KASPERSKY lab

Kaspersky Security 10.1 для Windows Server

643.46856491.00084-03 90 03

Руководство по эксплуатации для защиты сетевых хранилищ

Версия программы: 10.0.1.622

Уважаемый пользователь!

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

Дата редакции документа: 10.05.2018

Обозначение документа: 643.46856491.00084-03 90 03

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

Содержание

Об этом документе

Этот документ содержит описание подготовительных процедур и руководство по эксплуатации программного изделия «Kaspersky Security 10.1 для Windows Server» (далее также «Kaspersky Security для Windows Server», «программа») для защиты сетевых хранилищ.

Основные 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 специалистам, которые осуществляют установку и администрирование Kaspersky Security 10.1 для Windows Server, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security 10.1 для Windows Server для защиты сетевых хранилищ.

Подразумевается, что к моменту прочтения этого документа вы располагаете ключом с поддержкой функции защиты сетевых хранилищ, добавленным в программу.

Источники информации о Kaspersky Security 10.1 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 10.1 для Windows Server на веб-сайте "Лаборатории Касперского"

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

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

Страница Kaspersky Security 10.1 для Windows Server в Базе знаний

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

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

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

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 10.1 для Windows Server

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

О программе

Программное изделие «Kaspersky Security 10.1 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 10.1 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.

О Kaspersky Security 10.1 для Windows Server

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

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

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

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

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

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

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

Компоненты и функции Kaspersky Security 10.1 для Windows Server

В состав программы входят следующие компоненты:

- **Постоянная защита.** Kaspersky Security 10.1 для Windows Server проверяет объекты при обращении к ним. Kaspersky Security 10.1 для Windows Server проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - главную загрузочную запись и загрузочные секторы локальных жестких и съемных дисков.
- **Проверка по требованию.** Kaspersky Security 10.1 для Windows Server однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память защищаемого устройства, а также объекты автозапуска.

- **Защита RPC-подключаемых сетевых хранилищ** и **Защита ICAP-подключаемых сетевых хранилищ**. Kaspersky Security 10.1 для Windows Server, установленный на сервере под управлением операционной системы Microsoft Windows, защищает сетевые хранилища от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.
- **Контроль запуска программ.** Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Защита от шифрования** и **Защита от шифрования для NetApp**. Компоненты выполняют защиту общих сетевых папок защищаемых серверов и сетевых хранилищ от вредоносного щифрования, путем блокировки компьютеров, проявляющих подозрительную активность.
- **Проверка скриптов**. Этот компонент контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies.
- **Защита трафика.** Этот компонент перехватывает и проверяет объекты, передаваемые по веб-трафику (включая почтовый трафик), на наличие известных компьютерных и других угроз на защищаемом сервере.
- **Мониторинг файловых операций.** Kaspersky Security 10.1 для Windows Server обнаруживает изменения в файлах, которые входят в область мониторинга, указанную в параметрах задачи. Эти изменения могут свидетельствовать о нарушении безопасности на защищаемом сервере.
- **Анализ журналов.** Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

В программе реализованы следующие функции:

- **Обновление баз и модулей программы.** Kaspersky Security 10.1 для Windows Server загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.
- **Карантин.** Kaspersky Security 10.1 для Windows Server помещает объекты, которые он признает возможно зараженными, на карантин, то есть переносит объекты из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.
- **Резервное хранилище.** Kaspersky Security 10.1 для Windows Server сохраняет зашифрованные копии объектов со статусом *Зараженный* или *Возможно зараженный* в *резервном хранилище* перед тем, как выполнить лечение или удаление этих объектов.
- **Уведомления администратора и пользователей.** Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Security 10.1 для Windows Server и состоянием антивирусной защиты компьютера.
- **Импорт и экспорт параметров.** Вы можете экспортировать параметры Kaspersky Security 10.1 для Windows Server в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Security 10.1 для Windows Server из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.
- **Применение шаблонов.** Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Security 10.1 для Windows Server.
- **Права доступа к функциям Kaspersky Security 10.1 для Windows Server.** Вы можете настраивать права на управление Kaspersky Security 10.1 для Windows Server и службами Windows, которые

регистрирует программа, для пользователей и групп пользователей.

- **Запись событий в журнал событий программы.** Kaspersky Security 10.1 для Windows Server записывает в журналы информацию о параметрах функциональных компонентов программы, текущем состоянии задач, событиях, возникших за время их выполнения, а также о событиях, связанных с управлением Kaspersky Security 10.1 для Windows Server, и информацию, необходимую для диагностики сбоев в работе программы.
- **Иерархическое хранилище.** Kaspersky Security 10.1 для Windows Server может работать в режиме использования систем управления иерархическим хранилищем (HSM-систем). Использование HSM-системы позволяет перемещать данные между быстрыми локальными дисками и медленными устройствами долговременного хранения информации.
- **Доверенная зона.** Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Security 10.1 для Windows Server будет применять в задачах проверки по требованию и постоянной защиты файлов.
- **Защита от эксплойтов.** Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.
- **Хранилище Заблокированных узлов.** Вы можете заблокировать компьютеры, пытающиеся получить доступ к общим сетевым папкам сервера, при обнаружении вредоносной активности с их стороны.

Интеграция Kaspersky Security 10.1 для Windows Server с сетевыми хранилищами

Этот раздел содержит информацию о принципах совместной работы Kaspersky Security 10.1 для Windows Server и сетевых хранилищ.

Защита сетевого хранилища EMC группы Celerra / VNX

Kaspersky Security 10.1 для Windows Server взаимодействует с сетевым хранилищем EMC группы Celerra / VNX с помощью программного агента CAVA (Celerra Antivirus Agent), работающего на компьютере с установленным Kaspersky Security 10.1 для Windows Server. После запуска Kaspersky Security 10.1 для Windows Server проверяет наличие на компьютере установленного агента CAVA, соответствующего требованиям Kaspersky Security 10.1 для Windows Server.

При попытке чтения или изменения файла, размещенного на сетевом хранилище, сетевое хранилище инициирует сетевой запрос и передает файл агенту CAVA. Агент CAVA записывает полученный файл на локальный диск компьютера в специально созданную папку. Компонент Постоянная защита файлов перехватывает файловую операцию и выполняет проверку файла в соответствии с параметрами, заданными в задаче Постоянная защита файлов, например, лечит или удаляет файл. Агент CAVA анализирует действия Kaspersky Security 10.1 для Windows Server, и на основании этой информации формирует, а затем передает сетевому хранилищу результат проверки.

Защита RPC-подключаемых сетевых хранилищ.

Для взаимодействия Kaspersky Security 10.1 для Windows Server и RPC-подключаемого сетевого хранилища (такого как NetApp или Hitachi NAS в режиме RPC) используется протокол RPC (Remote Procedure Call).

Kaspersky Security 10.1 для Windows Server поддерживает постоянное соединение с сетевым хранилищем, периодически инициируя к нему запросы RPC. При попытке чтения или создания / изменения файла, размещенного на сетевом хранилище, сетевое хранилище предоставляет Kaspersky Security 10.1 для Windows Server прямой доступ к этому файлу по протоколу CIFS. Компонент программы Защита RPC-подключаемых сетевых хранилищ выполняет проверку файла в соответствии с параметрами, заданными в задаче Защита RPC-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security 10.1 для Windows Server выполняет над файлом действия, заданные в параметрах задачи (в том числе лечение или удаление файла), и передает результат проверки сетевому хранилищу.

Защита ICAP-подключаемых сетевых хранилищ

Для ICAP-подключаемого сетевого хранилища (такого как EMC Isilon, IBM NAS или Hitachi NAS в режиме ICAP) Kaspersky Security 10.1 для Windows Server представляет собой службу, работающую по протоколу ICAP (Internet Content Adaptation Protocol).

При попытке чтения или создания / изменения файла, размещенного на сетевом хранилище, сетевое хранилище формирует ICAP-запрос к Kaspersky Security 10.1 для Windows Server и передает файл внутри этого запроса. Компонент программы Защита ICAP-подключаемых сетевых хранилищ выполняет проверку файла в соответствии с параметрами, заданными в задаче Защита ICAP-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security 10.1 для Windows Server выполняет над файлом действия, заданные в параметрах задачи, и возвращает результат проверки сетевому хранилищу. Если в параметрах задано действие Лечить, и файл удалось вылечить, Kaspersky Security 10.1 для Windows Server возвращает сетевому хранилищу вылеченный файл в ответе на запрос.

Подготовка к запуску задач защиты сетевых хранилищ

Этот раздел содержит инструкции по подготовке сервера под управлением Microsoft Windows с установленным Kaspersky Security 10.1 для Windows Server к интеграции с сетевыми хранилищами данных и к дальнейшему запуску задач защиты сетевых хранилищ.

Настройка параметров безопасности локальных политик в редакторе локальной групповой политики

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы настроить параметры безопасности локальных политик в редакторе локальной групповой политики, выполните следующие действия:*

1. Откройте **Редактор локальной групповой политики** одним из следующих способов:
   - Если вы настраиваете параметры локально, нажмите на кнопку **Пуск**, введите в поисковой строке команду `gpedit.msc` и нажмите на клавишу **ENTER**.
   - Если вы настраиваете параметры с другого компьютера, выполните следующие действия:
     a. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

        Откроется окно консоль управления.
     b. В открывшемся окне выберите **Файл** > **Добавить или удалить оснастку**.

        Откроется окно **Добавление и удаление оснасток**.
     c. В списке доступных оснасток выберите оснастку **Редактор объектов групповой политики** и нажмите на кнопку **Добавить**.

        Запустится **Мастер групповой политики**.
     d. В окне мастера нажмите на кнопку **Обзор**.

        Откроется окно **Поиск объекта групповой политики**.
     e. В открывшемся окне на закладке **Компьютеры** выберите вариант **Другой компьютер** и укажите сервер с установленным Kaspersky Security 10.1 для Windows Server одним из следующих способов:
        - в поле ввода укажите доменное имя сервера с установленным Kaspersky Security 10.1 для Windows Server;
        - нажмите на кнопку **Обзор** и в открывшемся окне выбора компьютера выберите сервер с установленным Kaspersky Security 10.1 для Windows Server, используя поиск по домену или рабочей группе.
2. Нажмите на кнопку **ОК**.

   Внесенные изменения будут сохранены.
3. Выберите **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности**.

4. Укажите следующие значения параметров сетевого доступа:
   - **Сетевой доступ: разрешать применение разрешений «Для всех» к анонимным пользователям – Включен;**
   - **Сетевой доступ: не разрешать перечисление учетных записей SAM анонимным пользователям – Отключен;**
   - **Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам – Отключен.**
5. Перезагрузите сервер с установленным Kaspersky Security 10.1 для Windows Server.

Внесенные изменения вступят в силу.

Настройка входящих и исходящих подключений в брандмауэре Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы настроить входящие и исходящие подключения в брандмауэре Windows, выполните следующие действия:*

1. Откройте окно настройки брандмауэра Windows одним из следующих способов:
   - Если вы настраиваете брандмауэр Windows локально, нажмите на кнопку **Пуск**, введите в поисковой строке команду `wf.msc` и нажмите на клавишу **ENTER**.
   - Если вы настраиваете брандмауэр Windows с другого компьютера, выполните следующие действия:
     a. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

        Откроется окно **Консоль управления**.
     b. В открывшемся окне выберите **Файл → Добавить или удалить оснастку**.

        Откроется окно **Добавление и удаление оснасток**.
     c. В списке доступных оснасток выберите оснастку **Брандмауэр Windows** и нажмите на кнопку **Добавить**.

        Откроется окно **Выбор компьютера**.
     d. В открывшемся окне выберите вариант **Другой компьютер** и укажите сервер с установленным Kaspersky Security 10.1 для Windows Server одним из следующих способов:
        - в поле ввода укажите доменное имя сервера с установленным Kaspersky Security 10.1 для Windows Server;
        - нажмите на кнопку **Обзор** и в открывшемся окне выбора встроенного субъекта безопасности выберите сервер с установленным Kaspersky Security 10.1 для Windows Server, используя поиск по домену или рабочей группе.

2. Нажмите на кнопку **ОК**.

   Внесенные изменения будут сохранены.

3. Создайте правила для входящих и исходящих подключений со следующими параметрами:

   - Разрешите входящие подключения со всех удаленных портов к локальным портам TCP 137 – 139, TCP 445.
   - Разрешите исходящие подключения со всех локальных портов к удаленным портам TCP 137 – 139, TCP 445.

     По умолчанию брандмауэр Windows разрешает все исходящие соединения, для которых нет запрещающих правил. Если используются параметры по умолчанию, правило для исходящих соединений создавать не требуется.

Параметры брандмауэра Windows могут также определяться групповой или доменной политикой.

Работа с Консолью Kaspersky Security 10.1

Этот раздел содержит информацию о Консоли Kaspersky Security 10.1 и об управлении Kaspersky Security 10.1 для Windows Server через Консоль Kaspersky Security 10.1, установленную на защищаемом сервере или на другом компьютере.

В этом разделе

О Консоли Kaspersky Security 10.1

Консоль Kaspersky Security 10.1 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять Kaspersky Security 10.1 для Windows Server через Консоль Kaspersky Security 10.1, установленную на защищаемом сервере или на другом компьютере в сети организации.

Подробная информация об установке и настройке Консоли Kaspersky Security 10.1 приведена в *Руководстве пользователя Kaspersky Security 10.1 для Windows Server.*

Если Консоль Kaspersky Security 10.1 и Kaspersky Security 10.1 для Windows Server установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в доставке информации от Kaspersky Security 10.1 для Windows Server в Консоль Kaspersky Security 10.1. Например, после старта какой-либо задачи Kaspersky Security 10.1 для Windows Server статус этой задачи может не обновиться в Консоли.

При установке Консоли Kaspersky Security 10.1 мастер установки сохраняет файл kavfs.msc в папке установки и добавляет оснастку Kaspersky Security 10.1 для Windows Server в список изолированных оснасток Microsoft Windows.

Вы можете открыть Консоль Kaspersky Security 10.1 из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Security 10.1 для Windows Server или добавить оснастку программы в существующую консоль Microsoft Management Console как новый элемент в ее дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Security 10.1 для Windows Server только в Microsoft Management Console 32-разрядной 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 Kaspersky Security 10.1 для Windows Server, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Security 10.1 для Windows Server.

Запуск Консоли Kaspersky Security 10.1 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 10.1 для Windows Server → Средства администрирования → Консоль Kaspersky Security 10.1**.

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

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

1. В меню **Пуск** выберите **Программы → Kaspersky Security 10.1 для Windows Server → Средства администрирования**.
2. В контекстном меню программы Консоль Kaspersky Security 10.1 выберите команду **Автор**.

Консоль Kaspersky Security 10.1 будет запущена в авторском режиме.

При запуске Консоли на защищаемом сервере откроется окно Консоли.

Если вы запустили Консоль Kaspersky Security 10.1 не на защищаемом сервере, а на другом компьютере, подключитесь к защищаемому серверу.

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

1. В дереве Консоли Kaspersky Security 10.1 для Windows Server 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 **ОК**.

Консоль Kaspersky Security 10.1 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.

Интерфейс Консоли Kaspersky Security 10.1

Консоль Kaspersky Security 10.1 отображается в дереве Microsoft Management Console в виде узла с именем **Kaspersky Security**.

После подключения к Kaspersky Security 10.1 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 10.1 для Windows Server <Имя компьютера> как <имя учетной записи>**. При подключении к Kaspersky Security 10.1 для Windows Server, установленному на том же сервере, что и Консоль, название узла имеет вид: **Kaspersky Security**.

По умолчанию окно Консоли Kaspersky Security 10.1 содержит следующие элементы:

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

Также вы можете включить отображение в окне Консоли Kaspersky Security 10.1 области описания и панели действия.

Дерево Консоли

В дереве Консоли отображается узел Kaspersky Security 10.1 для Windows Server и вложенные в него узлы функциональных компонентов программы.

В состав узла **Kaspersky Security 10.1 для Windows Server** входят следующие вложенные узлы:

- **Постоянная защита**: управление постоянной защитой файлов и проверкой скриптов, а также параметрами использования служб KSN. Узел Постоянная защита позволяет управлять следующими задачами:
  - **Постоянная защита файлов;**
  - **Проверка скриптов;**
  - **Использование KSN;**
  - **Защита трафика.**
- **Контроль компьютера**: контроль подключаемых устройств, а также контроль программ, запускаемых на защищаемом сервере. Узел Контроль компьютера позволяет управлять следующими задачами:
  - **Защита от шифрования;**
  - **Контроль запуска программ;**
  - **Контроль устройств;**
  - **Управление сетевым экраном.**
- **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 создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль Kaspersky Security 10.1.

- **Диагностика системы**: настройка контроля файловых операций и анализа системного журнала операционной системы.
  - **Мониторинг файловых операций;**
  - **Анализ журналов.**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы;**
  - **Проверка важных областей;**
  - **Проверка объектов на карантине;**
  - **проверка целостности модулей программы;**
  - Пользовательские задачи **<Имя задач>** (если есть).

    В узле отображаются системные задачи, созданные при установке программы, добавленные пользовательские задачи, а также групповые задачи проверки по требованию, сформированные и переданные на компьютер с помощью Kaspersky Security Center.

    В узле отображаются все пользовательские и групповые задачи обновления и переданные на компьютер с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Security 10.1 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 обновления 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 локальных задач, журналом событий безопасности и журналом системного аудита Kaspersky Security 10.1 для Windows Server.
  - **Журнал событий безопасности;**
  - **Журнал системного аудита;**
  - **Журналы выполнения задач.**
- **Лицензирование**: добавление и удаление ключей и кодов активации Kaspersky Security 10.1

для Windows Server, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел Kaspersky Security 10.1 для Windows Server, в панели результатов отображается информация о текущем состоянии защиты сервера, информация о Kaspersky Security 10.1 для Windows Server, состоянии защиты его функциональных компонентов и статусе лицензии или ключа.

Контекстное меню узла Kaspersky Security 10.1 для Windows Server

С помощью пунктов контекстного меню узла Kaspersky Security 10.1 для Windows Server вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключиться к другому компьютеру для управления установленным на этом компьютере Kaspersky Security 10.1 для Windows Server. Для выполнения этой операции вы также можете воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Security 10.1 для Windows Server**.
- **Запустить программу** / **Остановить программу** (**Запустить** / **Остановить**). Запустить или остановить программу или выбранную задачу. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Параметры проверки съемных дисков**. Вы можете настроить проверку съемных дисков, подключаемых по USB к защищаемому серверу.
- **Защита от эксплойтов: общие параметры**. Настроить режим защиты от эксплойтов и превентивные меры.
- **Защита от эксплойтов: параметры защиты процессов**. Добавить защищаемые процессы и указать техники снижения рисков.
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны.
- **Изменить права пользователей на управление программой**. Просмотреть и изменить права доступа пользователей к функциям Kaspersky Security 10.1 для Windows Server.
- **Изменить права пользователей на управление Kaspersky Security Service**. Просмотреть и настроить права доступа к управлению службой Kaspersky Security Service.
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационном файле формата XML. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла формата XML. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Security 10.1 для Windows Server и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли Kaspersky Security 10.1. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Security 10.1 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 10.1 для Windows Server** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Security 10.1 для Windows Server. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель быстрого доступа и контекстное меню задач Kaspersky Security 10.1 для Windows Server

Вы можете управлять задачами Kaspersky Security 10.1 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. 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. Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Перейти к просмотру и работе с журналом выполнения задачи. Операция доступна для всех задач.
- **Сохранить задачу**. Сохранить и применить измененные параметры задачи. Операция доступна для задач постоянной защиты файлов и задач проверки по требованию.
- **Удалить задачу**. Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Статистика**. Перейти к просмотру статистики задачи. Операция доступна для задачи проверки целостности программы.
- **Шаблоны параметров**. Перейти к работе с шаблонами. Операция доступна для задач постоянной защиты файлов и проверки по требованию.

Просмотр информации о состоянии защиты сетевых хранилищ

► *Чтобы просмотреть информацию о состоянии защиты сетевых хранилищ,*

Выберите узел **Kaspersky Security 10.1 для Windows Server** в дереве Консоли.

По умолчанию информация в панели результатов Консоли Kaspersky Security 10.1 обновляется автоматически:

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

► *Чтобы вручную обновить информацию в узле Kaspersky Security 10.1 для Windows Server,*

в контекстном меню узла Kaspersky Security 10.1 для Windows Server выберите пункт **Обновить**.

В панели результатов узла **Kaspersky Security 10.1 для Windows Server** на закладке **Защита сетевых**

хранилищ отображается информация о состоянии защищаемых сетевых хранилищ (см. таблицу ниже).

В блоке **Постоянная защита** отображается информация о задачах защиты RPC- и ICAP-подключаемых сетевых хранилищ, а также о состоянии интеграции с хранилищем Celerra / VNX (см. таблицу ниже).

Таблица 1. Информация о защите сетевых хранилищ

Блок Защита сетевых хранилищ	Информация

Индикатор состояния защиты сетевых хранилищ	Цвет панели с названием блока является индикатором состояния задач, описанных в блоке. Индикатор может принимать следующие значения:
	• Зеленый цвет панели отображается в случае, если обе задачи Защита RPC-подключаемых сетевых хранилищ и Защита ICAP-подключаемых сетевых хранилищ запущены.
	• Желтый цвет панели отображается в следующих случаях:
	  • Запущена одна из задач: Защита RPC-подключаемых сетевых хранилищ и Защита ICAP-подключаемых сетевых хранилищ.
	  • Запущен Антивирусный агент Celerra / VNX.
	• Красный цвет панели отображается в случае, если обе задачи защиты хранилищ не запущены и Антивирусный агент Celerra / VNX не найден.

Защита RPC-подключаемых сетевых хранилищ.	**Статус задачи** – текущее состояние задачи, например, Выполняется или Остановлена. **Обнаружено** – количество вредоносных объектов, обнаруженных в общих папках RPC-подключаемых сетевых хранилищ. Если количество обнаруженных вредоносных программ превышает 0, значение строки выделяется красным цветом.
Защита ICAP-подключаемых сетевых хранилищ	**Статус задачи** – текущее состояние задачи, например, Выполняется или Остановлена. **Обнаружено** – количество вредоносных объектов, обнаруженных в общих папках ICAP-подключаемых сетевых хранилищ. Если количество обнаруженных вредоносных программ превышает 0, значение строки выделяется красным цветом.
Интеграция с EMC Celerra / VNX	Возможны следующие состояния: • **Антивирусный агент Celerra / VNX не найден**. Kaspersky Security 10.1 для Windows Server не удалось найти программное обеспечение от компании EMC или произошла ошибка в интеграционном коде. • **Защита отключена**. Kaspersky Security 10.1 для Windows Server установил соединение с программным обеспечением от компании EMC, но в Kaspersky Security 10.1 для Windows Server задача постоянной защиты файлов не выполняется. • **Защита включена**. Kaspersky Security 10.1 для Windows Server установил соединение с программным обеспечением от компании EMC, и в Kaspersky Security 10.1 для Windows Server выполняется задача постоянной защиты файлов.

В блоке **Защита от шифрования** (см. таблицу ниже) отображается информация о задаче Защита от шифрования для NetApp.

Таблица 2. Информация о статусе Защиты от шифрования

Блок Контроль	Информация
Индикатор состояния Защиты от шифрования	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – задача Защита от шифрования для NetApp выполняется. • Красный цвет панели – задача Защита от шифрования для NetApp не выполняется.
Защита от шифрования для NetApp	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим** – один из двух доступных режимов задачи Защита от шифрования для NetApp. **Заблокировано узлов** – количество скомпрометированных компьютеров, заблокированных при попытке доступа к общим сетевым папкам на защищаемом сервере.

Управление задачами защиты сетевых хранилищ

Этот раздел содержит информацию о задачах Kaspersky Security 10.1 для Windows Server: их создании, задании параметров и ручном либо автоматическом запуске или остановке 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

► *Чтобы запустить или остановить задачу защиты сетевых хранилищ, выполните следующие действия:*

1. Откройте контекстное меню названия задачи в Консоли Kaspersky Security 10.1.
2. Выберите один из пунктов: **Запустить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита.

Работа с расписанием задач

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

Настройка параметров расписания запуска задач

В Консоли Kaspersky Security 10.1 вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

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

1. Откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.
3. Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск задачи по расписанию запрещен действием политики программы Kaspersky Security Center.

5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. В списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество часов, и укажите количество часов в поле **Раз в <количество> ч**;
      - **Ежесуточно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут**;
      - **Еженедельно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество недель, и укажите количество недель в поле **Раз в <количество> нед**; укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, если хотите, чтобы задача запускалась при каждом запуске

Kaspersky Security 10.1 для Windows Server;

- **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.

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

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

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

6. 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.

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

   Откроется окно **Параметры задачи**.

3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:

   - установите флажок **Запускать задачу по расписанию**, если хотите включить запуск задачи по расписанию;
   - снимите флажок **Запускать задачу по расписанию,** если хотите выключить запуск задачи по расписанию.

   Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Защита сетевых хранилищ EMC группы Celerra / VNX

Этот раздел содержит информацию о защите сетевых хранилищ EMC группы Celerra / VNX (далее также Celerra / VNX) и об интеграции Kaspersky Security 10.1 для Windows Server с сетевым хранилищем Celerra / VNX.

В этом разделе

О защите сетевых хранилищ EMC группы Celerra / VNX

Kaspersky Security 10.1 для Windows Server, установленный на сервере под управлением операционной системы Microsoft Windows, защищает сетевые хранилища EMC группы Celerra / VNX от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.

Kaspersky Security 10.1 для Windows Server проверяет файлы, размещенные в сетевых общих папках (network share) в сетевом хранилище EMC группы Celerra / VNX, при попытке чтения или изменения этих файлов с рабочих станций. Сетевое хранилище разрешает чтение или изменение файла, если Kaspersky Security 10.1 для Windows Server признал этот файл безопасным. Если Kaspersky Security 10.1 для Windows Server признал файл зараженным или возможно зараженным, сетевое хранилище запрещает чтение или изменение файла.

В Kaspersky Security 10.1 для Windows Server вы можете настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

По умолчанию Kaspersky Security 10.1 для Windows Server выполняет следующие действия:

- лечит зараженные файлы;
- удаляет зараженные файлы, если лечение невозможно;
- помещает возможно зараженные файлы на карантин;
- помещает копию зараженного файла в резервное хранилище перед лечением или удалением этого файла.

Для защиты сетевого хранилища вам нужно обеспечить интеграцию Kaspersky Security 10.1 для Windows Server с сетевым хранилищем Celerra / VNX.

Защита сетевого хранилища Celerra / VNX выполняется задачей Постоянная защита файлов.

Подробная информация о задаче Постоянная защита файлов содержится в *Руководстве администратора Kaspersky Security 10.1 для Windows Server*.

Интеграция Kaspersky Security 10.1 для Windows Server с сетевым хранилищем EMC группы Celerra / VNX

Для защиты сетевого хранилища вам нужно обеспечить интеграцию Kaspersky Security 10.1 для Windows Server с сетевым хранилищем Celerra / VNX.

Интеграция Kaspersky Security 10.1 для Windows Server с сетевым хранилищем Celerra / VNX выполняется, если соблюдены следующие условия:

1. На компьютере, который защищен Kaspersky Security 10.1 для Windows Server, установлен программный агент CAVA (Celerra Antivirus Agent), входящий в комплект программного обеспечения EMC Celerra / VNX. Kaspersky Security 10.1 for Windows Server взаимодействует с сетевым хранилищем Celerra / VNX с помощью этого программного агента.
2. Задача Постоянная защита файлов выполняется.

   Подробная информация о задаче Постоянная защита файлов и инструкции по настройке ее параметров содержатся в Руководстве администратора *Kaspersky Security 10.1 для Windows Server.*

Статус интеграции Kaspersky Security 10.1 для Windows Server с сетевым хранилищем Celerra / VNX отображается в панели результатов узла Kaspersky Security 10.1 для Windows Server (см. раздел «Просмотр информации о состоянии защиты сетевых хранилищ» на стр. 21).

Защита RPC-подключаемых сетевых хранилищ.

Этот раздел содержит информацию о задаче защиты сетевых хранилищ, подключаемых по протоколу RPC, о настройке соединения между сетевым хранилищем и Kaspersky Security 10.1 для Windows Server, а также инструкции по настройке параметров задачи Защита RPC-подключаемых сетевых хранилищ и по настройке параметров безопасности в задаче.

В этом разделе

О защите RPC-подключаемых сетевых хранилищ

Kaspersky Security 10.1 для Windows Server, установленный на сервере под управлением операционной системы Microsoft Windows, защищает RPC-подключаемые сетевые хранилища (например, сетевые хранилища от NetApp) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.

Kaspersky Security 10.1 для Windows Server проверяет файлы, размещенные в сетевых общих папках (network share) в RPC-подключаемом сетевом хранилище (далее также сетевом хранилище), при попытке чтения или изменения этих файлов с рабочих станций. Сетевое хранилище разрешает чтение или изменение файла, если Kaspersky Security 10.1 для Windows Server признал этот файл безопасным. Если Kaspersky Security 10.1 для Windows Server признал файл зараженным или возможно зараженным, сетевое хранилище выполняет требуемые действия в соответствии с настроенными параметрами (например, запрещает чтение или изменение файла).

В Kaspersky Security 10.1 для Windows Server вы можете настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

По умолчанию Kaspersky Security 10.1 для Windows Server выполняет следующие действия:

- лечит зараженные файлы;
- удаляет зараженные файлы, если лечение невозможно;
- помещает возможно зараженные файлы на карантин;
- помещает копию зараженного файла в резервное хранилище перед лечением или удалением этого файла.

Вы можете защитить одно сетевое хранилище или несколько сетевых хранилищ с помощью одного сервера с установленным Kaspersky Security 10.1 для Windows Server. Для улучшения быстродействия сетевого хранилища и сервера с установленным Kaspersky Security 10.1 для Windows Server вы можете использовать несколько серверов с установленным Kaspersky Security 10.1 для Windows Server для защиты одного сетевого хранилища. В этом случае сетевое хранилище распределяет нагрузку между присоединенными серверами с установленным Kaspersky Security 10.1 для Windows Server.

Для защиты сетевого хранилища вам нужно добавить его в качестве области защиты и настроить соединение между сетевым хранилищем и сервером с установленным Kaspersky Security 10.1 для Windows Server. В Kaspersky Security 10.1 для Windows Server предусмотрена задача защиты RPC-подключаемых сетевых хранилищ под названием Защита RPC-подключаемых сетевых хранилищ.

Задача Защита RPC-подключаемых сетевых хранилищ создана по умолчанию и является системной задачей Kaspersky Security 10.1 для Windows Server. Вы не можете удалить или переименовать эту задачу. Вы не можете создать пользовательские задачи защиты RPC-подключаемых сетевых хранилищ.

Вы можете настраивать задачу Защита RPC-подключаемых сетевых хранилищ. Параметры, настроенные в свойствах задачи Защита RPC-подключаемых сетевых хранилищ, применяются ко всем добавленным областям защиты. Также вы можете настраивать параметры безопасности каждой области защиты.

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security 10.1 для Windows Server не будет обрабатывать возможно зараженные объекты.

Компонент Защита ICAP-подключаемых сетевых Network хранилищ доступен в составе решения Kaspersky Security для систем хранения данных.
Подробная информация о решениях для защиты организации, в состав которых входит Kaspersky Security 10.1 для Windows Server, содержится в *Руководстве администратора Kaspersky Security 10.1 для Windows Server*.

О проверке символических ссылок

Символическая ссылка (symbolic link) – это специальный тип файла, который содержит указатель на другой объект в форме абсолютного или относительного пути. Символическая ссылка может указывать, например, на объект, который находится в сетевой общей папке другого сетевого хранилища.

Проверка символических ссылок в сетевых хранилищах имеет следующие особенности. Kaspersky Security 10.1 для Windows Server проверяет файл, на который указывает символическая ссылка, только если этот файл входит в область защиты. Если файл, на который указывает символическая ссылка, находится за пределами области защиты, Kaspersky Security 10.1 для Windows Server не проверяет этот файл. Если в сетевом хранилище разрешен переход по символической ссылке за пределы папки, в которой находится символическая ссылка, рекомендуется убедиться, что папка назначения входит в область защиты. Например, если разрешен переход по символической ссылке между общими сетевыми папками внутри защищаемого сетевого хранилища, рекомендуется убедиться, что для всех общих сетевых папок включена функция антивирусной проверки.

О проверке снэпшотов и других томов и папок, доступных только для чтения

Kaspersky Security 10.1 для Windows Server проверяет файлы, находящиеся в снэпшотах (snapshot) и других томах и папках, доступных только для чтения, но не выполняет никаких действий над файлами в этих томах и папках, например, не блокирует доступ к зараженным файлам. Чтобы исключить угрозу заражения рабочих станций, рекомендуется делать снэпшоты и другие тома и папки, доступные только для чтения, скрытыми от пользователей и предоставлять доступ к снэпшотам и другим томам и папкам, доступным только для чтения, через обращение к администратору.

Настройка соединения между RPC-подключаемым сетевым хранилищем и Kaspersky Security 10.1 для Windows Server

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security 10.1 для Windows Server не будет обрабатывать возможно зараженные объекты.

Для защиты RPC-подключаемых сетевых хранилищ вам нужно настроить подключение сетевого хранилища к Kaspersky Security 10.1 для Windows Server.

► *Чтобы настроить соединение между сетевым хранилищем и Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. На сервере с установленным Kaspersky Security 10.1 для Windows Server настройте следующие параметры:
   - Добавьте сетевое хранилище в Kaspersky Security 10.1 для Windows Server (см. раздел «Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security 10.1 для Windows Server» на стр. 33).
   - В Консоли Kaspersky Security 10.1 укажите учетную запись, с правами которой вы хотите запускать задачу Защита RPC-подключаемых сетевых хранилищ (см. раздел «Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ» на стр. 32).
   - В редакторе локальной групповой политики настройте параметры безопасности локальных политик (см. раздел «Настройка параметров безопасности локальных политик в редакторе локальной групповой политики» на стр. 13).
   - В окне настройки брандмауэра Windows настройте правила входящих и исходящих подключений в брандмауэре Windows (см. раздел «Настройка входящих и исходящих подключений в брандмауэре Windows» на стр. 14).
   - Если требуется, установите программу-коннектор для RPC-подключаемого сетевого хранилища, которое будет защищать Kaspersky Security 10.1 для Windows Server.

   Вы можете найти информацию об установке программы-коннектора для защищаемого сетевого хранилища в документации к этому сетевому хранилищу.

2. В сетевом хранилище настройте следующие параметры:
   - Включить функцию антивирусной защиты (vscan).
   - Добавьте учетную запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ, в группу Backup Operators.

   Вы можете найти информацию о настройке используемого вами сетевого хранилища в документации к этому сетевому хранилищу.

Соединение между RPC-подключаемым сетевым хранилищем и Kaspersky Security 10.1 для Windows Server будет установлено.

Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ

Требуется, чтобы учетная запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ, имела права администратора на сервере с установленным Kaspersky Security 10.1 для Windows Server и входила в группу Backup Operators на сетевом хранилище.

Если сетевое хранилище и сервер с установленным Kaspersky Security 10.1 для Windows Server находятся в одном домене, вы можете использовать доменную учетную запись. Если сетевое хранилище и сервер с установленным Kaspersky Security 10.1 для Windows Server находятся в одной рабочей группе, вы можете использовать локальные учетные записи с одинаковым именем пользователя и одинаковым паролем.

Для сетевых хранилищ, находящихся под управлением операционной системы Data ONTAP 8.2.1 или выше в режиме cluster-mode, доступно использование только доменной учетной записи.

Если на сервере Kaspersky Security 10.1 для Windows Server существует более одной учетной записи пользователя, убедитесь, что пользователь, который настроил и запускает задачу Защита RPC-подключаемых сетевых хранилищ, есть в списке пользователей с привилегированным доступом для работы с NetApp. Если учетная запись не обладает необходимыми правами, папки общего доступа в сетевом хранилище будут доступны, но при выполнении задач защиты проверка данных папок производиться не будет.

► *Чтобы указать учетную запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в блоке **Параметры соединения с сетевым хранилищем** введите имя учетной записи, с правами которой запускается задача, пароль этой учетной записи и подтверждение пароля.
5. Нажмите на кнопку **ОК**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Формирование области защиты в задаче Защита RPC-подключаемых сетевых хранилищ

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Защита RPC-подключаемых сетевых хранилищ.

Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security 10.1 для Windows Server

► *Чтобы добавить RPC-подключаемое сетевое хранилище в область защиты Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Добавление области защиты**.
5. В окне **Добавление области защиты** введите доменное имя или IP-адрес сетевого хранилища.

   Если вы используете сетевое хранилище NetApp под управлением операционной системы NetApp Clustered Data ONTAP, укажите в этом поле IP-адрес компьютера, на котором установлена программа-коннектор, то есть 127.0.0.1.
6. Нажмите на кнопку **ОК**, чтобы добавить сетевое хранилище в Kaspersky Security 10.1 для Windows Server.

   Сетевое хранилище появится в списке защищаемых сетевых хранилищ.
7. Нажмите на кнопку **Сохранить**.

Настроенные параметры области защиты будут сохранены.

Kaspersky Security 10.1 для Windows Server подключается к сетевому хранилищу в момент запуска задачи Защита RPC-подключаемых сетевых хранилищ. Если вы указали неправильное доменное имя или неправильный IP-адрес сетевого хранилища, задача завершается с ошибкой. Kaspersky Security 10.1 для Windows Server записывает информацию об этом событии в журнал системного аудита и в журнал выполнения задачи.

Если вы используете сетевое хранилище NetApp под управлением операционной системы NetApp Clustered Data ONTAP, Kaspersky Security 10.1 для Windows Server подключается к программе-коннектору, которая установлена на защищаемом сервере. Рекомендуется удостовериться, что соединение между программой-коннектором и сетевым хранилищем NetApp настроено правильно и Kaspersky Security 10.1 для Windows Server защищает добавленное сетевое хранилище.

Активация и деактивация функции защиты добавленного RPC-подключаемого сетевого хранилища

► *Чтобы деактивировать функцию защиты добавленного RPC-подключаемого сетевого хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ снимите флажок рядом с именем сетевого хранилища, для которого вы хотите временно выключить функцию защиты.
5. Нажмите на кнопку **Сохранить**.

Kaspersky Security 10.1 для Windows Server разорвет соединение с выбранным сетевым хранилищем.

Если вы выключите функцию защиты для всех добавленных сетевых хранилищ, Kaspersky Security 10.1 для Windows Server остановит задачу Защита RPC-подключаемых сетевых хранилищ.

► *Чтобы активировать функцию защиты добавленного RPC-подключаемого сетевого хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ установите флажок рядом с именем сетевого хранилища, для которого вы хотите включить функцию защиты.
5. Нажмите на кнопку **Сохранить**.

Если задача Защита RPC-подключаемых сетевых хранилищ выполняется, Kaspersky Security 10.1 для Windows Server установит соединение с сетевым хранилищем. Если задача Защита RPC-подключаемых сетевых хранилищ остановлена, вам нужно запустить ее, чтобы установить соединение Kaspersky Security 10.1 для Windows Server с сетевым хранилищем.

Удаление RPC-подключаемого сетевого хранилища из области защиты

► *Чтобы удалить RPC-подключаемое сетевое хранилище из задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, которое хотите удалить из области защиты задачи.
5. В контекстном меню имени или IP-адреса сетевого хранилища, которое вы хотите удалить из области защиты задачи, выберите пункт **Удалить из списка**.

Выбранное сетевое хранилище будет удалено из списка защищаемых сетевых хранилищ.

Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ

По умолчанию задача Защита RPC-подключаемых сетевых хранилищ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

После того как вы измените параметры задачи, например, укажете новую область защиты, Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Kaspersky Security 10.1 для Windows Server сохранит в журнале системного аудита дату и время изменения параметров задачи.

Таблица 3. Параметры задачи Защита RPC-подключаемых сетевых хранилищ по умолчанию

Параметр	Значение по умолчанию	Комментарий
Область защиты	Отсутствует.	Вам нужно добавить сетевое хранилище в Kaspersky Security 10.1 для Windows Server.
Уровень безопасности	Применяется уровень безопасности **Рекомендуемый**.	Вы можете применить к защищаемому сетевому хранилищу один из предустановленных уровней безопасности, также вы можете настроить значения параметров безопасности вручную.
Эвристический анализатор	Применяется уровень анализа Средний.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Доверенная зона	Применяется.	Вы можете включать и выключать применение доверенной зоны и настраивать параметры доверенной зоны.

Параметр	Значение по умолчанию	Комментарий
Использование KSN	Применяется.	Вы можете включать и выключать использование служб KSN в задаче Защита RPC-подключаемых сетевых хранилищ.
Параметры соединения с сетевым хранилищем	• **Имя пользователя** и **Пароль** учетной записи, с правами которой запускается задача, – отсутствуют; • Тайм-аут между попытками восстановления соединения (сек.): 5; • Максимальное количество попыток восстановления соединения: 3; • **Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы** – флажок снят.	Вам нужно указать учетную запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ. Также вы можете изменять другие параметры соединения с сетевыми хранилищами.
Запуск задачи по расписанию	Не применяется. Флажок **Запускать задачу по расписанию** снят. Задача запускается вручную.	Вы можете настроить запуск задачи по расписанию, например, при запуске Kaspersky Security 10.1 для Windows Server.

► *Чтобы настроить параметры задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** настройте следующие параметры задачи:
   - Применение эвристического анализатора (на стр. 37).
   - Запуск задачи с правами учетной записи (см. раздел «Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ» на стр. 32).
   - Соединение с RPC-подключаемым сетевым хранилищем (см. раздел «Настройка общих параметров соединения с RPC-подключаемым сетевым хранилищем» на стр. 39).
   - Интеграция с другими компонентами Kaspersky Security 10.1 для Windows Server (см. раздел «Подготовка к запуску задач защиты сетевых хранилищ» на стр. 13).
5. На закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач» на стр. 24).
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.
7. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** выберите закладку **Настройка области защиты**.

8. Выполните следующие действия:
   - Добавьте RPC-подключаемые сетевые хранилища в область защиты Kaspersky Security 10.1 для Windows Server (см. раздел «Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security 10.1 для Windows Server» на стр. 33).
   - В списке добавленных сетевых хранилищ, подключаемых по протоколу RPC, выберите сетевые хранилища, защиту которых хотите активировать.
   - Выберите один из предустановленных уровней безопасности (см. раздел «Применение предустановленного уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ» на стр. 42) или настройте параметры защиты объектов вручную (см. раздел «Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ» на стр. 42).
9. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Применение эвристического анализатора

В задаче Защита ICAP-подключаемых сетевых хранилищ вы можете применять эвристический анализатор и настраивать уровень анализа.

► *Чтобы настроить параметры использования эвристического анализатора в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** в блоке **Эвристический анализатор** выполните следующие действия:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

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

     Существуют следующие уровни детализации проверки:

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

       Этот уровень выбран по умолчанию.

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

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

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Интеграция с другими компонентами Kaspersky Security 10.1 для Windows Server

Вы можете использовать задачу Защита RPC-подключаемых сетевых хранилищ совместно со следующими функциональными компонентами Kaspersky Security 10.1 для Windows Server:

- Доверенная зона;
- задача Использование KSN.

Доверенная зона – это заранее сформированный список исключений из области защиты или проверки.

Вы можете включить или выключить применение доверенной зоны в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите доверенную зону, исключения в ней начнут или перестанут действовать немедленно.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программ.

Вы можете включить или выключить применение KSN в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите применение KSN, задача начнет или перестанет выносить заключения о репутации проверяемых файлов на основе информации, полученной от KSN.

Для запуска задачи Использование KSN необходимо принять Положение о KSN.

Подробная информация о доверенной зоне и задаче Использование KSN приведена в Руководстве администратора Kaspersky Security 10.1 для Windows Server.

► *Чтобы включить или выключить применение других компонентов программы в задаче Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в блоке Интеграция с другими компонентами Kaspersky Security 10.1 для Windows Server выполните следующие действия:

   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

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

     Если флажок снят, Kaspersky Security 10.1 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**.

     Флажок включает или выключает использование служб Kaspersky Security Network (KSN) задачей Защита ICAP-подключаемых сетевых хранилищ.

     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 Защита ICAP-подключаемых сетевых хранилищ не использует службы KSN.

     По умолчанию флажок установлен.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройка общих параметров соединения с RPC-подключаемым сетевым хранилищем

► *Чтобы настроить общие параметры соединения с RPC-подключаемым сетевым хранилищем, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** в блоке Параметры соединения с сетевым хранилищем выполните следующие действия:

   - Введите значение тайм-аута между попытками восстановления соединения с сетевым хранилищем.
   - Введите количество попыток восстановления соединения с сетевым хранилищем.

Рекомендуется оставлять значения, указанные по умолчанию, или указывать большие значения.

- Если вы хотите, чтобы после каждого обновления баз программы Kaspersky Security 10.1 для Windows Server очищал кеш проверенных файлов сетевого хранилища, установите флажок **Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы**.
- Если вы хотите, чтобы после каждого обновления баз программы Kaspersky Security 10.1 для Windows Server сохранял кеш проверенных файлов сетевого хранилища, снимите флажок **Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы**.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Уровни безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

Этот раздел содержит описание параметров безопасности и инструкции по применению предустановленных уровней безопасности и настройке параметров безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ.

Об уровнях безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

В задаче Защита RPC-подключаемых сетевых хранилищ для каждого защищаемого хранилища вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней безопасности имеет свой набор параметров безопасности (см. таблицу ниже). Вы также можете настроить значения параметров безопасности вручную, уровень безопасности для сетевого хранилища в этом случае изменится на **Другой**.

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Security 10.1 для Windows Server на серверах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых серверов. Этот уровень рекомендован специалистами "Лаборатории Касперского", как достаточный для защиты файловых 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 4. Параметры предустановленных уровней безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	Объекты, проверяемые по списку расширений, указанному в антивирусных базах.	Объекты, проверяемые по формату.	Объекты, проверяемые по формату.
Защита составных объектов	Упакованные объекты	• SFX-архивы • Упакованные объекты • OLE-объекты	• SFX-архивы • Упакованные объекты • OLE-объекты
Действия над зараженными объектами	Блокировать доступ и лечить. Удалять, если лечение невозможно	Блокировать доступ и выполнять рекомендуемое действие	Блокировать доступ и лечить. Удалять, если лечение невозможно
Действия над возможно зараженными объектами	Блокировать доступ и помещать на карантин	Блокировать доступ и выполнять рекомендуемое действие	Блокировать доступ и помещать на карантин
Действия в зависимости от типа обнаруженного объекта	нет	нет	нет
Исключать файлы.	нет	нет	нет
Не обнаруживать	нет	нет	нет
Останавливать проверку, если она длится более (сек.)	60	60	60
Не проверять составные объекты размером более (МБ).	8	8	нет

Применение предустановленного уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

► *Чтобы применить один из предустановленных уровней безопасности для RPC-подключаемого сетевого хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, для которого вы хотите выбрать предустановленный уровень безопасности.
5. На закладке **Уровень безопасности** выберите в списке один из следующих предустановленных уровней безопасности:
   - **Максимальная защита**;
   - **Рекомендуемый**;
   - **Максимальное быстродействие**.

   На закладке **Уровень безопасности** отображаются основные значения параметров выбранного уровня безопасности. Применяемый уровень безопасности отображается рядом с именем сетевого хранилища в списке защищаемых сетевых хранилищ.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры уровня безопасности будут сохранены и применены в выполняющейся задаче.

Также вы можете настроить параметры безопасности защищаемого сетевого хранилища вручную (см. раздел «Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ» на стр. 42).

Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ

► *Чтобы вручную настроить параметры безопасности для RPC-подключаемого сетевого хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, параметры безопасности которого вы хотите настроить.

   Вы можете применить предварительно созданный шаблон параметров безопасности.

5. Настройте параметры для выбранного сетевого хранилища в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:

   - На закладке **Общие** выполните следующие действия:

     - В блоке **Защита объектов** укажите объекты, которые проверяет Kaspersky Security 10.1 для Windows Server:

       - **Все объекты**;

         Kaspersky Security 10.1 для Windows Server проверяет все объекты.

       - **Объекты, проверяемые по формату**;

         Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании формата файла.

         Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

         Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании расширения файла.

         Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

         Kaspersky Security 10.1 для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

       Этот параметр вы также можете настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security 10.1 для Windows Server, то сетевое хранилище отсылает объект на проверку, а Kaspersky Security 10.1 для Windows Server признает объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отсылает объект на проверку. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленным Kaspersky Security 10.1 для Windows Server рекомендуется настраивать параметры, ограничивающие проверяемые объекты, в сетевом хранилище.

     - В блоке **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security 10.1 для Windows Server.

   - На закладке **Действия** выполните следующие действия:

     - В блоке **Действия над зараженными объектами** укажите, какое действие выполняет Kaspersky Security 10.1 для Windows Server при обнаружении зараженного объекта.

     - В блоке **Действия над возможно зараженными объектами** укажите, какое действие выполняет Kaspersky Security 10.1 для Windows Server при обнаружении возможно зараженного объекта.

     - Выберите действия над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять неизлечимый составной объект при обнаружении вложенного зараженного или другого объекта**.

Флажок включает или выключает форсированное удаление составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта.

Если флажок установлен и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Блокировать доступ и удалять**, Kaspersky Security 10.1 для Windows Server принудительно выполняет удаление всего составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

Если флажок снят, и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Блокировать доступ и удалять**, Kaspersky Security 10.1 для Windows Server не выполняет указанное действие для родительского составного объекта при обнаружении вложенного вредоносного или другого обнаруживаемого объекта в случае, если составной объект неизменяем.

- На закладке **Производительность** выполните следующие действия:
  - В блоке **Исключения** укажите, какие объекты Kaspersky Security 10.1 для Windows Server исключает из проверки одним из следующих способов:
    - Если вы хотите исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
    - Если вы хотите исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии (http://www.securelist.ru/).
  - В блоке **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.

    Если вы используете сетевое хранилище NetApp, работающее под управлением операционной системы Clustered Data ONTAP, этот параметр вы также можете настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security 10.1 для Windows Server, то сетевое хранилище отсылает объект на проверку, а Kaspersky Security 10.1 для Windows Server признает объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отсылает объект на проверку. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленным Kaspersky Security 10.1 для Windows Server рекомендуется настраивать параметры, ограничивающие проверяемые объекты, в сетевом хранилище.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры пользовательского уровня безопасности будут сохранены и применены в выполняющейся задаче.

Работа с шаблонами параметров уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

Этот раздел содержит инструкции по работе с шаблонами параметров уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ.

Создание шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Security 10.1 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 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 **ОК**.

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**.

Применение шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Security 10.1 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 файловых ресурсов сервера выберите узел, для которого вы хотите применить шаблон.
4. Выберите **Применить шаблон** > **<Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню названия 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 Kaspersky Security 10.1 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 файловых ресурсов сервера выберите узел, для которого вы хотите применить шаблон.
4. Выберите **Применить шаблон** > **<Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню названия 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**.

Просмотр параметров безопасности в шаблоне

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

1. В дереве Консоли Kaspersky Security 10.1 выберите задачу, шаблон безопасности которой хотите просмотреть.
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 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.

Удаление шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Security 10.1 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.

Просмотр статистики задачи Защита RPC-подключаемых сетевых хранилищ

Если задача Защита RPC-подключаемых сетевых хранилищ выполняется, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Security 10.1 для Windows Server обработал с момента запуска этой задачи по текущий момент, то есть статистику задачи.

► *Чтобы просмотреть статистику задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов выберите закладку **Обзор и управление**.

В блоке **Статистика** отобразится таблица, содержащая информацию об объектах, которые Kaspersky Security 10.1 для Windows Server обработал с момента запуска задачи по текущий момент (см. таблицу ниже).

Таблица 5. Полная статистика задачи Защита RPC-подключаемых сетевых хранилищ

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Security 10.1 для Windows Server. Например, если Kaspersky Security 10.1 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 10.1 для Windows Server признал зараженными, или обнаруженное легальное программное обеспечение, которое не было исключено из области действия задач постоянной защиты или проверки.
Обнаружены возможно зараженные объекты.	Количество объектов, которые Kaspersky Security 10.1 для Windows Server признал возможно зараженными.
Не вылечено объектов	Количество объектов, которые Kaspersky Security 10.1 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 10.1 для Windows Server попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Не удалено объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.
Не проверено объектов	Количество объектов в области защиты, которые Kaspersky Security 10.1 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 10.1 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 10.1 для Windows Server вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Security 10.1 для Windows Server поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Security 10.1 для Windows Server сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Security 10.1 для Windows Server пропустил, так как эти объекты защищены паролем.

Поле	Описание
Поврежденных объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server пропустил, так как их формат искажен.
Обработано объектов	Количество рабочих процессов Kaspersky Security 10.1 для Windows Server в текущий момент.

Защита ICAP-подключаемых сетевых хранилищ

Этот раздел содержит информацию о задаче защиты сетевых хранилищ, подключаемых по протоколу ICAP, о настройке подключения сетевого хранилища к Kaspersky Security 10.1 для Windows Server, а также инструкции по настройке параметров задачи защиты и по настройке параметров безопасности ICAP-подключаемых сетевых хранилищ.

В этом разделе

О защите ICAP-подключаемых сетевых хранилищ

Kaspersky Security 10.1 для Windows Server, установленный на сервере под управлением операционной системы Microsoft Windows, защищает ICAP-подключаемые сетевые хранилища (например, EMC Isilon) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.

Kaspersky Security 10.1 для Windows Server не имеет прямого доступа к файлам, размещенным в ICAP-подключаемом сетевом хранилище (далее также *сетевом хранилище*). При попытке чтения, создания или изменения файла, сетевое хранилище формирует ICAP-запрос к Kaspersky Security 10.1 для Windows Server и передает файл внутри этого запроса. Программа выполняет антивирусную проверку файла в соответствии с параметрами, заданными в задаче Защита ICAP-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security 10.1 для Windows Server выполняет над файлом действия, заданные в параметрах задачи, и передает результат проверки сетевому хранилищу. Если в параметрах задачи задано действие Лечить, и файл удалось вылечить, Kaspersky Security 10.1 для Windows Server возвращает сетевому хранилищу вылеченный файл в ответе на запрос.

В Kaspersky Security 10.1 для Windows Server вы можете настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

При использовании KSN в задаче Защита ICAP-подключаемого сетевого хранилища Kaspersky Security 10.1 для Windows Server не может удалять или блокировать файлы, которые используются ICAP-подключаемым сетевым хранилищем, так как на момент получения недоверенного заключения от служб KSN программа не имеет прямого доступа к сетевым каталогам хранилища. Информация о получении недоверенного заключения фиксируется в журнале выполнения задачи Использование KSN.

Вы можете защитить одно сетевое хранилище с помощью одного сервера с установленным Kaspersky Security 10.1 для Windows Server. Для улучшения быстродействия сетевого хранилища и сервера с установленным Kaspersky Security 10.1 для Windows Server вы можете использовать несколько серверов с установленным Kaspersky Security 10.1 для Windows Server для защиты одного сетевого хранилища. В этом случае сетевое хранилище распределяет нагрузку между присоединенными серверами с установленным Kaspersky Security 10.1 для Windows Server.

Задача Защита ICAP-подключаемых сетевых хранилищ создана по умолчанию и является системной задачей Kaspersky Security 10.1 для Windows Server. Вы не можете удалить или переименовать эту задачу. Вы не можете создать пользовательские задачи защиты ICAP-подключаемых сетевых хранилищ. Вы можете настраивать задачу Защита ICAP-подключаемых сетевых хранилищ.

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security 10.1 для Windows Server не будет обрабатывать возможно зараженные объекты.

Компонент Защита ICAP-подключаемых сетевых Network хранилищ доступен в составе решения Kaspersky Security для систем хранения данных.
Подробная информация о решениях для защиты организации, в состав которых входит Kaspersky Security 10.1 для Windows Server содержится в Руководстве администратора *Kaspersky Security 10.1 для Windows Server.*

Настройка соединения между ICAP-подключаемым сетевым хранилищем и Kaspersky Security 10.1 для Windows Server

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security 10.1 для Windows Server не будет обрабатывать возможно зараженные объекты.

Для защиты ICAP-подключаемых сетевых хранилищ вам нужно настроить подключение сетевого хранилища к Kaspersky Security 10.1 для Windows Server.

► *Чтобы настроить соединение между сетевым хранилищем и Kaspersky Security 10.1 для Windows Server, выполните следующие действия:*

1. На сервере с установленным Kaspersky Security 10.1 для Windows Server настройте следующие параметры:
   - В Консоли Kaspersky Security 10.1 укажите параметры соединения с ICAP-подключаемым сетевым хранилищем, которое будет защищать Kaspersky Security 10.1 для Windows Server (см. раздел «Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем» на стр. 54).
   - В редакторе локальной групповой политики настройте параметры безопасности локальных политик (см. раздел «Настройка параметров безопасности локальных политик в редакторе локальной групповой политики» на стр. 13).
   - В окне настройки брандмауэра Windows настройте правила входящих и исходящих подключений в брандмауэре Windows (см. раздел «Настройка входящих и исходящих подключений в брандмауэре Windows» на стр. 14).
2. В сетевом хранилище настройте следующие параметры:
   - Включите функцию антивирусной защиты.
   - Укажите адрес подключения к Kaspersky Security 10.1 для Windows Server в параметрах сетевого хранилища.

   Вы можете найти информацию о настройке используемого вами сетевого хранилища в документации к этому сетевому хранилищу.

Соединение между ICAP-подключаемым сетевым хранилищем и Kaspersky Security 10.1 для Windows Server будет установлено.

Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ

По умолчанию задача Защита ICAP-подключаемых сетевых хранилищ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

После того как вы измените параметры задачи, например, измените уровень безопасности, Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Kaspersky Security 10.1 для Windows Server сохранит в журнале системного аудита дату и время изменения параметров задачи.

Таблица 6. Параметры задачи Защита ICAP-подключаемых сетевых хранилищ по умолчанию

Параметр	Значение по умолчанию	Комментарий
Уровень безопасности	Применяется уровень безопасности **Рекомендуемый**.	Вы можете применить к защищаемому сетевому хранилищу один из предустановленных уровней безопасности, также вы можете настроить значения параметров безопасности вручную.

Параметр	Значение по умолчанию	Комментарий
Эвристический анализатор	Применяется уровень анализа **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Использование KSN для защиты	Применяется.	Вы можете включать и выключать использование служб KSN для защиты ICAP-подключаемых сетевых хранилищ.
Параметры соединения с сетевым хранилищем	• **Номер сетевого порта ICAP-сервера** – 1344; • **Идентификатор службы** – avscan.	Также вы можете изменять другие параметры соединения с сетевыми хранилищами. Эти изменения должны быть учтены на сетевых хранилищах.
Запуск задачи по расписанию	Не применяется. Флажок **Запускать задачу по расписанию** снят. Задача запускается вручную.	Вы можете настроить запуск задачи по расписанию, например, при запуске Kaspersky Security 10.1 для Windows Server.

► *Чтобы настроить параметры задачи Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** настройте следующие параметры задачи:

   - Соединение с ICAP-подключаемым сетевым хранилищем (см. раздел «Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем» на стр. 54).
   - Применение эвристического анализатора (на стр. 54).
   - Использование KSN для защиты (см. раздел «Использование KSN для защиты» на стр. 55).

   В блоке **Уровень безопасности**:

   - Выберите один из предустановленных уровней безопасности (см. раздел «Об уровнях безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ» на стр. 56) или настройте параметры защиты объектов вручную (см. раздел «Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ» на стр. 58).
5. На закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел «Работа с расписанием задач» на стр. 24).
6. Нажмите на кнопку **ОК**.

Kaspersky Security 10.1 для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем

► *Чтобы настроить параметры соединения с ICAP-подключаемым сетевым хранилищем, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в полях блока Параметры соединения введите следующие данные:
   - Номер сетевого порта **ICAP-сервера**.

     Номер сетевого порта ICAP-сервера для подключения сетевого хранилища к программе.
   - **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 – 1344, а идентификатор службы ICAP – avscan, то эти параметры составляют следующий адрес RESPMOD URI – `icap://192.168.10.10/avscan:1344`.
5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

После того, как вы настроили параметры соединения, необходимо сформировать и указать на сетевом хранилище адрес подключения к Kaspersky Security 10.1 для Windows Server. Параметры соединения включаются в этот адрес. Например, при значениях параметров, заданных по умолчанию, адрес подключения имеет следующий вид:

```
icap://<IP-адрес компьютера с установленным Kaspersky Security 10.1 для Windows Server>/avscan:1344
```

Применение эвристического анализатора

В задаче Защита ICAP-подключаемых сетевых хранилищ вы можете применять эвристический анализатор и настраивать уровень анализа.

► *Чтобы настроить параметры использования эвристического анализатора в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в блоке **Эвристический анализатор** выполните следующие действия:

   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

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

     Существуют следующие уровни детализации проверки:

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

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

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

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Использование KSN для защиты

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программ.

Вы можете включить или выключить применение KSN в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите применение KSN, задача начнет или перестанет выносить заключения о репутации проверяемых файлов на основе информации, полученной от KSN.

Для запуска задачи Использование KSN необходимо принять Положение о KSN. По умолчанию задача Использование KSN не запускается автоматически при старте Kaspersky Security 10.1 для Windows Server.

Подробная информация о задаче Использование KSN приведена в *Руководстве администратора Kaspersky Security 10.1 для Windows Server.*

► *Чтобы включить или выключить использование KSN в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** в блоке Использование KSN снимите или установите флажок **Использовать KSN для защиты**.

   Флажок включает или выключает использование служб Kaspersky Security Network (KSN) задачей Защита ICAP-подключаемых сетевых хранилищ.

   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 Защита ICAP-подключаемых сетевых хранилищ не использует службы KSN.

   По умолчанию флажок установлен.
5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Уровни безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

Этот раздел содержит описание параметров безопасности и инструкции по применению предустановленных уровней безопасности и настройке параметров безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ.

Об уровнях безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

В задаче Защита ICAP-подключаемых сетевых хранилищ для каждого защищаемого хранилища вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней безопасности имеет свой набор параметров безопасности (см. таблицу ниже). Вы также можете настроить значения параметров безопасности вручную, уровень безопасности для сетевого хранилища в этом случае изменится на **Другой**.

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Security 10.1 для Windows Server на серверах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых серверов. Этот уровень рекомендован специалистами "Лаборатории Касперского", как достаточный для защиты файловых 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 7. Параметры предустановленных уровней безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	Объекты, проверяемые по списку расширений, указанному в антивирусных базах.	Объекты, проверяемые по формату.	Объекты, проверяемые по формату.
Защита составных объектов	Упакованные объекты	• SFX-архивы • Упакованные объекты • OLE-объекты	• SFX-архивы • Упакованные объекты • OLE-объекты
Действия над зараженными объектами	Лечить	Выполнять рекомендуемое действие	Лечить
Действия над возможно зараженными объектами	Помещать на карантин	Выполнять рекомендуемое действие	Помещать на карантин
Исключать файлы.	нет	нет	нет
Не обнаруживать	нет	нет	нет
Останавливать проверку, если она длится более (сек.)	60	60	60
Не проверять составные объекты размером более (МБ).	8	8	нет

Применение предустановленного уровня безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

► *Чтобы применить один из предустановленных уровней безопасности*

для ICAP-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Уровень безопасности** выберите в списке один из следующих предустановленных уровней безопасности:
   - **Максимальная защита.**
   - **Рекомендуемый.**
   - **Максимальное быстродействие**

   Основные значения параметров выбранного уровня безопасности отображаются под списком.
5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Также вы можете настроить параметры безопасности защищаемого сетевого хранилища вручную (см. раздел «Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ» на стр. 58).

Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ

► *Чтобы вручную настроить параметры безопасности для ICAP-подключаемого сетевого хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
5. Настройте параметры в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:
   - На закладке **Общие** выполните следующие действия:
     - В блоке **Защита объектов** укажите объекты, которые проверяет Kaspersky Security 10.1 для Windows Server:
       - **Все объекты**.

         Kaspersky Security 10.1 для Windows Server проверяет все объекты.
       - **Объекты, проверяемые по формату**;

Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

  Kaspersky Security 10.1 для Windows Server проверяет только потенциально заражаемые объекты на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security 10.1 для Windows Server.

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

  Kaspersky Security 10.1 для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

Этот параметр вы также можете настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security 10.1 для Windows Server, то сетевое хранилище отсылает объект на проверку, а Kaspersky Security 10.1 для Windows Server признает объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отсылает объект на проверку. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленным Kaspersky Security 10.1 для Windows Server рекомендуется настраивать параметры, ограничивающие проверяемые объекты, в сетевом хранилище.

- В блоке **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security 10.1 для Windows Server.

- На закладке **Действия** выполните следующие действия:
  - В блоке **Действия над зараженными объектами** укажите, какое действие выполняет Kaspersky Security 10.1 для Windows Server при обнаружении зараженного объекта.
  - В блоке **Действия над возможно зараженными объектами** укажите, какое действие выполняет Kaspersky Security 10.1 для Windows Server при обнаружении возможно зараженного объекта.
- На закладке **Производительность** выполните следующие действия:
  - В блоке **Исключения** укажите, какие объекты Kaspersky Security 10.1 для Windows Server исключает из проверки одним из следующих способов:
    - Если вы хотите исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
    - Если вы хотите исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии (http://www.securelist.ru/).
  - В блоке **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.

6. В окне **Параметры безопасности** нажмите на кнопку **OK**.

Окно **Параметры безопасности** будет закрыто.

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

Настроенные параметры пользовательского уровня безопасности будут сохранены.

Просмотр статистики задачи Защита ICAP-подключаемых сетевых хранилищ

Если задача Защита ICAP-подключаемых сетевых хранилищ выполняется, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Security 10.1 для Windows Server обработал с момента запуска этой задачи по текущий момент, то есть статистику задачи.

► *Чтобы просмотреть статистику задачи Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.

На закладке **Обзор и управление** панели результатов в блоке **Статистика** отобразится таблица, содержащая информацию об объектах, которые Kaspersky Security 10.1 для Windows Server обработал с момента запуска задачи по текущий момент (см. таблицу ниже).

Таблица 8. Статистика задачи Защита RPC-подключаемых сетевых хранилищ

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Security 10.1 для Windows Server. Например, если Kaspersky Security 10.1 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 10.1 для Windows Server признал зараженными, или обнаруженное легальное программное обеспечение, которое не было исключено из области действия задач постоянной защиты или проверки.
Обнаружены возможно зараженные объекты	Количество объектов, которые Kaspersky Security 10.1 для Windows Server признал возможно зараженными.
Не вылечено объектов	Количество объектов, которые Kaspersky Security 10.1 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 10.1 для Windows Server попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Не удалено объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.

Поле	Описание
Не проверено объектов	Количество объектов в области защиты, которые Kaspersky Security 10.1 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 10.1 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 10.1 для Windows Server вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Security 10.1 для Windows Server поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Security 10.1 для Windows Server сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Security 10.1 для Windows Server пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые Kaspersky Security 10.1 для Windows Server пропустил, так как их формат искажен.
Обработано объектов	Количество рабочих процессов Kaspersky Security 10.1 для Windows Server в текущий момент

Защита от шифрования для NetApp

Этот раздел содержит информацию о задаче Защита от шифрования для NetApp и инструкции по настройке параметров этой задачи.

В этом разделе

О задаче Защита от шифрования для NetApp

Защита от шифрования для NetApp обеспечивает защиту от шифрования для папок в сетевых хранилищах данных. При обнаружении вредоносного шифрования Kaspersky Security для Windows Server 10.1 блокирует доступ к папкам общего доступа в защищаемом сетевого хранилище данных.

Чтобы осуществлять работу на сетевом хранилище, сервер с программой Kaspersky Security 10.1 для Windows Server должен быть присоединен к данному хранилищу в качестве *внешнего модуля*. Подключение подразумевает получение уведомлений о файловых операциях, выполняемых на защищаемом сетевом хранилище данных, анализ полученных шаблонов файловых операций, отправление заключений о файловой активности (можно ли ее оценить как попытку шифрования) и блокирование скомпрометированных компьютеров. Чтобы запустить задачу Защита от шифрования для NetApp, сервер (с установленным Kaspersky Security 10.1 для Windows Server) должен быть указан как основной сервер FPolicy на стороне сетевого хранилища. *FPolicy* – это система уведомления о доступе к файлам, которая нужна для отслеживания и управления событиями доступа к файлам в виртуальной системе хранения данных (Storage Virtual Machine, SVM) с томами FlexVol. Система создает уведомления, рассылаемые на внешние серверы FPolicy.

Компонент Защита от шифрования для NetApp нельзя настроить для защиты сетевых хранилищ данных с томами FlexGroup, так как FPolicy не поддерживает тома FlexGroup.

Уведомления от сетевого хранилища передаются на внешний сервер по протоколу FPolicy только в синхронном режиме. Сервер анализирует каждое уведомление, прежде чем разрешить файловую операцию.

Взаимосвязь между внешним модулем (сервером с программой Kaspersky Security 10.1 для Windows Server) и защищаемым сетевым хранилищем данных осуществляется по протоколу FPolicy. Чтобы установить защиту, выполните следующие действия:

1. Создайте и настройте FPolicy на стороне защищаемого сетевого хранилища данных.
2. Укажите сервер с программой Kaspersky Security для Windows Server 10.1 как сервер FPolicy на стороне защищаемого сетевого хранилища данных. Kaspersky Security 10.1 для Windows Server будет распознаваться как внешний сервер.

3. Настройте параметры компонента Защита от шифрования для NetApp на стороне Kaspersky Security 10.1 для Windows Server.

Чтобы выполнить необходимую настройку, вам потребуются следующие данные:

- Строковое имя машины SVM.
- IP-адрес и имя внешнего сервера.
- Полный список узлов кластеров защищаемых сетевых хранилищ данных с именами.
- Адрес интерфейса управления кластером.
- Имя созданного протокола FPolicy.
- Порт для создания соединения между защищаемым сетевым хранилищем данных и внешним сервером.
- Учетные данные (имя и пароль):
  - для пользователя, которому разрешен доступ к папкам в сетевом хранилище данных;
  - для локального администратора CDOT.

Все эти параметры потребуется указать во время создания FPolicy (см. раздел "Создание и настройка FPolicy" на стр. 64) и настройки задачи Защита от шифрования для NetApp в Kaspersky Security 10.1 для Windows Server (см. раздел "Настройка параметров задачи Защита от шифрования для NetApp" на стр. 70).

Подробные инструкции по созданию FPolicy см. в данной статье.

Создание и настройка FPolicy

При создании FPolicy впервые специалисты "Лаборатории Касперского" рекомендуют применять настройки, указанные в таблице ниже.

Таблица 9. Параметры FPolicy

Параметр	Строка	Значение	Примечание
_EVENT CREATE Этот параметр определяет файловые операции, которые будут перехватываться и о которых будут отправляться уведомления для анализа и обнаружения шифрования.	**Vserver**	<имя_svm>	Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования на стороне внешнего модуля (Kaspersky Security 10.1 для Windows Server).
	Событие	<источник_событий>	Будет использован как источник для FPolicy.
	Протокол	cifs	
	Операции с файлами	create, open, rename, write, close, setattr, delete	
	Фильтры	close-with-modification, first-write, write-with-size-change, open-with-delete-intent, open-with-write-intent	
	Требуются ли дисковые операции	false	
_ENGINE CREATE Этот параметр регулирует подключение к внешнему модулю (или серверу FPolicy).	**Vserver**	<имя_svm>	Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования для NetAppна стороне внешнего модуля.

Параметр	Строка	Значение	Примечание
	Модуль	<имя_модуля>	Строковое имя внешнего модуля. Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования для NetAppна стороне внешнего модуля.
	Основные серверы FPolicy	<ip-адрес_основного_сервера>	Можно указать только один сервер.
	Номер порта службы FPolicy	<номер_порта>	Рекомендуется указать значение 1346. Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.
	Вспомогательные серверы FPolicy	<ip-адрес_вспомогательного_сервера>	Если основной сервер выбран, использование вспомогательного сервера невозможно.
	Тип внешнего модуля	Синхронный	Асинхронный режим не поддерживается.
	Вариант SSL для внешнего соединения	No-auth	
	FQDN или CCN	-	
	Серийный номер сертификата	-	
	Центр сертификации	-	

Параметр	Строка	Значение	Примечание
_POLICY CREATE Этот параметр определяет будущую конфигурацию FPolicy.	**Vserver**	<имя_svm>	Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования на стороне внешнего модуля.
	Fpolicy	<имя_fpolicy>	Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования на стороне внешнего модуля.
	Отслеживаемые события	<источник_событий>	
	Модуль FPolicy	<имя_модуля>	Строковое имя внешнего модуля. Значение должно совпадать со значением, установленным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.
	Требуется ли обязательная проверка	true	
	Разрешить привилегированный доступ	yes	

Параметр	Строка	Значение	Примечание
	Имя пользователя для привилегированного доступа	<имя_пользователя>	То же значение должно быть указано в параметрах задачи Защита от шифрования для NetApp в поле Учетные данные для доступа к папкам общего доступа в сетевом хранилище данных.
	Включено ли транзитное чтение	false	
_SCOPE CREATE Этот параметр определяет область защиты для внешнего модуля.	**Vserver**	<имя_svm>	Рекомендуется указать максимально широкую область защиты на стороне сетевого хранилища данных. Рекомендуется добавить исключения в параметрах задачи Защита от шифрования для NetApp.
	Политика	<имя_fpolicy>	

Рекомендуется задать выделенные значения, указанные в таблице. Прочие значения могут варьироваться в зависимости от ваших требований.

Если параметры FPolicy были изменены на стороне сетевого хранилища данных во время работы задачи Защита от шифрования для NetApp, потребуется перезапустить задачу Защита от шифрования для NetApp, чтобы применить новые параметры.

Настройка Kaspersky Security 10.1 для Windows Server

Чтобы установить соединение между компонентом Защита от шифрования Kaspersky Security 10.1 для Windows Server и защищаемым сетевым хранилищем данных, необходимо настроить параметры задачи Защита от шифрования для NetApp (см. таблицу ниже).

Таблица 10. Настройки задачи Защита от шифрования

Параметр	Возможные значения	По умолчанию
Режим	• Только статистика • Активный.	Активный.
Эвристический анализатор	Поверхностный – Средний – Глубокий	Средний
Исключения	Применяется для всех защищаемых ресурсов общего доступа. Критерии исключений: • маска (папка, объект, расширение); • IP-адрес клиентского компьютера; • Доверенные пользователи	Не задана
Адресация	• IP-адрес кластера • Полный список кластеров • Учетные данные (имя и пароль) для локального администратора CDOT. Следующий параметр дублирует значение, установленное для параметра _POLICY CREATE (строка с именем пользователя для привилегированного доступа): Учетные данные (имя и пароль) для пользователя, которому разрешен доступ к папкам общего доступа в сетевом хранилище данных. Следующие параметры дублируют значения, установленные для параметра _ENGINE CREATE на стороне сетевого хранилища данных. • Имя FPolicy • Имя SVM (Vserver); • Порт (1346).	Не задана
Расписание задачи	-	Не задана

Использование Хранилища заблокированных узлов

Хранилище заблокированных узлов заполняется при выполнении следующих условий:

- Задача Защита от шифрования для NetApp запущена в **активном** режиме.
- Защита от шифрования для NetApp определяет попытки шифрования защищаемых ресурсов общего доступа NetApp.

После обнаружения попытки шифрования компонент Защита от шифрования отправляет информацию о скомпрометированном компьютере в **Хранилище заблокированных узлов**. После этого Kaspersky Security 10.1 для Windows Server создает критическое событие блокировки компьютера и блокирует любые файловые операции, выполняемые с этого компьютера.

По умолчанию Kaspersky Security 10.1 для Windows Server автоматически разблокирует компьютеры через 30 минут после их добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка недоверенных.

Список заблокированных узлов можно изменять следующими способами:

- разблокировать компьютеры вручную;
- настраивать длительность блокировки.

При настройке задачи Защита от шифрования обратите внимание на тип внешнего модуля, используемый в параметрах FPolicy (параметр _ENGINE CREATE).

Kaspersky Security 10.1 для Windows Server регистрирует событие с результатом полученного заключения и выполняет действия согласно режиму работы.

Kaspersky Security 10.1 для Windows Server поддерживает две конфигурации:

#	Режим работы СХД	Режим защиты от шифрования для NetApp	Описание
1	Синхронный	Только статистика	Эта конфигурация обеспечивает защиту от шифрования в режиме аудита: программа только регистрирует события шифрования. Вы можете переключиться на конфигурацию 2 из Kaspersky Security 10.1 для Windows Server.
2	Синхронный	Активный	Эта конфигурация обеспечивает полную защиту: программа добавляет все скомпрометированные компьютеры в Хранилище заблокированных узлов и блокирует все файловые операции, выполняемые с этих компьютеров. Вы можете переключиться на конфигурацию 1 на стороне защищаемого сетевого хранилища данных или на стороне внешнего сервера.

Подробнее о том, как настроить Хранилище заблокированных узлов, см. в Руководстве администратора или Руководстве пользователя Kaspersky Security 10.1 для Windows Server.

Настройка параметров задачи Защита от шифрования для NetApp

Настройте параметры внешнего сервера и сетевого хранилища данных, чтобы запустить и настроить задачу Защита от шифрования для NetApp.

Настройка параметров задачи через Консоль Kaspersky Security 10.1

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

1. В дереве Консоли Kaspersky Security 10.1 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. На закладке **Общие** настройте следующие параметры:
   - В блоке **Режим работы** выберите режим работы задачи.
   - В блоке **Эвристический анализатор** настройте использование эвристического анализатора и уровень эвристического анализа.
5. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. 72).
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
7. Нажмите на кнопку **ОК**.

► *Чтобы настроить список исключений для задачи Защита от шифрования для NetApp, выполните следующие действия:*

1. В дереве Консоли Kaspersky Security 10.1 разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита от шифрования для NetApp**.
3. Перейдите по ссылке **Список исключений** в панели результатов.

   Откроется окно **Список исключений**.
4. Настройте список исключений (см. раздел "Изменение списка исключений" на стр. 73).

Настройка параметров задачи через Kaspersky Security Center

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства политики, которую хотите изменить.

3. В разделе **Защита сетевых хранилищ** в блоке **Защита от шифрования для NetApp** нажмите на кнопку **Параметры**.
4. На закладке **Общие** настройте режим работы задачи и эвристический анализатор.
5. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. 72).
6. На закладке **Исключения** добавьте исключения из области защиты (см. раздел "Изменение списка исключений" на стр. 73).
7. На закладке **Управление задачей** запустите задачу на базе расписания.
8. Нажмите на кнопку **ОК**.

Настройка общих параметров задачи

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

1. На закладке **Общие** настройте следующие параметры:
   - Режим работы задачи:
     - **Только статистика.**

       Выберите этот вариант, чтобы получать уведомления об обнаруженных попытках шифрования файлов. Программа создает события в журнале выполнения задачи.

     - **Активный.**

       Выберите этот вариант, чтобы блокировать файловые операции, выполняемые в сетевом хранилище данных скомпрометированными компьютерами. При обнаружении попытки шифрования файлов программа добавляет компьютеры в Хранилище заблокированных узлов. Все файловые операции с этого компьютера будут заблокированы на период, указанный в параметрах хранилища.
   - Эвристический анализатор:
     - Снимите или установите флажок **Использовать эвристический анализатор**.

       Флажок включает или выключает использование эвристического анализатора при проверке объектов.

       Если флажок установлен, эвристический анализатор включен.

       Если флажок снят, эвристический анализатор выключен.

       По умолчанию флажок установлен.

     - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

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

       Существуют следующие уровни детализации проверки:

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

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

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

2. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. 72).
3. На закладке **Исключения** добавьте исключения из области защиты (см. раздел "Изменение списка исключений" на стр. 73).
4. На закладке **Управление задачей** запустите задачу на базе расписания.
5. Нажмите на кнопку **ОК**.

Настройка адресации

► *Чтобы настроить соединение с защищаемыми кластерами и получить доступ к сетевому хранилищу данных, выполните следующие действия:*

1. В параметрах задачи откройте закладку **Адресация**.
2. В блоке **Соединение** настройте следующие параметры:
   - **IP-адрес защищаемого кластера**

     Укажите IP-адрес кластера. Кластер содержит следующие типы серверов Vserver:

     - сервер администрирования Vserver;
     - узел Vserver;
     - кластер Vserver.
   - **Имя сервера Vserver**

     Укажите имя виртуального сервера хранения.
   - **Имя FPolicy**

     Введите имя FPolicy. Прежде чем FPolicy сможет проверять доступ к файлам, требуется создать конфигурацию FPolicy и включить ее на сервере Vserver, для которого нужны службы FPolicy.
   - **Порт**

3. Чтобы изменить список защищаемых узлов кластера, выполните следующие действия:
   a. В блоке **Соединение** нажмите на кнопку **Список узлов кластера**.
   b. Введите имя узла.
   c. Нажмите на кнопку **Добавить**.
   d. Нажмите на кнопку **ОК**.

   > Все существующие узлы защищаемого кластера требуется добавить в список.

4. В блоке **Аутентификация** введите следующие данные:
   - учетные данные пользователя с привилегированным доступом к папкам сетевого хранилища данных: имя и пароль.

     > Эта учетная запись должна совпадать с той, которую вы указали в параметре _POLICY CREATE на стороне сетевого хранилища данных.

   - учетные данные администратора CDOT: имя и пароль;
5. В окне **Защита от шифрования для NetApp** нажмите на кнопку **ОК**.

Настроенные параметры адресации будут сохранены.

Изменение списка исключений

Вы можете добавить исключения на основе следующих критериев:

- путь;
- IP-адрес;
- Имя пользователя.

Для исключений можно использовать любые сочетания этих критериев. Чем больше критериев вы укажете, тем строже будут параметры исключения. Kaspersky Security 10.1 для Windows Server не анализирует файловые операции для указанных исключений. Обратите внимание, что добавленные в этот список исключения используются для всех папок в сетевом хранилище данных.

> Если вы одновременно настраиваете антивирусную проверку (Vscan) и FPolicy на одном сетевом хранилище, доступ к общим сетевым папкам будет возможен только при запущенных задачах Защита RPC-подключаемого сетевого хранилища и Защита от шифрования для NetApp.

Внешний модуль должен иметь только одну сетевую плату с одним IP-адресом.

► *Чтобы добавить или изменить список исключений, выполните следующие действия:*

1. В параметрах задачи откройте закладку **Исключения**.
2. Установите флажок **Не обнаруживать шифрование для указанных исключений**.

   Если флажок установлен, разрешены все файловые операции, выполняемые указанным в списке ниже пользователем, с указанного IP-адреса или по указанному пути.

   Если флажок снят, Kaspersky Security 10.1 для Windows Server обнаруживает активность шифрования всех пользователей и компьютеров и со всех путей.

   По умолчанию флажок снят.

   Список исключений будет активирован.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры исключений**.
4. Чтобы добавить исключение на основе папки, выполните следующие действия:
   a. На закладке **Маски** установите флажок **Исключать по маске пути**.
   b. Нажмите на кнопку **Обзор**.
   c. Выберите папку, которую хотите исключить.
   d. Нажмите на кнопку **ОК**.

      Маска папки будет добавлена в поле.
   e. Нажмите на кнопку **Добавить**.
   f. Маска будет добавлена в список.
5. Чтобы добавить исключение на основе IP-адреса, выполните следующие действия:
   a. На закладке **IP-адрес** установите флажок **Исключать по IP-адресу клиента**.
   b. Введите IP-адрес.
   c. Нажмите на кнопку **Добавить**.
6. Чтобы добавить исключение на основе пользователей, выполните следующие действия:
   a. Установите флажок **Исключать по имени пользователя**.
   b. Нажмите на кнопку **Добавить**.

      Откроется окно **Выбор пользователей**.
   c. Выберите пользователей, которых вы хотите исключить.
   d. Нажмите на кнопку **ОК**.
7. В окне **Параметры исключений** нажмите на кнопку **ОК**.

   Список исключений заполняется указанными исключениями.

Управление задачами защиты сетевых хранилищ из Kaspersky Security Center

Этот раздел содержит информацию об управлении задачами защиты сетевых хранилищ с помощью Сервера администрирования Kaspersky Security Center, а также инструкции по настройке параметров задач для группы серверов и для одного сервера из Kaspersky Security Center.

В этом разделе

О защите сетевых хранилищ из Kaspersky Security Center

Вы можете управлять задачами защиты сетевых хранилищ из Kaspersky Security Center следующими способами:

- **Использование политик Kaspersky Security Center**. Вы можете настроить единые параметры защиты сетевых хранилищ и применить их в задачах выбранной группы серверов.
- **В окне Параметры программы**. Вы можете настроить параметры защиты сетевых хранилищ отдельно для каждого сервера, на котором установлен Kaspersky Security 10.1 для Windows Server.

Настройка параметров защиты сетевых хранилищ с помощью политик

По умолчанию задачи защиты сетевых хранилищ в политике Kaspersky Security Center имеют параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 11. Параметры задач защиты сетевых хранилищ в политике Kaspersky Security Center

Задача защиты сетевых хранилищ	Параметры
Защита RPC-подключаемых сетевых хранилищ	В разделе **Защита RPC-подключаемых сетевых хранилищ** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать предустановленный уровень безопасности или настроить параметры безопасности вручную; • настроить применение эвристического анализатора; • настроить применение доверенной зоны и использование KSN; • настроить параметры соединения с сетевым хранилищем; • Настройте параметры запуска задачи.

Задача защиты сетевых хранилищ	Параметры
Защита ICAP-подключаемых сетевых хранилищ	В разделе **Защита ICAP-подключаемых сетевых хранилищ** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • настроить применение эвристического анализатора; • настроить параметры соединения с сетевым хранилищем; • задать уровень безопасности для выбранной области защиты: вы можете выбрать предустановленный уровень безопасности или настроить параметры безопасности вручную; • Настройка задачи Использование KSN • Настройте параметры запуска задачи.
Защита от шифрования для NetApp	В разделе **Защита от шифрования для NetApp**, по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи: • Режим работы задачи. • Использование эвристического анализатора. • Настройки соединения и аутентификации. • Укажите исключения из области защиты.

► *Чтобы настроить параметры задач защиты сетевых хранилищ в политике Kaspersky Security Center, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните группу администрирования, параметры политики которой вы хотите настроить, затем выберите в панели результатов закладку **Политики**.
2. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства** и в открывшемся окне в списке разделов выберите **Защита сетевых хранилищ**.
3. В открывшемся окне выполните следующие действия:
   - Если вы хотите настроить параметры задачи Защита RPC-подключаемых сетевых хранилищ, в блоке **Защита RPC-подключаемых сетевых хранилищ** нажмите на кнопку **Настройка**.

     В открывшемся окне **Параметры** настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.
   - Если вы хотите настроить параметры задачи Защита ICAP-подключаемых сетевых хранилищ, в блоке **Защита ICAP-подключаемых сетевых хранилищ** нажмите на кнопку **Настройка**.

     В открывшемся окне **Параметры** настройте параметры задачи в соответствии с вашими требованиями (см. раздел «Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ» на стр. 52). Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.
   - Если вы хотите настроить параметры задачи Защита от шифрования для NetApp, в блоке **Защита от шифрования для NetApp** нажмите на кнопку **Настройка**.

     В открывшемся окне **Параметры** настройте параметры задачи в соответствии с вашими требованиями (см. раздел «Настройка параметров задачи Защита от шифрования для NetApp» на стр. 70). Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.
4. В окне **Свойства: <Имя политики>** нажмите на кнопку **ОК**.

Настроенные параметры задач защиты сетевых хранилищ будут сохранены и применены в активной политике.

Подробная информация о работе Kaspersky Security 10.1 для Windows Server с политиками Kaspersky Security Center, а также информация о политиках Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center* и *Руководстве администратора Kaspersky Security 10.1 для Windows Server*.

Настройка параметров защиты сетевых хранилищ для одного сервера в Kaspersky Security Center

► *Чтобы настроить параметры защиты сетевых хранилищ для одного сервера из Kaspersky Security Center, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом сервере и выберите пункт **Свойства**.
3. В окне **Свойства: Свойства: <Имя компьютера>** в разделе **Задачи** откройте контекстное меню названия задачи защиты сетевых хранилищ, которую вы хотите настроить, и выберите пункт **Свойства**.
4. В открывшемся окне настройте параметры задачи защиты сетевых хранилищ в соответствии с вашими требованиями:
   - Защита RPC-подключаемых сетевых хранилищ (см. раздел «Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ» на стр. 35).
   - Задача Защита ICAP-подключаемых сетевых хранилищ.
5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены и применены в выполняющейся задаче для одного сервера.

Если к программе применяется политика Kaspersky Security Center и в этой политике наложен запрет на изменение параметров задачи, эти параметры недоступны для изменения через окно **Свойства:. <Имя компьютера>**.

Подробная информация о работе Kaspersky Security 10.1 для Windows Server с политиками Kaspersky Security Center, а также информация о политиках Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center* и *Руководстве администратора Kaspersky Security 10.1 для Windows Server*.

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.com/faq/companyaccount_help.).

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Security 10.1 для Windows Server и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять компьютер на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки компьютера.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Глоссарий

А

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

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.

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.

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.

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.

О

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

П

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.

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.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы “Лаборатории Касперского». Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, “Лаборатория Касперского” – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (“IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня “Лаборатория Касперского” – это международная группа компаний с 38 офисами в 33 стране мира. В компании работает более 3 000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, “Лаборатория Касперского” стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей, а количество организаций, являющихся ее клиентами, превышает 270 000.

Веб-сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru
Вирусная лаборатория:	http://newvirus.kaspersky.ru (для проверки подозрительных файлов и веб-сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.ru

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Citrix, XenApp и XenDesktop – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Celerra, EMC, Isilon, OneFS и VNX – товарные знаки или зарегистрированные в США и/или других странах товарные знаки EMC Corporation.

Dell, Dell Compellent - товарные знаки Dell, Inc.

Hitachi - товарный знак Hitachi, Ltd.

IBM, Lotus Notes, Domino и System Storage – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Excel, Hyper-V, Microsoft, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Data ONTAP и NetApp – товарные знаки или зарегистрированные в США и/или других странах товарные знаки NetApp, Inc.

Предметный указатель

Г

И

К

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 12. 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 13. 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 10.1 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 10.1 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.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
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.
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.