей, которые Kaspersky Security для Windows Server будет считать доверенными для выбранной области мониторинга.
9. Нажмите на кнопку **OK**.

По умолчанию Kaspersky Security для Windows Server считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 162), и формирует для них события с уровнем важности Критическое событие.

10. Выберите закладку **Маркеры файловых операций**.
11. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
    b. В открывшемся списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 162) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Security для Windows Server контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы Kaspersky Security 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 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 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**.
13. 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 для Windows Server будет пропускать области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Security для Windows Server будет фиксировать события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Обзор папок**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите кнопку **Добавить**.

Указанная папка добавится в список исключенных областей.

> Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

14. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры правил.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

В этом разделе

О задаче Анализ журналов 170

Настройка параметров предзаданных правил задачи 172

Настройка правил анализа журналов 173

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Security для Windows Server выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Security 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 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 поджурналжурнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал, 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 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/ru-ru/library/cc952128.aspx).

Настройка параметров предзаданных правил задачи

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. Перейдите на закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Security для Windows Server применяет эвристический анализатор для обнаружения аномальной активности на защищаемом сервере.

   Если этот флажок не установлен, эвристический анализатор выключен, Kaspersky Security 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, перейдите на закладку **Расширенные**.
8. В блоке **Обработка перебора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка сетевого входа** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Security 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 **OK**.

Указанный пользователь добавится в список доверенных.

12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:

a. Введите IP-адрес.

b. Нажмите кнопку **Добавить**.

Указанный IP-адрес добавится в список доверенных.

13. Выберите закладку **Управление задачей**, чтобы настроить расписание запуска задачи.

14. Нажмите на кнопку **OK**.

Параметры задачи Анализ журналов будут сохранены.

Настройка правил анализа журналов

Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.

Откроется окно **Правила анализа журналов**.

4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Security 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 для Windows Server применяет параметры правил по умолчанию.

По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

Вы можете контролировать применение предзаданных правил в списке правил. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать новое пользовательское правило, выполните следующие действия:

a. Введите имя нового правила.

b. Нажмите кнопку **Добавить**.

Созданное правило добавится в общий список правил.

6. Чтобы настроить любое правило, выполните следующие действия:

a. Выберите правило в списке нажатием левой кнопкой мыши.

В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

Комментарии для нового правила пусты.

b. Выберите закладку **Параметры правила**.

c. В блоке **Общие отредактируйте Имя** правила, если требуется.

d. Выберите **Источник для анализа данных**.

7. В блоке **Идентификаторы событий** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

   a. Введите числовое значение идентификатора.

   b. Нажмите кнопку **Добавить**.

      Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

   c. Нажмите на кнопку **Сохранить**.

      Настроенные параметры правил анализа журналов будут применены.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и по настройке параметров безопасности защищаемого сервера.

В этом разделе

О задачах проверки по требованию 175

Статистика задач проверки по требованию 176

Настройка параметров задач проверки по требованию 179

Область проверки в задачах проверки по требованию 186

Проверка съемных дисков 201

Создание задачи проверки по требованию 202

Удаление задачи 205

Переименование задачи 205

О задачах проверки по требованию

Kaspersky Security для Windows Server однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Security для Windows Server проверяет файлы, оперативную память сервера, а также объекты автозапуска.

В Kaspersky Security для Windows Server предусмотрено четыре системные задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при старте Kaspersky Security для Windows Server. Kaspersky Security для Windows Server проверяет загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Security для Windows Server создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет возможно зараженный сектор резервной копией.
- Задача Проверка важных областей по умолчанию выполняется еженедельно по расписанию. Kaspersky Security для Windows Server проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы, которые содержатся в системных папках, например, в папке %windir%\system32. Kaspersky Security для Windows Server применяет параметры безопасности, значения которых соответствуют уровню Рекомендуемый (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 194). Вы можете изменять параметры задачи Проверка важных областей.
- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз. Вы не можете изменять параметры задачи Проверка объектов на карантине.

- Задача Проверка целостности программы запускается каждый раз при старте Kaspersky Security для Windows Server. Она обеспечивает проверку модулей Kaspersky Security для Windows Server на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Значения параметров расписания запуска задачи можно изменять.

Вы можете создавать пользовательские задачи проверки по требованию. Например, вы можете создать задачу проверки папок общего доступа на сервере.

Kaspersky Security для Windows Server может одновременно выполнять несколько задач проверки по требованию.

Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые Kaspersky Security для Windows Server обработал с момента запуска задачи по текущий момент.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач" на стр. 245).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые Kaspersky Security для Windows Server обработал с момента запуска задачи по текущий момент, в таблице ниже.

Таблица 30. Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Security для Windows Server. Например, если Kaspersky Security для Windows Server обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруженных объектов	Количество объектов, которые Kaspersky Security для Windows Server признал зараженными, или обнаруженных объектов, являющихся легальными программами, которые не были исключены из области действия задач постоянной защиты или проверки, и были определены как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
Возможно зараженных объектов	Количество объектов, которые Kaspersky Security для Windows Server признал возможно зараженными.
Объектов не вылечено	Количество объектов, которые Kaspersky Security для Windows Server не вылечил по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов, не помещенных на карантин	Количество объектов, которые Kaspersky Security для Windows Server попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые Kaspersky Security для Windows Server попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server попытался сохранить в резервном хранилище, но это ему не удалось, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые Kaspersky Security для Windows Server вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Security для Windows Server поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Security для Windows Server сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Security для Windows Server удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Security для Windows Server пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые Kaspersky Security для Windows Server пропустил, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые Kaspersky Security для Windows Server обработал.

Вы также можете посмотреть статистику задач проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи проверки по требованию рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Настройка параметров задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Таблица 31. Параметры задач проверки по требованию

Параметр	Значение	Как настроить
Область проверки	Применяется в системных и пользовательских задачах: • Проверка при старте операционной системы: весь сервер, исключая папки общего доступа и объекты автозапуска. • Проверка важных областей: весь сервер, исключая папки общего доступа и некоторые файлы операционной системы • Пользовательские задачи проверки по требованию: весь сервер.	Вы можете изменить область проверки. Вы не можете настроить область защиты для системных задач Проверка объектов на карантине и Проверка целостности программы.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**	Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете выполнить следующие действия: • выбрать другой предустановленный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Эвристический анализатор	Для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач проверки применяется с уровнем анализа **Средний**. Для задачи Проверка объектов на карантине применяется с уровнем анализа **Глубокий.**	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Применение эвристического анализатора в задаче Проверка целостности программы не предусматривается.
Доверенная зона	Применяется	Единый список исключений, который вы можете применять в выбранных задачах.

Параметр	Значение	Как настроить
Использование KSN	Применяется	Вы можете увеличить эффективность защиты сервера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.
Выполнение в фоновом режиме (низкий приоритет)	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Расписание запуска задачи	Применяется в системных задачах: • Проверка при старте операционной системы - **При запуске программы**; • Проверка важных областей - **Еженедельно**; • Проверка объектов на карантине - **После обновления баз программы**; • Проверка целостности программы - **При запуске программы**. Не применяется во вновь созданных пользовательских задачах.	Вы можете настраивать параметры запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты сервера	Статус защиты сервера обновляется еженедельно после выполнения задачи Проверка важных областей.	Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами: • изменяя параметры расписания запуска задачи Проверка важных областей; • изменяя область защиты задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

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

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов узла на закладке **Обзор и управление** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи** Настройте следующие параметры задачи:

- На закладке **Общие**:
- На закладке **Общие**:
  - **Использовать эвристический анализатор** (см. раздел "**Использование эвристического анализатора**" на стр. 71)
  - Выполнение задачи в фоновом режиме (см. раздел "Выполнение задачи проверки по требованию в фоновом режиме" на стр. 185).
  - Использование KSN (на стр. 88).
  - Применение доверенной зоны (см. раздел "Включение и выключение применения доверенной зоны в задачах Kaspersky Security для Windows Server" на стр. 47).
  - Регистрация выполнения задачи Проверка важных областей (см. раздел "Регистрация выполнения задачи Проверка важных областей" на стр. 186)
- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53)
- На закладке **Запуск с правами**:
  - Параметры запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 56)

4. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.

5. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов сервера выберите узлы, которые хотите включить в область проверки.
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 194) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 83).

6. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Kaspersky Security 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 анализатор и настроить уровень анализа для задач Проверка по требованию и Постоянная защита файлов.

► *Чтобы настроить применение эвристического анализатора, выполните следующие действия:*

1. В зависимости от задачи:
   - Для задачи Проверка по требованию:
     a. В дереве Консоли программы разверните узел **Проверка по требованию**.
     b. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
     c. В панели результатов перейдите по ссылке **Свойства**.
   - Для задачи Постоянная защита файлов:
     a. В Консоли программы разверните узел **Постоянная защита файлов**.
     b. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
2. Снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.
4. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены. немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Выполнение задачи проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Security для Windows Server, имеют базовый приоритет **Средний** (Normal).

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, базовый приоритет **Низкий** (Low). Понижение приоритета процесса увеличивает время выполнения задачи, но также может положительно повлиять на скорость выполнения процессов других активных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Вы можете установить максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, приоритет которой вы хотите изменить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

   Флажок изменяет приоритет задачи.

   Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему сервера со стороны других задач Kaspersky Security 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 для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

   По умолчанию флажок снят.
5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Использование KSN

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

► *Чтобы настроить использование KSN в задачах проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Установите или снимите флажок **Использовать KSN для проверки**.

   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.

> Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Регистрация выполнения проверки важных областей

По умолчанию статус защиты сервера отображается в панели результатов узла **Kaspersky Security** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты сервера привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. Флажок установлен только для задачи Проверка важных областей и недоступен для редактирования.

> Вы можете перепривязать задачу проверки по требованию к статусу защиты сервера только из Kaspersky Security Center.

Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

В этом разделе

Об области проверки 187

Настройка параметров отображения файловых ресурсов области проверки 187

Предопределенные области проверки 188

Формирование области проверки 189

Включение в область проверки сетевых объектов 191

Создание виртуальной области проверки 192

Параметры безопасности выбранного узла в задачах проверки по требованию 193

Выбор предустановленных уровней безопасности в задачах проверки по требованию 194

Настройка параметров безопасности вручную 196

Об области проверки

Вы можете настроить область проверки для задач Проверка при старте операционной системы и Проверка важных областей, а также для пользовательских задач проверки по требованию.

По умолчанию задачи проверки по требованию проверяют все объекты файловой системы сервера. Если по требованиям к безопасности нет необходимости проверять все объекты файловой системы, вы можете ограничить область проверки.

В Консоли программы область проверки представляет собой дерево или список файловых ресурсов сервера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого сервера отображаются в виде списка.

► *Чтобы включить отображение файловых ресурсов компьютера в виде дерева,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области защиты**, выберите пункт **Показывать в виде дерева**.

Узлы в списке или дереве файловых ресурсов сервера отображаются следующим образом:

Узел включен в область проверки.

Узел исключен из области проверки.

По крайней мере, один из узлов, вложенных в этот узел, исключен из области проверки или параметры безопасности вложенного узла (узлов) отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области проверки для выбранного вложенного узла.

Имена виртуальных узлов области проверки отображаются шрифтом синего цвета.

Настройка параметров отображения файловых ресурсов области проверки

► *Чтобы выбрать способ отображения файловых ресурсов компьютера при настройке параметров области проверки, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:
   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.

- Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

По умолчанию файловые ресурсы защищаемого сервера отображаются в виде списка.

5. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут применены.

Предопределенные области проверки

Дерево или список файловых ресурсов сервера отображается в панели результатов узла выбранной задачи проверки по требованию по ссылке Настроить область проверки.

Дерево или список файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Security для Windows Server предусмотрены следующие предопределенные области проверки:

- **Мой компьютер**. Kaspersky Security для Windows Server проверяет весь сервер.
- **Локальные жесткие диски**. Kaspersky Security для Windows Server проверяет объекты на жестких дисках компьютера. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Kaspersky Security для Windows Server проверяет объекты на внешних устройствах, например, компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, которую вы используете для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются под системной учетной записью.
- **Системная память**. Kaspersky Security для Windows Server проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Security для Windows Server проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули программ, которые автоматически запускаются при старте компьютера.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом сервере.
- **Виртуальные диски**. Вы можете включать в область проверки динамические диски, папки и файлы, а также диски, которые монтируются на сервер, 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 проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**
  - **Съемные диски**
  - **Системная память**
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows);
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
- Пользовательские задачи проверки по требованию:
  - **Локальные жесткие диски** (исключая папки Windows);
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
  - **Папки общего доступа**

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов сервера в Консоли программы. Чтобы проверить объекты на псевдодиске, включите в область проверки папку на сервере, с которой этот псевдодиск связан.
Подключенные сетевые диски также не отображаются в дереве файловых ресурсов сервера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Формирование области проверки

Если вы управляете Kaspersky Security для Windows Server на защищаемом сервере удаленно, через Консоль программы, установленную на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом сервере, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы измените область проверки в задачах Проверка при старте системы и Проверка важных областей, вы можете восстановить область проверки по умолчанию в этих задачах, выполнив восстановление Kaspersky Security для Windows Server (**Пуск** → **Программы** → **Kaspersky Security для Windows Server** → **Изменение или удаление**). В мастере установки установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 187). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

► *Чтобы сформировать область проверки, работая с деревом файловых ресурсов, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
     - если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на сервере, установите флажок **Съемные диски**);
     - если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
6. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область защиты, работая со списком файловых ресурсов, выполните следующие действия*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.

c. В открывшемся окне **Добавление области проверки** выберите тип объекта, который вы хотите добавить в область проверки:

- **Предопределенная область**, если вы хотите включить в область проверки одну из предопределенных областей на защищаемом сервере. Затем в раскрывающемся списке выберите необходимую область.
- **Диск, папка или сетевой объект**, если вы хотите включить в область проверки отдельный диск, папку или сетевой объект нужного типа. Затем выберите необходимый файл по кнопке **Обзор**.
- **Файл**, если вы хотите включить в область проверки только отдельный файл на диске. Затем выберите необходимый файл по кнопке **Обзор**.

Вы не можете добавить объект в область проверки, если он уже добавлен в качестве исключения из области защиты.

5. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:

   a. Откройте контекстное меню области проверки по правой клавише мыши.

   b. В контекстном меню выберите пункт **Добавить исключение**.

   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.

6. Чтобы изменить добавленную область проверки или исключение, в контекстном меню области, которую хотите изменить, выберите пункт **Изменить область**.

7. Чтобы скрыть отображение ранее добавленной области проверки или исключения в списке файловых ресурсов, в контекстном меню области, которую хотите скрыть, выберите пункт **Удалить из списка**.

   Область проверки исключается из области действия задачи проверки по требованию при ее удалении из списка файловых ресурсов.

8. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы не можете сканировать сетевые папки при работе под системной учетной записью.

► *Чтобы добавить в область проверки сетевой объект, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу **проверки по требованию**, в область проверки которой вы хотите добавить сетевой путь.

3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В контекстном меню названия узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
   - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
6. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
7. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
8. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
9. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Вы можете включать в область проверки динамические диски, папки и файлы – создавать виртуальную область проверки.

> Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 187).

► *Чтобы добавить в область проверки виртуальный диск, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В дереве файловых ресурсов сервера откройте контекстное меню на узле **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.
6. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► *Чтобы добавить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в которой вы хотите создать виртуальную область проверки.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В дереве файловых ресурсов сервера откройте контекстное меню диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если хотите добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, если хотите добавить виртуальный файл в область защиты.
6. В поле ввода задайте имя для папки или файла.

   Указывая имя файла, вы можете задать его маску с помощью специальных символов * и ?.
7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область проверки.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задачах проверки по требованию

В выбранной задаче проверки по требованию вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты или проверки, так и различными для разных узлов в дереве или списке 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.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех предустановленных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов в дереве или списке файловых ресурсов сервера (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

Выбор предустановленных уровней безопасности в задачах проверки по требованию

Можно применить один из трех предустановленных уровней безопасности для узла, выбранного в дереве файловых ресурсов сервера: Максимальное быстродействие, Рекомендуемый и Максимальная защита. Каждый из предустановленных уровней безопасности 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 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 влияния 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 безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Проверка объектов	По формату	Все объекты.	Все объекты.
Оптимизация	Включена	Выключено	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно (**Выполнять рекомендуемое действие**)	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Карантин	Помещать на карантин (**Выполнять рекомендуемое действие**)	Карантин
Исключать файлы.	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.).	60 сек.	Нет	Нет
Не проверять составные объекты размером более (МБ).	8 MB	Нет	Нет

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков MBR.	Да	Да	Да
Проверять составные объекты.	• SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • почтовые базы* • файлы почтовых форматов* • упакованные объекты* • вложенные OLE-объекты* * Все объекты

Параметры безопасности: **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** – не входят в набор параметров предустановленных уровней безопасности. Если вы измените состояние параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, или **Использовать эвристический анализатор**, выбранный вами предустановленный уровень безопасности не изменится.

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

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В дереве или в списке файловых ресурсов сервера выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.
5. Убедитесь, что выбранный узел включен в область проверки.
6. В правой части окна на закладке **Уровень безопасности** выберите уровень безопасности, который вы хотите применить.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
7. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый** (см. раздел "Выбор предустановленных уровней безопасности" на стр. 82).

Вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области проверки, 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, выполните следующие действия:*

1. В Консоли Kaspersky Security для Windows Server разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   Предопределенный шаблон с параметрами безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 60) можно применить к выбранному узлу в области проверки.
5. Настройте 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 **Проверка объектов** укажите объекты, которые вы хотите включить в область проверки:
     - **Все объекты.**

       Kaspersky Security для Windows Server проверяет все объекты.
     - **Объекты, проверяемые по формату.**

       Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

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

       Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
     - **Объекты, проверяемые по указанному списку расширений.**

       Kaspersky Security 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**.

- **Загрузочные секторы дисков MBR.**

  Включение защиты загрузочных секторов дисков и главных загрузочных записей.

  Если флажок установлен, Kaspersky Security 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 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 для Windows Server новыми или измененными с момента последней проверки.

  Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

  Если флажок снят, Kaspersky Security 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 **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Все / Только новые архивы.**

  Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

  Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет SFX-архивы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Security 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 для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Security для Windows Server пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

Вы можете выбрать проверку всех или только новых составных объектов, если установлен флажок **Проверка только новых и измененных файлов**. Если флажок **Проверка только новых и измененных файлов** снят, Kaspersky Security для Windows Server проверяет все указанные составные объекты.

- На закладке **Действия**, если требуется, выполните следующие действия:
  - выберите действие над зараженными и другими обнаруживаемыми объектами;
  - выберите действие над возможно зараженными объектами;
  - если требуется, настройте действия в зависимости от типа обнаруженного объекта;

- Выберите действия над неизменяемыми контейнерами: снимите или установите флажок **Форсировать удаление родительского файла-контейнера при обнаружении вложенного зараженного или другого объекта**, если изменение контейнера невозможно.

  Флажок включает или выключает форсированное удаление 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 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 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 для Windows Server пропускает при проверке указанные объекты.

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

    Если флажок снят, Kaspersky Security 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 составные объекты размером более (МБ).**

  Исключение из проверки составных объектов больше указанного размера.

  Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Security 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 для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Security для Windows Server проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

- **Проверять подпись Microsoft у файлов**

  Флажок включает или выключает проверку файлов на наличие цифровой подписи Microsoft.

  Если флажок установлен, Kaspersky Security для Windows Server пропускает файлы с цифровой подписью Microsoft в ходе выполнения задачи проверки по требованию.

  Если флажок снят, программа не проверяет файлы на наличие цифровой подписи Microsoft.

  По умолчанию флажок установлен для всех уровней безопасности.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

Проверка съёмных дисков

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

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

Kaspersky Security 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 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 33. 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 для Windows Server не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.

Параметр	Значение по умолчанию	Описание
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 программы откройте контекстное меню узла **Kaspersky Security** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съёмных дисков**.

2. 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 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.

3. Нажмите на кнопку **OK**.

   Настроенные параметры будут сохранены и применены.

Создание задачи проверки по требованию

Вы можете создавать пользовательские задачи в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Security для Windows Server создание пользовательских задач не предусмотрено.

► *Чтобы создать новую задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.
3. Введите следующую информацию о задаче:
   - **Имя** – имя задачи, не более 100 символов, может содержать любые символы, кроме **% ? I \ | / : * < >**.

     Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано имя задачи.
   - **Описание** – любая дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.
4. Если требуется, настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Использовать эвристический анализатор**

       Флажок включает или выключает использование эвристического анализатора при проверке объектов.

       Если флажок установлен, эвристический анализатор включен.
       Если флажок снят, эвристический анализатор выключен.
       По умолчанию флажок установлен.
     - **Выполнять задачу в фоновом режиме.**

       Флажок изменяет приоритет задачи.

       Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему сервера со стороны других задач Kaspersky Security 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 для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

       По умолчанию флажок снят.
     - **Применять доверенную зону.**

       Флажок включает или выключает применение доверенной зоны в работе задачи.

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

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

       По умолчанию флажок установлен.

- **Считать выполнение задачи проверкой важных областей.**

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты 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 для Windows Server. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует событие Выполнена проверка важных областей и обновляет статус защиты 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.

- **Использовать KSN для проверки.**

  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.

- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53)
- На закладке **Запуск с правами**:
  - Параметры запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 56)

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

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли. Операция регистрируется в журнале системного аудита (на стр. 241).

6. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов сервера выберите узлы, которые хотите включить в область проверки.
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 194) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 83).

7. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Пользовательская задача проверки по требованию будет создана. Настроенные параметры будут применены при последующем запуске задачи.

Удаление задачи

В Консоли программы вы можете удалять только пользовательские задачи проверки по требованию. Вы не можете удалять системные или групповые задачи.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите удалить.
3. Выберите пункт **Удалить задачу**.

   Откроется окно подтверждения операции.
4. Нажмите на кнопку **Да**, чтобы подтвердить операцию удаления.

Задача будет удалена, операция удаления будет зарегистрирована в журнале системного аудита.

Переименование задачи

В Консоли программы вы можете переименовывать только пользовательские задачи проверки по требованию. Вы не можете переименовывать системные или групповые задачи.

► *Чтобы переименовать задачу, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите переименовать.
3. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**
4. В открывшемся окне введите новое имя задачи в поле **Имя**.
5. Нажмите на кнопку **OK**.

Задача будет переименована. Операция будет зарегистрирована в журнале системного аудита.

Обновление баз и модулей Kaspersky Security для Windows Server

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Security для Windows Server, копировании обновлений и откате обновления баз Kaspersky Security для Windows Server, а также инструкции по настройке параметров задач обновления баз и модулей программы.

В этом разделе

О задачах обновления 206

Об обновлении модулей Kaspersky Security для Windows Server 207

Об обновлении баз Kaspersky Security для Windows Server 208

Схемы обновления баз и модулей антивирусных программ в организации 208

Настройка задач обновления 212

Откат обновления баз Kaspersky Security для Windows Server 218

Откат обновления программных модулей 218

Статистика задач обновления 219

О задачах обновления

В Kaspersky Security для Windows Server предусмотрены четыре системные задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Security для Windows Server соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского". Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. 212), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Security для Windows Server применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

Обновление баз программы

По умолчанию Kaspersky Security for Windows Server копирует базы из источника обновлений на защищаемый сервер и сразу переходит к их использованию в выполняющейся задаче Постоянная защита. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление баз программы ежечасно.

Обновление модулей программы

По умолчанию Kaspersky Security для Windows Server копирует обновления программных модулей из источника обновлений на защищаемый сервер. Для применения установленных программных модулей может потребоваться перезагрузка компьютера и / или перезапуск Kaspersky Security для Windows Server.

По умолчанию Kaspersky Security for Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого сервера). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Security для Windows Server, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Security для Windows Server загружает файлы обновлений баз и программных модулей и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

Откат обновления баз программы

В ходе выполнения задачи Kaspersky Security для Windows Server возвращается к использованию баз с предыдущими установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении модулей Kaspersky Security для Windows Server

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Security для Windows Server. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Security for Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого сервера).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматизированной установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Security для Windows Server с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждый защищаемый сервер или использовать один компьютер в качестве посредника, копируя обновления на него без их установки, а затем распределяя их на серверы защищаемой сети. Чтобы копировать и сохранять обновления без их установки, используйте задачу Копирование обновлений.

Перед тем как установить обновления модулей, Kaspersky Security для Windows Server создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Security для Windows Server автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений. На время установки полученных обновлений служба Kaspersky Security Service автоматически останавливается, а затем снова запускается.

Об обновлении баз Kaspersky Security для Windows Server

Базы Kaspersky Security for Windows Server, хранящиеся на защищаемом сервере, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения компьютера к минимуму, регулярно получайте обновления баз.

По умолчанию, если базы Kaspersky Security для Windows Server не обновляются в течение недели с момента создания последних установленных обновлений баз, возникает событие *Базы устарели.* Если базы не обновляются в течение двух недель, возникает событие *Базы сильно устарели*. Информация об актуальности баз (см. раздел "Просмотр состояния защиты и информации о Kaspersky Security для Windows Server" на стр. 23) отображается в узле Kaspersky Security дерева Консоли. Вы можете использовать общие параметры Kaspersky Security для Windows Server, чтобы указать другое количество дней до возникновения этих событий. Вы также можете настроить уведомления для администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. 255).

Kaspersky Security 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.

Вы можете загружать обновления на каждый защищаемый сервер или использовать один сервер в качестве посредника, копируя обновления на него и затем распределяя их на компьютеры. Если вы используете программу Kaspersky Security Center для централизованного управления защитой серверов в организации, вы можете использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз вручную или по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 53). По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление баз программы ежечасно.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Security для Windows Server автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Security для Windows Server вы можете сами откатить базы (см. раздел "Откат обновления баз Kaspersky Security для Windows Server" на стр. 218) до предыдущих установленных обновлений.

Схемы обновления баз и модулей антивирусных программ в организации

Ваш выбор источника обновлений в задачах обновления зависит от того, какую схему обновления баз и модулей антивирусных программ вы используете в организации.

Вы можете обновлять базы и модули Kaspersky Security для Windows Server на защищаемых серверах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый сервер (схема 1);
- загружать обновления из интернета на компьютер-посредник и распределять обновления на серверы с этого компьютера.

Посредником может служить любой компьютер, на котором установлена одна из следующих программ:

- Kaspersky Security для Windows Server (один из защищаемых серверов) (схема 2);
- Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через компьютер-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность компьютеров сети..

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление напрямую из интернета

Данная схема обновлений не рекомендуется при использовании программы в сертифицированной конфигурации, так как при работе через интернет напрямую Kaspersky Security для Windows Server отправляет данные через запросы на скачивание.

► *Чтобы настроить получение обновлений Kaspersky Security для Windows Server напрямую из интернета,*

на каждом защищаемом сервере в настройках параметров задач Обновление баз программы и Обновление модулей программы в качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

Вы можете указать в качестве источника обновлений другие HTTP- или FTP-серверы, которые содержат папку с файлами обновлений.

Схема 2. Обновление через один из защищаемых серверов

► *Чтобы настроить получение обновлений Kaspersky Security для Windows Server через один из защищаемых серверов, выполните следующие действия:*

1. Скопируйте обновления на выбранный защищаемый сервер. Для этого выполните следующие действия:
   - На выбранном сервере настройте параметры задачи Копирование обновлений:
     a. В качестве источника обновлений укажите компьютеры обновлений "Лаборатории Касперского".
     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.

2. Распределите обновления на остальные защищаемые серверы. Для этого выполните следующие действия:
   - На каждом из защищаемых серверов настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже):
     a. В качестве источника обновлений укажите папку на диске компьютера-посредника, в которую вы скопировали обновления.

Kaspersky Security для Windows Server будет получать обновления через один из защищаемых серверов.

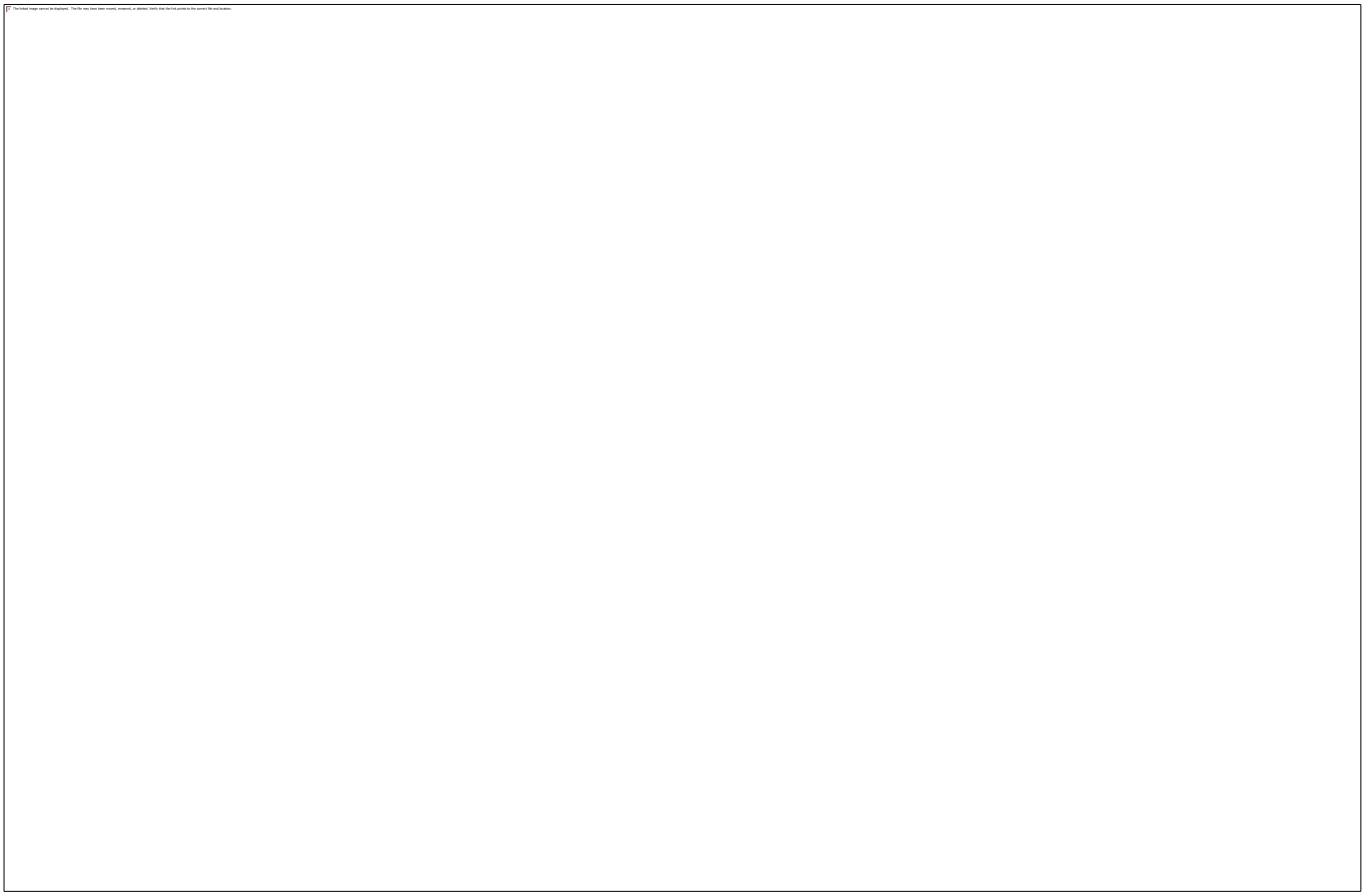

Схема 3. Обновление через Сервер администрирования Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров, вы можете загружать обновления через Сервер администрирования Kaspersky Security Center (см. рис. ниже).

► *Чтобы настроить получение обновлений Kaspersky Security для Windows Server через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с сервера обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора компьютеров:
     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".
2. Распределите обновления на защищаемые серверы. Для этого выполните одно из следующих действий:
   - Настройте на Сервере администрирования Kaspersky Security Center групповую задачу обновления для распределения обновлений на защищаемые серверы:
     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

     Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

Вы не можете указывать частоту запуска После получения обновлений Сервером администрирования в Консоли программы.

- Настройте на каждом из защищаемых серверов задачи Обновление баз программы и Обновление модулей программы:
  a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.
  b. Если требуется, настройте расписание задачи.

При редких обновлениях антивирусных баз Kaspersky Security для Windows Server (от одного раза в месяц, до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

Kaspersky Security для Windows Server будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых серверов программный компонент Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Security для Windows Server на сервере. Подробная информация об Агенте администрирования и его настройке с помощью программы Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center*.

Настройка задачи Обновление

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Security для Windows Server.

В этом разделе

Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server 212

Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы 215

Настройка параметров задачи Копирование обновлений 216

Настройка параметров задачи Обновление модулей программы 217

Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, вы можете указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► *Чтобы указать тип источника обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Источник обновлений** выберите тип источника обновлений Kaspersky Security для Windows Server:
   - **Сервер администрирования Kaspersky Security Center**

     Kaspersky Security для Windows Server использует в качестве источника обновления Сервер администрирования Kaspersky Security Center.

     Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" выполняется с помощью системы удаленного управления Kaspersky Security Center и на защищаемом сервере установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь компьютеров с Сервером администрирования.
   - **Серверы обновлений "Лаборатории Касперского".**

     Kaspersky Security для Windows Server использует в качестве источника обновлений интернет-сайты "Лаборатории Касперского", на которых публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

     Данный вариант выбран по умолчанию.
   - **Другие HTTP-,FTP-серверы и сетевые ресурсы**

     Kaspersky Security для Windows Server использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы, папки на компьютерах локальной сети.

     Вы можете сформировать список источников, которые содержат актуальный набор обновлений, нажав на ссылку **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:
   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
      i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.
      ii. Нажмите на кнопку **OK**.
   b. В блоке **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны** устанавливаете флажок.

      Флажок включает или выключает функцию использования серверов обновлений

"Лаборатории Касперского" в качестве источника обновлений, если выбранные вами источники обновлений недоступны.

Если флажок установлен, функция активна.

По умолчанию флажок установлен.

Вы можете установить флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, когда выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского".**

     Флажок включает / выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского", или установлен флажок Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны.

     Если флажок установлен, параметры прокси-сервера используются.

     Если флажок снят, параметры прокси-сервера не используются.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

     Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант Другие HTTP-, FTP-серверы или сетевые ресурсы.

     Если флажок установлен, параметры прокси-сервера используются.

     По умолчанию флажок снят.

7. Нажмите на кнопку **OK**.

Настроенные параметры источника обновлений Kaspersky Security для Windows Server будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Security для Windows Server.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.

5. Выполните следующие действия:
   - Чтобы добавить новый пользовательский источник обновления, в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере; укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

     По умолчанию добавленная папка используется в качестве источника обновлений.
   - Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
   - Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
   - Чтобы изменить очередность обращения Kaspersky Security для Windows Server к пользовательским источникам, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, хотите вы использовать его раньше или позже.
   - Чтобы изменить путь к пользовательскому источнику, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
   - Чтобы удалить пользовательский источник, выберите его в списке и нажмите на кнопку **Удалить**.

     Вы не можете удалить единственный пользовательский источник из списка.
6. Нажмите на кнопку **OK**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Security для Windows Server размещает файлы обновлений на локальном диске сервера. Вы можете снизить нагрузку на дисковую подсистему сервера за счет размещения файлов обновлений на виртуальном диске в оперативной памяти в процессе выполнения задачи обновления.

Эта функция доступна для Microsoft Windows Vista®, Microsoft Windows Server® 2008 и более поздних версиях операционных систем.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

► *Чтобы снизить нагрузку на дисковую подсистему компьютера при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.

3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.
4. Откроется окно **Параметры задачи** на закладке **Общие**.
5. В блоке Оптимизация использования дисковой подсистемы настройте следующие параметры:
   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

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

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.
   - В поле **Объем оперативной памяти, используемый для оптимизации**, укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ.
6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений.**
3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server" на стр. 212).
5. На закладке **Общие** в блоке **Параметры копирования обновлений** выполните следующие действия:
   - Укажите условия копирования обновлений программы:
     - **Копировать обновления программы**.

       Kaspersky Security для Windows Server загружает только обновления баз Kaspersky Security для Windows Server.

       Данный вариант выбран по умолчанию.
     - **Копировать критические обновления модулей программы**.

       Kaspersky Security для Windows Server загружает только срочные обновления программных модулей Kaspersky Security для Windows Server.
     - **Копировать обновления баз программы и критические обновления модулей программы**.

Kaspersky Security для Windows Server загружает обновления баз и срочные обновления программных модулей Kaspersky Security для Windows Server.

- Укажите локальную или сетевую папку, в которую Kaspersky Security для Windows Server будет копировать полученные обновления.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 53).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуск задачи" на стр. 56).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. В панели результатов узла **Обновление модулей программы** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server" на стр. 212).
5. На закладке **Общие** в блоке **Параметры обновления** настройте параметры обновления модулей программы:

   - **Только проверять наличие доступных критических обновлений модулей программы.**

     Kaspersky Security для Windows Server выполняет уведомление об имеющихся на источнике срочных обновлениях программных модулей без скачивания обновлений

     Уведомление производится, если оповещение о событиях этого типа настроено.

     Данный вариант выбран по умолчанию.
   - **Копировать и устанавливать критические обновления модулей программы.**

     Kaspersky Security для Windows Server копирует и устанавливает срочные обновления программных модулей.
   - **Разрешать перезагрузку компьютера.**

     Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.

     Если флажок установлен, Kaspersky Security для Windows Server выполняет перезагрузку операционной системы после установки обновлений, требующих перезагрузки.

     Флажок активен, если выбран вариант **Копировать и устанавливать критические обновления модулей программы**.

По умолчанию флажок снят.

- **Получать информацию о доступных обновлениях модулей программы.**

  Получение уведомлений обо всех имеющихся на источнике плановых обновлений программных модулях Kaspersky Security для Windows Server. Kaspersky Security для Windows Server выполняет уведомления в том случае, если настроено оповещение о событиях этого типа.

  Если флажок установлен, Kaspersky Security для Windows Server выполняет уведомление обо всех имеющихся на источнике плановых обновлениях программных модулей.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 53). По умолчанию Kaspersky Security for Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого сервера).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 56).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступно плановое обновление модулей программы*, в котором будет содержаться адрес страницы веб-сайта, с которой вы можете загрузить плановые обновления.

Откат обновления баз Kaspersky Security для Windows Server

Перед применением обновления баз Kaspersky Security для Windows Server создает резервные копии баз, которые использовались ранее. Если обновление прервалось или завершилось с ошибкой, Kaspersky Security для Windows Server автоматически возвращается к использованию баз с предыдущими установленными обновлениями.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз.

► *Чтобы запустить задачу Откат обновления баз,*

перейдите по ссылке Запустить в панели результатов узла **Откат обновления баз программы**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Security для Windows Server создает резервные копии модулей, используемых в текущий момент. Если обновление модулей прервалось или завершилось с ошибкой, Kaspersky Security для Windows Server автоматически возвращается к использованию модулей с последними установленными обновлениями.

Чтобы откатить программные модули, используйте компонент панели управления Microsoft Windows **Установка и удаление программ**.

Статистика задач обновления

Пока выполняется задача обновления, вы можете просматривать в реальном времени информацию об объеме данных, полученных с момента запуска задачи по текущий момент, а также другую информацию о выполнении задачи.

После завершения или остановки задачи эту информацию можно просмотреть в журнале выполнения задачи.

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Если вы просматриваете задачу Обновление баз программы или задачу Копирование обновлений, в блоке **Статистика** отображается объем данных, загруженных Kaspersky Security для Windows Server на текущий момент (**Полученные данные**).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Таблица 34. Информация о задаче Обновление модулей программы

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Вы можете просмотреть название обновления, при применении которого возникла ошибка, в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач" на стр. 245).

Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

В этом разделе

Изолирование возможно зараженных объектов.Карантин 220

Резервное копирование объектов.Резервное хранилище..... 229

Блокирование доступа к сетевым файловым ресурсамЗаблокированные узлы.236

Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

В этом разделе

Об изолировании возможно зараженных объектов..... 220

Просмотр объектов на карантине 221

Проверка объектов на карантине..... 222

Восстановление содержимого карантина..... 224

Помещение объектов на карантин..... 226

Удаление объектов из карантина..... 226

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" 226

Настройка параметров карантина..... 228

Статистика карантина..... 229

Об изолировании возможно зараженных объектов

Kaspersky Security 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.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов на карантине,*

отсортируйте объекты (см. раздел "Сортировка объектов на карантине" на стр. 221) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. 221).

Сортировка объектов на карантине

По умолчанию объекты в списке объектов на карантине отсортированы по дате помещения в обратном хронологическом порядке. Чтобы найти нужный объект, вы можете отсортировать объекты по содержимому столбцов с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты в списке.

Объекты в списке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, вы можете отфильтровать объекты в списке – отобразить только те объекты, которые удовлетворяют заданным вами критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы покинете и снова откроете узел Карантин или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать один или несколько фильтров, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню названия узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.

b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в списке **Название поля**.

c. В поле **Значение поля** введите или выберите в списке значение фильтра.

d. Нажмите кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

- Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы изменить фильтр, выберите фильтр из списка в окне **Параметры фильтра**. Затем измените нужные значения в полях **Имя поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

1. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы снова отобразить все объекты в списке объектов на карантине,*

в контекстном меню названия узла **Карантин** выберите пункт **Снять фильтр**.

Проверка карантина

По умолчанию после каждого обновления баз Kaspersky Security для Windows Server выполняет системную задачу Проверка объектов на карантине. Параметры задачи приводятся в таблице ниже. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Вы можете настраивать расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 53), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 56), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Security для Windows Server может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Security для Windows Server может признать зараженными и выполнить над ними действия, указанные параметрами задачи проверки по требованию Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Таблица 35. Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки; их значения приводятся в следующей таблице.

Таблица 36. Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверка объектов	Все объекты области проверки
Оптимизация	Выключено
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Пропускать
Исключать объекты	Нет
Не обнаруживать	Нет
Останавливать проверку, если длится более (сек.)	Не задано
Не проверять составные объекты размером более (МБ).	Не задано
Альтернативные потоки NTFS	Включена
Загрузочные секторы дисков MBR.	Выключено
Использовать технологию iChecker	Выключено
Использовать технологию iSwift	Выключено
Проверять составные объекты.	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Проверка только новых и измененных файлов выключена.
Проверка подписи Microsoft у файлов	Не выполняется
Использовать эвристический анализатор	Включено с уровнем анализа **Глубокий**
доверенная зона;	Не применяется

Восстановление содержимого карантина

Kaspersky Security для Windows Server помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстановить любой объект из карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для сервера и хотите его использовать. Чтобы Kaspersky Security для Windows Server не изолировал этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать объекты** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в доверенную зону (см. раздел "Настройка доверенной зоны" на стр. 45).

При восстановлении объекта вы можете выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановления на защищаемом сервере или в указанной вами папке на сервере, на котором установлена Консоль программы, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом сервере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению сервера.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Security для Windows Server не включает его снова составной объект при восстановлении, а сохраняет отдельно, в указанной папке.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты из карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выполните одно из следующих действий:
   - чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**;
   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на одном из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект. (Название файла отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:

   - чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**;
   - чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления в параметрах выберите **Восстановить в серверную папку, используемую по умолчанию**.
   - чтобы сохранить объект в другой папке на сервере, на котором установлена Консоль Kaspersky Security для Windows Server, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

5. Если вы хотите сохранить копию объекта в папке карантина после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

6. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

7. Нажмите на кнопку **OK**.

   Kaspersky Security для Windows Server начнет восстанавливать первый из выбранных вами объектов.

8. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Security для Windows Server:

      - **Заменить**, чтобы сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
      - **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции используемую будет зарегистрирована в журнале системного аудита.

   Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню названия узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **OK**.

   Kaspersky Security для Windows Server поместит указанный файл на карантин.

Удаление объектов из карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Security для Windows Server автоматически удаляет из папки карантина объекты, статус которых при проверке карантина с использованием обновленных баз изменился на *зараженный или обнаруживаемый* и которые Kaspersky Security для Windows Server не удалось вылечить. Остальные объекты Kaspersky Security для Windows Server не удаляет.

Вы можете вручную удалить из карантина один или несколько объектов.

► *Чтобы удалить из карантина один или несколько объектов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт **Удалить**.
4. **В открывшемся окне нажмите на кнопку** Да, чтобы подтвердить операцию.

Выбранные объекты будут удалены из карантина.

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-либо файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Security для Windows Server признает этот файл незараженным, то, возможно, вы встретились с неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись и алгоритм лечения в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Security для Windows Server признает его зараженным и ему удастся его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы из карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Вы не можете отправлять объекты из карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

► *Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:*

1. Если файл не находится на карантине, предварительно **поместите его на карантин**.
2. В узле **Карантин**, в списке объектов на карантине, откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.
3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.
4. Если на сервере, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** сообщения содержит адрес электронной почты "Лаборатории Касперского" newvirus@kaspersky.com. Поле Тема содержит текст "Объект карантина".

   Тело сообщения содержит текст "Файл будет отправлен в "Лабораторию Касперского" для исследования". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

   В сообщение вложен архив <имя объекта>.cab. Он содержит файл <uuid>.klq с зашифрованным объектом (где uuid – уникальный идентификатор объекта в Kaspersky Security для Windows Server), файл <uuid>.txt с информацией, полученной Kaspersky Security для Windows Server об объекте, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Security для Windows Server и операционной системе на сервере:

   - название и версию операционной системы;
   - название и версию Kaspersky Security для Windows Server;
   - дата выпуска последних установленных обновлений баз;
   - номер активного ключа.

   Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и эффективнее проанализировать файл. Однако если вы не хотите передавать ее, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на сервере, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл вы можете переслать в "Лабораторию Касперского" самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **Да**.
2. Выберите папку на диске защищаемого сервера или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

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

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню названия вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Параметры хранилища** настройте нужные параметры карантина в соответствии с вашими требованиями:
   - В блоке **Параметры карантина**:
     - **Папка карантина**

       Путь к папке карантина в формате UNC (Universal Naming Convention).

       По умолчанию установлен путь C:\ProgramData\Kaspersky Security for Windows Server\10.1\Quarantine\.
     - **Максимальный размер карантина.**

       Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Security для Windows Server фиксирует событие Превышен максимальный размер карантина и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

       Если флажок установлен, Kaspersky Security для Windows Server отслеживает суммарный размер размещенных в карантине объектов.

       Если флажок снят, Kaspersky Security для Windows Server не отслеживает суммарный размер объектов в карантине.

       По умолчанию флажок снят.
     - **Порог доступного пространства.**

       Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Security для Windows Server фиксирует событие Превышен порог свободного места в резервном хранилище и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

       Если флажок установлен, Kaspersky Security для Windows Server отслеживает размер свободного места в резервном хранилище.

Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

По умолчанию флажок установлен.

Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Security для Windows Server уведомит вас об этом, не переставая помещать объекты на карантин.

- В блоке **Параметры восстановления объектов**:
  - **Папка, в которую восстанавливаются объекты.**

5. Нажмите на кнопку **OK**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в контекстном меню названия узла **Карантин** в дереве Консоли программы выберите пункт **Статистика**.

В окне **Статистика** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

Поле	Описание
Возможно зараженных объектов	Количество объектов, которые Kaspersky Security для Windows Server признал возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которые получили статус *Ложное срабатывание*, так как при проверке карантина с применением обновленных баз были признаны незараженными..
Вылечено объектов	Количество объектов, которые после проверки карантина получили статус *Вылеченный*.
Всего объектов	Общее количество объектов на карантине.

Резервное копирование объектов. Резервное хранилище:

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

В этом разделе

О резервном копировании объектов перед лечением или удалением 230
Просмотр объектов в резервном хранилище 230
Восстановление файлов из резервного хранилища 232
Удаление файлов из резервного хранилища 234
Настройка параметров резервного хранилища 234
Статистика резервного хранилища 236

О резервном копировании объектов перед лечением / удалением

Kaspersky Security для Windows Server сохраняет зашифрованные копии объектов со статусами *зараженный или обнаруживаемый* и *возможно зараженный* в *резервном хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Security для Windows Server сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Security для Windows Server признал зараженным один из объектов в составе почтовой базы, он резервирует всю почтовую базу.

Если объект, который Kaspersky Security для Windows Server копирует в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске вашего компьютера.

Вы можете восстанавливать файлы из резервного хранилища, как в исходную папку, так и в другую папку на защищаемом сервере или другом компьютере в локальной сети организации. Вы можете восстановить файл из резервного хранилища, например, если исходный зараженный или возможно зараженный файл содержал важную информацию, но при лечении этого файла Kaspersky Security для Windows Server не удалось сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению сервера.

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только через Консоль программы, в узле **Резервное хранилище**. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище,*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов в резервном хранилище,*

отсортируйте объекты или отфильтруйте их.

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их сохранения в обратном хронологическом порядке. Чтобы найти нужный файл, вы можете отсортировать файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы покинете и снова откроете узел Резервное хранилище или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В списке файлов в **резервном хранилище** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат фильтрации сохранится, если вы покинете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
2. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, со значениями которого будет сравниваться указанное вами значение фильтра при отборе.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.
   c. В поле **Значение поля** введите или выберите значение фильтра.
   d. Нажмите кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

- Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► *Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,*

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

Восстановление файлов из резервного хранилища

Kaspersky Security для Windows Server хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный файл, который оказался зараженным, содержал важную информацию, при лечении файла Kaspersky Security для Windows Server не удалось сохранить его целостность, и в результате информация в файле стала недоступной;
- если вы считаете файл безопасным для сервера и хотите его использовать. Чтобы Kaspersky Security для Windows Server не признавал файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и задачах проверки по требованию. Для этого укажите файл в качестве параметра **Исключать объекты** или параметра **Не обнаруживать** этих задач.

Восстановление файлов из резервного хранилища может привести к заражению сервера.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходную папку (по умолчанию), в специальную папку для восстановленных объектов на защищаемом сервере или в указанную вами папку на сервере, на котором установлена Консоль программы, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом сервере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 234).

По умолчанию, когда Kaspersky Security для Windows Server восстанавливает файл, он сохраняет его копию в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:
   - чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**;
   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на одном из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.
4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект. (Название файла отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:
   - чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**;
   - чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления в параметрах выберите **Восстановить в серверную папку, используемую по умолчанию**.
   - чтобы сохранить объект в другой папке на сервере, на котором установлена Консоль Kaspersky Security для Windows Server, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.
5. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалять объекты из хранилища после восстановления** (по умолчанию флажок снят).
6. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.
7. Нажмите на кнопку **OK**.

   Kaspersky Security для Windows Server начнет восстанавливать первый из выбранных вами объектов.
8. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Security для Windows Server:
      - **Заменить**, чтобы сохранить восстановленный объект вместо существующего;

- **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
- **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

c. Нажмите на кнопку **OK**.

Файл будет восстановлен. Информация об операции используемую будет зарегистрирована в журнале системного аудита.

Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

► *Чтобы удалить из резервного хранилища один или несколько файлов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - **чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу** Ctrl **или клавишу** Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт** Удалить.
4. **В открывшемся окне нажмите на кнопку** Да, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню названия вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Параметры хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

   В блоке **Параметры резервного хранилища**:

   - **Папка резервного хранилища.**

Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

По умолчанию установлен путь C:\ProgramData\Kaspersky Security for Windows Server\10.1\Backup\.

- **Максимальный размер хранилища (МБ)**

  Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Security для Windows Server фиксирует событие Превышен максимальный размер резервного хранилища и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

  Если флажок установлен, Kaspersky Security для Windows Server отслеживает суммарный размер размещенных в резервном хранилище объектов.

  Если флажок снят, Kaspersky Security для Windows Server не отслеживает суммарный размер объектов Резервное хранилище.

  По умолчанию флажок снят.

- **Порог доступного пространства (МБ).**

  Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Security для Windows Server фиксирует событие Превышен порог свободного места в резервном хранилище и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

  Если флажок установлен, Kaspersky Security для Windows Server отслеживает размер свободного места в резервном хранилище.

  Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

  По умолчанию флажок установлен.

Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Security для Windows Server уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В блоке **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты.**

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

  Путь по умолчанию: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Вы можете просматривать информацию о состоянии резервного хранилища в текущий момент – статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли откройте контекстное меню на узле **Резервное хранилище** и выберите команду **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о состоянии резервного хранилища в текущий момент (см. таблицу ниже).

Таблица 37. Информация о текущем состоянии резервного хранилища

Поле	Описание
Текущий размер резервного хранилища	Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде
Всего объектов	Количество объектов в резервном хранилище в текущий момент

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 236
Включение блокирования доступа к сетевым файловым ресурсам 237
Настройка параметров заблокированных компьютеров 238

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 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. Любые попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

По умолчанию Kaspersky Security 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 компьютеры будут автоматически разблокированы.

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, хотя бы 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 программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

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

Настроенные параметры задачи будут сохранены.

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

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. Если задача не была запущена, откройте закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
5. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

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

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита от шифрования для NetApp**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**
4. Если задача не была запущена, откройте закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
5. В окне **Параметры задачи** нажмите на кнопку **OK**.

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

Настройка параметров заблокированных компьютеров

► *Чтобы настроить хранилище заблокированных компьютеров, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security для Windows Server разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированные компьютеры**.
3. Выберите пункт меню **Свойства**.

   Откроется окно **Параметры хранилища заблокированных компьютеров**.
4. В блоке **Действия** укажите количество суток, часов и минут, через которые, с момента блокировки, заблокированные компьютеры получают доступ к сетевым файловым ресурсам сервера.
5. Нажмите на кнопку **OK**.

6. Чтобы восстановить доступ для всех заблокированных компьютеров, выполните следующие действия:
   a. Откройте контекстное меню вложенного узла **Заблокированные компьютеры**.
   b. Выберите пункт **Разблокировать все**.

      Все узлы будут удалены из списка и разблокированы.
7. Чтобы удалить несколько компьютеров из списка недоверенных, выполните следующие действия:
   a. Выберите один или несколько узлов в списке недоверенных в панели результатов.
   b. Откройте контекстное меню вложенного узла **Заблокированные компьютеры**.
   c. Выберите пункт **Разблокировать выбранные**.

      Выбранные компьютеры будут разблокированы.

Регистрация событий. Журналы Kaspersky Security для Windows Server

Этот раздел содержит информацию о работе с журналами Kaspersky Security для Windows Server: журналом системного аудита, журналами выполнения задач Kaspersky Security для Windows Server и журналом событий Kaspersky Security для Windows Server.

В этом разделе

Способы записи событий Kaspersky Security для Windows Server 240

Журнал системного аудита 241

Журналы выполнения задач 243

Журнал событий безопасности 247

Просмотр журнала событий Kaspersky Security для Windows Server в консоли Просмотр событий 247

Настройка параметров журналов в Консоли программы 248

Способы записи событий Kaspersky Security для Windows Server

События Kaspersky Security для Windows Server делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Security для Windows Server;.
- события, связанные с управлением Kaspersky Security для Windows Server, например, запуск программы, создание или удаление задач, запуск задач, изменение параметров задач..

Kaspersky Security для Windows Server использует следующие способы для записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о параметрах задачи, текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Security для Windows Server.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Security для Windows Server. Журнал событий доступен в консоли Просмотр событий Microsoft Windows.
- **Журнал событий безопасности**. Журнал событий безопасности содержит информацию о событиях, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом сервере.

Если в работе Kaspersky Security для Windows Server возникла проблема (например, Kaspersky Security для Windows Server или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать файл трассировки и файл дампа процессов Kaspersky Security для Windows Server и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

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

Kaspersky Security 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 для Windows Server. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Security для Windows Server" на стр.29) и разрешить доступ к журналам, файлам трейса и дампа только для выбранных пользователей.

Журнал системного аудита

Kaspersky Security для Windows Server ведет системный аудит событий, связанных с управлением Kaspersky Security для Windows Server. Программа сохраняет информацию о, например, запуске программы, запуске и остановке задач Kaspersky Security для Windows Server, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли программы.

По умолчанию Kaspersky Security для Windows Server хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которой Kaspersky Security для Windows Server сохраняет файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в списке событий.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите кнопку **Добавить**.

      Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

   В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

   В списке событий журнала системного аудита отобразятся все события.

Удаление событий из журнала системного аудита

По умолчанию Kaspersky Security для Windows Server хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► *Чтобы удалить события из журнала системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.

3. Выполните одно из следующих действий:
   - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
   - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Security для Windows Server и инструкции по работе с ними.

В этом разделе

О журналах выполнения задач 243

Просмотр списка событий в журналах выполнения задач 244

Сортировка событий в журналах выполнения задач 244

Фильтрация событий в журналах выполнения задач 244

Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач 245

Экспорт информации из журнала выполнения задачи 246

Удаление событий из журналов выполнения задач 246

О журналах выполнения задач

Информация о выполнении задач Kaspersky Security для Windows Server отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи вы можете просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи по текущий момент, а также параметры задачи.

По умолчанию Kaspersky Security для Windows Server хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Security для Windows Server сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Также вы можете выбрать события, записи о которых Kaspersky Security для Windows Server сохраняет в журналах выполнения задач.

Просмотр списка событий в журналах выполнения задач

► *Чтобы просмотреть список событий в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.

Список событий, сохраненных в журналах выполнения задач Kaspersky Security для Windows Server, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

Сортировка событий в журналах выполнения задач

По умолчанию события отображаются в журналах выполнения задач в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в журналах выполнения задач Kaspersky Security для Windows Server.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация событий в журналах выполнения задач

Вы можете отобразить в списке событий журналов выполнения задач только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите кнопку **Добавить**.

      Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:
   - Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в списке событий журналов выполнения задач.

В списке событий журналов выполнения задач отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке событий журналов выполнения задач отобразятся все события.

Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска по текущий момент, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.
4. В открывшемся окне отображается следующая информация:
   - на закладке **Статистика** отображается время запуска и завершения задачи и ее статистика;
   - на закладке **События** отображается список событий, зафиксированных при выполнении задачи;
   - на закладке **Параметры** отображаются параметры задачи.

5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.
6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.
7. Нажмите на кнопку **Закрыть**.

Окно **Журнал выполнения** будет закрыто.

Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.
4. В нижней части окна **Журнал выполнения нажмите на кнопку** Экспорт.

   Откроется окно **Сохранить как**.
5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

Удаление событий из журналов выполнения задач

По умолчанию Kaspersky Security для Windows Server хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете вручную удалить все события из журналов выполнения задач, завершившихся на данный момент.

> События из журналов задач, выполняющих в данный момент и журналов, используемых другими пользователями, удалены не будут.

► *Чтобы удалить события из журналов выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы**.

2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Если вы хотите удалить события из всех журналов выполнения задач, завершившихся на данный момент, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Если вы хотите очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню события, которое возникло в задаче, журнал выполнения которой вы хотите очистить, и выберите пункт **Удалить**.
   - Если вы хотите очистить журналы выполнения нескольких задач, выполните следующие действия:
     a. В панели результатов с помощью клавишей **Ctrl** или **Shift**, выберите события, которые возникли в задачах, журналы выполнения которых вы хотите очистить.
     b. Откройте контекстное меню любого выбранного события и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление.

Выбранные журналы выполнения задач будут очищены. Удаление событий из журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал событий безопасности

Kaspersky Security 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 (см. раздел "Удаление событий из журнала системного аудита" на стр. 242). При этом Kaspersky Security для Windows Server фиксирует событие системного аудита об очистке Журнала событий безопасности.

Просмотр журнала событий Kaspersky Security для Windows Server в консоли Просмотр событий

С помощью оснастки Просмотр событий для Microsoft Management Console вы можете просматривать журнал событий Kaspersky Security для Windows Server. В нем Kaspersky Security для Windows Server регистрирует события, которые нужны для диагностики сбоев в работе Kaspersky Security для Windows Server.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий;**
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным

является уровень Информационные события, при котором регистрируются события всех уровней важности; наименее подробным является уровень Критические события, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента Обновление установлен уровень детализации Важные события (регистрируются только важные и критические события); для компонента Обновление установлен уровень Информационные события.

► *Чтобы просмотреть журнал событий Kaspersky Security для Windows Server, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется окно Microsoft Management Console.

2. Выберите Файл → **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите компьютер, на котором установлен Kaspersky Security для Windows Server, и нажмите на кнопку **OK**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **OK**.

   В дереве Консоли появится узел **Просмотр событий**.

6. В дереве Консоли раскройте узел **Просмотр событий** и выберите вложенный узел Журналы приложений и служб → **Kaspersky Security для Windows Server**.

Откроется журнал событий Kaspersky Security для Windows Server.

Настройка параметров журналов в Консоли программы

Вы можете настраивать следующие параметры журналов Kaspersky Security для Windows Server:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;.
- местоположение папки, в которой Kaspersky Security для Windows Server сохраняет файлы журналов выполнения задач и журнала системного аудита;.
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*;.
- события, которые Kaspersky Security для Windows Server сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Security для Windows Server в консоли Просмотр событий;.
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер..

► *Чтобы настроить параметры журналов Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. В окне **Параметры журналов и уведомлений** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, выберите события, которые Kaspersky Security для Windows Server сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Security для Windows Server в консоли Просмотр событий. Для этого выполните следующие действия:

     - В списке **Компонент** выберите функциональный компонент Kaspersky Security для Windows Server, уровень детализации событий которого вы хотите настроить.

       Для компонентов Постоянная защита файлов, Защита RPC-подключаемых сетевых хранилищ, Защита ICAP-подключаемых сетевых хранилищ, Проверка скриптов, Проверка по требованию и Обновление предусмотрена запись событий в журналы выполнения задач и журнал событий. Для этих компонентов таблица списка событий содержит графы **Журналы** и **Журнал событий**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица списка событий содержит графы **Аудит** и **Журнал событий**.

     - В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного функционального компонента.

       В таблице списка событий ниже установлены флажки рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

     - Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:

     a. В списке **Уровень важности** выберите **Другой**.

     b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

   - На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий о статусе защиты сервера:

     - В блоке **Хранение журналов**:

       - **Папка журналов**

         Путь к папке с журналами в формате UNC (Universal Naming Convention).

         Путь по умолчанию: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Reports\.

       - **Удалять журналы выполнения задач и событий старше, чем (дни).**

         Флажок включает / выключает функцию, которая удаляет журналы о результатах выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода (по умолчанию 30 дней).

         Если флажок установлен, Kaspersky Security для Windows Server удаляет журналы о результатах выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода.

         По умолчанию флажок установлен.

- **Удалять события журнала аудита старше, чем (дни).**

  Флажок включает / выключает функцию, которая удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода (по умолчанию 60 дней).

  Если флажок установлен, Kaspersky Security для Windows Server удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода.

  По умолчанию флажок установлен.

- В блоке **Пороги формирования событий**:
  - количество дней, после которого будут возникать события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*;.

Таблица 38. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих трех типов: Базы программы устарели и Базы программы сильно устарели. Событие возникает, если базы Kaspersky Security для Windows Server не обновляются в течение указанного параметром количества дней с момента создания последних установленных обновлений баз. Вы можете настроить уведомление администратора по этим событиям. Проверка важных областей давно не выполнялась. Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком Считать выполнение задачи проверкой важных областей.
Возможные значения:	Количество дней от 1 до 365.
Значение по умолчанию	Базы программы устарели – 7 дней; Базы программы сильно устарели – 14 дней; Проверка важных областей давно не выполнялась – 30 дней.

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач (см. раздел "Настройка параметров интеграции с SIEM" на стр. 251) на syslog-сервере.

3. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Об интеграции с SIEM

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

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

Вы можете использовать интеграцию с SIEM в двух режимах:

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

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

Рекомендуется выбирать формат событий на основе конфигурации используемой SIEM.

Параметры надежности

Вы можете снизить риск неудачной отправки событий в SIEM задав параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если подключение к основному syslog-серверу или его использование недоступны.

Также Kaspersky Security для Windows Server уведомляет вас о неудачной попытке подключения к SIEM и об ошибках отправки событий в SIEM с помощью событий системного аудита.

Настройка параметров интеграции с SIEM

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

Таблица 39. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.
Протокол подключения	TCP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UPD или TCP с помощью выпадающего списка.

Параметр	Значение по умолчанию	Описание
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
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 программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

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

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

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

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

   По умолчанию флажок снят.
5. Если требуется, 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.

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

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В блоке **Параметры 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.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Security для Windows Server о событиях программы и состоянии сервера, а также инструкцию по настройке уведомлений.

В этом разделе

Способы уведомления администратора и пользователей 254

Настройка уведомлений администратора и пользователей 255

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому серверу, о событиях, связанных с работой Kaspersky Security для Windows Server и состоянием антивирусной защиты сервера.

Программа обеспечивает выполнение следующих задач:

- 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*, возникших в задаче Постоянная защита файлов.

В Консоли программы вы можете активировать уведомления администратора или пользователей несколькими способами:

- способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения терминальных пользователей, если защищаемый сервер является терминальным.

  b. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows. Этот способ не применяется, если защищаемый сервер работает под управлением Microsoft Windows Server 2008 или выше.
- способы уведомления администраторов:
  a. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows. Этот способ не применяется, если защищаемый сервер работает под управлением Microsoft Windows Server 2008 или выше.

  b. Запуск исполняемого файла.

     Этот способ запускает по событию исполняемый файл, который хранится на локальном диске защищаемого сервера.

c. Отправка по электронной почте.

Этот способ использует для передачи сообщений электронную почту.

Вы можете создавать текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется предустановленный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► *Чтобы настроить уведомления о событиях, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** укажите способы уведомлений:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Вы можете настроить уведомления пользователей только для события **Обнаружен объект**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**.

   b. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после того как вы выбрали способ уведомлений для одного типа событий, выберите, используя клавишу **Ctrl** или клавишу **Shift**, остальные типы событий, для которых вы хотите составить такой же текст сообщения, перед тем как нажать на кнопку **Текст сообщения**.

   c. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   d. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Если вы хотите настроить параметры для способов уведомлений администраторов о выбранном событии, в окне **Уведомления** нажмите на кнопку **Настройка** и в окне **Дополнительные параметры** выполните настройку выбранных способов. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте откройте закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса символом "точка с запятой"), имя или сетевой адрес SMTP-сервера, а также его порт. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** вы также можете включать переменные с информацией о событии (см. таблицу ниже).

      Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

   b. Для уведомлений средствами **службы сообщений** на закладке **Служба сообщений**, составьте список компьютеров-получателей уведомлений: для каждого компьютера, который вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

      > Уведомления с помощью Службы сообщений не используются для отсылки уведомлений, если защищаемый сервер работает под управлением Microsoft Windows Server 2008 и последующих версий Microsoft Windows Server.

   c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите на локальном диске защищаемого сервера файл, который будет выполняться на сервере по событию, или введите полный путь к нему. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

      Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

      Если вы хотите ограничить количество уведомлений по событиям одного типа в единицу времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите нужное количество раз и единицу времени.

5. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Таблица 40. Поля с информацией о событии

Переменная	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя обнаруженного объекта согласно классификации Вирусной энциклопедии (http://www.securelist.ru). Это имя входит в полное название обнаруженного объекта, которое Kaspersky Security для Windows Server возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Security для Windows Server в журналах выполнения задач" на стр. 245).
%VIRUS_TYPE%	Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Security для Windows Server возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%USER_COMPUTER%	В задачах Постоянная защита файлов и Защита RPC-подключаемых сетевых хранилищ имя компьютера пользователя, который обратился к объекту на сервере.
%USER_NAME%	В задачах Постоянная защита файлов и Защита RPC-подключаемых сетевых хранилищ имя пользователя, который обратился к объекту на сервере.
%FROM_COMPUTER%	Имя защищаемого сервера, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (применяется только для события "внутренняя ошибка задачи").
%TASK_NAME%	Имя задачи (имеется только у событий, связанных с выполнением задач).

Управление Иерархическим хранилищем

Этот раздел содержит информацию об антивирусной проверке файлов, расположенных в иерархических хранилищах и системах резервного копирования.

В этом разделе

Об иерархическом хранилище 258

Настройка параметров HSM-системы 259

Об иерархическом хранилище

Система управления иерархическим хранилищем (Hierarchical Storage Management, HSM) (далее HSM-система) позволяет перемещать данные между быстрыми локальными дисками и медленными устройствами долговременного хранения информации. Несмотря на очевидные преимущества быстрых запоминающих устройств, для большинства организаций их использование оказывается слишком дорогим. HSM-системы обеспечивают перенос неиспользуемой информации на недорогие устройства удаленного хранения, сокращая экономические издержки компании.

HSM-системы сохраняют часть информации в удаленных хранилищах, восстанавливая ее в случае необходимости. При этом HSM-системы ведут постоянный мониторинг использования файлов, определяя, какие из них можно переместить в удаленное хранилище, а какие целесообразно оставить на устройствах локального хранения. Файлы перемещаются на удаленное хранилище, если к ним не поступает обращений за установленный период времени. Если пользователь обращается к файлу, расположенному в удаленном хранилище, этот файл переносится обратно на локальный диск. Этот принцип обеспечивает пользователям быстрый доступ к большим объемам информации, существенно превышающим размеры доступного дискового пространства.

При перемещении файла из локального в удаленное хранилище HSM-система сохраняет ссылку на фактическое расположение данного файла. При обращении к файлу, содержащему ссылку, система определяет местоположение данных на архивном устройстве. Замена файлов ссылками на место их хранения позволяет получить хранилище практически неограниченного объема.

Некоторые HSM-системы позволяют сохранять части файлов в локальном хранилище. При этом в удаленное хранилище перемещается большая часть файла, а в локальном хранилище остается небольшая часть исходного файла.

В HSM-системах применяется два способа доступа к информации, помещенной в иерархическое хранилище:

- точки повторной обработки;
- расширенные атрибуты файла.

Настройка параметров HSM-системы

Если вы не используете HSM-системы, оставьте значение параметра Тип доступа к иерархическому хранилищу, установленное по умолчанию (Не HSM-система).

Для настройки доступа к иерархическому хранилищу вам нужно указать, каким образом HSM-система определяет местоположение сканируемого файла. Вы можете найти эту информацию в документации к используемой HSM-системе.

► *Чтобы указать способ доступа к иерархическому хранилищу, выполните следующие действия:*

1. В дереве Консоли откройте контекстное меню узла **Kaspersky Security**.
2. Выберите пункт **Иерархическое хранилище**.

   Откроется окно **Параметры HSM-системы**.
3. На закладке **Иерархическое хранилище** укажите параметры HSM-системы:
   - **Не HSM-система**.

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

     Данный вариант выбран по умолчанию.
   - **HSM-система использует точки повторной обработки**.

     Kaspersky Security 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\10.0\Restored\.
   - **Неизвестная HSM-система**.

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

     Не рекомендуется использовать этот вариант.

     Если вы укажете неверный вариант или выберете вариант **Неизвестная HSM-система**, Kaspersky Security для Windows Server может неверно определять местонахождение объектов, что увеличит время обработки объектов.
4. Нажмите на кнопку **OK**.

Настроенные параметры HSM-системы будут сохранены.

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки 260

Техническая поддержка через Kaspersky CompanyAccount 260

Использование файла трассировки и скрипта AVZ 261

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 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 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.

Microsoft, Internet Explorer, Excel, JScript, Outlook, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

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.

К

Карантин

Папка, в которую программа “Лаборатории Касперского” перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой “Лаборатории Касперского” как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

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.

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 времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит 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

F

FTP-сервер 233, 237, 238

H

HTTP-сервер 229, 233, 237, 238

K

Kaspersky Embedded Systems Security
    запуск при запуске системы 23

А

Альтернативные потоки NTFS 85
Антивирусная проверка хранилищ 243
Архивы 85

Б

базы 227, 229
    автоматическое обновление 54, 229, 233
    дата создания 24
    обновление вручную 233

В

Восстановление объекта 245, 253
Восстановление параметров по умолчанию 83, 215

Г

Главное окно 12

Д

Дезинфекция объектов ... 85
Действие
Зараженные объекты ... 85
Подозрительные объекты ... 85
Действия над объектами ... 85, 91, 215
Доверенные устройства ... 158

Ж

Журнал событий ... 261, 268

З

Задача ... 52
Запуск пропущенных задач ... 54
Значок в области уведомлений панели задач ... 16

И

Интерфейс программы ... 12, 36
значок в области уведомлений панели задач ... 16
Исключения из области проверки ... 85
Исполняемый файл ... 49, 85, 132, 136, 142, 147, 151
Источник обновлений ... 233, 237, 238

К

Карантин
восстановление объекта ... 245
порог свободного места ... 249
просмотр объектов ... 242
удаление объектов ... 247
Карантин и резервное хранилище ... 241
Консоль ... 12, 36, 37, 44
Запустить ... 22
соединение ... 44

М

Максимальный размер
Карантин ... 249
Проверенные объекты ... 85

Н

Настройка
задача ... 52, 69, 91, 132, 151, 159, 169, 200, 233
параметров безопасности ... 83, 85, 214, 215

О

Обновление
Модули программы ... 227
по расписанию ... 54, 233
Очистка журнала системного аудита ... 263

П

Папка для восстановления
Карантин ... 249
Папка для сохранения обновлений ... 237
Папка журналов ... 269
Папка резервного хранилища ... 255
Постоянная защита ... 66
Правила ... 142, 146, 151, 161, 165, 169
Контроль запуска программ ... 142, 144, 146, 147, 150, 151
Контроль устройств ... 161, 163, 164, 165, 167, 168, 169
принципом блокировки по умолчанию (Default Deny) ... 158, 159
Проверка
Максимальная длительность проверки объекта ... 85
Только новые и измененные объекты ... 85
уровень безопасности ... 83, 215
Прокси-сервер ... 233

Р

Расписание задач 54, 55
Режим защиты 71
Резервное хранилище
    восстановление объектов 253
    удаление объектов 255
    настройка параметров 255
Резервное хранилище: 250, 251

С

Содержимое обновлений 237
Статистика. 24

Т

Тип угрозы
    Действие 85

Ф

Файлы iSwift 83, 85, 215, 243

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 41. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный

Приложение

Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.
Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 42. Параметры и их значения для программы в сертифицированном состоянии

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметры установки		
Компонент Контроль устройств	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (флажок снят)
Компонент Постоянная защита	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Контроль запуска программ	Выбор компонентов для установки на защищаемый сервер.	Установлен (по умолчанию)
Компонент Управление сетевым экраном	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (по умолчанию)
Настройки прав доступа и функциональных компонентов		
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Security. • **Запущена** • **Остановлена**	Запущена

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Права на управление программой	Доступ к функциям Kaspersky Security для Windows Server: • **Разрешить** • **Запретить**	Учетные записи пользователей- администраторов безопасности должны быть добавлены в группу KSWS Administrators. Для всех пользователей и групп, кроме KSWS Administrators и SYSTEM, установлены флажки **Запретить**.
Права на управление службой	Доступ к функциям службы Kaspersky Security Service: • **Разрешить** • **Запретить**	Учетные записи пользователей- администраторов безопасности должны быть добавлены в группу KSWS Administrators. Для всех пользователей и групп, кроме KSWS Administrators и SYSTEM, установлены флажки **Запретить**.
Задача Постоянная защита файлов	Антивирусная проверка файлов на защищаемом сервере при обращении к этим файлам. • **Выполняется** • **Остановлена**	Выполняется
Лицензирование	Активация программы с помощью ключа.	Добавлен файл ключа. По окончании срока действия ключа программа выходит из сертифицированного состояния.
Использовать Локальный KSN	Взаимодействие с Глобальным или Локальным KSN, настраеваемое в Kaspersky Security Center.	Запускать задачу Использование KSN следует только при использовании Локального KSN (флажок **Настроить Локальный KSN** установлен), в том числе при отсутствии управления программой через Kaspersky Security Center.
Параметры задач Постоянная защита / проверка по требованию		
Архивы	Проверка архивов в указанной области защиты в параметрах задачи Постоянной защиты файлов. • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Применяется (флажок установлен).

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Загрузочные секторы дисков и MBR	Проверять загрузочные секторы и загрузочные надписи на жестких и съемных дисках сервера. • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Применяется (флажок установлен).
Область защиты	Папки и файлы находящиеся под защитой задач Постоянная защита и Проверка по требованию. • Любые локальные и сетевые папки.	По умолчанию. Исключение папок из области защиты, установленной по умолчанию, ведет к выходу из сертифицируемого состояния.
Пропускать для любого типа объектов	Действия при обнаружении объектов: • **Лечить** • **Удалять** • **Помещать на карантин** • **Пропускать**	Не выбрано. При выборе действия **Пропускать** для любого типа объектов, программа выходит из сертифицированного состояния.
Объекты, проверяемые по указанному списку расширений	На закладке **Общие**, выберите объекты, которые необходимо защищать: • **Все объекты;** • **Объекты, проверяемые по формату;** • **Объекты, проверяемые по списку расширений, указанному в антивирусных базах;** • **Объекты, проверяемые по указанному списку расширений.**	Флажок снят. Наполнение списка расширений объектов вручную ведет к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Исключать файлы	Исключение файлов из проверки по имени файла или маске имени файла: • Применяется (флажок установлен). • Не применяется (флажок снят).	Не применяется (Флажок снят).
Не обнаруживать	Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта: • Применяется (флажок установлен). • Не применяется (флажок снят).	Не применяется (Флажок снят).
Использовать эвристический анализатор	Применение эвристического анализатора: • Применяется (флажок установлен). • Не применяется (флажок снят).	Применяется (флажок установлен). Снятие флажка ведет к выходу программы из сертифицированного состояния.
Параметры задач обновления		
Серверы обновлений «Лаборатории Касперского» на компьютере-ретрансляторе (Задача Копирование обновлений)	Источник обновлений баз программы: • **Сервер администрирования Kaspersky Security Center.** • **Серверы обновлений «Лаборатории Касперского»**. • **Другие HTTP-, FTP-серверы или сетевые ресурсы.**	На компьютере-ретрансляторе выбран вариант **Серверы обновлений «Лаборатории Касперского»**. Для работы программы в сертифицированной конфигурации, задачи обновления должны осуществляться через один из защищаемых компьютеров сети.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Копировать обновления программы (Задача Копирование обновлений)	Укажите условия копирования обновлений программы: • **Копировать обновления программы.** • **Копировать критические обновления модулей программы.** • **Копировать обновления баз программы и критические обновления модулей программы.**	Выбран вариант **Копировать обновления программы**. Kaspersky Security для Windows Server загружает только обновления баз Kaspersky Security.
Другие HTTP-, FTP-серверы или сетевые ресурсы на серверах-ресиверах.	Источник обновлений баз программы: • **Сервер администрирования Kaspersky Security Center.** • **Серверы обновлений «Лаборатории Касперского»**. • **Другие HTTP-, FTP-серверы или сетевые ресурсы.**	На серверах-ресиверах выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**. В качестве источника должна быть указана сетевая папка, настроенная в качестве папки локального источника обновлений в задаче Копирование обновлений на компьютере- ретрансляторе.
Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны на серверах-ресиверах. (Задача Обновление баз программы)	При выборе источника обновления **Другие HTTP-, FTP-серверы или сетевые ресурсы**, активируется функция использования серверо обновлений «Лаборатории Касперского». • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Не применяется (флажок снят). Обновление через сервера обновлений «Лаборатории Касперского» запрещено.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Частота запуска задачи Обновление баз программы	Промежуток времени, через которое задача осуществляет проверку наличия обновлений: • **Ежечасно** • **Ежесуточно** • **Еженедельно** • **При запуске программы** • **После получения обновлений Сервером администрирования**	**Ежечасно** (по умолчанию). Снижение частоты запусков задачи, установленного по умолчанию ведет к выходу программы из сертифицированного состояния.
Настройка параметров аудита		
События для компонентов постоянной защиты, проверки по требованию, KSN, лицензирования и обновлений баз программы.	Регистрация событий в параметрах журналов. • **Все события** • **Набор событий по умолчанию**	Для компонентов **Постоянная защита**, **Проверка по требованию**, **Использование KSN**, **Лицензирование** и задачи **Обновление баз программы** установлены оповещения о событиях по умолчанию.
Удалять события в журналах выполнения задач старше, чем (сут.)	Очистка журнала выполнения задач через заданный прометужок времени.	**30** сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Удалять события в журнале системного аудита старше, чем (сут.)	Очистка журнала системного аудита через заданный прометужок времени.	**60** сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Пороги формирования событий	Промежуток времени, через который возникают события: • **Базы программы устарели.** • **Базы программы сильно устарели.** • **Проверка важных областей компьютера давно не выполнялась**.	По умолчанию выставлены следующие значения: **7** (сут) **14** (сут) **30** (сут) Уменьшение порога формирования событий ведет к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройка сигналов тревоги		
Путем запуска исполняемого файла	Способы уведомления администраторов: • **Средствами службы сообщений**; • **Путем запуска исполняемого файла**; • **По электронной почте**.	Флажок **Путем запуска исполняемого файла** установлен для событий: • *Обнаружен объект* • *Объект не вылечен* • *Объект не удален* • *Запуск программы запрещен* • *Запуск программы запрещен по прецеденту* • *Объект не помещен на карантин* • *Объект не помещен в резервное хранилище*
Данные сигнала тревоги	Переменные в составе сообщения сигнала тревоги.	Переменные **Тип обнаруженного объекта** (%VIRUS_TYPE%), **Обнаружено** (%VIRUS_NAME%) и **Событие** (%EVENT_TYPE%) присутствуют в сообщении сигнала тревоги.