kaspersky

Программное изделие «Kaspersky Web Traffic Security 6.1»

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.1

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 20.05.2020

Обозначение документа:
643.46856491.00047-05 90 01

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

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Web Traffic Security" (далее также "Kaspersky Web Traffic Security", "программа").

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Web Traffic Security, а также поддержка организаций, использующих Kaspersky Web Traffic Security.

kaspersky

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Web Traffic Security:

- страница Kaspersky Web Traffic Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Web Traffic Security на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 199).

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

Страница Kaspersky Web Traffic Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Web Traffic Security (https://www.kaspersky.com/small-to-medium-business-security/proxy-web-traffic) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

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

Страница Kaspersky Web Traffic Security в Базе знаний

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

На странице Kaspersky Web Traffic Security в Базе знаний (https://support.kaspersky.com/kwts6) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Электронная справка Kaspersky Web Traffic Security (справка веб-интерфейса)

С помощью веб-интерфейса вы можете управлять Kaspersky Web Traffic Security через браузер. Справка содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя через веб-интерфейс Kaspersky Web Traffic Security (далее также

"веб-интерфейс").

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 в нашем сообществе (https://community.kaspersky.com).

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

Kaspersky Web Traffic Security

Программное изделие Kaspersky Web Traffic Security представляет собой средство антивирусной защиты типа "Б" второго класса защиты и предназначено для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Web Traffic Security, 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;
- фильтрация сообщений протокола ICAP;
- идентификация и аутентификация.

В этом разделе

О действиях программы над объектами

В зависимости от статуса, присвоенного объекту по результатам антивирусной проверки, проверки на фишинг и контентной фильтрации, программа Kaspersky Web Traffic Security выполняет действия над объектами. Результат проверки программа записывает в журнал событий.

В параметрах правила вы можете указать действия, которые программа выполняет над объектами с определенным статусом.

Для параметров, определяющих действия, вы можете задать следующие значения:

- Для правил доступа:
  - **Заблокировать**, если вы хотите добавить правило запрета доступа.
  - **Разрешить**, если вы хотите добавить правило разрешения доступа.
  - **К следующей группе**, если вы хотите добавить переход к следующей группе правил.
  - **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.
- Для правил защиты:
  a. **Вредоносная программа**:
     - **Заблокировать**.
     - **Заблокировать, по возможности вылечить**.
     - **Пропустить проверку**.

     По умолчанию установлено значение **Заблокировать, по возможности вылечить**.
  b. **Объекты, обнаруженные KATA**, **Фишинг**, **Вредоносная ссылка**, **Зашифрованный объект** и **Документ с макросом**:
     - **Заблокировать**.
     - **Пропустить проверку**.

     По умолчанию установлено значение **Заблокировать**.

О задачах программы

Задачи Kaspersky Web Traffic Security реализуют часть функциональности программы. Например, задача обновления антивирусных баз UpdaterAVS выполняет загрузку и установку обновлений антивирусных баз.

В состав Kaspersky Web Traffic Security входят следующие задачи:

- Auth (ID=1).
- Facade (ID=4).
- EventManager (ID=7).
- Licenser (ID=8).
- Notifier (ID=9).
- Statistics (ID=10).
- Updater (ID=11).
- SmtpSender (ID=15).
- Snmp (ID=16).
- DailyReport (ID=17).
- WeeklyReport (ID=18).
- MonthlyReport (ID=19).

- EventLogger (ID=20).
- ScanServer (ID=21).
- Ksn (ID=23).
- ICAPServer (ID=24).
- LdapCache (ID=26).

Большинство задач являются системными и не предназначены для настройки администратором.

Задачи Kaspersky Web Traffic Security могут находиться в одном из следующих статусов выполнения:

- *Started* – выполняется.
- *Starting* – запускается.
- *Stopped* – остановлена.
- *Failed* – завершена с ошибкой.

Основные компоненты программы

В состав Kaspersky Web Traffic Security входят следующие компоненты:

- *Подчиненный узел*.

  Выполняет проверку интернет-ресурсов согласно правилам обработки трафика, полученным от Управляющего узла.

- *Управляющий узел*.

  Позволяет администратору управлять параметрами программы через веб-интерфейс. Установленные значения параметров передаются на Подчиненные узлы.

kaspersky

Принцип работы программы

Kaspersky Web Traffic Security проверяет HTTP-, HTTPS- и FTP-трафик пользователей, проходящий через прокси-сервер.

На всех серверах устанавливается одинаковый пакет Kaspersky Web Traffic Security, включающий как функциональность для обработки трафика, так и возможность управлять параметрами программы. После установки все серверы объединяются в *кластер*.

В кластере необходимо назначить одному из серверов роль *Управляющий узел*. Остальные серверы получат роль *Подчиненный узел*. Вы можете настроить на всех узлах, в том числе и на Управляющем узле, обработку трафика. Отличие Управляющего узла от Подчиненных узлов состоит в том, что на Управляющем узле вы можете изменять параметры программы. С Управляющего узла они распространяются на все Подчиненные узлы в кластере.

Работа программы без балансировщика нагрузки

Если вы не используете балансировщик нагрузки, то вы можете направить весь трафик с прокси-сервера только на один узел кластера. Однако для обеспечения отказоустойчивости программы рекомендуется добавить в кластер хотя бы два узла – Управляющий узел и Подчиненный узел.

Обработка трафика осуществляется по следующему алгоритму:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на прокси-сервер.
2. Прокси-сервер передает запрос на узел кластера, обрабатывающий трафик.
3. Программа проверяет запрос по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 75), полученным от Управляющего узла. После этого результат проверки передается прокси-серверу.
4. Если доступ к веб-ресурсу разрешен, то прокси-сервер отправляет запрос на веб-сервер для доступа к запрашиваемому веб-ресурсу.
5. Прокси-сервер получает ответ от веб-сервера, на котором располагается запрашиваемый веб-ресурс.
6. Ответ также отправляется на узел кластера для проверки по правилам обработки трафика.
7. Узел кластера отправляет ответ на прокси-сервер.
8. Прокси-сервер передает ответ пользователю. В зависимости от заданных в программе действий пользователю могут отобразиться следующие страницы:
   - Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
   - Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. 140).
   - Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

Работа программы с балансировщиками нагрузки

При наличии большого количества прокси-серверов и серверов с установленной программой рекомендуется использовать балансировщики нагрузки HAProxy (см. раздел "Приложение 3. Настройка балансировки ICAP с помощью HAProxy" на стр. 224). В этом случае HAProxy определяет, какому серверу направить запрос на проверку, в соответствии с заданным способом балансировки.

Обработка трафика осуществляется по следующему алгоритму:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на первый балансировщик нагрузки.
2. Первый балансировщик нагрузки выбирает один из прокси-серверов согласно заданному способу балансировки и передает этому прокси-серверу запрос пользователя.
3. Прокси-сервер направляет запрос на второй балансировщик нагрузки.
4. Второй балансировщик нагрузки выбирает один из узлов кластера согласно заданному способу балансировки и передает этому узлу запрос.
5. Программа проверяет запрос по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 75), полученным от Управляющего узла. После этого результат проверки возвращается второму балансировщику нагрузки.
6. Второй балансировщик нагрузки передает результат проверки тому же прокси-серверу, от которого был получен запрос.
7. Если доступ к веб-ресурсу разрешен, то прокси-сервер отправляет запрос на веб-сервер в интернет.
8. Прокси-сервер получает ответ от веб-сервера, на котором располагается запрашиваемый веб-ресурс.
9. Ответ отправляется на второй балансировщик нагрузки.
10. Второй балансировщик нагрузки выбирает один из узлов кластера согласно заданному способу балансировки и передает этому узлу ответ веб-сервера для проверки по правилам обработки трафика.
11. Программа отправляет ответ второму балансировщику нагрузки.
12. Балансировщик нагрузки возвращает результат проверки тому же прокси-серверу, от которого был получен ответ веб-сервера.
13. Прокси-сервер передает ответ первому балансировщику нагрузки.
14. Первый балансировщик нагрузки направляет ответ пользователю. В зависимости от заданных в программе действий пользователю могут отобразиться следующие страницы:
    - Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
    - Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. 140).
    - Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

Вы можете использовать один и тот же балансировщик нагрузки для балансировки различных сервисов.

Рекомендуется дополнительно настроить обработку HTTPS-трафика (см. раздел "Настройка SSL Bumping в сервисе Squid" на стр. 205) на внешнем прокси-сервере.

kaspersky

Об информационных X-заголовках

По результатам проверки запроса пользователя программа добавляет к заголовку запроса специальные информационные X-заголовки:

- **Заголовок, содержащий IP-адрес клиента** – заголовок, который прокси-сервер использует для передачи IP-адреса пользователя прокси-сервера.

  По умолчанию установлено значение `X-Client-IP`.

  Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, программа не сможет корректно определять пользователей при проверке правил обработки трафика.

- **Заголовок, содержащий имя пользователя** – заголовок, который прокси-сервер использует для передачи имени пользователя прокси-сервера.

  По умолчанию установлено значение `X-Client-Username`.

  Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, программа не сможет корректно определять пользователей при проверке правил обработки трафика.

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Аппаратные требования к серверам для установки Kaspersky Web Traffic Security

- 8 ядер процессора;
- 16 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 200 ГБ на жестком диске, из которых:
  - 25 ГБ для хранения временных файлов;
  - 25 ГБ для хранения файлов журналов.

Аппаратные требования к серверу с гипервизором для развертывания ISO-образа виртуальной машины

При наличии на сервере менее 1 ГБ оперативной памяти или менее 100 ГБ дискового пространства установка прерывается.

- 8 ядер процессора;
- 16 ГБ оперативной памяти;
- 200 ГБ дискового пространства.

Программные требования к серверам для установки Kaspersky Web Traffic Security

Программа Kaspersky Web Traffic Security может быть установлена только на 64-битные операционные системы.

- Red Hat Enterprise Linux® 7.7, 8.
- Ubuntu 18.04.3 LTS.
- Debian 9.11, 10.1.

- SUSE Linux® Enterprise Server 15 SP1.
- CentOS 7.7.
- Astra Linux Special Edition 1.6.
- ALT Linux 8.

Программные требования к компьютерам локальной сети организации

- Windows® 8.1.
- Windows 10 (1809, 1903).

Программные требования к гипервизору для развертывания виртуальной машины

- VMware ESXi™ 6.5 Update 2 / 6.7 Update 1.
- Microsoft® Hyper-V® Server 2016 / 2019.

Программные требования для настройки интеграции с LDAP-сервером

- Windows Server® 2012 R2 Standard.
- Windows Server 2016 Standard.
- Windows Server 2019 Standard.

Дополнительные требования

- Nginx версий 1.10.3, 1.12.2 и 1.14.0.
- HAProxy версии 1.5 для балансировки нагрузки (не входит в комплект поставки).
- Squid версии 3.5.28, 4.6, 4.7, 4.8, если вы устанавливаете сервис Squid и программу Kaspersky Web Traffic Security на одном сервере.

  Для обработки трафика вашей сети программой Kaspersky Web Traffic Security необходимо, чтобы в вашей сети был установлен и настроен прокси-сервер HTTP(S) с поддержкой ICAP-протокола и служб Request Modification (REQMOD) и Response Modification (RESPMOD). Вы можете использовать отдельный прокси-сервер или, например, установить сервис Squid на сервер с программой Kaspersky Web Traffic Security.

Программные требования для работы с Kaspersky Web Traffic Security через веб-интерфейс

Для работы веб-интерфейса на компьютере должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ версии 69, 70.
- Internet Explorer® версии 11.
- Google Chrome™ версии 77, 78.
- Microsoft Edge версии 44 (для Windows 1809 и 1903 – Microsoft Edge 44.17763.1.0 и 44.18362.1.0 соответственно).

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с

эксплуатационной документацией.

2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

kaspersky

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Web Traffic Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

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

Предусмотрены следующие типы лицензий:

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

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

  Вы можете активировать программу по пробной лицензии только один раз.

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

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Web Traffic Security). Чтобы продолжить использование Kaspersky Web Traffic Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Для добавления ключа в программу необходимо ввести *код активации*.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Web Traffic Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Web Traffic Security или после заказа пробной версии Kaspersky Web Traffic Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 199).

О предоставлении данных

Для работы программы используются данные, на отправку и обработку которых требуется согласие администратора Kaspersky Web Traffic Security.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении.

  Согласно условиям принятого Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, которая требуется для повышения уровня защиты IT-инфраструктуры организации. Эта информация перечислена в Лицензионном соглашении в пункте Условия обработки данных:

  - идентификатор программы;
  - номер версии программы;
  - уникальный идентификатор установки программы;
  - идентификатор лицензии;
  - идентификатор сессии обновления;
  - уникальный идентификатор материнской платы.
- В Политике конфиденциальности.
- В Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network.

  При участии в Kaspersky Security Network и при отправке KSN-статистики в "Лабораторию Касперского" может передаваться информация, полученная в результате работы программы. Перечень передаваемых данных указан в Положении о Kaspersky Security Network и в

Дополнительном Положении о Kaspersky Security Network:

- IP-адрес компьютера пользователя.
- Информация о программе и компьютере: уникальный идентификатор компьютера, на котором установлена программа; уникальный идентификатор установки программы; полная версия установленной программы; идентификатор типа программы; тип, версия, редакция, разрядность и параметры режима работы операционной системы; информация об установленных пакетах обновлений.
- Информация о проверке URL-адресов модулями Антивирус и Анти-Фишинг: URL-адрес веб-ресурса, в котором обнаружена угроза; URL-адрес исходной страницы или страницы, с которой пользователь был перенаправлен на данный URL-адрес; дата и время выпуска баз программы; название организации и веб-ресурса, на которые была произведена атака; результат проверки (уровень доверия, вес и статус решения); время события.
- Информация о проверяемых файлах: имя, размер, MD5- или SHA256-хеш проверяемого файла; идентификаторы типа и формата файла; название обнаруженной угрозы согласно классификации "Лаборатории Касперского"; идентификаторы антивирусных баз и записи в антивирусных базах, которые использовались для проверки файла; дата и время выпуска антивирусных баз; URL-адрес, с которого был загружен проверяемый файл; имя файла процесса, выполнившего загрузку проверяемого объекта, сообщения или ссылки; отпечаток сертификата и SHA256-хеш открытого ключа сертификата для подписанных файлов.
- Информация об ошибках в работе программы: идентификатор компонента программы, в работе которого произошла ошибка; идентификатор типа ошибки; фрагменты отчетов о работе компонентов.
- Информация об обновлении баз и компонентов программы: версия компонента, для которого выполняется обновление баз; код ошибки обновления баз при ее возникновении; статус программы после обновления баз; количество неудачных попыток обновления баз; количество аварийных остановок компонента, для которого выполнялось обновление.
- Информация о работе компонента Updater: версия компонента Updater; результат выполнения обновления для компонента Updater; тип и идентификатор ошибки при обновлении компонента Updater при ее возникновении; код завершения задачи обновления для компонента Updater; количество аварийных остановок компонента Updater при выполнении задач обновления; количество неудачных попыток обновления компонента Updater.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Оперативная память Kaspersky Web Traffic Security может содержать любые обрабатываемые данные пользователей программы. Администратору Kaspersky Web Traffic Security необходимо обеспечить безопасность этих данных самостоятельно.

По умолчанию доступ к персональным данным пользователей имеют только учетная запись суперпользователя операционных систем root, учетная запись администратора Kaspersky Web Traffic Security Локальный администратор, а также системная учетная запись kluser, от имени которой работают компоненты программы. Возможность ограничить права администраторов и других пользователей

операционных систем, на которые установлена программа, средствами самой программы не предусмотрена. Администратору рекомендуется контролировать доступ к персональным данным других пользователей любыми системными средствами на его усмотрение.

Для ознакомления с полным перечнем данных пользователей, которые могут храниться в Kaspersky Web Traffic Security, см. таблицу ниже.

Таблица 1. Данные пользователей, которые могут храниться в Kaspersky Web Traffic Security

Тип данных	Где используются данные	Место хранения	Срок хранения
Основная функциональность программы			
• Имена учетных записей администратора и пользователей программы. • Права доступа учетных записей программы. • Хеш пароля Локального администратора. • IP-адреса пользователей. • Имя учетной записи и пароль подключения программы к прокси-серверу. • Keytab-файлы для подключения к LDAP-серверу. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.	Конфигурация программы	/var/opt/kaspersky	Бессрочно.
• Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. • IP-адреса пользователей. • Комментарии.	Правила обработки трафика	/var/opt/kaspersky	Бессрочно.

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация из запросов доступа к веб-ресурсам: • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ.	Статистика работы программы	/var/opt/kaspersky	Бессрочно.
Информация из запросов доступа к веб-ресурсам: • IP-адреса и User Agent пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. Информация о LDAP-атрибутах пользователей: • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.	Журнал событий обработки трафика	• /var/opt/kaspersky • журнал событий Syslog (настраивается администратором)	Согласно параметрам, заданным пользователем программы. По умолчанию устанавливается срок хранения 3 дня или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.

Тип данных	Где используются данные	Место хранения	Срок хранения
• Имя учетной записи пользователя, инициировавшего событие. • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания.	Журнал системных событий	• /var/opt/kaspersky • журнал событий Syslog (настраивается администратором)	Согласно параметрам, заданным пользователем программы. По умолчанию хранится 100 тысяч записей. При достижении этого ограничения более старые записи удаляются.
Информация из запросов доступа к веб-ресурсам: • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса	Файлы трассировки	/var/log/kaspersky	Бессрочно. При достижении объема 150 МБ для каждого потока трассировки более старые записи удаляются.

Тип данных	Где используются данные	Место хранения	Срок хранения
веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. Данные об обновлениях программы: • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. Информация об учетных записях пользователей: • Имена учетных записей пользователей, осуществивших вход в программу через веб-интерфейс. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.		/var/log/kaspersky/extra	Бессрочно. При достижении объема 400 МБ для каждого потока трассировки более старые записи удаляются.

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация из запросов доступа к веб-ресурсам: • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Тела HTTP-сообщений, содержащих cookies и скачиваемые файлы.	Временные файлы	/tmp/kwtstmp	До перезагрузки программы.
Интеграция с программой Kaspersky Anti Targeted Attack Platform (KATA)			
Файлы пользователей	Отправка файлов на сервер KATA	/tmp/kwtstmp	До перезагрузки программы. Максимально допустимый размер очереди составляет 5 тысяч файлов. При достижении этого ограничения файлы перестают помещаться в очередь.

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация из обнаружений KATA: • MD5- или SHA256-хеш файла. • URL-адреса.	Получение объектов, обнаруженных программой KATA	/var/opt/kaspersky/kwts/detects.cache	Согласно параметру **Срок хранения кеша (часы)**, заданному пользователем программы. По умолчанию установлено значение 48 часов.
Интеграция с Active Directory®			
• DN пользователя. • CN пользователя. • sAMAccountName. • UPN-суффикс. • objectSID.	• Правила обработки трафика. • Аутентификация с помощью технологии единого входа. • Автозаполнение учетных записей при работе с ролями и правами пользователей, а также при настройке правил обработки трафика.	/var/opt/kaspersky/kwts/ldap/cache.dbm	Бессрочно. Данные регулярно обновляются. При отключении интеграции программы с Active Directory данные удаляются.
Использование Kaspersky Security Network (KSN)			

Тип данных	Где используются данные	Место хранения	Срок хранения
• MD5- или SHA256-хеш проверяемого файла. • Идентификаторы типа и формата проверяемого файла. • Название обнаруженной угрозы согласно классификации "Лаборатории Касперского". • Идентификаторы антивирусных баз и записи в антивирусных базах, которые использовались для проверки файла. • Дата и время выпуска антивирусных баз. • URL-адрес, с которого был загружен проверяемый файл. • Имя файла процесса, выполнившего загрузку проверяемого объекта, сообщения или ссылки. • Нормализованные URL-адреса запрашиваемых веб-ресурсов, содержащие тип протокола и номер порта. • Отпечаток сертификата и SHA256-хеш открытого ключа сертификата для подписанных файлов.	Отправка KSN-запросов	/var/opt/kaspersky	Бессрочно. Максимальное количество хранимых записей составляет 360 тысяч. При достижении этого ограничения удаляются записи, к которым дольше всего не было обращений.

Тип данных	Где используются данные	Место хранения	Срок хранения
• IP-адрес пользователя. Информация о программе и компьютере: • Уникальный идентификатор компьютера, на котором установлена программа. • Уникальный идентификатор установки программы. • Полная версия установленной программы. • Идентификатор типа программы. • Тип, версия, редакция, разрядность и параметры режима работы операционной системы. • Информация об установленных пакетах обновлений. Информация о проверке URL-адресов модулями Антивирус и Анти-Фишинг: • URL-адрес веб-ресурса, в котором обнаружена угроза. • URL-адрес исходной страницы или страницы, с которой пользователь был перенаправлен на данный URL-адрес. • Дата и время выпуска баз программы. • Название организации и	KSN-статистика	/var/opt/kaspersky	До отправки статистики в KSN. После отключения отправки KSN-статистики в параметрах программы данные удаляются при следующей попытке отправки.

Тип данных	Где используются данные	Место хранения	Срок хранения
Функциональность, доступная только при развертывании программы из ISO-файла			
Расшифровка TLS/SSL-соединений: • Сертификаты для перехвата SSL-соединений. • Поля Common name и Organization из CSR-запроса. • SHA1- или SHA256-отпечатки доверенных сертификатов. • Файлы приватных ключей сертификатов[1]. Параметры Kerberos-аутентификации: • Keytab-файлы. • Токены (хеш-строки) пользователей. • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей. Параметры NTLM-аутентификации: • Адрес сервера Active Directory. • Сертификат сервера Active Directory.	Параметры встроенного прокси-сервера	/etc/squid/ /var/opt/kaspersky/	Бессрочно. Данные удаляются при удалении соответствующих параметров в веб-интерфейсе программы. Файлы сертификатов могут быть перезаписаны при замене сертификата.

[1] Доступ к файлам возможен только по протоколу SSH после загрузки открытого ключа SSH через веб-интерфейс программы.

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация из запросов доступа к веб-ресурсам: • URL-адреса веб-ресурсов, к которым запрашивается доступ. • IP-адреса и DNS-имена веб-серверов. • IP-адреса доверенных балансировщиков нагрузки. • IP-адрес ICAP-сервера. • IP-адреса пользователей. • HTTP-заголовки обрабатываемых HTTP-сообщений.	Журнал событий прокси-сервера	/var/log/squid/icap.log /var/log/squid/ssl.log /var/log/squid/squid.out /var/log/squid/access.log /var/log/squid/cache.log	Бессрочно. При достижении объема 3 ГБ для каждого потока трассировки более старые записи удаляются.
Параметры Kerberos-аутентификации: • Keytab-файлы. • Токены (хеш-строки) пользователей. • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей.	Журнал событий прокси-сервера	/var/log/squid/cache.log	Бессрочно. При достижении объема 10 ГБ для каждого потока трассировки более старые записи удаляются.

Тип данных	Где используются данные	Место хранения	Срок хранения
Параметры NTLM-аутентификации: • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей. • Тела NTLM-сообщений в кодировке Base-64. • Кодированные LDAP-сообщения.	Журнал событий прокси-сервера	/var/log/squid/cache.log	Бессрочно. При достижении объема 10 ГБ для каждого потока трассировки более старые записи удаляются.
Подключение по протоколу SSH: • IP-адрес пользователя. • Имя учетной записи пользователя. • Отпечаток ключа SSH. Подключение через веб-интерфейс: • IP-адрес пользователя. • Имя учетной записи пользователя.	Журнал событий авторизации	/var/log/secure	Не более 5 недель. Выполняется еженедельная ротация файлов.

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация из запросов доступа к веб-ресурсам: • IP-адреса и User Agent пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. Информация о LDAP-атрибутах пользователей: • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. Информация о системных событиях: • Имя учетной записи пользователя, инициировавшего событие. • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания.	Журнал системных событий и событий обработки трафика	/var/log/kwts-messages	Не более 5 недель. Выполняется еженедельная ротация файлов.

Работа с программой из консоли управления сервера, на котором установлена программа, под учетной записью суперпользователя позволяет управлять параметрами дампа. Дамп формируется при сбоях программы и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные,

включая фрагменты анализируемых файлов.

По умолчанию формирование дампа в Kaspersky Web Traffic Security отключено.

Доступ к этим данным может быть осуществлен из консоли управления сервера, на котором установлена программа, под учетной записью суперпользователя.

При передаче диагностической информации в Службу технической поддержки "Лаборатории Касперского" администратору Kaspersky Web Traffic Security необходимо обеспечить безопасность дампов и файлов трассировки самостоятельно.

Администратор Kaspersky Web Traffic Security несет ответственность за доступ к данной информации.

Просмотр информации о лицензии и активации программы

► *Чтобы просмотреть информацию о лицензии, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В блоке **Лицензия** перейдите по ссылке **Подробные сведения**.

   Откроется окно **Лицензия**.

В окне отображается информация о лицензиях на серверах с установленной программой.

► *Чтобы просмотреть информацию об активации программы,*

в окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Лицензирование**.

В окне отображается информация об активации программы или поле для ввода кода активации, если программа не была активирована.

Активация программы

Для активации программы необходимо добавить лицензионный ключ, активирующий Kaspersky Web Traffic Security. Для добавления лицензионного ключа необходимо ввести код активации.

► *Чтобы ввести код активации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. В поле **Ввести код активации** введите код активации программы в формате XXXXX-XXXXX-XXXXX-XXXXX, где X может быть буквами латинского алфавита (A-Z, кроме O и I (прописная i)) или цифрами (0-9).
3. Нажмите на кнопку **Активировать**.

Код активации будет отправлен на серверы активации "Лаборатории Касперского" для проверки.

Если введенный код неверен, отобразится сообщение о вводе ошибочного кода. Вы можете повторить попытку ввода кода активации.

Если введенный код верен, отобразится статус **Код активации успешно применен. Проверьте состояние активации программы на узлах кластера**.

Удаление лицензионного ключа

► *Чтобы удалить лицензионный ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. Нажмите на кнопку **Удалить**.

   Отобразится подтверждение удаления лицензионного ключа.
3. Нажмите на кнопку **Да**.

Лицензионный ключ будет удален.

kaspersky

Установка и первоначальная настройка программы из rpm- или deb-пакета

Rpm- и deb-пакеты предназначены для установки программы в операционной системе на физическом или виртуальном сервере. Вам требуется провести установку и первоначальную настройку программы на каждом сервере, на котором вы хотите обрабатывать сетевой трафик.

Сценарий установки и первоначальной настройки программы из rpm- или deb-пакета состоит из следующих этапов:

1. Отключение SELinux
2. Установка сервиса nginx
3. Настройка портов для работы программы (на стр. 43)
4. Установка пакета программы
5. Установка пакета локализации
6. Настройка программы с помощью скрипта настройки (см. раздел "Настройка программы вручную" на стр. 49)
7. Установка сервиса Squid, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid
8. Настройка сервиса Squid, если вы установили сервис Squid
9. Настройка SSL Bumping в сервисе Squid, если вы установили сервис Squid

После первоначальной настройки программы вам нужно объединить все узлы в кластер для управления программой через веб-интерфейс (см. раздел "Управление кластером" на стр. 121).

В этом разделе

kaspersky

Подготовка к установке программы

Серверы, предназначенные для установки программы, должны удовлетворять аппаратным и программным требованиям.

Учетная запись должна обладать правами суперпользователя.

Подготовка программы к установке включает в себя следующие этапы.

1. Отключение SELinux (на стр. 40)

   Применимо для операционных систем CentOS и Red Hat Enterprise Linux.
2. Установка сервиса nginx (на стр. 41)
3. Настройка портов для работы программы (на стр. 43)

   Применимо, если на сервере с установленной программой включен брандмауэр.
4. Установка пакета insserv-compat

   Если вы используете операционную систему SUSE Linux Enterprise Server 15, требуется установить пакет insserv-compat с помощью команды `zypper install insserv-compat`.

   Проверить наличие установленного пакета можно с помощью команды `rpm -q insserv-compat`.

В этом разделе

Отключение SELinux

Для работы Kaspersky Web Traffic Security на операционных системах CentOS или Red Hat Enterprise Linux необходимо отключить SELinux.

► *Чтобы отключить SELinux, выполните следующие действия:*

1. Проверьте параметры запуска SELinux при загрузке системы. Для этого выполните команду:

   `cat /etc/selinux/config`
2. Если параметр `SELINUX` имеет значение `enforcing`, отключите запуск SELinux при загрузке системы. Для этого в файле /etc/selinux/config укажите `SELINUX=disabled` вместо

`SELINUX=enforcing`.

3. Проверьте текущее состояние SELinux. Для этого выполните команду:

   ```
   sestatus
   ```

4. Если параметр `SELinux status` имеет значение `enabled`, отключите SELinux. Для этого выполните команду:

   ```
   setenforce 0
   ```

SELinux будет отключен.

Установка сервиса nginx

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Web Traffic Security не обеспечивает шифрование ICAP-трафика и аутентификацию пользователей на вашем прокси-сервере. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Web Traffic Security с помощью туннелирования трафика или средствами iptables.

► *Чтобы установить сервис nginx, выполните следующие действия:*

1. Если в используемой операционной системе предустановлен сервис Apache, отключите его.
2. Если для доступа в интернет сервера, предназначенного для установки Kaspersky Web Traffic Security, используется прокси-сервер, выполните следующие команды в зависимости от используемой операционной системы и требований к аутентификации пользователей на прокси-сервере:
   a. Если аутентификация пользователей не требуется:
      - для операционных систем CentOS или Red Hat Enterprise Linux выполните команду:

        ```
        echo "proxy=http://<имя прокси-сервера>:8080" >> /etc/yum.conf
        ```

      - для операционных систем Ubuntu или Debian выполните команды:

        ```
        echo 'Acquire::https::Proxy "http://<имя прокси-сервера>:8080";' >> /etc/apt/apt.conf
        ```

        ```
        echo 'Acquire::http::Proxy "http://<имя прокси-сервера>:8080";' >> /etc/apt/apt.conf
        ```

      - для операционной системы SUSE Linux Enterprise Server, укажите в файле /etc/sysconfig/proxy следующие строки:

        ```
        HTTP_PROXY="http://<имя прокси-сервера>:8080"
        ```

        ```
        HTTPS_PROXY="http://<имя прокси-сервера>:8080"
        ```

        ```
        RPOXY_ENABLED="yes"
        ```

        Выполните команду `reboot`.

   b. Если аутентификация пользователей требуется:
      - для операционной системы CentOS или Red Hat Enterprise Linux выполните команду:

```
echo "proxy=http://<имя пользователя>:<пароль>@<имя
прокси-сервера>:8080" >> /etc/yum.conf
```

- для операционной системы Ubuntu или Debian выполните команды:

```
echo 'Acquire::http::Proxy "http://<имя пользователя>:<пароль>@<имя
прокси-сервера>:8080";' >> /etc/apt/apt.conf
```

```
echo 'Acquire::https::Proxy "http://<имя пользователя>:<пароль>@<имя
прокси-сервера>:8080";' >> /etc/apt/apt.conf
```

- для операционной системы SUSE Linux Enterprise Server, укажите в файле /etc/sysconfig/proxy следующие строки:

```
HTTP_PROXY="http://<имя пользователя>:<пароль>@<имя
прокси-сервера>:8080"
```

```
HTTPS_PROXY="http://<имя пользователя>:<пароль>@<имя
прокси-сервера>:8080"
```

```
RPOXY_ENABLED="yes"
```

Выполните команду `reboot`.

3. Если вы используете CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server, включите поддержку репозиториев для установки сервиса nginx. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

- CentOS:

```
yum install -y epel-release
```

- Red Hat Enterprise Linux:

```
echo '[nginx]
name=nginx repo
baseurl=http://nginx.org/packages/rhel/7/$basearch/
gpgcheck=0
enabled=1' > /etc/yum.repos.d/nginx.repo
```

- SUSE Linux Enterprise Server:

```
zypper addrepo -G -t yum -c 'http://nginx.org/packages/sles/12' nginx
```

4. Установите пакет сервиса nginx. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux:

```
yum install -y nginx
```

- SUSE Linux Enterprise Server:

```
zypper install nginx
```

- Ubuntu или Debian:

```
apt-get install nginx
```

5. Добавьте сервис nginx в автозагрузку. Для этого выполните команду:

```
systemctl enable nginx
```

6. Запустите сервис nginx. Для этого выполните команду:

   ```
   service nginx start
   ```

7. Проверьте статус сервиса nginx. Для этого выполните команду:

   ```
   service nginx status
   ```

   Параметр **Active** должен содержать значение **active (running)**.

Сервис nginx будет установлен.

Настройка портов для работы программы

Выполняйте действия по настройке портов, если на сервере включен брандмауэр.

► *Чтобы настроить порты для работы программы, выполните следующие действия:*

1. Откройте доступ к требуемым портам. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

   - CentOS или Red Hat Enterprise Linux:

     ```
     firewall-cmd --add-port=<порт>/<протокол> --permanent
     ```

   - Ubuntu:

     ```
     ufw allow <порт>
     ```

   - Debian:

     ```
     apt-get install iptables-persistent
     iptables -A INPUT -p <протокол> --dport <порт> -j ACCEPT
     ```

   - Если вы используете операционную систему SUSE Linux Enterprise Server, укажите в файле /etc/sysconfig/SuSEfirewall2 параметр `FW_SERVICES_EXT_TCP="<номера портов через пробел>"`.

2. Примените внесенные изменения. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

   - CentOS или Red Hat Enterprise Linux:

     ```
     firewall-cmd --reload
     ```

   - SUSE Linux Enterprise Server:

     ```
     rcSuSEfirewall2 restart
     ```

   - Debian:

     ```
     netfilter-persistent save
     ```

   > Если вы используете операционную систему Ubuntu, внесенные изменения вступят в силу автоматически.

Порты будут настроены для работы программы.

kaspersky

Изменение языка операционной системы

Для корректной установки Kaspersky Web Traffic Security на операционных системах Debian или Ubuntu необходимо использовать в качестве языка операционной системы английский язык. В противном случае установка программы может завершиться с ошибкой.

► *Чтобы изменить язык операционной системы на английский, выполните следующие действия:*

1. Запустите утилиту настройки локализации. Для этого выполните команду:

   ```
   dpkg-reconfigure locales
   ```

   Откроется окно **Configuring locales**.
2. Выберите **en_US.UTF8** и нажмите на кнопку **OK**.
3. В окне настройки языка по умолчанию выберите **en_US.UTF-8** и нажмите на кнопку **OK**.

Язык операционной системы будет изменен на английский. После установки и первоначальной настройки программы вы можете вновь установить использованный ранее язык операционной системы.

Подготовка к установке программы в операционной системе Astra Linux

Перед установкой программы убедитесь, что для операционной системы Astra Linux установлен пакет обновлений версии Update 3 или выше.

В программе поддерживается работа как с hardened, так и с generic ядром операционной системы Astra Linux.

Во время установки программы потребуется доступ в интернет для загрузки дополнительных пакетов из публичных репозиториев Astra Linux. Для этого настройте на сервере сетевое подключение.

Подготовка к установке программы включает следующие этапы.

1. Отключение несовместимых механизмов защиты (на стр. 45)
2. Изменения языка операционной системы (см. раздел "Изменение языка операционной системы" на стр. 46)

   Для корректной работы программы необходимо установить в операционной системе язык en_US.UTF-8.
3. Установка сервиса nginx (на стр. 46)
4. Установка сервиса Squid (на стр. 47)

kaspersky

В этом разделе

Отключение несовместимых механизмов защиты

Для корректной работы программы требуется отключить в операционной системе следующие механизмы защиты:

- блокировка системных команд;
- блокировка консоли;
- блокировка интерпретаторов;
- блокировка bash;
- блокировка макросов;
- режим МКЦ;
- МКЦ файловой системы;
- блокировка бита исполнения;
- блокировка ptrace;
- блокировка sumac;
- блокировка sysrq;
- межсетевой экран UFW;
- ограничения ulimits;
- подпись ELF;
- подпись xattr;
- безопасное удаление.

Вы можете проверить текущий статус механизмов защиты с помощью команды `astra-security-monitor`.

Все указанные механизмы защиты, кроме мандатного контроля целостности файловой системы, вы можете отключить во время установки операционной системы. Способы отключения механизмов защиты после установки операционной системы описаны в документации к операционной системе Astra Linux.

► *Чтобы отключить мандатный контроль целостности файловой системы, выполните следующие действия:*

1. Выполните следующие команды:

```
astra-mic-control disable
unset-fs-ilev
```

2. Перезагрузите операционную систему.

Мандатный контроль целостности файловой системы будет отключен.

Изменение языка операционной системы

Для корректной работы программы требуется изменить язык операционной системы на английский.

► *Чтобы изменить язык операционной системы на английский, выполните следующие действия:*

1. В файле /etc/locale.gen удалите знак комментария в строке:

   ```
   en_US.UTF-8 UTF-8
   ```

2. Обновите конфигурацию. Для этого выполните команды:

   ```
   locale-gen
   update-locale
   ```

3. Проверьте список доступных языков операционной системы. Для этого выполните команду:

   ```
   locale -a
   ```

Язык операционной системы будет изменен на английский.

Установка сервиса nginx

Пакет для установки сервиса nginx загружается из публичного репозитория официального разработчика.

► *Чтобы установить сервис nginx, выполните следующие действия:*

1. Создайте файл /etc/apt/sources.list.d/nginx.list. Файл должен содержать следующую строку:

   ```
   deb http://nginx.org/packages/debian stretch nginx
   ```

2. Установите ключ для проверки цифровой подписи. Для этого выполните команду:

   ```
   curl -fs https://nginx.org/keys/nginx_signing.key | apt-key add -
   ```

3. Установите пакет nginx. Для этого выполните команды:

   ```
   apt-get update
   apt install nginx
   ```

4. Разрешите автоматический запуск сервиса nginx. Для этого выполните команду:

   ```
   systemctl enable nginx
   ```

Сервис nginx будет установлен.

Установка сервиса Squid

Пакет squid входит в комплект поставки операционной системы Astra Linux 1.6. Перед установкой сервиса Squid требуется подключить установочный диск согласно документации к операционной системе.

► *Чтобы установить сервис Squid, выполните следующие действия:*

1. Установите пакет squid. Для этого выполните команду:

   ```
   apt install squid
   ```

2. Разрешите автоматический запуск сервиса squid. Для этого выполните команду:

   ```
   systemctl enable squid
   ```

Сервис Squid будет установлен.

Подготовка к установке программы в операционной системе ALT Linux

Перед установкой программы в операционной системе ALT Linux требуется установить сервисы nginx (см. раздел "Установка сервиса nginx" на стр. 47) и Squid (см. раздел "Установка сервиса Squid" на стр. 47).

В этом разделе

Установка сервиса nginx

► *Чтобы установить сервис nginx, выполните следующие действия:*

1. Установите пакеты nginx из публичного репозитория ALT Linux. Для этого выполните команды:

   ```
   apt-get update
   apt-get install nginx
   ```

2. Разрешите автоматический запуск сервиса nginx. Для этого выполните команду:

   ```
   systemctl enable nginx
   ```

Сервис nginx будет установлен.

Установка сервиса Squid

► *Чтобы установить сервис Squid, выполните следующие действия:*

1. Установите пакеты Squid из публичного репозитория ALT Linux. Для этого выполните команды:

```
apt-get update
apt-get install squid
apt-get install squid-helpers
```

2. Разрешите автоматический запуск сервиса Squid. Для этого выполните команду:

```
systemctl enable squid
```

Сервис Squid будет установлен.

Установка программы

► *Чтобы установить программу из rpm- или deb-пакета, выполните следующие действия:*

1. Скопируйте пакет `kwts_6.1.0-<версия пакета>`, входящий в комплект поставки, в домашнюю директорию.
2. Запустите установку пакета. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server:

     ```
     rpm -ivh kwts_6.1.0-<версия пакета>.rpm
     ```

   - Ubuntu или Debian:

     ```
     dpkg -i kwts_6.1.0-<версия пакета>.deb
     ```

   - Astra Linux:

     ```
     apt install kwts_6.1.0-<версия пакета>.deb
     apt install kwts-l10n-ru_6.1.0.<версия пакета>.deb
     ```

   - ALT Linux:

     ```
     rpm -i kwts-6.1.0-<версия пакета>.rpm
     rpm -i kwts_ru-6.1.0.<версия пакета>.rpm
     ```

3. Ожидайте окончания установки.

После окончания установки в командной строке появится сообщение о необходимости запуска скрипта настройки программы (см. раздел "Первоначальная настройка программы" на стр. 49).

kaspersky

Первоначальная настройка программы

После установки программы вам нужно провести первоначальную настройку.

Вы можете выполнить настройку программы вручную (см. раздел "Настройка программы вручную" на стр. 49) или сохранить установленные значения параметров в файл (см. раздел "Создание файла автоматической настройки программы" на стр. 51). С помощью этого файла вы сможете выполнять настройку программы в автоматическом режиме (см. раздел "Запуск автоматической настройки программы" на стр. 51). Это позволит избежать повторного ввода параметров и сократить время на развертывание программы в инфраструктуре организации.

Учетная запись пользователя, выполняющего первоначальную настройку программы, должна обладать правами суперпользователя.

В этом разделе

Настройка программы вручную

Если вы используете Debian или Ubuntu не на английском языке, вам требуется изменить язык операционной системы (см. раздел "Изменение языка операционной системы" на стр. 44) перед запуском первоначальной настройки программы.

► *Чтобы настроить программу вручную, выполните следующие действия:*

1. Запустите скрипт настройки программы. Для этого выполните команду:

   `/opt/kaspersky/kwts/bin/setup.py --install`

2. Выберите язык просмотра Лицензионного соглашения и Политики конфиденциальности. Для этого введите число, расположенное рядом с языком, который вы хотите выбрать, и нажмите на клавишу **ENTER**.
3. Выразите свое согласие или несогласие с Лицензионным соглашением. Для этого выполните следующие действия:
   a. Нажмите на клавишу **ENTER**, чтобы ознакомиться с текстом Лицензионного соглашения.
   b. Нажмите на клавишу **Q** для выхода из режима просмотра.
   c. Выполните одно из следующих действий:
      - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.

- Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.

d. Нажмите на клавишу **ENTER**.

Если вы отклонили условия Лицензионного соглашения, настройка программы не выполняется.

4. Выразите свое согласие или несогласие с Политикой конфиденциальности. Для этого выполните следующие действия:
   a. Нажмите на клавишу **ENTER**, чтобы ознакомиться с текстом Политики конфиденциальности.
   b. Нажмите на клавишу **Q** для выхода из режима просмотра.
   c. Выполните одно из следующих действий:
      - Если вы хотите принять условия Политики конфиденциальности, введите `yes`.
      - Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.
   d. Нажмите на клавишу **ENTER**.

Если вы отклонили условия Политики конфиденциальности, настройка программы не выполняется.

5. Выразите свое согласие или несогласие со значениями параметров защиты, устанавливаемыми по умолчанию. Для этого выполните следующие действия:
   a. Нажмите на клавишу **ENTER**, чтобы ознакомиться с описанием параметров защиты по умолчанию.
   b. Нажмите на клавишу **Q** для выхода из режима просмотра.
   c. Выполните одно из следующих действий:
      - Если вы хотите принять параметры защиты по умолчанию, введите `yes`.
      - Если вы хотите отклонить параметры защиты по умолчанию, введите `no`.
   d. Нажмите на клавишу **ENTER**.

Если вы не согласны с установкой параметров защиты по умолчанию, настройка программы не выполняется.

Вы можете изменить эти параметры после установки в веб-интерфейсе программы в разделе **Правила**.

6. Введите IP-адрес сетевого интерфейса для взаимодействия с другими узлами кластера и нажмите на клавишу **ENTER**.

   По умолчанию используется текущий активный IP-адрес.

7. Укажите порт для взаимодействия с другими узлами кластера и нажмите на клавишу **ENTER**.

   Рекомендуется использовать значение по умолчанию: 9045.

8. Задайте пароль Локального администратора.

Пароль должен содержать:

- минимум 15 символов;
- только символы ASCII (A-Z, a-z), цифры и специальные символы;
- символы следующих типов:
  - символ верхнего регистра (A-Z);
  - символ нижнего регистра (a-z);
  - цифру;
  - специальный символ.

Вы можете изменить пароль Локального администратора (см. раздел "Изменение пароля учетной записи Administrator" на стр. 119) после установки программы в веб-интерфейсе.

Настройка программы будет завершена. После этого вам нужно добавить сервер в кластер (см. раздел "Добавление узла в кластер" на стр. 124) для управления параметрами программы через веб-интерфейс.

Создание файла автоматической настройки программы

► *Чтобы создать файл автоматической настройки, выполните команду:*

```
/opt/kaspersky/kwts/bin/setup.py --create-auto-install=<полный путь к файлу для сохранения параметров>
```

Во время создания файла автоматической настройки текущие параметры сервера не будут изменены. Если указанный файл автоматической настройки уже существует, его содержимое будет перезаписано.

Запуск автоматической настройки программы

Если вы используете Debian или Ubuntu не на английском языке, вам требуется изменить язык операционной системы (см. раздел "Изменение языка операционной системы" на стр. 44) перед запуском первоначальной настройки программы.

► *Чтобы запустить автоматическую настройку программы, выполните следующую команду:*

```
/opt/kaspersky/kwts/bin/setup.py --auto-install=<полный путь к файлу автоматической настройки>
```

Параметры файла автоматической настройки программы приведены в таблице ниже.

Таблица 2. Параметры файла автоматической настройки программы

Параметр	Описание	Возможные значения
`eula`	Согласие с условиями Лицензионного соглашения.	`yes`
`privacy_policy`	Согласие с условиями Политики конфиденциальности.	`yes`
`default_protection_settings`	Согласие с установкой параметров защиты по умолчанию.	`yes`
`nodeip`	Выбор IP-адреса сетевого интерфейса для взаимодействия с другими узлами кластера.	`<IP-адрес в формате IPv4 или IPv6>`
`nodeport`	Выбор порта для взаимодействия с другими узлами кластера. Рекомендуется использовать значение по умолчанию: 9045.	`<порт>`
`adminpassword`	Ввод пароля Локального администратора.	`<пароль, удовлетворяющий требованиям>`

Удаление программы

► *Чтобы удалить программу, выполните следующие действия:*

1. Удалите установочный пакет. Для этого выполните следующие действия в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux.

     Выполните команду:

     ```
     rpm -e kwts
     ```
   - SUSE Linux Enterprise Server:
     a. Выполните команду:

        ```
        rpm -e kwts
        ```
     b. Подтвердите удаление пакета. Для этого введите `Y` и нажмите на клавишу **ENTER**.
   - Ubuntu или Debian.

     Выполните команду:

     ```
     dpkg -r kwts
     ```

2. Запустите скрипт для удаления всех файлов и директорий программы:

   `/var/opt/kaspersky/kwts/cleanup.sh`

   Отобразится запрос подтверждения.
3. Введите `yes` и нажмите на клавишу **ENTER**.
4. Если вы используете Ubuntu или Debian, выполните следующую команду:

   `dpkg -P kwts`

Программа будет удалена.

kaspersky

Создание учетных записей пользователей

При установке программы создается учетная запись Administrator с правами суперпользователя. Она является локальной и позволяет входить в систему без использования внешних служб и доменов аутентификации. Вы можете изменить пароль для этой учетной записи после установки в разделе **Параметры**, подразделе **Локальный администратор**.

При первоначальной настройке программы после установки для соответствия требованиям ИТ.САВЗ.Б2.ПЗ рекомендуется создать следующие роли:

- Администратор сервера.
- Администратор безопасности.

Администратору сервера рекомендуется назначить следующие права:

- **Создавать/изменять/удалять узлы**.
- **Получать диагностическую информацию**.

Администратору безопасности рекомендуется назначить следующие права:

- **Создавать/изменять/удалять узлы**.
- **Получать диагностическую информацию**.
- **Проверять целостность данных**.
- **Просматривать информацию об узлах**.
- **Создавать/изменять рабочие области**.
- **Просматривать рабочие области**.
- **Удалять рабочие области**.
- **Создавать/изменять роли**.
- **Просматривать роли**.
- **Удалять роли**.
- **Создавать/изменять правила**.
- **Просматривать правила**.
- **Удалять правила**.
- **Просматривать события обработки трафика**.
- **Просматривать системные события**.
- **Просматривать разделы Мониторинг и Отчеты**.
- **Изменять параметры**.
- **Просматривать параметры**.

kaspersky

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу.
- Активный ключ добавлен.
- Базы Антивируса и Анти-Фишинга обновлены.

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

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

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

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR http://www.eicar.org/anti_virus_test_file.htm.

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

► *Чтобы проверить антивирусную защиту сообщений с использованием тестового файла EICAR,*

перейдите по ссылке и попробуйте загрузить файл EICAR с официального веб-сайта организации

EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Kaspersky Web Traffic Security сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

kaspersky

Интерфейс Kaspersky Web Traffic Security

Работа с программой осуществляется через веб-интерфейс.

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Web Traffic Security.
- **Отчеты**. Позволяет формировать отчеты о работе программы.
- **События**. Содержит информацию о событиях, обнаруженных в сетевом трафике.
- **Правила**. Позволяет работать с правилами обработки трафика.
- **Рабочие области**. Позволяет работать с рабочими областями и распределять сетевой трафик.
- **Пользователи**. Позволяет управлять пользователями программы.
- **Узлы**. Позволяет управлять узлами кластера.
- **Параметры**. Содержит разделы **Общие**, **Внешние службы**, **Журналы и события**, **Доступ к программе**, в которых вы можете настраивать параметры программы.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

kaspersky

Начало работы с программой

После завершения установки вы можете работать с программой с помощью веб-интерфейса через браузер любого компьютера.

Администратору Kaspersky Web Traffic Security требуется самостоятельно обеспечить защиту передачи данных между браузером и Управляющим узлом. Для обеспечения безопасности также рекомендуется настроить Kerberos-аутентификацию с использованием технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 193).

Для того, чтобы управлять параметрами программы, вам требуется подключиться к Управляющему узлу. При подключении к Подчиненным узлам вам доступно изменение роли сервера (см. раздел "Изменение роли узла в кластере" на стр. 126) и просмотр состояния других подключенных серверов.

В этом разделе

Настройка сетевых доступов

Если вы установили программу из rpm- или deb-пакета, то для корректной работы Kaspersky Web Traffic Security требуется предварительно настроить порты (см. раздел "Настройка портов для работы программы" на стр. 43) на серверах с установленной программой, а также на маршрутизаторах локальной сети организации, через которые проходит трафик. При развертывании операционной системы с предустановленной программой из iso-файла все необходимые для работы порты уже настроены.

Информация о необходимых сетевых доступах в соответствии с функциональностью программы представлена в таблице ниже.

Таблица 3. Сетевые доступы, необходимые для работы программы

Функциональность	Протокол	Порт	Направление	Назначение соединения
Работа с программой через веб-интерфейс	TCP	443	Входящее	Компьютер администратора программы
Взаимодействие между узлами кластера (см. раздел "Управление кластером" на стр. 121)	TCP	По умолчанию 9045 (возможно изменить в веб-интерфейсе программы)	Входящее и исходящее	Другие узлы кластера

Функциональность	Протокол	Порт	Направление	Назначение соединения
Соединение с ICAP-сервером (см. раздел "Параметры ICAP-сервера" на стр. 137)	TCP	По умолчанию 1344 (возможно изменить в веб-интерфейсе программы)	Входящее	ICAP-клиенты и балансировщики нагрузки
DNS-запросы	UDP	53	Исходящее	DNS-серверы
Соединение с внешним прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 150)	TCP	По умолчанию 8080 (возможно изменить в веб-интерфейсе программы)	Исходящее	Внешний прокси-сервер
Активация программы (на стр. 37)	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
Обновление баз программы (см. раздел "Обновление баз Kaspersky Web Traffic Security" на стр. 151)	TCP	80, 443	Исходящее	Серверы "Лаборатории Касперского"
KSN	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
KPSN (см. раздел "Настройка использования Kaspersky Private Security Network" на стр. 156)	TCP	443	Исходящее	Сервер KPSN
Соединение с LDAP-сервером (на стр. 157)	TCP	389	Исходящее	Серверы Active Directory
Kerberos-аутентификация в Active Directory (см. раздел "Добавление соединения с LDAP-сервером" на стр. 157)	UDP, TCP	88	Исходящее	Серверы Active Directory
NTLM-аутентификация с помощью технологии единого входа (см. раздел "Настройка NTLM-аутентификации" на стр. 194)	TCP	445	Исходящее	Серверы Active Directory

Функциональность	Протокол	Порт	Направление	Назначение соединения
Интеграция с программой KATA (см. раздел "Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform" на стр. 160)	TCP	По умолчанию 443 (возможно изменить в веб-интерфейсе программы)	Исходящее	Сервер KATA
Работа службы snmpd (см. раздел "Настройка службы snmpd в операционной системе" на стр. 184)	TCP	По умолчанию 705 (возможно изменить в веб-интерфейсе программы)	Исходящее	SNMP-сервер

Подключение к веб-интерфейсу программы

Если вы подключаетесь к веб-интерфейсу впервые после установки программы, перед началом работы вам потребуется создать новый кластер (см. раздел "Создание нового кластера" на стр. 121).

► *Чтобы подключиться к веб-интерфейсу программы, выполните следующие действия:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или FQDN Управляющего сервера>`

   Откроется страница авторизации веб-интерфейса с запросом имени и пароля пользователя.
2. В поле **Имя пользователя** введите `Administrator`.
3. В поле **Пароль** введите пароль администратора.

   Если вы введете неверный пароль пять раз, возможность авторизации будет заблокирована на пять минут.
4. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса программы.

Проверка работы Kaspersky Web Traffic Security в веб-интерфейсе

Выполняйте проверку работы Kaspersky Web Traffic Security в браузере на компьютере локальной сети организации.

► *Чтобы проверить работу Kaspersky Web Traffic Security, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Узлы**.
2. Убедитесь, что все Подчиненные узлы имеют статус **Синхронизирован**.
3. Перейдите по следующим ссылкам:
   - http://www.eicar.org/download/eicar.com;
   - https://www.eicar.org/download/eicar.com.

   Если программа настроена верно и в параметрах сервиса Squid включен SSL Bumping, отобразится сообщение о запрете доступа к этим ресурсам.

   Если программа настроена верно и в параметрах сервиса Squid выключен SSL Bumping, отобразится сообщение о запрете доступа только к первому ресурсу (http://www.eicar.org/download/eicar.com).
4. Откройте веб-сайт, доступ к которому не запрещен, например, https://www.kaspersky.ru.

   Если программа настроена верно, веб-сайт откроется.

kaspersky

Мониторинг работы программы

> В статистике обработанного трафика не учитываются веб-ресурсы, к которым были применены правила обхода (см. раздел "Добавление правила обхода" на стр. 78) или действия **Tunnel** и **Tunnel with SNI check** в рамках обработки SSL-соединений.

Вы можете осуществлять мониторинг работы программы с помощью графиков и информационных панелей. В окне веб-интерфейса программы в разделе **Мониторинг** отображается следующая информация:

- **Работоспособность системы**. Диаграмма ошибок в работе кластера. По ссылке **Перейти в раздел Узлы** вы можете перейти в раздел **Узлы** и посмотреть более подробные сведения о работоспособности каждого узла кластера.

  > Недоступно в веб-интерфейсе рабочей области.

- **Обнаружения по категории**. Диаграмма обнаруженных объектов по категориям контентной фильтрации, а также график обнаружений по времени. Эта информация позволит вам определить наиболее часто запрашиваемые категории веб-ресурсов в вашей организации.
- **Обработка данных**. График, показывающий объем обработанного входящего и исходящего сетевого трафика в течение времени. Эта информация поможет вам определить часы наибольшей активности пользователей вашей организации, а также оценить количество ресурсов, необходимых для обработки трафика.
- **Антивирус**. Графики, показывающие количество объектов, проверенных модулем Антивирус, и количество найденных угроз.
- **Анти-Фишинг**. Графики, показывающие количество объектов, проверенных модулем Анти-Фишинг, и количество найденных угроз.
- **Фильтр вредоносных ссылок**. Графики, показывающие общее количество проверенных ссылок и количество ссылок, признанных вредоносными.
- **KATA**. Графики, показывающие количество объектов, проверенных на основании информации с сервера KATA, и количество найденных угроз.
- **Последние 10 угроз**. Названия и время обнаружения последних 10 объектов.
- **Последние 10 заблокированных URL-адресов**. URL-адреса последних 10 веб-ресурсов, доступ к которым был заблокирован.
- **Последние 10 пользователей с заблокированными запросами**. IP-адреса последних 10 пользователей, запросы которых были заблокированы программой.

В общем веб-интерфейсе программы вы можете фильтровать данные мониторинга (см. раздел "Фильтрация данных мониторинга" на стр. 65) по следующим критериям:

- интервалу времени;
- узлам кластера;
- рабочим областям.

В веб-интерфейсе рабочей области доступна только фильтрация по интервалу времени.

Вы можете создавать новые схемы расположения графиков (см. раздел "Создание новой схемы расположения графиков" на стр. 63), переключаться между сохраненными схемами (см. раздел "Выбор схемы расположения графиков из списка" на стр. 65), а также устанавливать схему, отображаемую по умолчанию (см. раздел "Выбор схемы расположения графиков, отображаемой по умолчанию" на стр. 65).

В этом разделе

Создание новой схемы расположения графиков

► *Чтобы создать новую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Новая**.

   Отобразится набор графиков по умолчанию.
4. В поле **Название схемы расположения графиков** введите имя новой схемы расположения графиков.
5. Если вы хотите добавить графики в схему, нажмите на кнопку **Графики** и выполните следующие действия:
   a. В появившемся окне **Добавить график** включите переключатели рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   b. Нажмите на кнопку ✕.
6. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
7. Если вы хотите удалить график со схемы, нажмите на значок ✕ в правом верхнем углу графика.
8. Нажмите на кнопку **Сохранить**.

Новая схема будет добавлена в список схем расположения графиков в разделе **Графики**.

kaspersky

Изменение схемы расположения графиков

Вы не можете изменить предустановленную схему расположения графиков под названием **Схема по умолчанию**.

► *Чтобы изменить схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, которую вы хотите изменить.
3. В верхней части окна нажмите на кнопку ☰.
4. В раскрывающемся списке выберите **Изменить**.
5. Если вы хотите переименовать схему, в поле с текущим именем схемы расположения графиков введите новое имя.
6. Если вы хотите добавить графики в схему, нажмите на кнопку **Графики** и выполните следующие действия:
   a. В появившемся окне **Добавить график** включите переключатели рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   b. Нажмите на кнопку ✕.
7. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
8. Если вы хотите удалить график со схемы, нажмите на значок ✕ в правом верхнем углу графика.
9. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет изменена.

Удаление схемы расположения графиков

Вы не можете удалить предустановленную схему расположения графиков под названием **Схема по умолчанию**.

► *Чтобы удалить схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, которую вы хотите удалить.
3. Наведите курсор мыши на название схемы расположения графиков, которую вы хотите удалить.
4. Нажмите на значок 🗑 справа от названия схемы расположения графиков.

   Отобразится подтверждение удаления схемы расположения графиков.

5. Нажмите на кнопку **Удалить**.

Схема расположения графиков будет удалена.

Выбор схемы расположения графиков из списка

► *Чтобы выбрать схему расположения графиков из списка схем расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в списке схем расположения графиков выберите нужную схему расположения графиков.

Выбранная схема расположения графиков отобразится в окне веб-интерфейса программы.

Выбор схемы расположения графиков, отображаемой по умолчанию

► *Чтобы выбрать схему расположения графиков, отображаемую по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы раскройте список схем расположения графиков.
3. Выберите схему, которая должна отображаться по умолчанию.
4. Нажмите на значок ☆ слева от названия схемы.

Выбранная схема расположения графиков будет отображаться при выборе раздела **Мониторинг**.

Фильтрация данных мониторинга

► *Чтобы отфильтровать сведения, отображаемые на графиках, выполните следующие действия:*

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите общие параметры или название нужной рабочей области.
2. Выберите раздел **Мониторинг**.
3. Если вы хотите отфильтровать сведения по интервалу времени, в раскрывающемся списке **Прошедший час** выберите один из следующих вариантов:
   - **Прошедший час**.
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.

- **Прошедший месяц**.
- **Прошедший год**.

По умолчанию отображаются сведения за последний час.

4. Если вы хотите отфильтровать сведения по узлам кластера, в раскрывающемся списке **Все узлы** выберите IP-адрес нужного узла.

   По умолчанию отображаются сведения обо всех узлах.

   > Недоступно в веб-интерфейсе рабочих областей.

5. Если вы хотите отфильтровать сведения по рабочим областям, в раскрывающемся списке **Глобальная** выберите название нужной рабочей области.

   По умолчанию отображаются сведения обо всех рабочих областях.

   > Недоступно в веб-интерфейсе рабочих областей.

Сведения, отображаемые на графиках, будут отфильтрованы по заданным критериям.

kaspersky

Отчеты

Функциональность доступна только при наличии у пользователя права **Просматривать разделы Мониторинг и Отчеты**.

Вы можете создать отчет (см. раздел "Создание отчета" на стр. 67) по заданным критериям на основе статистики из раздела **Мониторинг**. Отчет содержит данные об обработанном трафике выбранной рабочей области за указанный период времени.

После создания отчет доступен для скачивания (см. раздел "Скачивание отчета на компьютер" на стр. 68) в формате PDF.

В этом разделе

Создание отчета

► *Чтобы создать отчет, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Отчеты**.
2. Нажмите на кнопку **Создать отчет**.

   Откроется окно **Новый отчет**.
3. В раскрывающемся списке **Период** выберите один из следующих периодов, за который вы хотите сформировать отчет:
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.
   - **Прошедший месяц**.
   - **Прошедший год**.
4. В раскрывающемся списке **Рабочая область** выберите рабочую область, данные о которой вы хотите включить в отчет.

   Если вы хотите получить данные обо всех рабочих областях, выберите **Глобальная**.
5. В раскрывающемся списке **Язык** выберите язык отчета.
6. Нажмите на кнопку **Добавить**.

Отчет будет создан и отобразится в первой строке таблицы отчетов. Вы можете сохранить созданный

отчет (см. раздел "Скачивание отчета на компьютер" на стр. 68) на жесткий диск компьютера.

Удаление отчета

► *Чтобы удалить отчет, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Отчеты**.
2. В таблице **Последние созданные отчеты** в правой части строки с отчетом, который вы хотите удалить, нажмите на значок .

Отчет будет удален.

Скачивание отчета на компьютер

Вы можете скачать отчет на любой компьютер, с которого вы вошли в веб-интерфейс программы.

► *Чтобы скачать отчет на компьютер, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Отчеты**.
2. В таблице **Последние созданные отчеты** в правой части строки с отчетом, который вы хотите скачать, нажмите на значок .

Файл отчета в формате PDF будет сохранен в папке загрузки браузера.

Просмотр содержимого отчета

PDF-файл сформированного отчета содержит данные об обработке трафика выбранной рабочей области за указанный период времени.

В заголовке отчета содержится следующая информация:

- Период, за который были получены данные.
- Рабочая область, к которой относятся данные об обрабатываемом трафике.

  Если был выбран раздел **Глобальная**, сначала отображаются суммарные данные об обработке всего трафика, а затем данные по каждой рабочей области.

- Язык отчета.

Тело отчета включает в себя следующие блоки информации:

- Количество обработанных объектов (**Обработано объектов**) и объем проверенного трафика (**Трафик**).
- Количество обработанных объектов (**Проверено**) и угроз (**Обнаружено**), обнаруженных следующими технологиями:

  - **Антивирус**.
  - **KATA**.
  - **Фильтр вредоносных ссылок**.
  - **Анти-Фишинг**.
- Количество посещенных URL-адресов, попадающих под следующие веб-категории:
  - **Для взрослых**.
  - **Алкоголь, табак, наркотические и психотропные вещества**.
  - **Культура и общество**.
  - **Программное обеспечение, аудио, видео**.
  - **Информационные технологии**.
  - **Интернет-магазины, банки, платежные системы**.
  - **Ненависть и дискриминация**.
  - **Общение в сети**.
  - **Образование**.
  - **Хобби и развлечения**.
  - **Красота, здоровье и спорт**.
  - **Азартные игры, лотереи, тотализаторы**.
  - **Другие**.
  - **Заблокировано законодательством Российской Федерации**.
  - **Запрещено полицией**.
- **Последние 10 заблокированных URL-адресов**. URL-адреса последних 10 веб-ресурсов, доступ к которым был заблокирован.
- **Последние 10 угроз**. Названия и время обнаружения последних 10 объектов.
- **Последние 10 пользователей с заблокированными запросами**. IP-адреса последних 10 пользователей, запросы которых были заблокированы программой.

kaspersky

Журнал событий Kaspersky Web Traffic Security

Во время работы Kaspersky Web Traffic Security возникают различного рода события. Они отражают изменение состояния программы. Для того, чтобы администратор программы мог самостоятельно проанализировать ошибки, допущенные при настройке параметров программы, а также для того, чтобы специалисты "Лаборатории Касперского" могли оказать эффективную техническую поддержку, Kaspersky Web Traffic Security записывает информацию об этих событиях в *журнале событий*.

Данные журнала событий хранятся на узлах программы. Файлы журнала событий автоматически ротируются по достижении максимально разрешенного размера файлов или по истечении максимального срока их хранения.

Программа распределяет записи о событиях по следующим уровням:

- **Ошибка** – сообщения об ошибках в работе программы.
- **Информация** – информационные сообщения.

В общем веб-интерфейсе программы отображаются события обработки трафика, а также системные события программы. Администратор может отфильтровать события по отдельной рабочей области, а также события, которые не относятся к рабочим областям.

В веб-интерфейсе рабочей области отображаются только события обработки трафика текущей рабочей области.

В этом разделе

Просмотр журнала событий

► *Чтобы просмотреть журнал событий Kaspersky Web Traffic Security, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Трафик**;
   - **Система**;
   - **KATA**.

3. В раскрывающемся списке справа от параметра **Максимальное количество событий** выберите количество записей для просмотра.
4. Нажмите на кнопку **Добавить условие**.
5. Настройте фильтр событий с помощью появившихся раскрывающихся списков:
   a. В левом раскрывающемся списке выберите критерий фильтрации.
   b. В центральном раскрывающемся списке выберите оператор сравнения.

      Для каждого критерия фильтрации доступен свой релевантный набор операторов сравнения. Например, при выборе критерия **Направление** доступны операторы **Равняется** и **Не равняется**.
   c. В зависимости от выбранного критерия фильтрации выполните одно из следующих действий:
      - Укажите в поле справа от оператора сравнения один или несколько символов, по которым вы хотите выполнить поиск событий.
      - В правом раскрывающемся списке выберите вариант условия, по которому вы хотите выполнить поиск событий.

      Например, для поиска полного совпадения по имени пользователя введите имя пользователя.
6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации.

Экспорт событий

Вы можете отфильтровать события из журнала событий (см. раздел "Просмотр журнала событий" на стр. 70) программы и экспортировать их в файл.

► *Чтобы экспортировать события, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Трафик**.
   - **Система**.
3. В раскрывающемся списке справа от параметра **Максимальное количество событий** выберите количество записей для просмотра.
4. Нажмите на кнопку **Добавить условие**.
5. Настройте фильтр событий с помощью появившихся раскрывающихся списков.
6. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтрации.
7. В правом верхнем углу окна нажмите на кнопку **Экспортировать**.

Файл экспорта событий в формате CSV будет сохранен в папке загрузки браузера.

kaspersky

Настройка отображения таблицы событий

► *Чтобы настроить отображение таблицы событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Нажмите на кнопку **Добавить условие**.
3. Укажите условия фильтрации событий с помощью появившихся раскрывающихся списков.
4. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтра.
5. По кнопке  откройте меню отображения таблицы событий.
6. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы событий будет настроено.

Фильтрация системных событий

Фильтр системных событий по деталям события в графе **Сведения** доступен только на английском языке. Соответствие описаний событий на английском и русском языках приведено в таблице ниже.

Таблица 4. Детали системных событий на русском и английском языках

Английский	Русский
Application started. Real-time scan started	Программа запущена. Проверка в режиме реального времени запущена
Audit started	Аудит запущен
Audit stopped	Аудит остановлен
Anti-Virus databases updated	Антивирусные базы обновлены
Anti-Phishing databases updated	Базы Анти-Фишинга обновлены
Anti-Virus databases are up-to-date	Антивирусные базы актуальны
Anti-Phishing databases are up-to-date	Базы Анти-Фишинга актуальны
Anti-Virus databases are out of date	Антивирусные базы устарели
Anti-Phishing databases are out of date	Базы Анти-Фишинга устарели
Anti-Virus databases are obsolete	Антивирусные базы сильно устарели
Anti-Phishing databases are obsolete	Базы Анти-Фишинга сильно устарели
Anti-Virus databases applied. Publication time: <publication time>	Применены антивирусные базы. Время публикации: {{publishingTime}}
Anti-Phishing databases applied. Publication time: <publication time>	Применены базы Анти-Фишинга. Время публикации: {{publishingTime}}

Английский	Русский
Error updating databases: <error reason>	Ошибка обновления баз: {{errorReason}}
Error loading Anti-Virus databases: <description>	Ошибка загрузки антивирусных баз: {{description}}
Error loading Anti-Phishing databases: <description>	Ошибка загрузки баз Анти-Фишинга
LDAP synchronization started	Запущена синхронизация LDAP
Update started	Обновление запущено
KATA cache reset	Очистка кеша KATA
Data integrity violation found	Обнаружены нарушения целостности данных
No data integrity violation	Нарушения целостности данных не обнаружены

► *Чтобы отфильтровать системные события по деталям события, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите закладку **Система**.
3. Нажмите на кнопку **Добавить условие**.
4. В раскрывающемся списке слева выберите **Сведения**.
5. В поле ввода справа укажите описание события или фрагмент описания на английском языке.

   Например, если вы хотите просмотреть только события запуска обновления, введите `Update started`.
6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации.

Настройка параметров журнала событий

При настройке длительности хранения событий и уровня ведения журнала необходимо учитывать доступное дисковое пространство на серверах с установленной программой.

Параметры журнала событий не влияют на параметры записи событий по протоколу Syslog (см. раздел "Настройка параметров Syslog" на стр. 169).

► *Чтобы настроить параметры журнала событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **События**.
2. В блоке **Трафик** выполните следующие действия:
   a. В раскрывающемся списке **Записывать события обработки трафика** выберите, какие события обработки трафика должны быть записаны в журнал. Вы можете выбрать один из следующих вариантов:

- **все события**;
- **после действий Заблокировать/Перенаправить**;
- **не записывать**.

b. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

c. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на сервере.

3. В блоке **KATA** выполните следующие действия:

a. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

b. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на сервере.

4. В блоке **Система** в поле **Максимальное количество событий** укажите количество записей о событиях Kaspersky Web Traffic Security, при превышении которого более старые записи будут удалены.

Параметры журнала событий будут настроены.

Работа с правилами обработки трафика

Вы можете регулировать доступ пользователей к веб-ресурсам с помощью правил обработки трафика. Эти правила делятся на правила обхода, правила доступа и правила защиты. Вы можете создавать группы правил доступа и группы правил защиты или добавлять правила вне групп.

Kaspersky Web Traffic Security начинает обработку трафика с проверки правил обхода. Если доступ к веб-ресурсу разрешен, то программа переходит к проверке трафика с помощью правил доступа. По результатам обработки правил доступа программа или блокирует веб-ресурс, или переходит к проверке трафика с помощью правил защиты. Алгоритм работы правил обработки трафика показан на рисунке ниже.

Kaspersky Web Traffic Security применяет правила в порядке их расположения в таблице правил (см. раздел "Просмотр таблицы правил обработки трафика" на стр. 97) сверху вниз. Если заданные в правиле условия не выполняются, программа переходит к следующему правилу. Как только заданные в очередном правиле условия выполняются, к трафику применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается.

При наличии рабочей области (см. раздел "Управление рабочими областями" на стр. 99) приоритет правил рабочей области определяется положением строки **Правила рабочей области** в таблице общих правил. В этом случае правила также применяются в порядке расположения в таблице сверху вниз. Правила рабочей области будут применены после проверки трафика по всем правилам, расположенным в таблице выше. Если ни одно из правил рабочей области не сработало, программа переходит к проверке трафика по правилам, расположенным в таблице под строкой **Правила рабочей области**.

При установке программы создается *правило обхода по умолчанию*. Согласно этому правилу, доступ к веб-ресурсам, для которых значение HTTP-заголовка Content-Length превышает 10240 КБ, разрешается всем пользователям без выполнения проверки модулями Антивирус и Анти-Фишинг. Это значение обеспечивает баланс между производительностью программы и безопасностью сетевого трафика. Вы можете изменить (см. раздел "Изменение правила обработки трафика" на стр. 89), отключить (см. раздел "Включение и отключение правила обработки трафика" на стр. 91) или удалить (см. раздел "Удаление правила обработки трафика" на стр. 89) правило обхода по умолчанию.

Если ни одно правило не содержит условий, подходящих для данного веб-ресурса, трафик обрабатывается согласно политике защиты по умолчанию. В этом случае программа разрешает доступ к веб-ресурсу, который не запрещен в результате проверки модулями Антивирус и Анти-Фишинг. Политика защиты по

умолчанию создается во время установки Kaspersky Web Traffic Security и отображается в разделе **Параметры**, в подразделе **Защита**. В параметрах политики защиты по умолчанию вы можете установить действия, которые программа будет выполнять с объектами разных типов.

В этом разделе

Сценарий настройки доступа к веб-ресурсам

Совокупность правил обработки трафика позволяет выполнять следующие задачи:

- Разграничивать доступ к веб-ресурсам для сотрудников разных подразделений.

  Для этого вы можете использовать существующие доменные группы, если настроена интеграция с Active Directory (см. раздел "Приложение 2. Настройка интеграции сервиса Squid с Active Directory" на стр. 210). Например, вы можете разрешить доступ ко всем веб-ресурсам для группы Администраторы и запретить категории **Социальные сети** или **Программное обеспечение, аудио, видео** для остальных сотрудников.

- Блокировать доступ к веб-ресурсам, запрещенным законами вашей страны.

  Для этого вы можете создать правила для всех рабочих областей, распространяющиеся на всех пользователей.

- Контролировать объем трафика.

  В целях экономии трафика вы можете запретить или ограничить загрузку мультимедийных файлов, а также доступ к веб-ресурсам, не связанным с работой.

- Получать статистику о запрошенных веб-ресурсах в вашей организации.

  Если в правиле обработки трафика выбрано действие **Разрешить**, то пользователь получает доступ к веб-ресурсу, но информация об этом запросе сохраняется в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 70). Вы можете фильтровать события в журнале, например, просмотреть все обращения пользователей к веб-сайту www.kaspersky.ru.

Рекомендуется настраивать правила обработки трафика в следующем порядке:

1. Создание рабочих областей (см. раздел "Управление рабочими областями" на стр. 99) и / или групп правил обработки трафика (см. раздел "Работа с группами правил обработки трафика" на стр. 92), если требуется

   Правила обработки трафика проверяются в соответствии с их расположением в таблице правил. Для того, чтобы сработало нужное правило, необходимо заранее продумать способ организации правил. Рекомендуется использовать рабочие области для крупных подразделений организации или для разных клиентов интернет-провайдера. Далее можно объединять правила в группы. Например, вы можете создать рабочие области *Филиал 1* и *Филиал 2*, а внутри рабочих областей добавить группы *Администраторы*, *Бухгалтеры* и т.д.

2. Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 78), если требуется

   С помощью правила обхода вы можете предоставить пользователям доступ к веб-ресурсам, не выполняя их проверку. Например, разрешить скачивание обновлений используемого в вашей организации программного обеспечения с официального сайта производителя. Это позволяет сократить ресурсы программы, затрачиваемые на обработку трафика из доверенных источников.

3. Добавление правил доступа и правил защиты

   Вы можете добавлять правила доступа (см. раздел "Добавление правила доступа" на стр. 79) и правила защиты (см. раздел "Добавление правила защиты" на стр. 81) как для отдельной рабочей области, так и для всех рабочих областей. Кроме того, правила можно объединять в группы или добавлять их вне групп.

4. Настройка инициатора срабатывания правила (на стр. 82)

   Для каждого добавленного правила требуется указать пользователя или программу, сетевые соединения которых будет проверять Kaspersky Web Traffic Security.

5. Настройка критериев фильтрации трафика (см. раздел "Настройка фильтрации трафика" на стр. 83)

   С помощью критериев фильтрации необходимо задать условия, при соблюдении которых запрошенный пользователем веб-ресурс будет проверен согласно правилу.

   > Для правил обхода доступны критерии **URL**, **MIME-тип HTTP-сообщения**, **Направление трафика**, **HTTP-метод**, **HTTP Content-Length, КБ**.

6. Добавление исключения для правила (см. раздел "Добавление исключения для правила обработки трафика" на стр. 86), если требуется

   Вы можете добавить в исключения инициатора срабатывания правила или критерий фильтрации. Например, вы можете запретить доступ к категории **Программное обеспечение, аудио, видео** для всех сотрудников доменной группы *Бухгалтерия*, кроме руководителя отдела. Или вы можете запретить загрузку файлов размером более 500 МБ, кроме файла с корпоративными стандартами организации и т.д.

7. Настройка расписания работы правила (см. раздел "Настройка расписания работы правила обработки трафика" на стр. 88), если требуется

   Расписание позволяет автоматически отключать правило в заданные часы. Например, вы можете

настроить работу правил только в рабочие часы организации или отключить правило в определенный день.

8. Настройка политики защиты по умолчанию (на стр. 94)

   Если веб-ресурс не удовлетворяет условиям фильтрации ни одного из правил обработки трафика, то применяется политика защиты по умолчанию. Параметры политики защиты по умолчанию распространяются на обработку трафика всех рабочих областей, а также вне рабочих областей.

Добавление правила обхода

Создание правил обхода для отдельных рабочих областей недоступно.

Веб-ресурсы, к которым применяются правила обхода, не учитываются в статистике обработанного трафика в разделе **Мониторинг**.

► *Чтобы добавить правило обхода, выполните следующие действия:*

1. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите закладку **Обход**.

   Откроется таблица правил обхода.
4. Нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
   - **Разрешить без проверки**, если вы хотите добавить правило разрешения.

     Программа не будет выполнять проверку объектов на вирусы, фишинг, некоторые легальные программы, которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу. Доступ к запрашиваемому веб-ресурсу будет разрешен без проверки.

   - **Заблокировать**, если вы хотите добавить правило запрета.
   - **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.

   По умолчанию установлено значение **Заблокировать**.

Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Перенаправить**, то соединение будет прервано. Пользователь не будет перенаправлен на заданный в правиле веб-ресурс, и ему не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. В поле **Название правила** введите название правила обхода.

   Название правила должно быть уникально среди правил в разделе **Глобальная**.

8. Если требуется, в поле **Комментарий** введите комментарий.
9. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.
10. Нажмите на кнопку **Добавить**.

Правило обхода будет добавлено.

Добавление правила доступа

► *Чтобы добавить правило доступа, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите закладку **Доступ**.

   Откроется таблица правил доступа.

4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
   - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.

5. Выберите закладку **Общие параметры**.
6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
   - **Заблокировать**, если вы хотите запрещать доступ к веб-ресурсам.

- **Разрешить**, если вы хотите разрешать доступ к веб-ресурсам.
- **К следующей группе**, если вы хотите пропустить проверку по правилам этой группы.

  Программа будет выполнять проверку по правилам, которые расположены в таблице после этой группы.
- **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.

По умолчанию установлено значение **Заблокировать**.

Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Перенаправить**, то соединение будет прервано. Пользователь не будет перенаправлен на заданный в правиле веб-ресурс, и ему не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. Если вы выбрали вариант **Заблокировать** и хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 142), выполните следующие действия:
   a. Установите флажок **Введите текст для отображения на странице блокировки**.
   b. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 140).Если вы выбрали вариант **Разрешить** и хотите удалять HTTP-заголовок Range, установите флажок **Удалять HTTP-заголовок Range**.

   Если флажок установлен, то все объекты будут загружаться целиком для дальнейшей проверки с помощью правил защиты. Загрузка объектов по частям в этом режиме невозможна.
9. Если вы выбрали вариант **Перенаправить**, в поле **URL-адрес перенаправления** укажите URL-адрес, на который будет перенаправлен исходный запрос.
10. В поле **Название правила** введите название правила доступа.

    Название должно быть уникально в рамках рабочей области, если вы создаете правило рабочей области, или среди правил раздела **Глобальная**, если вы создаете правило вне рабочих областей.
11. Если требуется, в поле **Комментарий** введите комментарий.
12. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.
13. Нажмите на кнопку **Добавить**.

Правило доступа будет добавлено.

kaspersky

Добавление правила защиты

► *Чтобы добавить правило защиты, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите закладку **Защита**.

   Откроется таблица правил защиты.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
   - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. В блоке параметров **Действия** в раскрывающихся списках выберите одно из действий для каждого из следующих параметров:
   a. **Вредоносная программа**:
      - **Заблокировать**.
      - **Заблокировать, по возможности вылечить**.
      - **Пропустить проверку**.

      По умолчанию установлено значение **Заблокировать, по возможности вылечить**.
   b. **Объекты, обнаруженные KATA**, **Фишинг**, **Вредоносная ссылка**, **Зашифрованный объект** и **Документ с макросом**:
      - **Заблокировать**.
      - **Пропустить проверку**.

      По умолчанию установлено значение **Заблокировать**.

   Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Заблокировать, по возможности вылечить**, то соединение будет прервано. Пользователю не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. Если вы хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 142), выполните следующие действия:
   a. Установите флажок **Введите текст для отображения на странице блокировки**.
   b. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 140).В поле **Название правила** введите название правила защиты.

   Название должно быть уникально в рамках рабочей области, если вы создаете правило рабочей области, или среди правил раздела **Глобальная**, если вы создаете правило вне рабочих областей.
9. Если требуется, в поле **Комментарий** введите комментарий.
10. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.
11. Нажмите на кнопку **Добавить**.

Правило защиты будет добавлено.

Настройка инициатора срабатывания правила

► *Чтобы настроить инициатора срабатывания правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, для которого вы хотите настроить инициатора срабатывания правила.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.

6. Нажмите на кнопку  в блоке **Инициатор**.
7. В появившемся раскрывающемся списке выберите один из следующих вариантов:
   - **Имя пользователя**.

     Вы можете выбрать учетную запись пользователя из Active Directory или добавить имя пользователя в формате `username@REALM`.
   - **LDAP: group canonicalName**.

     Вы можете выбрать доменную группу из Active Directory или добавить название группы в формате `domain.com/groups/groupname`.
   - **LDAP: user distinguishedName**.

     Вы можете выбрать отличительное имя (DN, Distinguished Name) пользователя из Active Directory или добавить имя пользователя в формате `cn=username,ou=users,dc=test,dc=ru`.
   - **IP-адрес**.

     Вы можете указать IP-адрес пользователя или диапазон IP-адресов в формате IPv4 или IPv6 (например, `192.168.0.1/32`).
   - **User agent**.

     Вы можете указать название браузера или программы, обрабатывающей веб-трафик (например, `*IE*`).
8. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.

   Вы можете использовать регулярные выражения.
9. Если вы добавили более одного критерия, в раскрывающемся списке рядом с названием блока **Инициатор** выберите логический оператор:
   - Если вы хотите, чтобы правило срабатывало при соблюдении хотя бы одного из добавленных условий, выберите **любой из**.
   - Если вы хотите, чтобы правило срабатывало только при одновременном соблюдении всех добавленных условий, выберите **все из**.
10. Нажмите на кнопку **Сохранить**.

Инициатор срабатывания правила будет настроен.

Настройка фильтрации трафика

Для корректной обработки HTTPS-трафика требуется настроить перехват SSL-соединений на внешнем прокси-сервере (при установке программы из rpm- или deb-пакета) или на встроенном прокси-сервере (при развертывании программы из ISO-файла). Если перехват SSL-соединений не настроен, критерии фильтрации трафика не будут применены и проверка веб-ресурса модулями Антивирус и Анти-Фишинг не будет выполняться.

► *Чтобы настроить фильтрацию трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, для которого вы хотите настроить критерии фильтрации.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Нажмите на кнопку  в блоке **Фильтрация трафика**.
7. В появившемся раскрывающемся списке выберите один из следующих вариантов:
   - **Категория**.

     С помощью этого критерия вы можете контролировать доступ пользователей к веб-ресурсам какой-либо тематики. Например, вы можете запретить доступ к социальным сетям, выбрав категорию **Социальные сети**. Список веб-категорий, поддерживаемых программой, см. в Приложении 6 (см. раздел "Приложение 6. Категории веб-ресурсов" на стр. 230).
   - **URL**.

     Вы можете добавить в критерии фильтрации не только URL-адреса, но и протокол или порт сетевых соединений.
     - Если вы хотите добавить в критерии фильтрации URL-адреса, введите их в поле в окне **URL** и нажмите на кнопку **Добавить**.

       Если URL-адрес не прошел процесс нормализации (см. раздел "Приложение 5. Нормализация URL-адресов" на стр. 228), он не будет добавлен в список и будет отображаться сообщение об ошибке.

       Убедитесь, что любая часть указанного URL-адреса не содержит символы ? и #, а части Домен и Порт не содержат символ @. В противном случае URL-адрес будет импортирован не полностью.
     - Если вы хотите добавить в критерии фильтрации протокол или порт сетевых соединений, то в окне **URL** введите в поле любое значение и нажмите на кнопку **Добавить**. В появившихся

ниже полях **Протокол** и **Порт** укажите необходимые значения.

Например, вы можете запретить доступ ко всем веб-ресурсам по протоколу HTTP.

- **Имя файла**.

  Вы можете добавить в критерии фильтрации название конкретного файла или использовать регулярные выражения. Например, вы можете запретить загрузку исполняемых файлов с расширением exe, указав значение `*.exe`.

- **Тип файла**.

  Вирус или другая программа, представляющая угрозу, может распространяться в исполняемом файле, переименованном в файл с другим расширением, например, txt. Если вы выбрали критерий фильтрации **Имя файла** и указали значение `*.exe`, то такой файл не будет обработан программой. Если же вы выбрали фильтрацию файлов по формату, то программа проверяет истинный формат файла, вне зависимости от его расширения. Если в результате проверки выясняется, что файл имеет формат EXE, то программа обрабатывает его в соответствии с правилом.

- **Размер файла, КБ**.

  С помощью этого критерия вы можете контролировать объем сетевого трафика организации. Например, запретить загрузку файлов, размер которых превышает 700 МБ.

- **MIME-тип части HTTP-сообщения**.

  С помощью этого критерия вы можете контролировать доступ к multipart-объектам в соответствии с содержимым их составных частей.

- **MIME-тип HTTP-сообщения**.

  С помощью этого критерия вы можете контролировать доступ к объектам в соответствии с их содержимым. Например, вы можете запретить воспроизведение потокового видео-контента, указав значение `video/*`. Примеры указания MIME-типов объектов см. в Приложении 4 (см. раздел "Приложение 4. MIME-типы объектов" на стр. 227).

  > При указании `multipart/*` учитывается общий заголовок Content-Type объекта. Отдельные составные части объекта не обрабатываются. Для фильтрации трафика по составным частям multipart-объекта требуется использовать критерий **MIME-тип части HTTP-сообщения**.

- **MD5**.

  Вы можете запретить доступ к объекту, указав его MD5-хеш. Это может понадобиться, если вы получили информацию о вирусе или другой программе, представляющей угрозу, из сторонней системы и знаете только его MD5-хеш.

- **SHA256**.

  Вы можете запретить доступ к объекту, указав его SHA2-хеш. Это может понадобиться, если вы получили информацию о вирусе или другой программе, представляющей угрозу, из сторонней системы и знаете только его SHA2-хеш.

- **Направление трафика**.

  С помощью этого критерия вы можете настроить обработку всех входящих или исходящих соединений.

- **HTTP-метод**.

С помощью этого критерия вы можете контролировать доступ к трафику в зависимости от используемого HTTP-метода.

- **HTTP Content-Length, КБ**.

  С помощью HTTP-заголовка Content-Length вы можете контролировать доступ к трафику в зависимости от длины тела HTTP-сообщения. Если заголовок Content-Length присутствует, то программа использует его значение для применения критериев фильтрации трафика. Если этот заголовок отсутствует, то значение Content-Length считается пустым и не учитывается при обработке трафика.

  Доступно только для правил обхода.

8. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
9. Если вы добавили более одного критерия, в раскрывающемся списке рядом с названием блока **Фильтрация трафика** выберите логический оператор:
   - Если вы хотите, чтобы правило срабатывало при соблюдении хотя бы одного из добавленных условий, выберите **любой из**.
   - Если вы хотите, чтобы правило срабатывало только при одновременном соблюдении всех добавленных условий, выберите **все из**.
10. Нажмите на кнопку **Сохранить**.

Фильтрация трафика будет настроена.

Добавление исключения для правила обработки трафика

► *Чтобы добавить исключение для правила обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.

4. Выберите правило обработки трафика, для которого вы хотите добавить исключение.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Выберите закладку **Исключения**.
7. Нажмите на кнопку **+ Добавить исключение**.

   Появится блок параметров исключения **Исключение**.
8. Добавьте инициатора соединения. Для этого нажмите на кнопку  .
9. Укажите следующие параметры:
   a. В раскрывающемся списке **Инициатор** выберите один из следующих вариантов:
      - **Имя пользователя**.
      - **LDAP: group canonicalName**.
      - **LDAP: user distinguishedName**.
      - **IP-адрес**.
      - **User agent**.
   b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
   c. Если вы хотите добавить нового инициатора соединения, повторите действия по добавлению инициатора соединения.
10. Добавьте критерий фильтрации трафика. Для этого нажмите на кнопку  .
11. Укажите следующие параметры:
    a. В раскрывающемся списке **Фильтрация трафика** выберите один из следующих вариантов:
       - **Категория**.
       - **URL**.
       - **Имя файла**.
       - **Тип файла**.
       - **Размер файла, КБ**.
       - **MIME-тип HTTP-сообщения**.
       - **MIME-тип части HTTP-сообщения**.
       - **MD5**.
       - **SHA256**.
       - **Направление трафика**.
       - **HTTP-метод**.
    b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
    c. Если вы хотите добавить новый критерий фильтрации, повторите действия по добавлению критерия.
12. Нажмите на кнопку **Сохранить**.

Исключение для правила обработки трафика будет добавлено.

Настройка расписания работы правила обработки трафика

► *Чтобы настроить расписание работы правила обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   > Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, расписание работы которого вы хотите настроить.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Выберите закладку **Расписание**.
7. Если вы хотите отключить правило после наступления запланированной даты, установите флажок **Отключить правило** и во всплывающем календаре укажите дату и время завершения действия правила.
8. Если вы хотите, чтобы правило действовало в определенные дни недели и часы, выполните следующие действия:
   a. Установите флажок **Задать расписание действия правила**.
   b. Установите флажки рядом с названиями дней недели, в которые будет действовать правило.
   c. Укажите период действия правила.
9. Нажмите на кнопку **Сохранить**.

Расписание работы правила обработки трафика будет настроено.

kaspersky

Изменение правила обработки трафика

► *Чтобы изменить правило обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, которое вы хотите изменить.

   Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно изменения правила.
6. Внесите необходимые изменения.
7. Нажмите на кнопку **Сохранить**.

Правило обработки трафика будет изменено.

Удаление правила обработки трафика

► *Чтобы удалить правило обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.

3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления правила обработки трафика.
6. Нажмите на кнопку **Да**.

Правило обработки трафика будет удалено.

Создание копии правила обработки трафика

► *Чтобы скопировать правило обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, которое вы хотите скопировать.

   Откроется окно с информацией о правиле обработки трафика.
5. Нажмите на кнопку **Копировать**.

   Откроется окно создания правила обработки трафика. Все параметры правила обработки трафика будут скопированы.
6. Измените имя копии правила обработки трафика.
7. Нажмите на кнопку **Добавить**.

Будет создана копия правила обработки трафика.

Включение и отключение правила обработки трафика

► *Чтобы включить или отключить правило обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, которое вы хотите включить или отключить.

   Откроется окно с информацией о правиле.
5. Выполните одно из следующих действий:
   - Если вы хотите включить правило, нажмите на кнопку **Включить**.

     Правило будет включено.
   - Если вы хотите отключить правило, нажмите на кнопку **Отключить**.

     Правило будет отключено.

Изменение порядка применения правил

Правила проверяются в порядке расположения в таблице правил обработки трафика сверху вниз. В рамках группы правила также проверяются по порядку сверху вниз. Изменение порядка применения правил выполняется с помощью перемещения в таблице правил обработки трафика.

► *Чтобы изменить порядок применения правил, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;

- для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

> Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. В строке с названием правила или группы правил в левой части окна нажмите на значок  и, удерживая левую клавишу мыши, перетащите эту строку в нужное место таблицы.

> Перемещая строку **Правила рабочей области**, вы изменяете приоритет правил рабочей области.

5. Нажмите на кнопку **Сохранить**.

Порядок применения правил будет изменен в соответствии с новым расположением правил в таблице.

Работа с группами правил обработки трафика

Вы можете объединять правила доступа и правила защиты в группы, чтобы задать порядок их проверки. Создание групп для правил обхода недоступно.

Kaspersky Web Traffic Security проверяет группы по списку сверху вниз. Внутри каждой группы правила также проверяются согласно следованию в таблице. Вы можете изменять приоритет группы и правила внутри группы, перемещая их вверх или вниз.

Создание группы правил обработки трафика

► *Чтобы создать группу правил обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

> Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Доступ**.
   - **Защита**.
4. Нажмите на кнопку **Добавить группу**.

   Откроется окно создания группы правил.
5. В поле **Название** введите название новой группы правил.

   Название должно быть уникально в рамках рабочей области, если вы создаете группу правил рабочей области, или среди групп раздела **Глобальная**, если вы создаете группу правил вне рабочих областей.
6. Нажмите на кнопку **Добавить**.

Группа правил обработки трафика будет создана.

Изменение группы правил обработки трафика

► *Чтобы изменить группу правил обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Доступ**.
   - **Защита**.
4. Выберите группу правил, которую вы хотите изменить.

   Откроется окно с информацией о группе правил.
5. Нажмите на кнопку **Изменить**.
6. В поле **Название** введите новое название группы правил.

   Название должно быть уникально в рамках рабочей области, если вы создаете группу правил рабочей области, или среди групп раздела **Глобальная**, если вы создаете группу правил вне рабочих областей.

7. Нажмите на кнопку **Сохранить**.

Группа правил обработки трафика будет изменена.

Удаление группы правил обработки трафика

► *Чтобы удалить группу правил обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Доступ**.
   - **Защита**.
4. Выберите группу правил, которую вы хотите удалить.

   Откроется окно с информацией о группе правил.
5. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления группы правил обработки трафика.
6. Нажмите на кнопку **Да**.

Группа правил обработки трафика будет удалена.

Настройка политики защиты по умолчанию

Политика защиты по умолчанию применяется к веб-ресурсам, которые не удовлетворили критериям фильтрации ни одного из правил обработки трафика. В параметрах политики вам требуется установить для каждого типа объекта действие, которое программа должна выполнять с этим объектом.

► *Чтобы настроить политику защиты по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Политика защиты по умолчанию** выберите действия, которые программы должна выполнять с объектами следующих типов:
   - **Вредоносная программа**:
     - **Заблокировать**.
     - **Заблокировать, по возможности вылечить**.

    - **Пропустить проверку**.
- **Объекты, обнаруженные KATA**:
    - **Заблокировать**.
    - **Пропустить проверку**.
- **Фишинг**:
    - **Заблокировать**.
    - **Пропустить проверку**.
- **Вредоносная ссылка**:
    - **Заблокировать**.
    - **Пропустить проверку**.
- **Зашифрованный объект**:
    - **Заблокировать**.
    - **Пропустить проверку**.
- **Документ с макросом**:
    - **Заблокировать**.
    - **Пропустить проверку**.

  По умолчанию для **Вредоносная программа** установлено значение **Заблокировать, по возможности вылечить**. Для остальных типов объектов установлено значение **Заблокировать**.

3. Нажмите на кнопку **Сохранить**.

Политика защиты по умолчанию будет настроена. Если по результатам проверки программа не обнаружит угроз, доступ к веб-ресурсу будет разрешен.

Мониторинг работы правил обработки трафика

После того как правила обработки трафика вступают в силу, вы можете просматривать информацию об их выполнении в разделе **События**. При возникновении вопросов о работе правила вы можете найти это правило в таблице раздела **Правила** и посмотреть заданные в нем параметры.

Обработка запросов пользователей о доступе к веб-ресурсам

Если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно, он может обратиться к администратору локальной сети организации. В этом случае необходимо выяснить, в рамках какого правила обработки трафика был запрещен доступ. Для этого нужно найти событие в журнале по указанным пользователем параметрам.

► *Чтобы выяснить причину блокировки доступа к веб-ресурсу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.

2. Выберите закладку **Трафик** при ее наличии.
3. Нажмите на кнопку **Добавить условие**.
4. Настройте фильтр по имени обратившегося пользователя:
   a. В левом раскрывающемся списке выберите **Пользователь**.
   b. В центральном раскрывающемся списке выберите **Равняется**.
   c. В правом поле введите имя пользователя.
5. Нажмите на кнопку **Добавить условие**.
6. Настройте фильтр по веб-адресу заблокированного веб-ресурса:
   a. В левом раскрывающемся списке выберите **URL**.
   b. В центральном раскрывающемся списке выберите **Равняется**.
   c. В правом поле введите веб-адрес заблокированного веб-ресурса.
7. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации. В графе **Название правила** вы можете посмотреть правило обработки трафика, согласно которому пользователю запрещен доступ к веб-ресурсу.

Получение статистики о доступе к веб-ресурсам

В целях мониторинга сетевой активности пользователей вам может потребоваться получить статистику о посещении определенного веб-ресурса или о сетевых соединениях конкретных пользователей. Для этого вы можете отфильтровать события в журнале событий и экспортировать полученный результат в файл формата CSV.

► *Чтобы получить статистику о доступе к веб-ресурсам, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите закладку **Трафик** при ее наличии.
3. Нажмите на кнопку **Добавить условие**.
4. Настройте фильтр событий с помощью появившихся раскрывающихся списков:
   a. В левом раскрывающемся списке выберите критерий фильтрации.
   b. В центральном раскрывающемся списке выберите оператор сравнения.

      Для каждого критерия фильтрации доступен свой релевантный набор операторов сравнения. Например, при выборе критерия **Направление** доступны операторы **Равняется** и **Не равняется**.

   c. В зависимости от выбранного критерия фильтрации выполните одно из следующих действий:
      - Укажите в поле справа от оператора сравнения один или несколько символов, по которым вы хотите выполнить поиск событий.
      - В правом раскрывающемся списке выберите вариант условия, по которому вы хотите выполнить поиск событий.

      Например, для поиска полного совпадения по имени пользователя введите имя пользователя.

5. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтрации.

6. Нажмите на кнопку **Экспортировать**.

Файл с отфильтрованными событиями будет сохранен в папке загрузки браузера в формате CSV.

При конвертации полученного файла CSV в другие форматы необходимо учитывать, что в качестве разделителя полей используется точка с запятой.

Просмотр таблицы правил обработки трафика

Таблица правил обработки трафика отображается в разделе **Правила**. Если вы перешли в веб-интерфейс отдельной рабочей области, то в таблице отображаются только правила обработки трафика для этой рабочей области.

В таблице правил обработки трафика содержится следующая информация:

1. **Название**. Название правила обработки трафика.
2. **Действие**. Действие, которое выполняет правило обработки трафика.

   В правилах обхода возможны следующие действия:

   - **Разрешить без проверки**.
   - **Заблокировать**.
   - **Перенаправить**.

   В правилах доступа возможны следующие действия:

   - **Заблокировать**.
   - **Разрешить**.
   - **К следующей группе**.
   - **Перенаправить**.

   В правилах защиты возможны следующие действия:

   - **Заблокировать**.
   - **Заблокировать, по возможности вылечить**.
   - **Пропустить проверку**.

3. **Статус**. Использование правила обработки трафика во время проверки веб-ресурсов.

   Правило обработки трафика может находиться в одном из следующих состояний:

   - **Выключено**.
   - **Включено**.

4. **Комментарий**. Комментарий к правилу обработки трафика.

kaspersky

Просмотр информации о правиле обработки трафика

► *Чтобы просмотреть информацию о правиле обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о правиле.

Окно содержит следующие закладки:

1. **Общие параметры**.

   Общие параметры правила обработки трафика:

   a. **Статус** – использование правила обработки трафика при проверке веб-ресурсов.

   b. **Действие** – действие, которое выполняет правило обработки трафика.

   c. **Название правила** – название правила обработки трафика.

   d. **Комментарий** – комментарий к правилу обработки трафика.
2. **Исключения**.

   Информация о каждом исключении из правила обработки трафика отображается в отдельном блоке параметров **Исключение**:

   a. **Инициатор** – инициатор соединения.

   b. **Фильтрация трафика** – фильтр трафика.
3. **Расписание**.

   Расписание работы правила обработки трафика. Отображается дата отключения правила, а также дни недели и периоды работы правила.

kaspersky

Управление рабочими областями

Рабочая область – набор параметров и прав доступа, применимых к выделенной группе пользователей. Например, вы можете создавать рабочие области для подразделений компании или для управляемых организаций (если вы являетесь поставщиком услуг).

Использование рабочих областей предоставляет следующие возможности:

- разграничение прав доступа к каждой рабочей области между разными администраторами;
- создание правил обработки трафика, действующих только для пользователей отдельной рабочей области;
- настройка индивидуальной страницы блокировки.

В этом разделе

Сценарий настройки рабочей области

Настройка рабочей области включает в себя следующие этапы.

1. Добавление рабочей области (на стр. 101)
2. Добавление роли администратора рабочей области (см. раздел "Добавление роли" на стр. 116), если требуется

   В программе доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. 114). Вы можете назначить учетной записи администратора одну из этих ролей. Если набор прав для ролей по умолчанию вам не подходит, вы можете добавить новую роль.
3. Назначение роли администратора рабочей области (см. раздел "Назначение роли" на стр. 118)

   После того, как вы назначили пользователю роль администратора рабочей области, он может войти в веб-интерфейс программы под своей доменной учетной записью. Пользователю будут доступны разделы веб-интерфейса в соответствии с предоставленными ему правами доступа.

   Вы можете добавлять несколько администраторов для одной рабочей области или создавать другие роли с нужным вам набором прав доступа.
4. Создание правил обработки трафика для этой рабочей области (см. раздел "Сценарий настройки доступа к веб-ресурсам" на стр. 76)

5. Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 142), если требуется

   После создания рабочей области пользователям отображается страница блокировки по умолчанию. Вы можете настроить индивидуальную страницу блокировки, которая будет отображаться только пользователям этой рабочей области.

Просмотр таблицы рабочих областей

Таблица рабочих областей отображается в разделе **Рабочие области** окна веб-интерфейса программы.

В таблице рабочих областей содержится следующая информация:

1. **Название** – название рабочей области.
2. **Критерии** – критерии для определения трафика рабочей области.
3. **Выделено лицензий** – количество лицензий, выделенных для этой рабочей области.
4. **Комментарий** – комментарий к рабочей области.

Просмотр информации о рабочей области

► *Чтобы просмотреть информацию о рабочей области, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.
2. Выберите рабочую область, информацию о которой вы хотите просмотреть.

   Откроется окно с информацией о рабочей области.

Окно содержит следующую информацию:

- Закладка **Общие**:
  - **Название** – название рабочей области.
  - **Комментарий** – комментарий к рабочей области.
  - **Закрепить клиентские лицензии за рабочей областью** – количество лицензий, выделенных для этой рабочей области.
  - **Критерии** – критерии для определения трафика рабочей области.
- Закладка **Страница блокировки** – параметры страницы блокировки для рабочей области (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 142).

Настройка отображения таблицы рабочих областей

► *Чтобы настроить отображение таблицы рабочих областей, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.

Откроется таблица рабочих областей.

2. По кнопке  откройте меню отображения таблицы рабочих областей.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице рабочих областей.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите обновить информацию о рабочих областях, нажмите на кнопку **Обновить**.

   Информация о рабочих областях будет обновлена.

Отображение таблицы рабочих областей будет настроено.

Добавление рабочей области

► *Чтобы добавить рабочую область, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.
2. Нажмите на кнопку **Добавить рабочую область**.

   Откроется окно добавления рабочей области.
3. В поле **Название** укажите название рабочей области.
4. В поле **Комментарий** укажите комментарий к рабочей области.

   Необязательный параметр.
5. Если вы хотите закрепить за этой рабочей областью часть клиентских лицензий, выполните следующие действия:
   a. Установите флажок **Закрепить клиентские лицензии за рабочей областью**.
   b. Укажите количество клиентских лицензий, которые вы хотите закрепить за этой рабочей областью.
6. Добавьте критерий для определения трафика рабочей области. Для этого выполните следующие действия:
   a. В блоке критериев для определения трафика рабочей области **Критерии** в раскрывающемся списке выберите один из следующих вариантов:
      - **LDAP: group canonicalName**.
      - **LDAP: user distinguishedName**.
      - **IP-адрес**.
   b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
7. Если вы хотите добавить новый критерий рабочей области, выполните следующие действия:
   a. Нажмите на кнопку  .
   b. Повторите действия пункта 6 по добавлению критерия рабочей области.
8. Если вы указали несколько критериев рабочей области, по ссылке справа от названия блока

Критерии вы можете выбрать один из следующих вариантов:

- **любые из**, если вы хотите, чтобы для определения трафика рабочей области было достаточно соответствия любому из добавленных критериев.
- **все из**, если вы хотите, чтобы для определения трафика рабочей области требовалось соответствие всем добавленным критериям.

9. Нажмите на кнопку **Добавить**.

Рабочая область будет добавлена.

Изменение параметров рабочей области

► *Чтобы изменить параметры рабочей области, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.

   Откроется таблица рабочих областей.
2. Выберите рабочую область, параметры которой вы хотите изменить.

   Откроется окно **Просмотреть рабочую область**.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить рабочую область**.
4. Внесите необходимые изменения в параметры рабочей области.
5. Нажмите на кнопку **Сохранить**.

Параметры рабочей области будут изменены.

Удаление рабочей области

► *Чтобы удалить рабочую область, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.

   Откроется таблица рабочих областей.
2. Выберите рабочую область, которую вы хотите удалить.

   Откроется окно с информацией о рабочей области.
3. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления рабочей области.
4. Нажмите на кнопку **Да**.

Рабочая область будет удалена.

kaspersky

Переключение между рабочими областями в веб-интерфейсе программы

Локальный администратор имеет доступ ко всем рабочим областям. Вы также можете предоставить одному пользователю доступ к нескольким рабочим областям.

При создании и настройке рабочих областей, а также впоследствии при работе с неисправностями программы пользователю может понадобиться переключаться между рабочими областями. Отображение раздела переключения между рабочими областями в дереве веб-интерфейса определяется по алгоритму, описанному в таблице ниже.

Таблица 5. Алгоритм отображения рабочих областей в веб-интерфейсе программы

Наличие рабочих областей	Права вне рабочих областей		Права на параметры рабочих областей	Отображение в веб-интерфейсе
	Наличие прав на действия с кластером и с параметрами программы	Наличие прав на действия с рабочими областями, ролями, правилами, событиями обработки трафика, а также просмотр раздела Мониторинг		
Нет	Не влияет на отображение раздела переключения	Не влияет на отображение раздела переключения.	Недоступно.	Раздел переключения между рабочими областями не отображается.
Есть	Нет	Есть	Нет.	Раздел переключения между рабочими областями не отображается.
	Нет	Нет	Есть права только в одной рабочей области.	В разделе переключения отображается название рабочей области, но список рабочих областей недоступен.
	Нет	Нет	Есть разрешения в нескольких рабочих областях.	В разделе переключения доступны только те рабочие области, в которых у пользователя есть хотя бы одно разрешение. Раздел **Глобальная** не отображается.

Наличие рабочих областей	Права вне рабочих областей		Права на параметры рабочих областей	Отображение в веб-интерфейсе
	Наличие прав на действия с кластером и с параметрами программы	Наличие прав на действия с рабочими областями, ролями, правилами, событиями обработки трафика, а также просмотр раздела Мониторинг		
	Нет	Есть	Не влияет на отображение раздела переключения.	В разделе переключения доступен список всех рабочих областей, но не отображается раздел **Глобальная**.
	Есть	Есть	Не влияет на отображение раздела переключения.	В разделе переключения доступен список всех рабочих областей, а также раздел **Глобальная**.

► *Чтобы переключиться между рабочими областями, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Глобальная**, если вы находитесь вне рабочих областей, или раздел с названием вашей организации, если вы находитесь в веб-интерфейсе рабочей области.
2. В раскрывшейся панели выберите название рабочей области, в которую вы хотите перейти.

Отобразится веб-интерфейс выбранной рабочей области. В дереве слева будут доступны разделы веб-интерфейса в соответствии с правами доступа текущего пользователя.

kaspersky

Работа с ролями и учетными записями пользователей

Вы можете создавать различные роли для учетных записей пользователей программы в зависимости от прав, которыми они должны обладать. Таблица ролей и учетных записей пользователей, обладающих этими ролями, отображается в разделе **Пользователи** окна веб-интерфейса программы.

Для каждой роли вы можете задать набор прав, которыми будет обладать роль. Кроме того, в программе доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. 114), создаваемые во время установки программы:

- *Superuser* с полным набором прав.
- *Viewer*, обладающая правами только на просмотр информации в веб-интерфейсе программы.

Удаление и изменение роли по умолчанию недоступно.

Вы можете добавлять роли для рабочей области или вне рабочих областей.

Если пользователю назначена роль для рабочей области, то права этой роли распространяются только на параметры данной рабочей области. Пользователь не сможет выполнять действия с параметрами в других рабочих областях.

Если пользователю назначена роль вне рабочих областей, то разрешения этой роли распространяются на параметры всех рабочих областей.

В этом разделе

Ролевое разграничение доступа к функциям программы

В зависимости от назначенной роли пользователю будут доступны определенные разделы веб-интерфейса и операции с параметрами программы.

Описание операций с параметрами программы в зависимости от назначенного права, приведено в таблице

ниже.

Таблица 6. Операции, доступные при назначении прав

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать разделы Мониторинг и Отчеты	Просмотр всей информации в разделах **Мониторинг** (см. раздел "**Мониторинг работы программы**" на стр. 62) и **Отчеты** (см. раздел "**Отчеты**" на стр. 67).	Да	Просмотр информации в разделе **Мониторинг** со следующими ограничениями: • не отображается график **Работоспособность системы**; • отсутствует возможность фильтрации по узлам и по рабочим областям. Просмотр, скачивание (см. раздел "Скачивание отчета на компьютер" на стр. 68) и удаление (см. раздел "Удаление отчета" на стр. 68) всех ранее созданных отчетов, а также создание новых отчетов (см. раздел "Создание отчета" на стр. 67) только для текущей рабочей области.
Просматривать события обработки трафика	Просмотр журнала событий (на стр. 70) обработки трафика рабочих областей и вне рабочих областей, а также экспорт событий обработки трафика в разделе **События**.	Да	Просмотр журнала событий (на стр. 70) обработки трафика рабочих областей, а также экспорт событий обработки трафика в разделе **События**.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать системные события	Просмотр журнала системных событий (см. раздел "Просмотр журнала событий" на стр. 70) программы, а также экспорт системных событий программы в разделе **События**.	Нет	Функциональность отсутствует.
Создавать/изменять правила	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 78), правил доступа (см. раздел "Добавление правила доступа" на стр. 79) и правил защиты (см. раздел "Добавление правила защиты" на стр. 81) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 89) в разделе **Правила**.	Да	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 78), правил доступа (см. раздел "Добавление правила доступа" на стр. 79) и правил защиты (см. раздел "Добавление правила защиты" на стр. 81) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 89) в разделе **Правила**.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать правила	Просмотр таблицы правил обработки трафика (на стр. 97) для рабочих областей и вне рабочих областей в разделе **Правила**. При назначении этого права пользователь не сможет добавлять или удалять правила, а также изменять их параметры.	Да	Просмотр таблицы правил обработки трафика (на стр. 97) для текущей рабочей области в разделе **Правила**. При назначении этого разрешения пользователь не сможет добавлять или удалять правила, а также изменять их параметры.
Удалять правила	Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 89) для рабочих областей и вне рабочих областей в разделе **Правила**.	Да	Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 89) для текущей рабочей области в разделе **Правила**.
Создавать/изменять рабочие области	Добавление рабочих областей (см. раздел "Добавление рабочей области" на стр. 101) и изменение параметров рабочих областей (см. раздел "Изменение параметров рабочей области" на стр. 102) в разделе **Рабочие области**.	Да	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать рабочие области	Просмотр таблицы рабочих областей (на стр. 100) в разделе **Рабочие области**. При назначении этого права пользователь не сможет добавлять и удалять рабочие области, а также изменять их параметры.	Да	Функциональность отсутствует.
Удалять рабочие области	Удаление рабочих областей (см. раздел "Удаление рабочей области" на стр. 102) в разделе **Рабочие области**.	Да	Функциональность отсутствует.
Создавать/изменять роли	Добавление ролей (см. раздел "Добавление роли" на стр. 116) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 117) в разделе **Пользователи**.	Да	Добавление ролей (см. раздел "Добавление роли" на стр. 116) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 117) в разделе **Пользователи**.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать роли	Просмотр списка ролей для рабочих областей и вне рабочих областей в разделе **Пользователи**. При назначении этого права пользователь не сможет добавлять или удалять роли, а также изменять их параметры.	Да	Просмотр списка ролей для текущей рабочей области в разделе **Пользователи**. При назначении этого разрешения пользователь не сможет добавлять или удалять роли, а также изменять их параметры.
Удалять роли	Удаление ролей (см. раздел "Удаление роли" на стр. 118) для рабочих областей и вне рабочих областей в разделе **Пользователи**.	Да	Удаление ролей (см. раздел "Удаление роли" на стр. 118) для текущей рабочей области в разделе **Пользователи**.
Создавать/изменять/удалять узлы	Добавление (см. раздел "Добавление узла в кластер" на стр. 124) и удаление узлов кластера (см. раздел "Удаление узла из кластера" на стр. 125), а также изменение их параметров (см. раздел "Изменение параметров узла" на стр. 125) в разделе **Узлы**.	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Получать диагностическую информацию	Запуск трассировки (на стр. 201), изменение уровня трассировки (на стр. 202), а также просмотр журналов трассировки (на стр. 202) узлов кластера. При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.
Проверять целостность данных	Проверка целостности данных (на стр. 127) на узлах кластера. При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать информацию об узлах	Просмотр информации об узлах (см. раздел "Просмотр информации об узле кластера" на стр. 122) в разделе **Узлы**. При назначении этого права пользователь не сможет добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.
Изменять параметры	Изменение параметров программы в разделе **Параметры**.	Нет	Функциональность отсутствует.
Просматривать параметры	Просмотр параметров программы в разделе **Параметры**, При назначении этого права пользователь не сможет изменять параметры программы.	Нет	Функциональность отсутствует.
Управлять доступом SSH	Добавление и удаление открытого ключа SSH (см. раздел "Подключение к узлам кластера по протоколу SSH" на стр. 128).	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Создавать/изменять страницу блокировки	Функциональность отсутствует.	Нет	Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 142) для текущей рабочей области.
Просматривать страницу блокировки	Функциональность отсутствует.	Нет	Просмотр страницы блокировки для текущей рабочей области.

Соответствие между доступными разделами веб-интерфейса программы и назначенными пользователю правами представлено в таблице ниже.

Таблица 7. Доступ к разделам веб-интерфейса в зависимости от назначенных прав

Область применения	Право	Раздел веб-интерфейса, к которому предоставляется доступ	
		вне рабочих областей	в рабочей области
Вне рабочих областей	**Просматривать разделы Мониторинг и Отчеты**	**Мониторинг**	**Мониторинг**
	Просматривать события обработки трафика	**События**	**События**
	Просматривать системные события	**События**	Недоступно
	Создавать/изменять правила	**Правила**	**Правила**
	Просматривать правила		
	Удалять правила		
	Создавать/изменять рабочие области	**Рабочие области**	**Параметры рабочей области**
	Просматривать рабочие области		
	Удалять рабочие области		
	Создавать/изменять роли	**Пользователи**	**Пользователи**
	Просматривать роли		

Область применения	Право	Раздел веб-интерфейса, к которому предоставляется доступ	
		вне рабочих областей	в рабочей области
	Удалять роли		
	Создавать/изменять/удалять узлы	**Узлы**	Недоступно
	Получать диагностическую информацию		
	Проверять целостность данных		
	Просматривать информацию об узлах		
	Изменять параметры	**Параметры**	Недоступно
	Просматривать параметры		
	Управлять доступом SSH		
В рабочей области	**Просматривать разделы Мониторинг и Отчеты**	Недоступно	**Мониторинг**
	Просматривать события обработки трафика	Недоступно	**События**
	Создавать/изменять правила	Недоступно	**Правила**
	Просматривать правила		
	Удалять правила		
	Создавать/изменять роли	Недоступно	**Пользователи**
	Просматривать роли		
	Удалять роли		
	Создавать/изменять страницу блокировки	Недоступно	**Параметры рабочей области**
	Просматривать страницу блокировки		

Набор прав для ролей по умолчанию

После установки программы в разделе **Пользователи** отображаются две роли по умолчанию. Кроме того, роли по умолчанию создаются в рамках каждой рабочей области. При удалении рабочей области роли по умолчанию, созданные в этой рабочей области, также удаляются.

Набор прав для ролей по умолчанию вне рабочих областей и в рабочей области представлен в таблице ниже.

Таблица 8. Набор прав для ролей по умолчанию

Право	Вне рабочих областей		В рабочей области	
	Superuser	Viewer	Superuser	Viewer
Просматривать разделы Мониторинг и Отчеты	Есть	Есть	Есть	Есть
Просматривать события обработки трафика	Есть	Есть	Есть	Есть
Просматривать системные события	Есть	Есть	Недоступно	Недоступно
Создавать/изменять правила	Есть	Нет	Есть	Нет
Просматривать правила	Есть	Есть	Есть	Есть
Удалять правила	Есть	Нет	Есть	Нет
Создавать/изменять рабочие области	Есть	Нет	Недоступно	Недоступно
Просматривать рабочие области	Есть	Есть	Недоступно	Недоступно
Удалять рабочие области	Есть	Нет	Недоступно	Недоступно
Создавать/изменять роли	Есть	Нет	Есть	Нет
Просматривать роли	Есть	Есть	Есть	Есть
Удалять роли	Есть	Нет	Есть	Нет
Создавать/изменять/удалять узлы	Есть	Нет	Недоступно	Недоступно
Получать диагностическую информацию	Есть	Нет	Недоступно	Недоступно
Проверять целостность данных	Есть	Нет	Недоступно	Недоступно
Просматривать информацию об узлах	Есть	Есть	Недоступно	Недоступно
Изменять параметры	Есть	Нет	Недоступно	Недоступно

Право	Вне рабочих областей		В рабочей области	
	Superuser	Viewer	Superuser	Viewer
Просматривать параметры	Есть	Есть	Недоступно	Недоступно
Управлять доступом SSH	Есть	Нет	Недоступно	Недоступно
Создавать/изменять страницу блокировки	Недоступно	Недоступно	Есть	Нет
Просматривать страницу блокировки	Недоступно	Недоступно	Есть	Есть

Добавление роли

► *Чтобы добавить роль, выполните следующие действия:*

1. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите добавить роль для одной рабочей области.
   - **Глобальная**, если вы хотите добавить роль вне рабочих областей.
2. Выберите раздел **Пользователи**.
3. Откроется список ролей и учетных записей.
4. Нажмите на кнопку **Добавить**.

   Откроется окно добавления роли.
5. В поле **Имя** введите имя роли.
6. В списке **Права** установите флажки рядом с теми правами, которыми должна обладать роль (см. раздел "Ролевое разграничение доступа к функциям программы" на стр. 105):
7. Нажмите на кнопку **Добавить**.

Роль будет добавлена.

Просмотр информации о роли

► *Чтобы просмотреть информацию о роли, выполните следующие действия:*

1. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите просмотреть информацию о роли конкретной рабочей области.
   - **Глобальная**, если вы хотите просмотреть информацию о роли вне рабочих областей.

2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.

3. В левой части окна выберите роль, информацию о которой вы хотите просмотреть.

Отобразится следующая информация:

- На закладе **Учетные записи** отображается список учетных записей пользователей, которым назначена выбранная роль. Вы можете отзывать роль (см. раздел "Отзыв роли" на стр. 119) или назначать ее (см. раздел "Назначение роли" на стр. 118) новым пользователям.
- На закладке **Права** отображается набор прав, которые получает пользователь при назначении ему этой роли. Вы можете изменять список прав (см. раздел "Изменение параметров роли" на стр. 117) для выбранной роли.

Изменение параметров роли

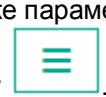
Изменение роли Superuser недоступно.

Вы можете изменить параметры роли: название роли, а также набор прав, которыми она обладает.

► *Чтобы изменить параметры роли, выполните следующие действия:*

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите изменить параметры роли для одной рабочей области
   - **Глобальная**, если вы хотите изменить параметры роли вне рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.

3. В блоке параметров **Роли** выберите роль, параметры которой вы хотите изменить, и нажмите на кнопку  .
4. В раскрывающемся списке выберите вариант **Изменить**.

   Откроется окно **Изменить роль**.

5. Если требуется, измените название роли в поле **Имя**.
6. Если требуется, измените набор прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Права**.
7. Нажмите на кнопку **Сохранить**.

Параметры роли будут изменены.

kaspersky

Удаление роли

Удаление роли Superuser недоступно.

► *Чтобы удалить роль, выполните следующие действия:*

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите удалить роль для одной рабочей области.
   - **Глобальная**, если вы хотите удалить роль вне рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В списке **Роли** выберите роль, которую вы хотите удалить.
4. Нажмите на кнопку  .
5. В раскрывающемся списке выберите вариант **Удалить**.

   Отобразится окно подтверждения удаления роли.
6. Нажмите на кнопку **Да**.

Роль будет удалена.

Назначение роли

► *Чтобы назначить роль для учетной записи, выполните следующие действия:*

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите предоставить пользователю разрешения на параметры одной рабочей области.
   - **Глобальная**, если вы хотите предоставить пользователю разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В списке **Роли** выберите роль, которую вы хотите назначить для учетной записи.
4. Нажмите на кнопку **Назначить роль**.

   Откроется окно **Назначить роль**.
5. В поле **Учетная запись (домен\имя для NTLM или user@REALM для Kerberos; значение чувствительно к регистру)** введите доменное имя учетной записи, которой вы хотите назначить роль.

6. Нажмите на кнопку **Сохранить**.

Роль будет назначена выбранной учетной записи.

Отзыв роли

► *Чтобы отозвать роль у пользователя, выполните следующие действия:*

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите отозвать у пользователя разрешения на параметры одной рабочей области.
   - **Глобальная**, если вы хотите отозвать у пользователя разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В левой части окна выберите роль, которую вы хотите отозвать.
4. На закладке **Учетные записи** установите флажки напротив тех пользователей, у которых вы хотите отозвать роль.
5. Нажмите на кнопку **Отозвать роль**.
6. В окне подтверждения нажмите на кнопку **Да**.

Роль будет отозвана у пользователя. Пользователь больше не сможет совершать действия с параметрами программы, которые были ему доступны в соответствии с правами этой роли.

Изменение пароля учетной записи Administrator

Учетная запись Administrator с правами суперпользователя позволяет входить в систему без использования внешних служб. Пароль данной учетной записи действует в течение одного года. После истечения срока действия пароля, при последующей попытке входа в веб-интерфейс программы администратору отобразится запрос на смену пароля. Аутентификация с учетной записью Administrator будет возможна только после смены пароля.

► *Чтобы изменить пароль учетной записи Administrator, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Локальный администратор**.
2. В поле **Старый пароль** введите текущий пароль учетной записи Administrator.

   > В первый раз этот пароль задается во время установки программы.

3. В поле **Новый пароль** введите новый пароль, удовлетворяющий требованиям к паролю.

   Требования к паролю приведены ниже под полем **Подтвердите пароль**.

4. В поле **Подтвердите пароль** введите новый пароль повторно.
5. Нажмите на кнопку **Сохранить**.

kaspersky

Управление кластером

После установки и первоначальной настройки (см. раздел "Установка и первоначальная настройка программы из rpm- или deb-пакета" на стр. 39) вы можете настраивать параметры в веб-интерфейсе программы. Для этого требуется объединить все узлы с установленной программой Kaspersky Web Traffic Security в кластер. Вы можете добавлять узлы в кластер (см. раздел "Добавление узла в кластер" на стр. 124) и удалять узлы из кластера (см. раздел "Удаление узла из кластера" на стр. 125). Вы можете назначить роль Управляющего узла (см. раздел "Изменение роли узла в кластере" на стр. 126) любому из узлов, входящих в кластер. Остальные серверы в кластере получат роль Подчиненный узел. Независимо от роли все узлы кластера будут осуществлять обработку трафика.

В разделе **Узлы** окна веб-интерфейса программы отображается таблица узлов кластера, а также следующая информация об узлах:

- **Состояние соединения с KSN/KPSN**.
- **Состояние баз**.
- **Лицензия**.

В этом разделе

Создание нового кластера

После установки программы требуется создать кластер для управления узлами через веб-интерфейс программы. Кроме того, вы можете создать несколько кластеров, чтобы управлять разными группами серверов отдельно друг от друга.

► *Чтобы создать новый кластер, выполните следующие действия:*

1. В веб-интерфейсе узла, которому вы хотите назначить роль Управляющий узел, нажмите на кнопку

Создать новый кластер.

2. Через несколько минут обновите страницу браузера.

   Откроется веб-интерфейс Управляющего узла.

Кластер будет создан. После этого вы можете добавлять в кластер Подчиненные узлы (см. раздел "Добавление узла в кластер" на стр. 124).

Настройка отображения таблицы узлов кластера

► *Чтобы настроить отображение таблицы узлов кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.

   Откроется таблица узлов кластера.

2. По кнопке  откройте меню отображения таблицы узлов кластера.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы узлов кластера будет настроено.

Просмотр информации об узле кластера

► *Чтобы просмотреть информацию об узле кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. Выберите узел, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об узле.

Окно содержит следующую информацию в зависимости от типа сервера:

1. Блок параметров **Информация об узле**:
   - **Отпечаток сертификата** – отпечаток сертификата сервера.
   - **Технология виртуализации** – название платформы виртуализации (отображается только при развертывании программы из ISO-файла на виртуальной машине).

     Возможны следующие значения:

     - **ACRN**.
     - **bhyve (гипервизор FreeBSD™)**.
     - **Bochs Emulator**.
     - **Linux KVM**.
     - **Microsoft Hyper-V**.

- **Не используется** – программа установлена на физическом сервере.
- **Oracle® VM VirtualBox**.
- **Parallels Desktop® или Server**.
- **QEMU**.
- **QNX**.
- **UML (user-mode Linux)**.
- **VMware™ Workstation или Server**.
- **Xen**.
- **z/VM**.

> В программе Kaspersky Web Traffic Security поддерживаются гипервизоры Microsoft Hyper-V и VMware ESXi, а также развертывание программы из ISO-файла на физическом сервере. Работоспособность программы при использовании других гипервизоров не гарантируется.

- **Комментарий** – дополнительная информация об узле. Необязательный параметр.
- **Роль текущего узла** – роль текущего узла в кластере.

2. Блок параметров **Обработка трафика**:
   - **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.
   - **Дата окончания срока действия лицензии**.
   - **Лицензия** – информация о лицензии и количестве дней до окончания срока действия лицензии.
   - **Тип лицензии** – тип лицензии (пробная или коммерческая).
   - **Серийный номер** – серийный номер лицензии.
   - **Состояние подключения к KSN/KPSN** – состояние соединения со службами KSN / KPSN.
   - **Антивирус** – состояние баз модуля Антивирус.
   - **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
   - **Отправка файлов в KATA** – наличие или отсутствие ошибок при отправке файлов в KATA (отображается только при включенном режиме **Отправлять файлы** (см. раздел "**Выбор режима интеграции**" на стр. 164)).
   - **Получение объектов из KATA** – наличие или отсутствие ошибок при получении объектов, обнаруженных KATA (отображается только при включенном режиме **Получать объекты** (см. раздел "**Выбор режима интеграции**" на стр. 164)).
   - **Обновление баз** – состояние баз программы, а также результат и время их последнего успешного обновления.
3. Блок параметров **Кеш LDAP** (отображается только при настроенной интеграции с доменом Active Directory):
   - **Подключение** – дата и время последнего успешного подключения к контроллеру домена Active Directory.
   - **Данные для подбора правил** – дата и время последнего успешного обновления данных об

учетных записях, используемых для подбора правил обработки трафика.

- **Автозаполнение учетных записей** – дата и время последнего успешного обновления данных, используемых для автозаполнения имен пользователей в веб-интерфейсе программы.

Если хотя бы на одном из этих этапов возникла ошибка, в таблице узлов кластера отображается сообщение об ошибке.

4. Блок параметров **Параметры**:
   - Для Управляющего узла:
     - **Применены** – время последнего успешного применения параметров к модулям программы.
     - **Время** – состояние синхронизации времени с гипервизором и с NTP-сервером (отображается только при развертывании программы из ISO-файла на виртуальной машине).
   - Для Подчиненного узла:
     - **Синхронизированы** – время последнего успешного получения параметров от Управляющего узла. Если параметры получены, вы можете назначить этому Подчиненному узлу роль Управляющего без потери заданных параметров.
     - **Применены** – время последнего успешного применения параметров к модулям программы.
     - **Время** – состояние синхронизации времени:
       - с сервером, на котором установлен Управляющий узел;
       - с гипервизором (отображается только при развертывании программы из ISO-файла на виртуальной машине);
       - с NTP-сервером (отображается только при развертывании программы из ISO-файла на виртуальной машине).

   Если статус имеет значение *Ошибка*, вы можете скопировать информацию об ошибке в буфер обмена по ссылке **Копировать** справа от статуса.

Добавление узла в кластер

► *Чтобы добавить узел в кластер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. Нажмите на кнопку **Добавить узел**.

   Откроется окно **Добавить узел**.
3. В поля **IP-адрес** и **Порт** введите IP-адрес и порт сервера с установленной программой, который вы хотите добавить в качестве узла кластера.
4. Если требуется, в поле **Комментарий** укажите дополнительную информацию о добавляемом узле.
5. В поле **Количество потоков проверки** укажите, сколько потоков трафика может обрабатывать ICAP-сервер одновременно.
6. Нажмите на кнопку **Далее**.
7. Сравните отпечатки сертификата в окне **Подтвердить узел** и в файле сертификата в папке сервиса nginx (/etc/nginx/kwts/controlapi.crt). Если отпечатки сертификата совпадают, нажмите на кнопку

Подтвердить.

Вы можете получить отпечаток сертификата с помощью следующей команды:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in
/etc/nginx/kwts/controlapi.crt
```

Узел будет добавлен в кластер и отобразится в таблице узлов на странице **Узлы**.

Изменение параметров узла

Вы не можете изменить IP-адрес и порт сервера, на котором установлена программа. При необходимости удалите узел из кластера (см. раздел "Удаление узла из кластера" на стр. 125) и добавьте в кластер новый узел (см. раздел "Добавление узла в кластер" на стр. 124) с нужным адресом.

► *Чтобы изменить параметры узла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите узел, параметры которого вы хотите изменить.

   Откроется окно параметров узла.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить узел**.
4. Если требуется, измените следующие параметры:
   - Дополнительную информацию об узле в поле **Комментарий**.
   - Количество одновременных потоков обработки трафика ICAP-сервером в поле **Количество потоков проверки**.

     Максимально допустимое значение: количество ядер процессора плюс один.
5. Нажмите на кнопку **Сохранить**.

   Если вы изменили параметр **Количество потоков проверки**, прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Параметры узла будут изменены.

Удаление узла из кластера

Удаление Управляющего узла недоступно.

При удалении узла из кластера программа не удаляется с сервера. Вы можете в любой момент добавить узел обратно в кластер и продолжить управление параметрами программы для этого узла.

► *Чтобы удалить узел из кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите удалить из кластера.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **Да**.

Узел будет удален из кластера. Информация об узле не будет отображаться в таблице узлов кластера.

Изменение роли узла в кластере

Вы можете назначить любому узлу кластера роль Управляющий узел. Остальные узлы будут иметь роль Подчиненный узел. Например, смена ролей может понадобиться при выходе из строя Управляющего узла или при необходимости удалить программу с этого сервера.

► *Чтобы назначить Управляющему узлу роль Подчиненный узел, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Назначить роль Подчиненный узел**.

Управляющий узел станет Подчиненным узлом. Откроется веб-интерфейс Подчиненного узла.

► *Чтобы назначить Подчиненному узлу роль Управляющий узел, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Перейти к управлению узлом**.

   В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль администратора программы.

   Откроется веб-интерфейс Подчиненного узла.
5. Нажмите на кнопку **Назначить роль Управляющий узел**.
6. В окне подтверждения нажмите на кнопку **Да**.

Подчиненный узел станет Управляющим узлом.

Удаление кластера

Удаление кластера возможно только при отсутствии Подчиненных узлов.

► *Чтобы удалить кластер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить кластер**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **Да**.

Кластер будет удален. Отобразится веб-интерфейс сервера с установленной программой, не входящего в кластер.

Проверка целостности данных

Чтобы убедиться, что компоненты программы установлены корректно, не изменены и не повреждены, вы можете запустить проверку целостности данных. При этом будут проверены MD5-хеши исполняемых файлов Kaspersky Web Traffic Security.

► *Чтобы проверить целостность данных, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Проверить целостность данных**.

   Откроется окно **Выбор узлов для проверки целостности данных**.
4. В таблице узлов кластера установите флажки напротив тех узлов, для которых вы хотите запустить проверку целостности.
5. Нажмите на кнопку **Запустить**.

   После окончания проверки отобразится таблица с результатами. Вы можете скачать список исполняемых файлов, в которых обнаружено нарушение целостности.

kaspersky

Подключение к узлам кластера по протоколу SSH

Администратор Kaspersky Web Traffic Security может подключиться к любому узлу кластера по протоколу SSH, чтобы работать с программой в режиме Technical Support Mode через командную строку. Для этого требуется сгенерировать ключи SSH и загрузить открытый ключ SSH через веб-интерфейс программы. После загрузки на сервер с Управляющим узлом этот ключ передается и сохраняется на всех узлах кластера.

Чтобы предотвратить несанкционированный доступ к системе, администратору требуется самостоятельно обеспечить защиту закрытого ключа SSH с помощью токена.

► *Чтобы загрузить открытый ключ SSH через веб-интерфейс программы, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры**, подраздел **Открытый ключ SSH**.
2. В поле **Описание** введите любую информацию о загружаемом ключе SSH.
3. В поле **Ключ SSH** скопируйте сгенерированный ранее открытый ключ SSH.
4. Нажмите на кнопку **Добавить**.

Открытый ключ SSH будет добавлен. Администратор Kaspersky Web Traffic Security сможет подключиться к любому узлу кластера при наличии соответствующего закрытого ключа SSH. Если вы хотите заменить ключ SSH, вам нужно удалить добавленный ранее ключ и добавить вместо него новый ключ.

► *Чтобы удалить открытый ключ SSH, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры**, подраздел **Ключ SSH**.
2. Нажмите на кнопку **Удалить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Открытый ключ SSH будет удален. Вы сможете добавить новый ключ.

Перезагрузка узла кластера

Перезагрузка через веб-интерфейс доступна только для программы, развернутой из ISO-образа. При установке из rpm- или deb-пакета перезагрузка выполняется средствами операционной системы.

Перезагрузка операционной системы узла может быть необходима для применения некоторых обновлений, например, обновления библиотеки OpenSSL. В этом случае в таблице узлов кластера отображается уведомление *Требуется перезагрузить операционную систему*.

► *Чтобы перезагрузить Управляющий узел через веб-интерфейс программы, выполните*

следующие действия:

1. В веб-интерфейсе программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно с информацией об узле.
3. Нажмите на кнопку **Перезагрузить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Перезагрузка операционной системы будет запущена. Это может занять некоторое время. Обновите страницу браузера через несколько минут. После завершения перезагрузки откроется страница подключения к веб-интерфейсу программы.

До завершения перезагрузки обработка трафика будет остановлена.

► *Чтобы перезагрузить Подчиненный узел через веб-интерфейс программы, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите перезагрузить.

   Откроется окно с информацией об узле.
3. По ссылке **Перейти к управлению узлом** перейдите к веб-интерфейсу Подчиненного узла.

   Страница подключения к веб-интерфейсу откроется в новой закладке браузера.
4. Введите учетные данные и подключитесь к Подчиненному узлу.
5. Нажмите на кнопку **Перезагрузить**.
6. В окне подтверждения нажмите на кнопку **Да**.

Перезагрузка операционной системы будет запущена. Это может занять некоторое время. Обновите страницу браузера через несколько минут. После завершения перезагрузки откроется страница подключения к веб-интерфейсу Подчиненного узла.

До завершения перезагрузки обработка трафика будет остановлена.

kaspersky

Работа программы в аварийном режиме

Kaspersky Web Traffic Security переходит в аварийный режим, если в системе два и более Управляющих узла. Например, Управляющий узел стал недоступен, и эта роль была назначена другому узлу в кластере. Через некоторое время первый Управляющий узел снова стал доступен, и в системе оказалось два Управляющих узла.

Аварийный режим программы не влияет на обработку сетевого трафика. Все узлы продолжают обрабатывать сетевой трафик в соответствии с последними значениями параметров, полученными от Управляющего узла до перехода программы в аварийный режим.

Управляющий узел

В окне аварийного режима на Управляющем узле отображается следующая информация:

- IP-адрес текущего узла.
- Роль текущего узла.
- Таблица узлов, входящих в кластер.

Таблица узлов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу.
- **Роль** – роль текущего узла в программе.
- **Управляющий узел** – IP-адрес Управляющего узла.

  Доступно только для Подчиненного узла.
- **Синхронизированы** – время последней синхронизации значений параметров.
- **Состояние соединения с Управляющим узлом** – доступность Управляющего узла по сети.

Значок  в строке таблицы означает, что в работе этого узла возникла проблема. Например, Подчиненный узел ошибочно стал Управляющим, или сервер недоступен по сети.

Если вы хотите передать управление программой другому узлу, вы можете назначить текущему Управляющему узлу роль Подчиненный узел с помощью кнопки **Назначить роль Подчиненный узел**.

Подчиненный узел

В окне аварийного режима на Подчиненном узле отображается следующая информация:

- IP-адрес текущего узла.
- Роль текущего узла.
- IP-адрес и доступность Управляющего узла.
- Дата и время последней синхронизации значений параметров.
- Таблица узлов, входящих в кластер.

Таблица узлов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу.

- **Роль** – роль узла в программе.

Если вы хотите управлять параметрами программы на этом узле, вы можете назначить ему роль Управляющий узел с помощью кнопки **Назначить роль Управляющий узел**.

kaspersky

Защита сетевого трафика

Kaspersky Web Traffic Security выполняет следующие действия по защите сетевого трафика:

- Проверяет сетевой трафик на вирусы, фишинг, вредоносные ссылки, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. 132), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу.
- Лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

В этом разделе

О защите трафика от некоторых легальных программ

Легальные программы – программы, разрешенные к установке и использованию на компьютерах пользователей и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред компьютеру пользователя или компьютерной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые функции таких программ для нарушения безопасности компьютера пользователя или компьютерной сети организации.

Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Подобные программы описаны в таблице ниже.

Таблица 9. Легальные программы

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на том компьютере, на котором они установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).

Тип	Название	Описание
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры для наблюдения за компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.

Тип	Название	Описание
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

Настройка параметров модуля Антивирус

► *Чтобы настроить параметры модуля Антивирус, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Антивирус** включите или отключите использование эвристического анализа при антивирусной проверке сетевого трафика с помощью переключателя **Использовать эвристический анализ**.
3. Если вы включили использование эвристического анализа, в списке **Уровень эвристического анализа** выберите один из следующих уровней эвристического анализа:
   - **Поверхностный** – максимально быстрый эвристический анализ.
   - **Средний** – эвристический анализ средней скорости и глубины.
   - **Глубокий** – максимально глубокий эвристический анализ.

   По умолчанию выбран уровень эвристического анализа **Средний**.
4. Включите или отключите блокировку объектов, во время проверки которых произошли ошибки, с помощью переключателя **Блокировать объекты с ошибками проверки**.
5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности антивирусной проверки объектов сетевого трафика в секундах.

   По умолчанию установлено значение 120.
6. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности проверяемых архивов.

   По умолчанию установлено значение 32.
7. Если требуется, установите флажок **Блокировать архивы при превышении уровня вложенности**.

   Если флажок снят, архив будет пропущен без выполнения антивирусной проверки. В журнал событий для этого объекта будет записан статус *Проверка не завершена*.
8. Включите или отключите обнаружение некоторых легальных программ с помощью переключателя **Обнаруживать некоторые легальные программы**.

   К таким легальным программам (см. раздел "О защите трафика от некоторых легальных программ" на стр. 132) относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями.

Если переключатель включен, то в случае обнаружения таких программ, они будут обработаны согласно правилам для зараженных объектов.

9. Нажмите на кнопку **Сохранить**.

Параметры модуля Антивирус будут настроены.

Настройка параметров модуля Анти-Фишинг

► *Чтобы настроить параметры модуля Анти-Фишинг, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Анти-Фишинг** включите или отключите использование эвристического анализа при проверке сетевого трафика на фишинг с помощью переключателя **Использовать эвристический анализ**.
3. Включите или отключите обнаружение рекламных ссылок с помощью переключателя **Отмечать рекламные ссылки как вредоносные**.

   Программы рекламного характера связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, программы рекламного характера передают эту информацию разработчику с разрешения пользователя.

   Если переключатель включен, программа отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.
4. Включите или отключите обнаружение ссылок, связанных с некоторыми легальными программами (см. раздел "О защите трафика от некоторых легальных программ" на стр. 132), с помощью переключателя **Отмечать ссылки, связанные с некоторыми легальными программами, как вредоносные**.

   Легальные программы могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы в качестве вспомогательного компонента вредоносной программы.

   Если переключатель включен, программа отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.
5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности проверки объектов сетевого трафика на фишинг в секундах.

   По умолчанию установлено значение 120.
6. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Фишинг будут настроены.

kaspersky

Настройка обработки архивов

Во время проверки на вирусы, фишинг, некоторые легальные программы, которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, Kaspersky Web Traffic Security по умолчанию распаковывает архивы во временную директорию /tmp/kwtstmp. Вы можете изменить директорию, в которую будут распаковываться проверяемые архивы.

► *Чтобы настроить директорию для распаковки архивов, выполните следующие действия:*

1. Откройте файл /var/opt/kaspersky/apps/2022 в текстовом редакторе на узле кластера.
2. В секции `[paths]` укажите путь к директории в качестве значения параметра `tmp`.

Пример:

```
tmp=</path/to/tmp/for/archives>
```

> Убедитесь, что указанная директория существует. Необходимо предоставить доступ к директории пользователю kluser и группе klusers.

3. Перезапустите Kaspersky Web Traffic Security.

Архивы будут распаковываться в указанную директорию.

kaspersky

Параметры ICAP-сервера

Чтобы выполнять проверку трафика, а также регулировать доступ пользователей вашей сети к веб-ресурсам, требуется фильтровать и изменять данные HTTP-сообщений (HTTP-запросов и HTTP-ответов). Для этого необходимо настроить интеграцию вашего прокси-сервера с Kaspersky Web Traffic Security по протоколу ICAP:

- Настроить параметры ICAP-сервера в Kaspersky Web Traffic Security.
- Настроить ваш прокси-сервер на передачу данных в Kaspersky Web Traffic Security по протоколу ICAP.

В этой интеграции Kaspersky Web Traffic Security выступает в роли ICAP-сервера, а ваш прокси-сервер выступает в роли ICAP-клиента.
Значения параметров, настраиваемых на вашем прокси-сервере, должны соответствовать значениям параметров в Kaspersky Web Traffic Security.

В этом разделе

Настройка параметров подключения к ICAP-серверу

Если вы используете отдельный прокси-сервер, требуется настроить параметры подключения Kaspersky Web Traffic Security к ICAP-серверу.

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Web Traffic Security не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Web Traffic Security с помощью туннелирования трафика или средствами iptables.

► *Чтобы настроить параметры подключения к ICAP-серверу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **ICAP-сервер**.
2. В списке **Адрес ICAP-сервера** выберите одно из следующих значений:
   - 127.0.0.1 (адрес IPv4), если прокси-сервер и программа Kaspersky Web Traffic Security установлены на одном сервере. Программа будет обрабатывать трафик только с текущего сервера.
   - 0.0.0.0 (адрес IPv4), если вы используете отдельный прокси-сервер. Программа будет

обрабатывать трафик с любых серверов.

- ::1 (адрес IPv6, аналог адреса 127.0.0.1), если прокси-сервер и программа Kaspersky Web Traffic Security установлены на одном сервере. Программа будет обрабатывать трафик только с текущего сервера.
- :: (адрес IPv6, аналог адреса 0.0.0.0), если вы используете отдельный прокси-сервер. Программа будет обрабатывать трафик с любых серверов.

3. Введите порт подключения к ICAP-серверу.

   Допустимые значения – от 1 до 65535, кроме портов 22, 80, 443, 705 и 9045.

4. В поле **Максимальное количество соединений про протоколу ICAP** установите ограничение на количество одновременных подключений к ICAP-серверу.

   Вы можете указать значение от 1000 до 10 000. По умолчанию установлено значение 5000.

5. Нажмите на кнопку **Сохранить**.

Параметры подключения к ICAP-серверу будут настроены.

Настройка параметров обработки трафика на ICAP-сервере

Параметры обработки трафика на ICAP-сервере применяются на всех серверах с установленной программой.

► *Чтобы настроить параметры обработки трафика на ICAP-сервере, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **ICAP-сервер**.
2. В поле **Заголовок, содержащий IP-адрес клиента** введите заголовок, который прокси-сервер использует для передачи IP-адреса пользователя прокси-сервера.

   По умолчанию установлено значение `X-Client-IP`.

   Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, программа не сможет корректно определять пользователей при проверке правил обработки трафика.

3. В поле **Заголовок, содержащий имя пользователя** введите заголовок, который прокси-сервер использует для передачи имени пользователя прокси-сервера.

   По умолчанию установлено значение `X-Client-Username`.

   Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, программа не сможет корректно определять пользователей при проверке правил обработки трафика.

4. Если прокси-сервер передает имена пользователей в кодировке Base64, установите флажок **Имя пользователя в кодировке Base64**.

5. В поле **Путь службы модификации запросов** укажите путь службы Request Modification (REQMOD), которая обрабатывает исходящий трафик.
6. В поле **Путь службы модификации ответов** укажите путь службы Response Modification (RESPMOD), которая обрабатывает входящий трафик.
7. Если вы хотите, чтобы браузер пользователя не прерывал соединение с ошибкой превышения времени ожидания при загрузке объектов большого размера, выполните следующие действия:
   a. Переведите переключатель **Начинать передачу HTTP-сообщений до окончания их проверки** в положение **Включено**.

      Если этот параметр включен, а проверка объекта занимает продолжительное время, Kaspersky Web Traffic Security передает часть объекта браузеру, не дожидаясь завершения проверки. Kaspersky Web Traffic Security продолжает проверять объект по правилам обработки трафика. Если по результатам проверки доступ к объекту разрешен, то объект передается браузеру полностью. Если доступ к объекту запрещен, то сессия браузера прерывается и оставшаяся часть объекта не передается. В этом случае загрузка запрещенного объекта прерывается без объяснения причин. Пользователю не выводится сообщение о запрете загрузки, и не производится перенаправление на другую страницу.
   b. В поле **Скорость передачи данных (КБ/с)** укажите количество байт, которое будет передаваться браузеру каждую секунду до завершения проверки HTTP-сообщения программой.

      Вы можете указать целое число от 1 до 1024.
   c. В поле **Задержка отправки (сек.)** укажите время задержки в секундах. Программа начнет передавать объект браузеру через указанное количество секунд.

      Вы можете указать целое число от 1 до 3600.
8. Нажмите на кнопку **Сохранить**.

Параметры обработки трафика на ICAP-сервере будут настроены.

kaspersky

Страница блокировки

Если в результате проверки веб-ресурса по правилам обработки трафика доступ заблокирован, пользователю отображается страница блокировки.

Вы можете использовать следующие шаблоны страницы блокировки:

- по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 142);
- для рабочих областей (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 142);
- для правил обработки трафика (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. 143).

Алгоритм выбора страницы блокировки представлен на рисунке ниже.

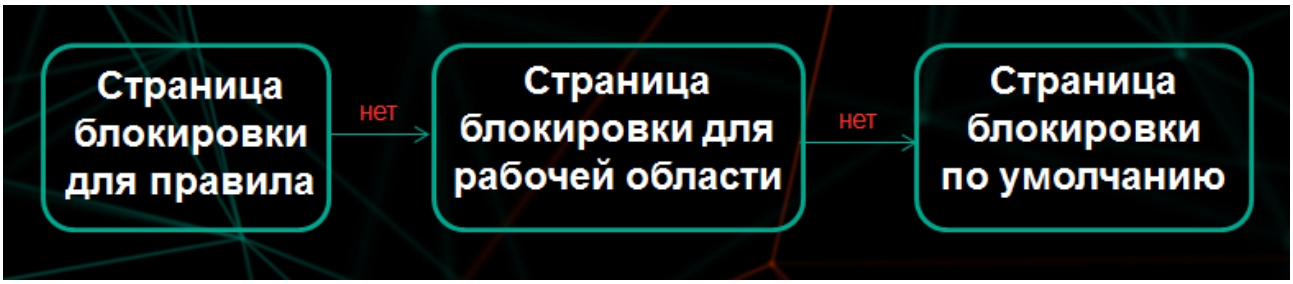


Рисунок 1. Алгоритм применения шаблона для страницы запрета доступа

Если веб-ресурс заблокирован по правилу обработки трафика, в параметрах которого настроена страница блокировки, то пользователю отображается текст, заданный на странице блокировки для этого правила. Если страница блокировки для правила не настроена, то программа проверяет наличие страницы блокировки для рабочей области. Если страница блокировки для рабочей области настроена, то программа использует ее. Если не настроена ни одна страница блокировки, то будет использована страница блокировки по умолчанию.

В этом разделе

Список поддерживаемых макросов

Вы можете использовать следующие макросы в тексте страницы блокировки:

- %DATE% – дата и время события.
- %APPLICATION% – название программы.

- %BUILD% – номер сборки программы.
- %SERVER_NAME% – имя компьютера, на котором был обработан HTTP-запрос.
- %TYPE% – тип HTTP-сообщению (Request или Response).
- %METHOD% – метод HTTP-сообщения.
- %RULE_NAME% – название правила обработки трафика, согласно которому веб-ресурс был заблокирован.
- %THREAT% – имя обнаруженного вредоносного объекта.
- %CURED_LIST% – список угроз, которые были вылечены.
- %SCAN_RESULT% – тип обнаруженной угрозы, которая представляет наибольшую опасность среди всех угроз, обнаруженных в данном объекте.

  Например, если в одном объекте обнаружены вирус и фишинговая ссылка (`av_status="detected" и ap_status="detected"`), то в качестве значения макроса будет указан вирус.
- %CATEGORY% – категория обработанного веб-ресурса по тематике его содержания.
- %PROCESSING_TIME% – продолжительность обработки HTTP-сообщения.
- %WORKSPACE_NAME% – имя рабочей области, к которой относится обработанный трафик.
- %USER_NAME% – имя учетной записи пользователя, который является источником HTTP-запроса.
- %USER_AGENT% – программа на компьютере пользователя, инициировавшая HTTP-запрос (User Agent).
- %CLIENT_IP% – IP-адрес компьютера, с которого был направлен HTTP-запрос.
- %URL% – URL-адрес веб-сайта, доступ к которому запрещен.
- %MIME_TIPE% – MIME-тип HTTP-сообщения и его частей.
- %FILE_NAME% – имена заблокированных файлов.
- %FILE_TYPE% – тип заблокированных файлов.

kaspersky

Настройка страницы блокировки по умолчанию

► *Чтобы настроить страницу блокировки по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Страница блокировки по умолчанию**.
2. Если требуется, измените текст страницы в поле **Макрос %TEXT%** и / или разметку страницы в поле **HTML-код**.
3. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 140).

   Вы также можете использовать макрос %TEXT% – содержимое поля **Макрос %TEXT%** (доступен только для поля **HTML-код**).

   При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
4. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
5. Нажмите на кнопку **Сохранить**.

Страница блокировки по умолчанию будет настроена. Эта страница будет отображаться, если не настроены страницы блокировки для рабочей области и для сработавшего правила обработки трафика.

Настройка страницы блокировки для рабочей области

Настройка страницы блокировки для рабочей области доступна в общем веб-интерфейсе, а также в веб-интерфейсе рабочей области.

► *Чтобы настроить страницу блокировки для рабочей области, выполните следующие действия:*

1. Перейдите в раздел настройки страницы блокировки в общем веб-интерфейсе или в веб-интерфейсе рабочей области. Для этого выполните следующие действия:
   - В общем веб-интерфейсе.
2. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите общие параметры.
3. Выберите раздел **Рабочие области**.
4. Выберите рабочую область, для которой вы хотите настроить отдельную страницу блокировки.

   Откроется окно с информацией о рабочей области.
5. Выберите закладку **Страница блокировки**.
6. В правом нижнем углу нажмите на кнопку **Изменить**.
   - В веб-интерфейсе рабочей области.
7. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите

название нужной рабочей области.

8. Выберите раздел **Параметры рабочей области**.
9. Выберите вариант **Создать индивидуальную страницу блокировки**.
10. Если вы хотите скопировать текст и разметку страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 142), заданной в общих параметрах, нажмите на ссылку **Скопировать из страницы блокировки по умолчанию** в правом нижнем углу окна.
11. Измените текст страницы в поле **Макрос %TEXT%** и / или разметку страницы в поле **HTML-код**.
12. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 140).

    Вы также можете использовать макрос %TEXT% – содержимое поля **Макрос %TEXT%** (доступен только для поля **HTML-код**).

    При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
13. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
14. Нажмите на кнопку **Сохранить**.

Страница блокировки для рабочей области будет настроена. Пользователям, входящим в эту рабочую область, будет отображаться заданный текст. Остальным пользователям будет отображаться страница блокировки по умолчанию.

Если сработало правило, в котором настроена страница блокировки, то используется страница блокировки для правила (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. 143), а не страница для рабочей области или страница по умолчанию.

Настройка страницы блокировки для правила обработки трафика

Вы можете изменить только текст страницы блокировки для отдельного правила обработки трафика. Разметка страницы определяется параметрами страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 142).

► *Чтобы изменить текст страницы блокировки для правила обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, для которого вы хотите настроить страницу блокировки.

   Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить правило**.
6. Установите флажок **Введите текст для отображения на странице блокировки**.
7. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 140).

   При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
9. Нажмите на кнопку **Сохранить**.

Страница блокировки для правила обработки трафика будет настроена.

kaspersky

Экспорт и импорт параметров

Функциональность доступна при наличии у пользователя права **Изменять параметры**.

Экспорт и импорт параметров Kaspersky Web Traffic Security может быть использован для следующих целей:

- Резервное копирование параметров программы.

  Если Управляющий узел выйдет из строя, вы сможете импортировать ранее экспортированные параметры после повторной установки программы.

- Развертывание программы на новом сервере.

  Вы можете настроить параметры на одном сервере, затем экспортировать их и создать одинаковую конфигурацию программы на всех серверах.

- Миграция программы на новую версию.

  Перед обновлением программы вы можете экспортировать параметры из старой версии и импортировать их в новую версию.

  Миграция с более новой на более старую версию не поддерживается.

При экспорте параметров (см. раздел "Экспорт параметров Kaspersky Web Traffic Security" на стр. 146) создается конфигурационный файл со следующей информацией:

- Версия программы.
- Параметры программы вне рабочих областей:
  - правила защиты и доступа, не относящиеся к рабочим областям;
  - роли и права пользователей;
  - учетные записи пользователей, имеющих роли вне рабочих областей;
  - страницы блокировки;
  - параметры защиты.
- Параметры рабочих областей:
  - критерии принадлежности трафика к рабочей области;
  - правила защиты и доступа, созданные в рамках рабочей области;
  - роли и права пользователей, относящиеся ко всем рабочим областям.

Созданный конфигурационный файл сохраняется локально на Управляющем узле.

При импорте конфигурационного файла (см. раздел "Импорт параметров Kaspersky Web Traffic Security" на стр. 146) вы можете выбрать, какие параметры должны быть применены:

- отдельные параметры программы вне рабочих областей;
- рабочие области, для которых будут применены все параметры.

kaspersky

При импорте правил защиты из версии 6.0 в версию 6.1 для типа объектов **Вредоносная ссылка** устанавливается действие **Заблокировать**.

Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров Kaspersky Web Traffic Security

► *Чтобы экспортировать параметры Kaspersky Web Traffic Security, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Экспорт**.
3. Нажмите на кнопку **Экспортировать**.

   В блоке **Последние операции экспорта конфигурации** отобразится текущее состояние операции экспорта. После успешного завершения операции отобразится строка с датой и временем экспорта.
4. Нажмите на значок в нужной строке.

Конфигурационный файл с экспортированными параметрами будет сохранен в папке загрузки браузера.

Импорт параметров Kaspersky Web Traffic Security

Не рекомендуется импортировать несколько конфигурационных файлов одновременно. В этом случае будут применены параметры только из одного файла.

► *Чтобы импортировать параметры Kaspersky Web Traffic Security, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Импорт**.
3. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл с ранее экспортированными параметрами.

Откроется окно **Выберите параметры для импорта**.

5. Установите флажки напротив тех параметров, которые вы хотите импортировать.
6. Установите флажок под таблицей параметров, подтверждающий согласие на импорт.
7. Нажмите на кнопку **Импортировать**.

Отобразится сообщение о результате запуска операции импорта.

Настройка хранения экспортированных файлов

Вы можете ограничить количество экспортированных конфигурационных файлов, которые хранятся на сервере. В случае превышения установленного ограничения ранее экспортированные файлы будут удалены.

► *Чтобы настроить хранение экспортированных файлов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Экспорт**.
3. В поле **Максимальное количество хранимых конфигурационных файлов** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.

Количество экспортированных файлов будет ограничено заданным значением.

kaspersky

Обновление программы

Функциональность доступна только при развертывании программы из ISO-образа.

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Web Traffic Security. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, или плановые обновления, добавляющие новые или улучшающие существующие функции программы.

Службы Kaspersky Web Traffic Security могут быть приостановлены на время установки обновления. Процесс обновления может занять несколько минут. После запуска не следует прерывать процесс обновления или выключать сервер. После установки обновлений может потребоваться перезапуск программы.

► *Чтобы запустить обновление системы на Управляющем узле, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Общие** → **Обновление системы**.
2. Справа от поля ввода нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
3. Выберите архив, содержащий пакет обновлений, и нажмите на кнопку **Open**.

   Название выбранного архива отобразится в поле ввода.
4. Нажмите на кнопку **Загрузить файл**.

Запустится мастер установки пакета обновлений. Следуйте указаниям мастера.

► *Чтобы запустить обновление системы на Подчиненном узле, выполните следующие действия:*

1. Войдите в веб-интерфейс Подчиненного узла под учетной записью администратора.
2. В правом верхнем углу нажмите на кнопку **Установить обновление**.

   Откроется страница **Установить обновление**.
3. Справа от поля ввода нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
4. Выберите архив, содержащий пакет обновлений, и нажмите на кнопку **Open**.

   Название выбранного архива отобразится в поле ввода.
5. Нажмите на кнопку **Загрузить файл**.

Запустится мастер установки пакета обновлений. Следуйте указаниям мастера.

kaspersky

Настройка времени сервера

Функциональность доступна только при развертывании программы из ISO-образа.

Вы можете настроить время сервера, используемое в параметрах программы. Обновления баз и правила обработки трафика, для которых задано расписание, будут применяться согласно установленному времени.

► *Чтобы настроить время сервера, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Общие** → **Дата и время**.
2. В блоке параметров **Часовой пояс** выполните следующие действия:
   a. В раскрывающемся списке **Страна** выберите страну, к которой относится нужный часовой пояс.
   b. В раскрывающемся списке **Часовой пояс** выберите часовой пояс.

   Выбранный часовой пояс будет выделен на карте под раскрывающимся списком.
3. В блоке параметров **Синхронизация времени** включите или отключите синхронизацию с NTP-сервером с помощью переключателя **Синхронизировать с NTP-сервером**.

   Если вы развернули программу из ISO-образа на виртуальной машине VMware, то при включении синхронизации с NTP-сервером синхронизация времени с гипервизором будет отключена автоматически. Если вы используете другой гипервизор, вам требуется самостоятельно отключить синхронизацию в параметрах гипервизора.
4. Если вы включили синхронизацию с NTP-сервером, в поле **NTP-сервер** введите полное доменное имя (FQDN) или IP-адрес NTP-сервера в формате IPv4 или IPv6.
5. Если вы хотите добавить еще один NTP-сервер для синхронизации, нажмите на кнопку ⊞ и в появившемся поле ввода укажите его адрес.
6. Нажмите на кнопку **Сохранить**.

Время сервера будет настроено. Внесенные изменения будут сохранены на Управляющем узле и распространены на все узлы кластера. Состояние синхронизации времени будет отображаться в информации о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 122).

kaspersky

Настройка параметров соединения с прокси-сервером

Заданные параметры прокси-сервера будут использованы для обновления баз, активации программы и работы внешних служб.

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с прокси-сервером**.
2. Включите переключатель рядом с параметром **Использовать прокси-сервер**.
3. В блоке параметров **Адрес прокси-сервера** введите адрес и порт прокси-сервера.
4. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси для локальных адресов**.
5. Если вы хотите использовать аутентификацию при подключении к прокси-серверу, в полях **Имя пользователя (необязательно)** и **Пароль (необязательно)** введите имя пользователя и пароль подключения к прокси-серверу.
6. Нажмите на кнопку **Сохранить**.

kaspersky

Обновление баз Kaspersky Web Traffic Security

Базы модулей Антивирус и Анти-Фишинг (далее также "базы") представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Эти записи содержат информацию о контрольных участках вредоносного кода и алгоритмы лечения объектов, в которых содержатся угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Чтобы свести риск заражения защищаемого сервера к минимуму, рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений, загружая их с веб-сайта "Лаборатории Касперского".

Во время установки Kaspersky Web Traffic Security получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". Это специальные интернет-сайты, на которые выкладываются обновления баз и программных модулей для всех программ "Лаборатории Касперского". Если для доступа в интернет вы используете прокси-сервер, вам нужно настроить параметры соединения с прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 150).

Чтобы уменьшить интернет-трафик, вы можете выбрать *пользовательский источник обновлений (см. раздел "Выбор источника обновлений баз" на стр. 151)*. Это могут быть указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

В этом разделе

Выбор источника обновлений баз

► *Чтобы выбрать источник обновлений баз, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В раскрывающемся списке **Источник обновлений** выберите один из следующих источников обновлений:
   - **Серверы "Лаборатории Касперского" (безопасное соединение)**.
   - **Серверы "Лаборатории Касперского" (небезопасное соединение)**.
   - **Пользовательский**.

3. Если на предыдущем шаге вы выбрали **Пользовательский**, в поле **Пользовательский источник** укажите URL-адрес пользовательского источника, из которого вы хотите получать пакеты обновлений.

   Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории Касперского"**, если вы хотите получать пакеты обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен.

4. Нажмите на кнопку **Сохранить**.

Настройка расписания и параметров обновления баз

Программа загружает обновления баз из выбранного источника обновлений на все узлы кластера.

► *Чтобы настроить расписание и параметры обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В блоке параметров **Расписание** в раскрывающемся списке выберите один из вариантов и выполните следующие действия:
   - **Вручную**.
   - **Один раз**. В появившемся поле укажите дату и время запуска обновления баз.
   - **Ежедневно**. В появившемся поле укажите время ежедневного запуска обновления баз.
   - **Еженедельно**. В появившихся полях укажите день недели и время запуска обновления баз.
   - **Ежемесячно**. В появившихся полях укажите день месяца и время запуска обновления баз.
   - **Запускать каждые**. В появившихся полях укажите периодичность запуска обновления баз в минутах, часах или днях.

     Первое обновление баз запустится сразу после сохранения внесенных изменений.
3. В поле **Случайное отклонение (мин)** укажите интервал отклонения от заданного расписанием времени в минутах. Программа будет запускать обновление баз не на всех узлах одновременно, а случайным образом в течение заданного интервала. Рекомендуется использовать эту опцию для распределения нагрузки на сеть при большом количестве узлов в кластере.
4. В поле **Максимальная длительность (мин)** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.
5. Переведите переключатель **Запускать пропущенные задачи** в положение **Включено**, если вы хотите запускать пропущенные задачи обновления баз при последующем запуске программы.

   Если запуск пропущенных задач выключен, то пропущенные задачи обновления баз не будут запущены при последующем запуске программы. Следующий запуск обновления баз будет выполнен согласно расписанию.
6. Нажмите на кнопку **Сохранить**.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В верхней части окна **Параметры** нажмите на кнопку **Обновить базы**.

   Появится сообщение о запуске обновления баз.

kaspersky

Использование внешних служб "Лаборатории Касперского"

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Web Traffic Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Web Traffic Security на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Web Traffic Security, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Web Traffic Security передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Web Traffic Security, его можно изменить в любой момент.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения программы Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

kaspersky

В этом разделе

Настройка участия в Kaspersky Security Network

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network.

► *Чтобы настроить участие в Kaspersky Security Network, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **KSN/KPSN**.
2. Выберите один из следующих вариантов:
   - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
   - **Kaspersky Security Network (KSN)**, если вы хотите участвовать в Kaspersky Security Network.
3. Если вы выбрали участие в Kaspersky Security Network, в блоке **Положение о KSN** просмотрите Положение о Kaspersky Security Network и выполните следующие действия:
   - Если вы согласны с условиями, установите флажок **Я согласен участвовать в KSN**.
   - Если вы не согласны с условиями, снимите флажок **Я согласен участвовать в KSN**.
4. Если вы хотите участвовать в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", установите флажок **Отправлять KSN-статистику для повышения уровня обнаружения угроз**.
5. Если вы выбрали участие в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", в блоке **Дополнительное Положение о KSN** просмотрите Дополнительное Положение о Kaspersky Security Network и выполните следующие действия:
   - Если вы согласны с условиями, установите флажок **Я согласен отправлять KSN-статистику**.
   - Если вы не согласны с условиями, снимите флажок **Я согласен отправлять KSN-статистику**.
6. Нажмите на кнопку **Сохранить**.

Участие в Kaspersky Security Network будет настроено.

Настройка использования Kaspersky Private Security Network

► *Чтобы настроить использование Kaspersky Private Security Network, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите один из следующих вариантов:
   - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
   - **KPSN**, если вы хотите использовать Kaspersky Private Security Network.
3. Если вы выбрали использование Kaspersky Private Security Network, в блоке **Конфигурационный файл KPSN** загрузите конфигурационный файл KPSN. Для этого выполните следующие действия:
   a. Нажмите на кнопку **Загрузить**.

      Откроется окно выбора файлов.

   b. Выберите конфигурационный файл KPSN, который вы хотите добавить.

   Для получения конфигурационного файла необходимо включить компонент Additional Services в программе KPSN, а затем отправить запрос в "Лабораторию Касперского". Более подробную информацию вы можете найти в *Руководстве администратора Kaspersky Private Security Network*.

   Конфигурационный файл KPSN должен быть в формате ZIP-архива.
4. Нажмите на кнопку **Open**.

   Окно выбора файлов закроется.
5. Нажмите на кнопку **Сохранить**.

Использование Kaspersky Private Security Network будет настроено.

kaspersky

Соединение с LDAP-сервером

Kaspersky Web Traffic Security позволяет подключаться к серверам внешних служб каталогов, используемых в вашей организации, по протоколу LDAP.

Соединение с внешней службой каталогов по протоколу LDAP предоставляет администратору Kaspersky Web Traffic Security возможность выполнять следующие задачи:

- добавлять пользователей из внешней службы каталогов в правила обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 75);
- создавать учетные записи пользователей (см. раздел "Работа с ролями и учетными записями пользователей" на стр. 105) для работы с Kaspersky Web Traffic Security.

В этом разделе

Добавление соединения с LDAP-сервером

Вы можете добавить соединение с одним или несколькими LDAP-серверами.

Если вы настраиваете интеграцию с доменом, в названии которого содержится корневой домен `.local`, то для успешного соединения с LDAP-сервером требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы добавить соединение с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить соединение**.

3. В поле **Имя** введите имя LDAP-сервера, которое будет отображаться в веб-интерфейсе Kaspersky Web Traffic Security.

4. В блоке параметров **Keytab-файл** нажмите на кнопку **Загрузить**, чтобы загрузить keytab-файл.

   Откроется окно выбора файла.

5. Выберите keytab-файл и нажмите на кнопку **Open**.
6. В поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей.

   Вводите суффикс каталога в формате `ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>`.

   Например, вы можете ввести `ou=people, dc=example, dc=com`.

   Здесь `people` – уровень в схеме каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей (поиск осуществляется на уровне `people` и ниже. Объекты, расположенные выше этого уровня, исключаются из поиска), `example` – доменное имя каталога, в котором Kaspersky Web Traffic Security осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

7. Нажмите на кнопку **Добавить**.

Соединение с LDAP-сервером будет добавлено.

Удаление соединения с LDAP-сервером

► *Чтобы удалить соединение с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, который вы хотите удалить.

   Откроется окно **Просмотреть параметры соединения**.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

4. Нажмите на кнопку **Да**.

Соединение с LDAP-сервером будет удалено.

Изменение параметров соединения с LDAP-сервером

► *Чтобы изменить параметры соединения с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.

   Откроется окно **Просмотреть параметры соединения**.

3. Нажмите на кнопку **Изменить**.

4. Если требуется, измените следующие параметры:
   - Имя LDAP-сервера, которое отображается в веб-интерфейсе программы, в поле **Имя**.
   - Keytab-файл, нажав на кнопку **Заменить**.
   - Каталог, начиная с которого программа осуществляет поиск записей, в поле **База поиска**.
5. Нажмите на кнопку **Сохранить**.

Параметры соединения с LDAP-сервером будут изменены.

Запуск синхронизации с контроллером домена Active Directory вручную

Программа выполняет автоматическую синхронизацию данных с контроллером домена Active Directory каждые 30 минут. Если вам требуется обновить данные об учетных записях пользователей немедленно (например, при добавлении нового пользователя), вы можете запустить синхронизацию вручную.

► *Чтобы запустить синхронизацию с контроллером домена Active Directory вручную, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Синхронизировать**.

   Синхронизация данных с контроллером домена будет запущена. В результате будут обновлены данные об учетных записях пользователей, используемые при подборе правил и при автозаполнении имен пользователей в веб-интерфейсе программы.

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. 122).

kaspersky

Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform

Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform (далее также "KATA") доступна только при наличии у пользователя права **Изменять параметры**.

Kaspersky Anti Targeted Attack Platform – решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats.

Программа KATA позволяет интегрироваться с другими программами "Лаборатории Касперского", чтобы получать и обрабатывать проверяемые ими объекты. В качестве такой программы может выступать Kaspersky Web Traffic Security.

Администратору Kaspersky Web Traffic Security требуется выполнить настройку интеграции KATA (см. раздел "Сценарий настройки интеграции с программой KATA" на стр. 162) на Управляющем узле. После этого параметры интеграции отправляются на все Подчиненные узлы, входящие в кластер. Далее каждый узел кластера взаимодействует с сервером KATA самостоятельно, независимо от других узлов.

При интеграции с программой KATA доступно два режима: отправка файлов на сервер KATA и получение объектов, обнаруженных программой KATA.

Отправка файлов на сервер KATA

Kaspersky Web Traffic Security отправляет на сервер KATA объекты, которые не были заблокированы правилами обработки трафика или политикой защиты по умолчанию. При этом программа не ожидает от сервера KATA результатов проверки этих объектов.

При обработке каждого файла программа проверяет необходимость отправки его на сервер KATA. По результатам в журнал событий программы (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 70) записывается статус проверки. Возможны следующие статусы:

- *Неприменимо. Нет файла для проверки* – HTTP-сообщение не содержит файлов для проверки.
- *Отключено согласно параметрам программы* – режим отправки файлов на сервер KATA отключен в параметрах программы.
- *Пропущено согласно действию правила* – HTTP-сообщение было заблокировано программой (применены действия **Заблокировать** или **Перенаправить**) или пропущено по правилу обхода без проверки.
- *Отклонено фильтром KATA* – файл не удовлетворяет условиям отправки на сервер KATA.
- *Запланировано* – отправка файла запланирована.
- *Завершено с ошибкой* – запланировать отправку файла не удалось.

Для файлов со статусами *Запланировано* и *Завершено с ошибкой* в журнал также записывается подробная информация о результате отправки файла.

Все события, связанные с отправкой файлов на сервер KATA, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на

сервер KATA" на стр. 181).

Получение объектов, обнаруженных программой KATA

Kaspersky Web Traffic Security получает от сервера KATA информацию об объектах, обнаруженных программой KATA с помощью технологий Sandbox и YARA. Подробнее об этих технологиях см. *Справку Kaspersky Anti Targeted Attack Platform*.

Информация о полученных объектах сохраняется в кеш KATA. Каждый узел кластера хранит свой кеш KATA и получает объекты, обнаруженные программой KATA, независимо от других узлов. По истечении времени хранения информация об объектах удаляется из кеша. Эти объекты больше не учитываются при применении правил защиты (см. раздел "Добавление правила защиты" на стр. 81) и политики защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. 94).

В правилах защиты и в политике защиты по умолчанию вы можете настроить действия над объектами, информация о которых была получена с сервера KATA. При обнаружении в трафике пользователя таких объектов Kaspersky Web Traffic Security будет обрабатывать их согласно заданным в правилах параметрам. Это позволяет блокировать потенциально опасные объекты до того, как информация о них была добавлена в репутационные базы KSN, а также в локальные базы программы.

Результат проверки каждого объекта записывается в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 70). Возможны следующие статусы проверки:

- *Не обнаружено* – соответствий в кеше KATA не обнаружено.
- *Обнаружено* – обнаружены угрозы.
- *Не проверен* – проверка не выполнялась согласно параметрам программы.
- *Ошибка проверки* – проверка завершилась с ошибкой.

Все события, связанные с проверкой трафика на соответствие объектам KATA, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. 170).

В этом разделе

kaspersky

Сценарий настройки интеграции с программой KATA

Настройка интеграции Kaspersky Web Traffic Security с программой KATA состоит из следующих этапов.

1. Добавление сервера KATA (на стр. 162)

   При добавлении сервера KATA требуется сверить отпечатки сертификата, отображаемые в веб-интерфейсах KWTS и KATA. Если отпечатки совпадают, администратор подтверждает добавление сервера. После этого Управляющий узел отправляет адрес и сертификат сервера KATA на все узлы кластера, не дожидаясь подтверждения авторизации.

2. Выбор режима интеграции (на стр. 164)

   В Kaspersky Web Traffic Security доступно два режима интеграции с программой KATA. Вы можете отправлять файлы на проверку в KATA (в этом случае KWTS выступает в качестве внешней системы для программы KATA) и/или получать информацию об объектах, обнаруженных программой KATA. Эти режимы работают независимо друг от друга.

3. Настройка параметров кеша KATA (на стр. 165)

   При применении правил защиты и политики по умолчанию Kaspersky Web Traffic Security учитывает объекты, информация о которых хранится в кеше KATA. Вы можете настраивать период их хранения в кеше, по истечении которого эти объекты перестают учитываться при обработке трафика.

4. Авторизация Kaspersky Web Traffic Security в веб-интерфейсе программы KATA

   Во время добавления сервера KATA отправляется запрос на авторизацию внешней системы. Администратору KATA требуется подтвердить этот запрос в веб-интерфейсе KATA. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

Добавление сервера KATA

Вы можете настроить интеграцию только с одним сервером KATA.

► *Чтобы добавить сервер KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление сервера KATA**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес сервера KATA, на котором установлен компонент Central Node.
4. В поле **Порт** введите порт подключения к серверу KATA.

   По умолчанию указано значение 443.
5. Нажмите на кнопку **Далее**.

   Откроется окно **Подтверждение сервера KATA**.
6. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают,

нажмите на кнопку **Подтвердить**.

Сервер KATA будет добавлен. Информация о сервере отобразится в разделе **Интеграция KATA**, в блоке параметров **Сервер KATA**.

Изменение сервера KATA

В программе доступна интеграция только с одним сервером KATA. Если вы хотите настроить интеграцию с другим сервером, вы можете изменить сервер KATA.

► *Чтобы изменить сервер KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Заменить**.

   Откроется окно **Изменение сервера KATA**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес нового сервера KATA, на котором установлен компонент Central Node.
4. Нажмите на кнопку **Далее**.

   Откроется окно **Подтверждение сервера KATA**.
5. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет изменен.

Удаление сервера KATA

► *Чтобы удалить сервер KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Удалить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Сервер KATA будет удален. Информационные панели об интеграции с программой KATA в разделах **Мониторинг** и **Узлы** перестанут отображаться. Записи об обработанных ранее объектах в журнале событий программы и в журнале Syslog не будут удалены.

kaspersky

Выбор режима интеграции

Выбор режима интеграции доступен только при добавленном сервере KATA (см. раздел "Добавление сервера KATA" на стр. 162).

► *Чтобы выбрать режим интеграции с программой KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Режим интеграции KATA** включите нужный режим интеграции с помощью следующих переключателей:
   - **Получать объекты**.

     Kaspersky Web Traffic Security будет получать объекты, обнаруженные программой KATA, и использовать информацию об этих объектах в правилах защиты и в политике защиты по умолчанию.
   - **Отправлять файлы**.

     Kaspersky Web Traffic Security будет авторизован в программе KATA в качестве внешней системы. Файлы из проверяемого трафика пользователей, удовлетворяющие заданным в программе критериям, будут отправляться в KATA. Kaspersky Web Traffic Security не будет ожидать результатов проверки отправленных файлов.

   Эти режимы работают независимо друг от друга. Вы можете включить один из режимов или оба режима одновременно.
3. Нажмите на кнопку **Сохранить**.

Режим интеграции с программой KATA будет выбран. В зависимости от выбранного режима в разделе **Узлы** отобразятся информационные панели о состоянии интеграции (см. раздел "Мониторинг интеграции KATA" на стр. 165).

Пересоздание сертификата KWTS

При компрометации сертификата Kaspersky Web Traffic Security администратор программы KATA может отменить авторизацию KWTS как внешней системы. В этом случае вам требуется создать новый сертификат в веб-интерфейсе KWTS и пройти процедуру авторизации в программе KATA повторно (см. раздел "Сценарий настройки интеграции с программой KATA" на стр. 162).

► *Чтобы пересоздать сертификат для авторизации KWTS в программе KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Учетные данные KWTS** нажмите на кнопку **Создать новый сертификат**.
3. В окне подтверждения нажмите на кнопку **Да**.

Новый сертификат KWTS будет создан. В блоке параметров **Учетные данные KWTS** отобразятся SensorID и отпечаток нового сертификата.

Настройка параметров кеша KATA

Если включен режим **Получать объекты**, то Kaspersky Web Traffic Security сохраняет информацию об объектах, обнаруженных программой KATA, на всех узлах кластера в кеше KATA. При применении правил защиты и политики по умолчанию учитываются объекты, информация о которых хранится в кеше KATA.

► *Чтобы настроить параметры кеша KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Кеш KATA** в поле **Срок хранения кеша (часы)** введите время хранения информации об объектах, обнаруженных программой KATA, в часах.

   Допустимые значения – от 1 до 48. По умолчанию установлено значение 48.
3. Если вы хотите очистить кеш KATA, нажмите на кнопку **Очистить кеш** и в окне подтверждения нажмите на кнопку **Да**.

   Информация об этой операции записывается в журнал событий программы (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 70), а также в журнал операционной системы по протоколу Syslog (см. раздел "Журнал событий Syslog" на стр. 169).

Параметры кеша KATA будут настроены.

Мониторинг интеграции KATA

► *Чтобы проверить состояние интеграции Kaspersky Web Traffic Security с программой KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Узлы**.

   Откроется страница с информацией об узлах кластера. На странице отображаются следующие информационные панели об интеграции с программой KATA:

   - **Отправка файлов в KATA**. Количество узлов кластера со статусами отправки файлов на сервер KATA:
     - *Без ошибок*. Все файлы успешно отправлены на сервер KATA.
     - *Отключено*. Режим интеграции **Отправлять файлы** отключен.
     - *С ошибкой*. Во время отправки файлов на сервер KATA за последний час произошли ошибки.
   - **Получение объектов из KATA**. Количество узлов кластера со статусами получения объектов, обнаруженных программой KATA:
     - *Без ошибок*. Все объекты, обнаруженные программой KATA, получены успешно.

- *Отключено*. Режим интеграции **Получать объекты** отключен.
- *С ошибкой*. Во время получения объектов, обнаруженных программой KATA, произошли ошибки.

2. Перейдите по ссылке **Подробные сведения** в одной из информационных панелей об интеграции с программой KATA.

   Откроется страница **Интеграция KATA**.

3. В правом верхнем углу в раскрывающихся списках выберите период отображения данных, а также узлы кластера, статистику о которых вы хотите посмотреть.

На странице **Интеграция KATA** отобразится следующая информация:

- График **Отправка файлов в KATA**.

Отображается только при включенном режиме **Отправлять файлы**.

График показывает, какое количество файлов было отправлено на сервер KATA за выбранный период времени. Линии графиков представляют следующие статусы отправки файлов:

- *Успешно*.
- *Не удалось отправить файлы на сервер KATA из-за переполнения буфера*.
- *Ошибка*.
- Диаграмма **Детальная информация об ошибках**.

Отображается только при включенном режиме **Отправлять файлы**.

Детальная информация о типах ошибок, возникших при отправке файлов на сервер KATA, представлена в виде круговой и столбчатой диаграмм. Круговая диаграмма показывает соотношение количества ошибок определенного типа к общему количеству всех ошибок. Столбчатая диаграмма показывает количество ошибок определенного типа в заданном интервале времени.

Возможны следующие типы ошибок:

- Не удалось установить соединение с сервером KATA.
- SSL-сертификат сервера KATA не совпадает с доверенным.
- Требуется авторизация на сервере KATA.
- Превышено время ожидания соединения с сервером KATA.
- HTTP-код 4xx: ошибка клиента.
- HTTP-код 5xx: ошибка сервера.
- Внутренняя ошибка.
- Таблица **Состояние интеграции KATA**.

В таблице представлена сводная информация об обработанных объектах по узлам кластера. Таблица содержит следующие графы:

- **IP-адрес:порт**.

  IP-адрес и порт узла кластера, который интегрирован с программой KATA.

- **Отправка файлов в KATA**.

  Статус отправки файлов из трафика этого узла кластера на сервер KATA. Возможны следующие значения:

  - *ОК*.
  - *Ошибка*.
  - *Выключено*.

- **Получение объектов из KATA**.

  Статус получения объектов, обнаруженных программой KATA, на этом узле кластера. Возможны следующие значения:

  - *ОК*.
  - *Ошибка*.
  - *Выключено*.

- **Количество объектов в кеше KATA**.

  Количество объектов, обнаруженных программой KATA, которые были сохранены на всех узлах кластера в кеше KATA.

Если включен только один из режимов интеграции KATA, отображаются только графы, относящиеся к этому режиму.

Настройка отправки HTML-файлов в KATA

Действия, описанные в этом разделе, требуется выполнить на каждом узле кластера.

По умолчанию файлы формата HTML не отправляются в KATA. Вы можете настроить фильтр для отправки HTML-файлов в KATA по формату файла или по регулярным выражениям.

► *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по формату файла, выполните следующие действия:*

1. В файле с параметрами фильтра KATA /var/opt/kaspersky/kwts/kata-filters.json добавьте в секцию `includeFormats` новую строку следующего формата:

   `{"contentFormat": "<формат файла>", "nameMask": "<маска имени файла>"}`

   Возможные значения ключа `contentFormat`:

   - `GeneralHtml`;

- `GeneralHtmlStrict`.

Возможные значения ключа `nameMask`:

- `*.html`;
- `*.htm`;
- `*.xhtml`;
- `*.xht`;
- `*.xml`.
- `*.`

> Если вы хотите добавить несколько значений, то для каждого значения требуется добавить отдельную строку.

2. Перезагрузите компьютер с установленной программой Kaspersky Web Traffic Security.

Изменения, внесенные в конфигурационный файл фильтра KATA, будут применены. Программа будет отправлять в KATA все HTML-файлы, формат и имя которых соответствуют записям в конфигурационном файле.

► *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по регулярным выражениям, выполните следующие действия:*

1. Убедитесь, что в файле с параметрами фильтра KATA /var/opt/kaspersky/kwts/kata-filters.json в секции `includeFormats` отсутствуют записи об HTML-файлах.
2. Переименуйте файл с регулярными выражениями для фильтра KATA, расположенный по пути /var/opt/kaspersky/kwts/kata-html-regex_sample.txt, в kata-html-regex.txt.
3. Перезагрузите компьютер с установленной программой Kaspersky Web Traffic Security.

Программа будет отправлять в KATA только те HTML-файлы, которые удовлетворяют регулярным выражениям, указанным в файле kata-html-regex.txt.

kaspersky

Журнал событий Syslog

Вы можете настроить запись событий обработки трафика (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. 170), системных событий программы (см. раздел "Содержание syslog-сообщений о системных событиях программы" на стр. 178) и событий отправки файлов на сервер KATA (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на сервер KATA" на стр. 181) в журнал событий по протоколу Syslog (далее также "журнал событий Syslog"). Это позволит импортировать события в стороннюю SIEM-систему.

Информация о событиях записывается в отдельной категории журнала, установленной в параметрах Syslog (см. раздел "Настройка параметров Syslog" на стр. 169). Сведения о каждом событии отправляются как отдельное syslog-сообщение. Текст syslog-сообщения соответствует информации о событии, отображающейся в веб-интерфейсе программы в разделе **События**.

Для удаленной записи событий по протоколу Syslog рекомендуется использовать протокол TCP. Сетевые порты, используемые сервером Syslog, должны быть открыты.

В этом разделе

Настройка параметров Syslog

При настройке параметров Kaspersky Web Traffic Security рекомендуется учитывать параметры Syslog, установленные в операционной системе.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры → Журналы и события → Syslog**.
2. В раскрывающемся списке **Категория журнала** выберите категорию журнала, в который будет записываться информация о событиях.

   По умолчанию установлено значение Local1.

   При развертывании программы из iso-файла изменение параметра недоступно.

3. В раскрывающемся списке **Уровень события** выберите уровень важности событий, которые будут записываться по протоколу Syslog.

- **Ошибка** – сообщения об ошибках в работе программы.

  События обработки трафика не будут записаны в журнал Syslog.

- **Информация** – сообщения об ошибках в работе программы, а также события обработки трафика.

4. Если специалисты Службы технической поддержки попросили вас включить запись информации об объеме и параметрах потока трафика, обрабатываемого программой, в журнал событий Syslog, переведите переключатель **Записывать информацию о профиле трафика** в положение **Включено**.

   Включение этой опции увеличивает требования к дисковому пространству сервера с установленной программой, а также снижает производительность программы. Не рекомендуется включать эту опцию без запроса специалистов Службы технической поддержки.

Запись событий по протоколу Syslog будет настроена.

Содержание syslog-сообщений о событиях обработки трафика

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение `KWTS`).

Поля syslog-сообщения о событии обработки трафика, определяемые параметрами программы, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

```
Oct 9 10:13:06 localhost KWTS: type="Response": method="GET": action="Block":
blocked_by_rule="protection_rules [Workspace1/-/Rule2]":
processing_time="952": scan_result="Malware": workspace="Workspace1":
http_user_name="example@test.local": http_user_agent="curl/7.29.0":
http_user_ip="192.0.2.0": url="http://example.com/eicar.com":
kata-alert="NotDetected": "eicar.com", filesize="69",
kata_upload="SkippedByAction", guid="", rules="access_rules
[Workspace1/Group1/Rule1], protection_rules [Workspace1/-/Rule2]",
av-status="Detected", threats="EICAR-Test-File/Block",
ap-status="NotDetected", mlf-status="NotDetected", encrypted="NotDetected",
macros="NotDetected", kata-alert="NotDetected"
```

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 10. Информация о событиях обработки трафика в syslog-сообщении

Ключ	Описание и возможные значения
`type`	Тип HTTP-сообщения. Может принимать значения `Request` (запрос) или `Response` (ответ).
`method`	Метод HTTP-запроса.
`action`	Действие над обнаруженным объектом. Может принимать одно из следующих значений: • `Allow` – Разрешить. • `Block` – Заблокировать. • `Redirect` – Перенаправить.
`blocked_by_rule`	Название правила обработки трафика, по которому веб-ресурс был заблокирован. Отображается в следующем формате: • Для правил обхода: `"[<Название правила>]"`. • Для правил защиты и правил доступа: `"[<Название рабочей области>/<Название группы правил>/<Название правила>]"`.
`redirected_by_rule`	Название правила обработки трафика, по которому пользователь был перенаправлен на указанный URL-адрес. Отображается в следующем формате: • Для правил обхода: `"[<Название правила>]"`. • Для правил доступа: `"[<Название рабочей области>/<Название группы правил>/<Название правила>]"`.
`processing_time`	Продолжительность обработки HTTP-сообщения в миллисекундах. Учитывается время с начала обработки заголовка HTTP-сообщения до сохранения записи о выполненной проверке в журнале событий программы и в журнале событий Syslog.
`scan_result`	Результат проверки HTTP-сообщения. Если обнаружено несколько угроз, отображается название угрозы с наибольшим приоритетом. Если угрозы устранены или не обнаружены, отображается результат проверки с наибольшим приоритетом (*Вылечен*, *Не обнаружено*, *Не проверен*).
`workspace`	Название рабочей области, к которой относится событие обработки трафика. При отсутствии рабочей области отображается прочерк.
`http_user_name`	Имя учетной записи пользователя, инициировавшего HTTP-запрос.
`http_user_agent`	Клиентское приложение, инициировавшее HTTP-запрос.
`http_user_ip`	IP-адрес компьютера, с которого был отправлен HTTP-запрос.

Ключ	Описание и возможные значения
`url`	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.
`kata-alert`	Результат проверки URL-адреса на соответствие объектам, обнаруженным программой KATA. Возможны следующие значения: • `NotDetected` – URL-адрес проверен, угрозы не обнаружены. • `Detected` – обнаружено соответствие с объектом в кеше KATA. Указывается ID объекта, критерий совпадения и технология. Например, `kata-alert="Detected/128563/Url/Sb"`. • `NotScanned/AccessRuleSettings` – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • `NotScanned/BypassRuleSettings` – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • `NotScanned/ProtectionRuleSettings` – проверка не выполнена, так как в правиле защиты для типа объектов **Объекты, обнаруженные KATA** задано действие **Пропустить проверку**. • `NotScanned/ApplicationSettings` – проверка не выполнена, так как режим получения объектов, обнаруженных KATA или интеграция KATA отключены согласно параметрам программы. • `ScanError/InternalError` – проверка завершилась с ошибкой.
Для объекта MIME-типа multipart указывается информация обо всех составных частях. Для каждой составной части используется ключ `part` с порядковым номером, после которого передаются все атрибуты этой составной части (ключи `filename`, `filesize`, `part_mimetype`, `kata_upload`, `guid`, `rules`, `av_status`, `ap_status`, `mlf-status`, `encrypted`, `macros` и `kata-alert`). Например, `part1 "news.html", <атрибуты составной части 1>: part2 <атрибуты составной части 2>`.	
`filename`	Имя проверяемого объекта. Если HTTP-сообщение не содержит объектов, указывается `"nofile"`. В этом случае все последующие поля относятся к проверяемому URL-адресу.

Ключ	Описание и возможные значения
`filesize`	Размер проверяемого объекта. Если HTTP-сообщение не содержит объектов или для применения правил не требуется вычисление размера файла, указывается `"NotApplicable"`.
`part_mimetype`	MIME-тип составной части multipart-объекта. Используется значение заголовка Content-Type. Если HTTP-сообщение не содержит объектов или для применения правил не требуется определение MIME-типа, указывается `"NotApplicable"`.
`kata_upload`	Результат проверки объекта на необходимость отправки на сервер KATA. Возможны следующие значения: • `NotApplicable` – HTTP-сообщение не содержит файлов. • `Scheduled` – отправка файла запланирована. • `DisabledBySettings` – режим отправки файлов на сервер KATA или интеграция KATA отключены в параметрах программы. • `SkippedByAction` – HTTP-сообщение пропущено по правилу обхода без проверки или к нему применены действия **Заблокировать** или **Перенаправить**. • `RejectedByFilter` – файл не удовлетворяет условиям отправки на сервер KATA. • `Failed/QueueOverflowed` – файл должен быть отправлен на сервер KATA, но запланировать отправку не удалось из-за переполнения очереди. • `Failed/InternalError` – файл должен быть отправлен на сервер KATA, но запланировать отправку не удалось из-за внутренней ошибки программы.
`guid`	Идентификатор, присвоенный объекту программой. Идентификатор передается, только если при проверке необходимости отправки на сервер KATA был присвоен один из следующих статусов: • `Scheduled`. • `Failed/QueueOverflowed`. • `Failed/InternalError`. Для других статусов поле `guid` передается с пустым значением.

Ключ	Описание и возможные значения
rules	Названия сработавших правил обработки трафика в следующем формате: "bypass_rule [<Название правила>], access_rules [<Название рабочей области>/<Название группы правил>/<Название правила>], protection_rules [<Название рабочей области>/<Название группы правил>/<Название правила>]". Если правило не относится к рабочей области, вместо названия рабочей области отображается прочерк. Если правило не входит в группу правил, вместо названия группы отображается прочерк. Если не было применено ни одно правило обработки трафика, применяется политика защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. 94). Отображается значение "default_policy [Default Policy]".
av_status	Результаты проверки веб-ресурса модулем Антивирус. Возможны следующие значения: • Detected – в объекте найдены вирусы или другие программы, представляющие угрозу. Через запятую указываются имена обнаруженных угроз и действие программы над объектом. Например, av-status="Detected", threats="EICAR-Test-File/Block". • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • IncompleteScan/MaxNestingLevelReached – проверка не была выполнена, так как уровень вложенности проверяемого архива превышает максимально допустимый. • IncompleteScan/EncryptedArchive – проверка не была выполнена, так как объект зашифрован. • Disinfected – обнаружены угрозы, все угрозы вылечены. • NotDetected – объект проверен, угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
ap_status	Результаты проверки веб-ресурса модулем Анти-Фишинг. Возможны следующие значения: • Detected (local bases) – ссылка признана фишинговой на основе записей в локальных базах программы. • Detected (KSN) – ссылка признана фишинговой на основе проверки репутации в KSN. • Detected (heuristics) – ссылка признана фишинговой на основе данных эвристического анализа. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • NotDetected – объект проверен, угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
`mlf-status`	Результаты проверки ссылок на наличие вредоносных объектов. Возможны следующие значения: • `Detected (local bases)` – ссылка признана вредоносной на основе записей в локальных антивирусных базах. • `Detected (KSN)` – ссылка признана вредоносной на основе проверки репутации в KSN. • `ScanError/Timeout` – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • `ScanError/InternalError` – проверка завершилась с внутренней ошибкой. • `ScanError/BasesNotLoaded` – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • `NotDetected` – ссылка проверена, угрозы не обнаружены. • `NotScanned/AccessRuleSettings` – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • `NotScanned/BypassRuleSettings` – объект не проходил проверку, так как к нему было применено правило обхода. • `NotScanned/ProtectionRuleSettings` – объект не проходил проверку согласно действию, заданному в правиле защиты. • `NotScanned/ApplicationSettings` – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
encrypted	Информация о шифровании проверяемого объекта. Возможны следующие значения: • Detected – обнаружены угрозы. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • NotDetected – ссылка проверена, NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам программы.угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам программы.
macros	Информация о наличии макросов в проверяемом объекте. Возможны следующие значения: • Detected – обнаружены макросы. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • NotDetected – объект проверен, макросы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
`kata-alert`	Результат проверки файла, содержащегося в HTTP-сообщении, или составной части (для multipart-объектов) на соответствие объектам, обнаруженным программой KATA. Возможны следующие значения: • `NotDetected` – URL-адрес проверен, угрозы не обнаружены. • `Detected` – обнаружено соответствие с объектом в кеше KATA. Указывается ID объекта, критерий совпадения и технология. Например, `kata-alert="Detected/124567/Md5/Yara"`. • `NotScanned/AccessRuleSettings` – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • `NotScanned/BypassRuleSettings` – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • `NotScanned/ProtectionRuleSettings` – проверка не выполнена, так как в правиле защиты для типа объектов **Объекты, обнаруженные KATA** задано действие **Пропустить проверку**. • `NotScanned/ApplicationSettings` – проверка не выполнена, так как режим получения объектов, обнаруженных KATA или интеграция KATA отключены согласно параметрам программы. • `ScanError/InternalError` – проверка завершилась с ошибкой.

Содержание syslog-сообщений о системных событиях программы

Системные события программы содержат информацию о состоянии узлов кластера, модулей программы и лицензии.

В каждом syslog-сообщении для всех типов событий передаются следующие поля, определяемые параметрами Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение `KWTS`).

Пример:

```
Jan 5 03:39:01 hostname KWTS: Anti-Phishing bases applied:
publishing-time="2019-01-05T03:08:00"
```

Содержание syslog-сообщений в зависимости от типа системного события приведено в таблице ниже.

Таблица 11. Содержание syslog-сообщений в зависимости от типа системного события

Тип события	Описание события	Сообщение
Запуск / остановка программы	Программа запущена	`audit started`
	Программа остановлена	`audit stopped`
Обновление баз модуля Антивирус	Ошибка загрузки баз	`Anti-Virus bases loading error: <причина ошибки>`
	Ошибка обновления баз	`Anti-Virus bases update error: <причина ошибки>`
	Базы успешно загружены	`Anti-Virus bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>`
	Базы успешно обновлены	`Anti-Virus bases updated`
Обновление баз модуля Анти-Фишинг	Ошибка загрузки баз	`Anti-Phishing bases loading error: <причина ошибки>`
	Ошибка обновления баз	`Anti-Phishing bases update error: <причина ошибки>`
	Базы успешно загружены	`Anti-Phishing bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>`
	Базы успешно обновлены	`Anti-Phishing bases updated`

Тип события	Описание события	Сообщение
Лицензирование	Срок действия лицензии истек	`license key expired: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" expiration-date="<дата и время истечения срока действия лицензии>"`
	Ошибка лицензии	`license error: <описание ошибки>`
	Лицензионный ключ помещен в черный список	`license is blacklisted: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"`
	Код активации заблокирован до активации программы	`activation code cannot be installed as it is blocked`
	Лицензия отсутствует	`no license`
	Код активации успешно добавлен	`license installed: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"`
	Статус лицензионного ключа успешно обновлен	`license updated: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"`
	Код активации успешно удален	`license removed: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"`

Тип события	Описание события	Сообщение
	Срок действия лицензии скоро истекает	`license expires soon: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>`
	Действует льготный период действия лицензии	`license grace period: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>`
	Лицензия действительна	`license is ok: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"`
Процессы	Процесс программы завершился аварийно (при многократных аварийных остановках указывается количество остановок и период, за который они произошли)	`<имя процесса> crashed [<количество остановок> times during last <количество минут> minutes]`
	Процесс программы перезапущен (при многократных перезапусках процесса указывается количество перезапусков и период, за который они произошли)	`<имя процесса> restarted [<количество перезапусков> times during last <количество минут> minutes]`

Содержание syslog-сообщений о событиях отправки файлов на сервер KATA

Информация о помещении файла в очередь на отправку в KATA, а также результаты отправки файла в KATA записываются в журнал операционной системы по протоколу Syslog.

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение `KWTS`).

В зависимости от типа события передается поле `KATA upload scheduling` (помещение файла в очередь на отправку) или `KATA uploading` (отправка файла). Поля syslog-сообщения, определяемые параметрами программы, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

```
Oct 2 13:19:27 localhost KWTS: KATA uploading: result="Succeeded":
type="Request": http_user_name="example@test.local":
http_user_ip="192.0.2.0": url="http://example.com/TEST/test.pdf":
guid="A485A9DD-A740-4ED3-9933-63ACAEA964E4": filename="test.pdf":
filetype="OfficePdf"
```

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 12. Информация о событиях отправки файлов на сервер KATA в syslog-сообщениях

Ключ	Описание и возможные значения
`result`	Результат помещения файла в очередь на отправку или отправки файла. Возможны следующие значения: • `Succeeded` – операция выполнена успешно. • `Failed/<причина>` – не удалось поместить файл в очередь на отправку по указанной причине.
`type`	Тип HTTP-сообщения. Возможны следующие значения: • `Request` – запрос. • `Response` – ответ.
`http_user_name`	Имя учетной записи пользователя, от имени которого выполнена операция с файлом.
`http_user_ip`	IP-адрес компьютера, с которого был отправлен файл.
`url`	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.
`guid`	Идентификатор, который был присвоен файлу программой.
`filename`	Имя отправляемого файла.
`filetype`	Тип отправляемого файла.

kaspersky

Работа с программой по протоколу SNMP

SNMP (Simple Network Management Protocol – простой протокол сетевого управления) – протокол управления сетевыми устройствами.

В Kaspersky Web Traffic Security для работы по протоколу SNMP используется *SNMP-агент*, который отслеживает информацию о работе программы. Kaspersky Web Traffic Security может отправлять эту информацию в виде *SNMP-ловушек* – уведомлений о событиях работы программы.

Для работы по протоколу SNMP требуется предварительно настроить службу snmpd в операционной системе (см. раздел «Настройка службы snmpd в операционной системе» на стр. 184).

По протоколу SNMP вы можете получить доступ к следующей информации о программе:

- общим сведениям;
- статистике работы Kaspersky Web Traffic Security с момента установки программы;
- данным о событиях, возникающих в ходе работы программы.

Доступ предоставляется только на чтение информации.

Информация об SNMP-ловушках и статистике, отправляемой по протоколу SNMP, хранится в базе данных MIB (см. раздел "Описание объектов MIB Kaspersky Web Traffic Security" на стр. 188).

В этом разделе

Настройка службы snmpd в операционной системе

► *Чтобы настроить службу snmpd, выполните следующие действия:*

1. Добавьте в файл /etc/snmp/snmpd.conf следующие строки для соединений через Unix-сокет:

```
master agentx
agentXSocket unix:/var/run/agentx-master.socket
```

```
agentXPerms 770 770 kluser klusers
```

2. Перезапустите службу snmpd. Для этого выполните команду:

```
service snmpd restart
```

Служба snmpd будет настроена. Для работы с программой по протоколу SNMP вам требуется включить его использование (см. раздел "Включение и отключение использования SNMP в программе" на стр. 185) в веб-интерфейсе программы.

Если служба snmpd была настроена до установки Kaspersky Web Traffic Security, передача данных программы по протоколу SNMP может осуществляться некорректно. В этом случае требуется повторно перезапустить службу snmpd.

Включение и отключение использования SNMP в программе

► *Чтобы включить или отключить использование SNMP в работе программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите включить использование SNMP.
   - Выключите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите отключить использование SNMP.
3. Нажмите на кнопку **Сохранить**.

Настройка параметров подключения к SNMP-серверу

► *Чтобы настроить параметры подключения к SNMP-серверу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
2. В раскрывающемся списке **Тип сокета** выберите, какой сокет должен быть использован для подключения к SNMP-серверу.

   Для безопасной передачи данных рекомендуется выбирать **UNIX**.

3. Если вы выбрали **UNIX**, в поле **Путь к UNIX-сокету**, укажите путь к файлу сокета.
4. Если вы выбрали **TCP**, в блоке параметров **Адрес SNMP-сервера** введите IP-адрес или имя хоста SNMP-сервера и порт подключения к SNMP-серверу.
5. В поле **Время ожидания ответа сервера (сек.)** укажите максимальное время ожидания ответа от

SNMP-сервера в секундах. Вы можете указать значение в интервале от 1 до 255 секунд.

Значение по умолчанию: 15 секунд.

6. Нажмите на кнопку **Сохранить**.

Соединение с SNMP-сервером будет настроено.

Настройка шифрования SNMP-соединений

Сторонние программы могут получать доступ к данным, отправляемым по протоколу SNMP, или заменять эти данные своими данными. Для безопасной передачи данных по протоколу SNMP рекомендуется настроить шифрование SNMP-соединений.

Перед настройкой убедитесь, что на всех серверах с программой Kaspersky Web Traffic Security установлены службы snmpd и snmptrapd.

► *Чтобы настроить шифрование SNMP-соединений, выполните следующие действия:*

1. Получите EngineID, необходимый для обработки SNMP-ловушек. Для этого на Управляющем сервере выполните команду:

   ```
   snmpget -v2c -cpublic localhost SNMP-FRAMEWORK-MIB::snmpEngineID.0
   2>/dev/null | sed -ne 's/ //g; s/.*:/0x/p'
   ```

2. На каждом сервере настройте службу snmpd. Для этого выполните следующие действия:

   a. Остановите службу snmpd. Для этого выполните команду:

      ```
      service snmpd stop
      ```

   b. В зависимости от операционной системы добавьте строку `createUser kwts-snmp-user SHA "<password>" AES "<password>"` в следующий конфигурационный файл:

      - Ubuntu или Debian.

        /var/lib/snmpd/snmpd.conf

      - CentOS, SUSE Linux Enterprise Server или Red Hat Enterprise Linux.

        /var/lib/net-snmp/snmpd.conf

      Если в указанной директории нет конфигурационного файла, вам необходимо его создать.

   c. Создайте конфигурационный файл /etc/snmp/snmpd.conf со следующим содержанием:

      ```
      # accept KWTS statistics over unix socket
      agentXSocket unix:/var/run/agentx-master
      agentXPerms 770 770 kluser klusers
      master agentx
      ```

```
# accept incoming SNMP requests over UDP and TCP
agentAddress udp:localhost:161,tcp:localhost:161
rouser kwts-snmp-user priv .1.3.6.1
# comment the following line if you don't need SNMP traps forwarding over SNMPv3 connection
trapsess -e <EngineID> -v3 -l authPriv -u kwts-snmp-user -a SHA -A <password> -x AES -X <password> udp:localhost:162
```

d. Добавьте в конфигурационный файл /etc/snmp/snmp.conf следующие строки:

```
mibdirs +/opt/kaspersky/kwts/share/snmp-mibs/
mibs all
```

e. Запустите службу snmpd. Для этого выполните команду:

```
service snmpd start
```

f. Проверьте SNMP-соединение. Для этого выполните следующие команды:

```
snmpwalk -mALL -v3 -l authPriv -u kwts-snmp-user -a SHA -A <password> -x AES -X <password> udp:localhost:161 .1.3.6.1.4.1.23668
snmpget -v3 -l authPriv -u kwts-snmp-user -a SHA -A <password> -x AES -X <password> udp:localhost:161 .1.3.6.1.4.1.23668.2022.2.8.1.0
```

3. На сервере, на котором вы хотите получать SNMP-ловушки, настройте службу snmptrapd. Для этого выполните следующие действия:

a. Остановите службу snmptrapd. Для этого выполните команду:

```
service snmptrapd stop
```

b. В зависимости от операционной системы добавьте строку `createUser -e <EngineID> kwts-snmp-user SHA "<password>" AES "<password>"` в следующий конфигурационный файл:

- Ubuntu или Debian.

  /var/lib/snmpd/snmptrapd.conf

- CentOS, SUSE Linux Enterprise Server или Red Hat Enterprise Linux.

  /var/lib/net-snmp/snmptrapd.conf

Если в указанной директории нет конфигурационного файла, вам необходимо его создать.

c. Создайте конфигурационный файл /etc/snmp/snmptrapd.conf со следующим содержанием:

```
snmpTrapdAddr udp:<IP-address>:162,tcp:127.0.0.1:162
authUser log kwts-snmp-user priv
disableAuthorization no
```

> В качестве `<IP-address>` укажите IP-адрес, по которому сервис snmptrapd принимает сетевые соединения.

d. Запустите службу snmptrapd. Для этого выполните команду:

```
service snmptrapd start
```

e. Проверьте SNMP-соединение с помощью команды:

```
snmptrap -e <EngineID> -v3 -l authPriv -u kwts-snmp-user -a SHA -A
<password> -x AES -X <password> udp:localhost:162 0
.1.3.6.1.4.1.23668.2022.1.411
```

Шифрование SNMP-соединений будет настроено.

Включение и отключение отправки SNMP-ловушек

► *Чтобы включить или отключить отправку SNMP-ловушек событий, возникающих в ходе работы программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
2. Включите переключатель рядом с названием блока **Использовать SNMP**, если он выключен.
3. Выполните одно из следующих действий:
   - Установите флажок **Отправлять SNMP-ловушки**, если вы хотите включить отправку SNMP-ловушек.
   - Снимите флажок **Отправлять SNMP-ловушки**, если вы хотите отключить отправку SNMP-ловушек.
4. Нажмите на кнопку **Сохранить**.

Отправка SNMP-ловушек будет настроена.

Описание объектов MIB Kaspersky Web Traffic Security

В таблицах ниже приведена информация об объектах MIB Kaspersky Web Traffic Security.

События управления кластером

Таблица 13. События управления кластером

Символьное имя	Описание	Параметры
clusterConsistencyErrorEvent	Ошибка состояния серверов. Например, нет ни одного сервера с ролью Управляющий узел.	• Имя Управляющего узла. • Сообщение об ошибке.
clusterEmergencyStateEvent	Программа перешла в аварийный режим.	• Имя Управляющего узла. • Сообщение об ошибке.
settingsSynchronizationErrorEvent	Ошибка синхронизации параметров между Управляющим и Подчиненными узлами.	• Имя Управляющего узла. • Сообщение об ошибке.

События обработки трафика

Таблица 14. События обработки трафика

Символьное имя	Описание	Параметры
productStartEvent	Программа запущена. Это событие возникает после того, как запускаются все службы, необходимые для работы Kaspersky Web Traffic Security.	Нет параметров.
taskCrashEvent	Процесс программы завершился аварийно.	Полный путь к бинарному файлу.
taskRestartEvent	Процесс программы перезапущен.	Полный путь к бинарному файлу.
licenseInstalledEvent	Код активации добавлен.	Серийный номер лицензии.
licenseUpdatedEvent	Статус лицензионного ключа изменен.	• Серийный номер лицензии. • Тип лицензии. • Дата окончания срока действия лицензии.
licenseRevokedEvent	Код активации удален.	Серийный номер лицензии.
licenseExpiredEvent	Истек срок действия лицензии.	• Серийный номер лицензии. • Дата окончания срока действия лицензии.
licenseExpiresSoonEvent	Срок действия лицензии скоро истечет.	• Серийный номер лицензии. • Дата окончания срока действия лицензии.
licenseTrialPeriodIsOverEvent	Истек срок действия пробной лицензии.	• Серийный номер лицензии. • Дата окончания срока действия лицензии.

Символьное имя	Описание	Параметры
gracePeriodEvent	Начался льготный период действия лицензии.	• Серийный номер лицензии. • Количество дней до завершения льготного периода.
updateErrorEvent	Обновление баз программы завершилось ошибкой.	Причина ошибки.
avBasesOutdatedEvent	Базы модуля Антивирус устарели.	Нет параметров.
avBasesObsoletedEvent	Базы модуля Антивирус сильно устарели.	Нет параметров.
apBasesOutdatedEvent	Базы модуля Анти-Фишинг устарели.	Нет параметров.
apBasesObsoletedEvent	Базы модуля Анти-Фишинг сильно устарели.	Нет параметров.

Другие события программы

Таблица 15. Другие события программы

Символьное имя	Описание	Параметры
KsnConnectionStatusEvent	Изменение состояния подключения к службам KSN.	Новое состояние подключения: • `Ok`. • `Error`. • `KsnDisabled`. • `KsnRestrictedLicense`.
LdapCacheUpdateEvent	Запуск синхронизации данных с Active Directory.	• Статус синхронизации LDAP-кэша. • Статус синхронизации данных для автозаполнения учетных записей.

Статистика программы

Таблица 16. Статистика программы

Символьное имя	Описание
productName	Название программы.
productVersion	Версия программы.
installDate	Дата установки программы.
licenseExpireDate	Дата окончания срока действия лицензии.
licenseStatus	Состояние кода активации.

Статистика модуля Антивирус

Таблица 17. Статистика модуля Антивирус

Символьное имя	Описание
cleanObjects	Количество объектов, в которых не обнаружены угрозы.
infectedObjects	Количество зараженных объектов.
passwordProtectedObjects	Количество объектов, защищенных паролем.
docsWithMacro	Количество документов, содержащих макросы.
scanErrors	Количество ошибок, связанных с превышением максимального допустимого времени проверки.
notScannedSettingsObjects	Количество объектов, не проверенных в соответствии с параметрами правила обработки трафика.
notScannedDueToNestingLevel	Количество объектов, не проверенных из-за превышения допустимой глубины проверки архивов.

kaspersky

Аутентификация с помощью технологии единого входа

При включении технологии единого входа пользователям не требуется вводить данные учетной записи программы для подключения к веб-интерфейсу. Аутентификация осуществляется с помощью доменной учетной записи пользователя.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является самым надежным. При NTLM-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

В этом разделе

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имя субъекта-службы (далее также "SPN")* для каждого из этих узлов.

► *Чтобы создать keytab-файл, выполните следующие действия:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя с именем `control-<ваше имя>`.
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-<ваше имя>`. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN Управляющего
узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser
control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре>
-crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype
KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -out
C:\control-<ваше имя>.keytab
```

> Пример ввода имени узла: `node01.test.local@TEST.LOCAL`

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-<имя ранее созданного файла>.keytab -out C:\control-<новое имя>.keytab -setupn -setpass
   ```

Keytab-файл с именем `C:\control-<новое имя>.keytab` будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, при выполнении шага 3 вы создали файл под названием `control-tmp1.keytab`. Тогда для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp1.keytab -out C:\control-tmp2.keytab -setupn -setpass
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp2.keytab -out C:\control-tmp3.keytab -setupn -setpass
```

В результате будет создан файл с именем `control-tmp3.keytab`, содержащий все три добавленные SPN.

Настройка Kerberos-аутентификации

> Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS в зонах обратного просмотра присутствует PTR-запись для FQDN и URL (если URL отличается от FQDN) каждого узла кластера.

Если вы настраиваете аутентификацию с доменом, в названии которого содержится корневой домен `.local`, то для корректной работы Kerberos-аутентификации требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы настроить Kerberos-аутентификацию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **Kerberos-аутентификация** переведите переключатель **Использовать Kerberos** в положение **Включено**.
3. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 192).

   Keytab-файл должен содержать SPN Управляющего узла и Подчиненных узлов.

   Откроется окно выбора файла.
4. Выберите keytab-файл и нажмите на кнопку **Открыть**.
5. Нажмите на кнопку **Сохранить**.

   Если в keytab-файле не найдено SPN Управляющего узла или SPN какого-либо из Подчиненных узлов, то для этого узла в разделе **Узлы** отображается статус *Отсутствует SPN-идентификатор для службы единого входа Kerberos*. Если в keytab-файле не найдено SPN ни одного из узлов, кнопка **Сохранить** недоступна.

Kerberos-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При отключении Kerberos-аутентификации ранее загруженный keytab-файл удаляется.

Настройка NTLM-аутентификации

► *Чтобы настроить NTLM-аутентификацию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **NTLM-аутентификация** переведите переключатель **Использовать NTLM** в положение **Включено**.

3. В поле **IP-адрес/доменное имя контроллера домена** укажите IP-адрес или доменное имя доменного контроллера, с помощью которого будет осуществляться аутентификация.

   Вы можете указать два доменных контроллера. Для добавления второго контроллера необходимо нажать на кнопку  .

4. В поле **Порт** укажите порт для подключения к доменному контроллеру.

   По умолчанию используется порт 445.

5. Нажмите на кнопку **Сохранить**.

NTLM-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При подключении с компьютеров, не входящих в домен, пользователю потребуется указать данные своей доменной учетной записи.

Источники информации о программе

Страница Kaspersky Web Traffic Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Web Traffic Security (https://www.kaspersky.com/small-to-medium-business-security/proxy-web-traffic) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

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

Страница Kaspersky Web Traffic Security в Базе знаний

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

На странице Kaspersky Web Traffic Security в Базе знаний (https://support.kaspersky.com/kwts6) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе (https://community.kaspersky.com).

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 199).

kaspersky

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 (см. раздел "Источники информации о программе" на стр. 196), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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 (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файлы трассировки*. Файлы трассировки позволяют отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка. Вы можете выбрать, какие события будут записаны в файлы трассировки (ошибки или информационные сообщения). Все файлы трассировки помещаются в архив, который вы может передать в Службу технической поддержки.

Файлы трассировки могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Необходимо согласовать состав отправляемого архива со Службой безопасности вашей организации. Перед отправкой журнала трассировки удалите из него все данные, которые вы считаете конфиденциальными.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на сервере и другая диагностическая информация.

Отладочная информация о работе программы записывается в соответствии с заданным уровнем трассировки (см. раздел "Изменение уровня трассировки" на стр. 202). Место хранения зависит от комплекта поставки:

- категория Local0 журнала отладочной информации при развертывании программы из iso-файла;
- папка /var/log/kaspersky/kwts при установке программы из rpm- или deb-пакета.

В этом разделе

Запуск трассировки

► *Чтобы запустить трассировку, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Запустить трассировку**.

   Откроется окно **Выбор узлов для запуска трассировки**.

4. В таблице серверов установите флажки напротив тех серверов, для которых вы хотите сформировать файлы трассировки.
5. Нажмите на кнопку **Запустить**.

   Откроется окно **Журналы трассировки для Службы технической поддержки** с результатом запуска трассировки. Созданный журнал трассировки содержит отдельный файл для каждого сервера.

Изменение уровня трассировки

Изменение уровня трассировки сохраняется в конфигурации программы и не влияет на уже созданные файлы трассировки.

► *Чтобы выбрать уровень трассировки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Изменить уровень трассировки**.

   Откроется окно **Уровень трассировки**.
4. Выберите один из следующих вариантов:
   - **Уровень ошибки**.
   - **Уровень отладки**.

     Этот уровень трассировки значительно повышает требования к подсистеме хранения данных и снижает производительность программы. Используйте уровень отладки только если Служба технической поддержки "Лаборатории Касперского" просит предоставить файлы трассировки такого типа.
5. Нажмите на кнопку **Сохранить**.

   Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

   Трассировка будет производиться в соответствии с выбранным уровнем трассировки.

Просмотр журналов трассировки

► *Чтобы просмотреть журналы трассировки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Просмотреть журналы трассировки**.

Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.

4. Если вы хотите посмотреть, информация о каких серверах содержится в журнале трассировки, нажмите на кнопку  в выбранной строке.

Сохранение файла трассировки на компьютере

► *Чтобы сохранить файл трассировки на компьютере, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Просмотреть журналы трассировки**.

   Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.
4. Нажмите на кнопку  напротив названия журнала трассировки, файлы которого вы хотите загрузить.
5. В строке с нужным файлом нажмите на кнопку **Скачать**.

Файл трассировки будет сохранен на компьютере в папке загрузки браузера.

kaspersky

Приложение 1. Установка и настройка сервиса Squid

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Web Traffic Security не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Web Traffic Security с помощью туннелирования трафика или средствами iptables.

Вы можете не использовать отдельный прокси-сервер и вместо него установить сервис Squid.

В этом разделе

Установка сервиса Squid

► *Чтобы установить сервис Squid, выполните следующие действия:*

1. Установите пакет сервиса Squid. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     yum install -y squid
     ```
   - SUSE Linux Enterprise Server:

     ```
     zypper install squid
     ```
   - Ubuntu или Debian:

     ```
     apt-get install squid
     ```
2. Добавьте сервис Squid в автозагрузку. Для этого выполните команду:

   ```
   systemctl enable squid
   ```
3. Запустите сервис Squid. Для этого выполните команду:

   ```
   service squid start
   ```
4. Проверьте статус сервиса Squid. Для этого выполните команду:

   ```
   service squid status
   ```

   Параметр **Active** должен содержать значение **active (running)**.

Сервис Squid будет установлен.

Настройка сервиса Squid

► *Чтобы настроить сервис Squid, выполните следующие действия:*

1. Измените параметры сервиса Squid. Для этого выполните команды:

   ```
   echo "icap_enable on" >> /etc/squid/squid.conf
   ```

   ```
   echo "icap_send_client_ip on" >> /etc/squid/squid.conf
   ```

   ```
   echo "icap_service is_kav_req reqmod_precache 0
   icap://127.0.0.1:1344/av/reqmod" >> /etc/squid/squid.conf
   ```

   ```
   echo "icap_service is_kav_resp respmod_precache 0
   icap://127.0.0.1:1344/av/respmod" >> /etc/squid/squid.conf
   ```

   ```
   echo "adaptation_access is_kav_req allow all" >> /etc/squid/squid.conf
   ```

   ```
   echo "adaptation_access is_kav_resp allow all" >> /etc/squid/squid.conf
   ```

2. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   service squid restart
   ```

Настройка сервиса Squid завершится.

Настройка SSL Bumping в сервисе Squid

► *Чтобы настроить SSL Bumping в сервисе Squid, выполните следующие действия:*

1. Убедитесь, что используемый сервис Squid поддерживает необходимые опции. Для этого выполните команду:

   ```
   squid -v
   ```

   Параметр `configure options` должен содержать значения `--enable-ssl-crtd` и `--with-openssl`.

2. Перейдите в директорию сервиса Squid. Для этого выполните команду:

   ```
   cd /etc/squid
   ```

3. Создайте самоподписанный SSL-сертификат. Для этого выполните команду:

   ```
   openssl req -new -newkey rsa:2048 -days <количество дней действия
   сертификата> -nodes -x509 -keyout squidCA.pem -out squidCA.pem
   ```

   Отобразится предложение заполнить поля самоподписанного SSL-сертификата.

4. Заполните поля самоподписанного SSL-сертификата.

5. Создайте доверенный сертификат для импорта в браузер. Для этого выполните команду:

   ```
   openssl x509 -in squidCA.pem -outform DER -out squid.der
   ```

6. Импортируйте файл squid.der в браузеры пользователей локальных компьютеров.

   Способ импорта файла squid.der в браузер зависит от типа браузера.

7. Настройте права на использование файла самоподписанного сертификата. Для этого выполните следующие команды в зависимости от используемой операционной системы:

   - CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server:

     ```
     chown squid:squid squidCA.pem
     chmod 400 squidCA.pem
     ```

   - Ubuntu или Debian:

     ```
     chown proxy:proxy squidCA.pem
     chmod 400 squidCA.pem
     ```

8. Создайте директорию для будущих сертификатов. Для этого выполните следующие команды в зависимости от используемой операционной системы:

   - CentOS или Red Hat Enterprise Linux:

     ```
     mkdir -p /var/lib/squid
     /usr/lib64/squid/ssl_crtd -c -s /var/lib/squid/ssl_db
     chown -R squid:squid /var/lib/squid
     ```

   - Ubuntu:

     ```
     mkdir -p /var/lib/squid
     /usr/lib/squid/ssl_crtd -c -s /var/lib/squid/ssl_db
     chown -R proxy:proxy /var/lib/squid
     ```

   - SUSE Linux Enterprise Server:

     ```
     mkdir -p /var/lib/squid
     /usr/sbin/ssl_crtd -c -s /var/lib/squid/ssl_db
     chown -R squid:squid /var/lib/squid
     ```

   - В операционной системе Debian сервис Squid по умолчанию не поддерживает SSL Bumping. Если сервис Squid был скомпилирован с включенной поддержкой SSL Bumping, вам требуется создать директорию для будущих сертификатов с помощью следующих команд:

     ```
     mkdir -p /var/lib/squid
     <путь, указанный при компиляции>/ssl_crtd -c -s /var/lib/squid/ssl_db
     chown -R <пользователь, указанный при компиляции>:<группа, указанная при компиляции> /var/lib/squid
     ```

9. Измените параметры сервиса Squid. Для этого в файле /etc/squid/squid.conf выполните следующие действия:

   a. Замените `http_port 3128` на `http_port 3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/squidCA.pem`.

   b. Добавьте в конец файла следующие строки:

- CentOS или Red Hat Enterprise Linux:

```
sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/squid/ssl_db
-M 4MB

sslcrtd_children 5

ssl_bump server-first all

sslproxy_cert_error deny all
```

- Ubuntu:

```
sslcrtd_program /usr/lib/squid/ssl_crtd -s /var/lib/squid/ssl_db -M
4MB

sslcrtd_children 5

ssl_bump server-first all

sslproxy_cert_error deny all
```

- SUSE Linux Enterprise Server:

```
sslcrtd_program /usr/sbin/ssl_crtd -s /var/lib/squid/ssl_db -M 4MB

sslcrtd_children 5

ssl_bump server-first all

sslproxy_cert_error deny all
```

- Debian (если сервис Squid был скомпилирован с включенной поддержкой SSL Bumping):

```
sslcrtd_program <путь, указанный при компиляции>/ssl_crtd -s
/var/lib/squid/ssl_db -M 4MB

sslcrtd_children 5

ssl_bump server-first all

sslproxy_cert_error deny all
```

c. Если вы хотите исключить из проверки сертификаты для доверенных доменов, добавьте следующие строки:

- CentOS или Red Hat Enterprise Linux:

```
sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/squid/ssl_db
-M 4MB

sslcrtd_children 5

ssl_bump server-first all

acl BrokenButTrustedServers dstdomain <example.com>

sslproxy_cert_error allow BrokenButTrustedServers

sslproxy_cert_error deny all
```

- Ubuntu:

```
sslcrtd_program /usr/lib/squid/ssl_crtd -s /var/lib/squid/ssl_db -M
4MB
```

```
sslcrtd_children 5
ssl_bump server-first all
acl BrokenButTrustedServers dstdomain <example.com>
sslproxy_cert_error allow BrokenButTrustedServers
sslproxy_cert_error deny all
```

- SUSE Linux Enterprise Server:

```
sslcrtd_program /usr/sbin/squid/ssl_crtd -s /var/lib/squid/ssl_db -M
4MB
sslcrtd_children 5
ssl_bump server-first all
acl BrokenButTrustedServers dstdomain <example.com>
sslproxy_cert_error allow BrokenButTrustedServers
sslproxy_cert_error deny all
```

- Debian (если сервис Squid был скомпилирован с включенной поддержкой SSL Bumping):

```
sslcrtd_program <путь, указанный при компиляции>/ssl_crtd -s
/var/lib/squid/ssl_db -M 4MB
sslcrtd_children 5
ssl_bump server-first all
acl BrokenButTrustedServers dstdomain <example.com>
sslproxy_cert_error allow BrokenButTrustedServers
sslproxy_cert_error deny all
```

d. Если вы хотите отключить проверку сертификатов для всех доменов, добавьте следующие строки:

- CentOS или Red Hat Enterprise Linux:

```
sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/squid/ssl_db
-M 4MB
sslcrtd_children 5
ssl_bump server-first all
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER
```

- Ubuntu:

```
sslcrtd_program /usr/lib/squid/ssl_crtd -s /var/lib/squid/ssl_db -M
4MB
sslcrtd_children 5
ssl_bump server-first all
sslproxy_cert_error allow all
```

```
sslproxy_flags DONT_VERIFY_PEER
```

- SUSE Linux Enterprise Server:

```
sslcrtd_program /usr/sbin/squid/ssl_crtd -s /var/lib/squid/ssl_db -M 4MB
sslcrtd_children 5
ssl_bump server-first all
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER
```

- Debian (если сервис Squid был скомпилирован с включенной поддержкой SSL Bumping):

```
sslcrtd_program <путь зависит от настроек при компиляции>/ssl_crtd -s /var/lib/squid/ssl_db -M 4MB
sslcrtd_children 5
ssl_bump server-first all
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER
```

10. Перезагрузите сервис Squid. Для этого выполните команду:

```
service squid restart
```

Настройка SSL Bumping в сервисе Squid будет завершена.

kaspersky

Приложение 2. Настройка интеграции сервиса Squid с Active Directory

Интеграция с Active Directory позволяет добавлять пользователей из Active Directory в качестве инициатора срабатывания правила обработки трафика (см. раздел "Настройка инициатора срабатывания правила" на стр. 82);

Вы можете использовать следующие механизмы аутентификации:

- Kerberos-аутентификация.
- NTLM-аутентификация.
- Basic-аутентификация.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является самым надежным. При NTLM- и Basic-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

В этом разделе

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS присутствует PTR-запись для каждого контроллера домена.

Выполняйте действия по настройке Kerberos-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись должна обладать правами суперпользователя.

kaspersky

В этом разделе

Установка пакета Kerberos

► *Чтобы установить пакет Kerberos, выполните одну из следующих команд в зависимости от используемой операционной системы:*

- CentOS или Red Hat Enterprise Linux:

  ```
  yum install krb5-workstation
  ```

- SUSE Linux Enterprise Server:

  ```
  zypper install krb5-client
  ```

- Ubuntu или Debian:

  ```
  apt-get install krb5-user
  ```

Настройка синхронизации времени

► *Чтобы настроить синхронизацию времени с NTP-серверами, выполните следующие действия:*

1. Установите пакет chrony. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     yum install -y chrony
     ```

   - SUSE Linux Enterprise Server:

     ```
     zypper install chrony
     ```

   - Ubuntu или Debian:

     ```
     apt-get install chrony
     ```

2. Включите автозапуск сервиса chronyd. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - Ubuntu или Debian:

     ```
     systemctl enable chrony
     ```

   - Остальные операционные системы:

```
systemctl enable chronyd
```

3. В зависимости от используемой операционной системы откройте один из следующих файлов:
   - CentOS, Red Hat Enterprise Linux, SUSE Linux Enterprise Server или Debian:

     /etc/chrony.conf
   - Ubuntu:

     /etc/chrony/chrony.conf
4. Добавьте строки с IP-адресами тех NTP-серверов, с которыми вы хотите настроить синхронизацию времени. Например:

   ```
   server <IP-адрес NTP-сервера> iburst
   ```
5. Закомментируйте (добавьте символ # в начало строки) строки с IP-адресами тех NTP-серверов, которые вы не хотите использовать для синхронизации времени.
6. Если для синхронизации времени вы используете контроллер домена Windows®, добавьте строку:

   ```
   maxdistance 16.0
   ```
7. Сохраните и закройте файл chrony.conf.
8. Перезапустите сервис chronyd. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - Ubuntu или Debian:

     ```
     systemctl restart chrony
     ```
   - Остальные операционные системы:

     ```
     systemctl restart chronyd
     ```
9. Проверьте синхронизацию времени. Для этого выполните команду:

   ```
   chronyc sources -v
   ```

   Если отобразившиеся IP-адреса совпадают с адресами NTP-серверов, которые вы указали в файле chrony.conf, то синхронизация настроена верно.

Синхронизация времени сервера Squid и NTP-серверов будет настроена.

Настройка DNS

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

1. Укажите IP-адрес DNS-сервера (серверов), который используется для работы с Active Directory, на сервере с сервисом Squid.

   Подробнее о способах настройки DNS в различных операционных системах см. в документации к этим операционным системам.
2. Убедитесь, что DNS-зона Active Directory доступна. Для этого выполните команду:

   ```
   dig +short <домен Active Directory>
   ```

> Для использования утилиты dig может потребоваться предварительная установка пакета bind-utils.

Отобразятся A-записи контроллеров домена Active Directory.

3. Убедитесь, что для каждого контроллера домена присутствует PTR-запись. Для этого выполните команду:

   ```
   host <IP-адрес контроллера домена>
   ```

   > Для использования утилиты host может потребоваться предварительная установка пакета bind-utils.

   Отобразится PTR-запись контроллера домена Active Directory.

4. Укажите имя сервера с сервисом Squid. Для этого выполните команду:

   ```
   hostnamectl set-hostname <имя сервера с сервисом Squid>
   ```

   Имя сервера с сервисом Squid должно совпадать с именем этого сервера на DNS-сервере.

5. Добавьте A- и PTR-записи на DNS-сервере Active Directory для сервера с сервисом Squid.

   > Для создания PTR-записи вам может потребоваться добавить обратную зону.

6. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команду:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.

7. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

Параметры DNS будут настроены.

Создание keytab-файла для сервиса Squid

► *Чтобы создать keytab-файл для сервиса Squid, выполните следующие действия:*

1. Подключитесь к контроллеру домена Active Directory.
2. В оснастке Domains Users and Computers создайте пользователя с именем squid-user.
3. Запустите создание keytab-файла для пользователя squid-user. Для этого выполните команду:

   ```
   C:\Windows\system32\ktpass.exe /princ HTTP/<имя сервера с сервисом Squid>@<realm Active Directory в верхнем регистре> /mapuser squid-user@<realm Active Directory в верхнем регистре> /crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> /ptype KRB5_NT_PRINCIPAL
   ```

```
/pass <пароль пользователя squid-user> /out squid.keytab
```

> Имя сервера с сервисом Squid требуется указывать в нижнем регистре (например, `proxy.company.com`).

Keytab-файл для сервиса Squid будет создан.

Настройка клиентской части Kerberos

Если вы настраиваете аутентификацию с доменом, в названии которого содержится корневой домен `.local`, то для корректной работы Kerberos-аутентификации требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы настроить клиентскую часть Kerberos, выполните следующие действия:*

1. Переименуйте файл squid.keytab в файл krb5.keytab и переместите в директорию etc. Для этого выполните команду:

   ```
   mv /tmp/squid.keytab /etc/krb5.keytab
   ```

2. Измените владельца файла krb5.keytab и идентификатор группы на squid. Для этого выполните следующую команду в зависимости от используемой операционной системы:

   - CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server:

     ```
     chown squid:squid krb5.keytab
     ```

   - Ubuntu или Debian:

     ```
     chown proxy:proxy krb5.keytab
     ```

   По умолчанию владельцем файла krb5.keytab является суперпользователь.

3. Добавьте в начало файла /etc/squid/squid.conf следующие параметры в зависимости от используемой операционной системы:

   - CentOS или Red Hat Enterprise Linux:

     ```
     auth_param negotiate program /usr/lib64/squid/negotiate_kerberos_auth
     -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory в верхнем
     регистре>
     auth_param negotiate children 10
     auth_param negotiate keep_alive on
     acl lan proxy_auth REQUIRED
     ```

```
icap_send_client_username on
http_access allow lan
```

- SUSE Linux Enterprise Server:

```
auth_param negotiate program /usr/sbin/negotiate_kerberos_auth -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory в верхнем регистре>
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl lan proxy_auth REQUIRED
icap_send_client_username on
http_access allow lan
```

- Ubuntu или Debian:

```
auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory в верхнем регистре>
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl lan proxy_auth REQUIRED
icap_send_client_username on
http_access allow lan
```

4. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `-d` в первую строку:

   - CentOS или Red Hat Enterprise Linux:

```
auth_param negotiate program /usr/lib64/squid/negotiate_kerberos_auth -d -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory>
```

   - SUSE Linux Enterprise Server:

```
auth_param negotiate program /usr/sbin/negotiate_kerberos_auth -d -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory в верхнем регистре>
```

   - Ubuntu или Debian:

```
auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -d -s HTTP/<имя сервера с сервисом Squid>@<realm Active Directory>
```

   Отладочные события будут записаны в файл /var/log/squid/cache.log.

5. Перезагрузите сервис Squid. Для этого выполните команду:

```
service squid restart
```

6. На компьютерах локальной сети организации в параметрах браузера укажите FQDN-адрес сервера с сервисом Squid в качестве прокси-сервера.

Клиентская часть Kerberos будет настроена.

Настройка NTLM-аутентификации

Рекомендуется использовать Kerberos-аутентификацию для обеспечения безопасности передачи данных. Используйте NTLM-аутентификацию, только если невозможно использовать Kerberos-аутентификацию. Если вы используете NTLM-аутентификацию, необходимо включить протокол Samba версии 2.

Выполняйте действия по настройке NTLM-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись должна обладать правами суперпользователя.

В этом разделе

Установка сервиса Samba

► *Чтобы установить сервис Samba и пакеты, необходимые для работы сервиса Samba, выполните одну из следующих команд в зависимости от используемой операционной системы:*

- CentOS или Red Hat Enterprise Linux:

  ```
  yum install samba samba-client samba-winbind samba-winbind-clients
  pam_krb5 krb5-workstation
  ```

- SUSE Linux Enterprise Server:

  ```
  zypper install samba samba-client samba-winbind
  ```

- Ubuntu или Debian:

  ```
  apt-get install samba winbind
  ```

kaspersky

Настройка синхронизации времени

► *Чтобы настроить синхронизацию времени с NTP-серверами, выполните следующие действия:*

1. Установите пакет chrony. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     yum install -y chrony
     ```
   - SUSE Linux Enterprise Server:

     ```
     zypper install chrony
     ```
   - Ubuntu или Debian:

     ```
     apt-get install chrony
     ```
2. Включите автозапуск сервиса chronyd. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - Ubuntu или Debian:

     ```
     systemctl enable chrony
     ```
   - Остальные операционные системы:

     ```
     systemctl enable chronyd
     ```
3. В зависимости от используемой операционной системы откройте один из следующих файлов:
   - CentOS, Red Hat Enterprise Linux, SUSE Linux Enterprise Server или Debian:

     /etc/chrony.conf
   - Ubuntu:

     /etc/chrony/chrony.conf
4. Добавьте строки с IP-адресами тех NTP-серверов, с которыми вы хотите настроить синхронизацию времени. Например:

   ```
   server <IP-адрес NTP-сервера> iburst
   ```
5. Закомментируйте (добавьте символ # в начало строки) строки с IP-адресами тех NTP-серверов, которые вы не хотите использовать для синхронизации времени.
6. Если для синхронизации времени вы используете контроллер домена Windows, добавьте строку:

   ```
   maxdistance 16.0
   ```
7. Сохраните и закройте файл chrony.conf.
8. Перезапустите сервис chronyd. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - Ubuntu или Debian:

     ```
     systemctl restart chrony
     ```
   - Остальные операционные системы:

     ```
     systemctl restart chronyd
     ```

9. Проверьте синхронизацию времени. Для этого выполните команду:

   ```
   chronyc sources -v
   ```

   Если отобразившиеся IP-адреса совпадают с адресами NTP-серверов, которые вы указали в файле chrony.conf, то синхронизация настроена верно.

Синхронизация времени сервера Squid и NTP-серверов будет настроена.

Настройка DNS

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

1. Укажите IP-адрес DNS-сервера (серверов), который используется для работы с Active Directory, на сервере с сервисом Squid.

   > Подробнее о способах настройки DNS в различных операционных системах см. в документации к этим операционным системам.

2. Убедитесь, что DNS-зона Active Directory доступна с сервера с сервисом Squid. Для этого выполните команду:

   ```
   dig +short <домен Active Directory>
   ```

   > Для использования утилиты dig может потребоваться предварительная установка пакета bind-utils.

   Отобразятся A-записи контроллеров домена Active Directory.

3. Укажите имя сервера с сервисом Squid. Для этого выполните команду:

   ```
   hostnamectl set-hostname <имя сервера с сервисом Squid>
   ```

4. Добавьте A- и PTR-записи на DNS-сервере Active Directory для сервера с сервисом Squid.

   > Для создания PTR-записи вам может потребоваться добавить обратную зону.

5. Убедитесь, что имя сервера с сервисом Squid совпадает с именем этого сервера на DNS-сервере Active Directory.

6. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команду:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.

7. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

Параметры DNS будут настроены.

kaspersky

Настройка Samba на сервере с сервисом Squid

► *Чтобы настроить сервис Samba, выполните следующие действия:*

1. Добавьте Samba в автозагрузку. Для этого выполните одно из следующих действий в зависимости от используемой операционной системы:
   - CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server.

     Выполните команды:

     ```
     systemctl start smb
     systemctl enable smb
     systemctl start nmb
     systemctl enable nmb
     ```
   - Ubuntu или Debian.

     Выполните команды:

     ```
     systemctl start smbd
     systemctl enable smbd
     systemctl start nmbd
     systemctl enable nmbd
     ```
2. Добавьте в файл /etc/samba/smb.conf следующие параметры:

   ```
   [global]
     workgroup = <NetBIOS-имя домена Active Directory>
     password server = <DNS-имя контроллера домена Active Directory>
     realm = <имя домена Active Directory в верхнем регистре>
     security = ads
     idmap uid = 10000-20000
     idmap gid = 10000-20000
     winbind use default domain = no
   ```
3. Добавьте сервер в домен Active Directory. Для этого выполните команду:

   ```
   net ads join -U <администратор домена>
   ```

   Отобразится предложение ввести пароль администратора домена или пользователя с правами администратора домена.
4. Введите пароль администратора и нажмите на клавишу **ENTER**.

   Сервер будет добавлен в домен Active Directory.
5. Проверьте добавление сервера в домен Active Directory. Для этого выполните команду:

   ```
   net ads testjoin
   ```

   Если сервер добавлен в домен Active Directory, в консоли отобразится `Join is OK`.

6. Запустите службу winbind. Для этого выполните команду:

   ```
   systemctl start winbind
   ```

7. Добавьте службу winbind в автозагрузку. Для этого выполните команду:

   ```
   systemctl enable winbind
   ```

8. Если вы используете операционную систему Ubuntu или Debian, вам требуется добавить пользователя proxy в группу winbindd_priv. Для этого выполните команду:

   ```
   usermod -a -G winbindd_priv proxy
   ```

Настройка Samba будет завершена. Перейдите к проверке параметров Samba.

Проверка параметров Samba на сервере с сервисом Squid

► *Чтобы проверить параметры сервиса Samba, выполните следующие действия:*

1. Проверьте получение сервером списка доменных групп. Для этого выполните команду:

   ```
   wbinfo -g
   ```

   Отобразится список доменных групп сервера.

2. Проверьте получение сервером списка пользователей. Для этого выполните команду:

   ```
   wbinfo -u
   ```

   Отобразится список пользователей сервера.

Если авторизация выполнена успешно, параметры сервиса Samba на сервере с сервисом Squid настроены верно.

Настройка сервиса Squid

► *Чтобы настроить сервис Squid, выполните следующие действия:*

1. Добавьте в начало файла /etc/squid/squid.conf следующие строки:

   ```
   auth_param ntlm program /usr/bin/ntlm_auth
   --helper-protocol=squid-2.5-ntlmssp --domain=DOMAIN

   auth_param ntlm children 10

   auth_param ntlm keep_alive off

   icap_send_client_username on

   acl lan proxy_auth REQUIRED

   http_access allow lan
   ```

2. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `--diagnostics` в следующей строке:

   ```
   auth_param ntlm program /usr/bin/ntlm_auth --diagnostics
   --helper-protocol=squid-2.5-ntlmssp --domain=DOMAIN
   ```

   События отладки будут записаны в файл /var/log/squid/cache.log.

3. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   service squid restart
   ```

Настройка сервиса Squid завершится.

Настройка клиентской части NTLM-аутентификации

► *Чтобы настроить клиентскую часть NTLM-аутентификации, выполните следующие действия:*

1. На сервере с сервисом Squid убедитесь, что в файле /etc/resolv.conf первый параметр `nameserver` содержит IP-адрес DNS-сервера с зоной Active Directory. Для этого выполните команду:

   ```
   cat /etc/resolv.conf
   ```

2. На DNS-сервере Active Directory добавьте A- и PTR-записи для сервера с сервисом Squid.

   > Для создания PTR-записи вам может потребоваться добавить обратную зону.

3. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команды:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.

   ```
   telnet <имя контроллера домена Active Directory> 445
   ```

   Если контроллер домена Active Directory доступен, соединение будет успешно установлено.

4. Введите `^]` и нажмите на клавишу **ENTER**.
5. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

6. На компьютерах локальной сети организации в параметрах браузера укажите FQDN-адрес сервера с сервисом Squid в качестве прокси-сервера.

Клиентская часть NTLM-аутентификации будет настроена.

Настройка NTLM-аутентификации хоста, не входящего в домен

► *Чтобы настроить NTLM-аутентификацию хоста, не входящего в домен Active Directory, выполните следующие действия:*

1. На компьютерах локальной сети организации в параметрах браузера укажите FQDN сервера с сервисом Squid в качестве прокси-сервера.
2. Если вы хотите сохранить учетные данные в операционной системе, чтобы не вводить их при каждом запуске браузера, откройте Диспетчер учетных данных Windows (**Пуск** → **Панель управления** → **Диспетчер учетных данных**).

3. Нажмите на ссылку **Добавить учетные данные Windows**.
4. В открывшемся окне укажите FQDN сервера с сервисом Squid, а также доменную учетную запись пользователя.
5. Нажмите на кнопку **OK**.

NTLM-аутентификация будет настроена.

Настройка Basic-аутентификации

Выполняйте действия по настройке Basic-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись должна обладать правами суперпользователя.

► *Чтобы настроить Basic-аутентификацию, выполните следующие действия:*

1. Добавьте в начало файла /etc/squid/squid.conf следующие строки в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -b
     "dc=<доменное имя второго уровня>,dc=<доменное имя первого уровня>" -D
     "<имя пользователя>@<домен Active Directory>" -w "<пароль пользователя>"
     -f "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>
     auth_param basic children 10
     auth_param basic realm Squid proxy-caching web server
     auth_param basic casesensitive off
     auth_param basic credentialsttl 1 minute
     acl auth proxy_auth REQUIRED
     http_access allow auth
     ```

   - SUSE Linux Enterprise Server:

     ```
     auth_param basic program /usr/sbin/basic_ldap_auth -R -b "dc=<доменное
     имя второго уровня>,dc=<доменное имя первого уровня>" -D "<имя
     пользователя>@<домен Active Directory>" -w "<пароль пользователя>" -f
     "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>
     auth_param basic children 10
     auth_param basic realm Squid proxy-caching web server
     auth_param basic casesensitive off
     auth_param basic credentialsttl 1 minute
     acl auth proxy_auth REQUIRED
     http_access allow auth
     ```

   - Ubuntu или Debian:

     ```
     auth_param basic program /usr/lib/squid/basic_ldap_auth -R -b
     ```

```
"dc=<доменное имя второго уровня>,dc=<доменное имя первого уровня>" -D
"<имя пользователя>@<домен Active Directory>" -w "<пароль пользователя>"
-f "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>

auth_param basic children 10

auth_param basic realm Squid proxy-caching web server

auth_param basic casesensitive off

auth_param basic credentialsttl 1 minute

acl auth proxy_auth REQUIRED

http_access allow auth
```

2. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `-d` в первую строку. Например:

   ```
   auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -d -b
   "dc=<доменное имя второго уровня>,dc=<доменное имя первого уровня>" -D
   "<имя пользователя>@<домен Active Directory>" -w "<пароль пользователя>"
   -f "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>
   ```

   События отладки будут записаны в файл /var/log/squid/cache.log.

3. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   service squid restart
   ```

Basic-аутентификация будет настроена.

kaspersky

Приложение 3. Настройка балансировки ICAP с помощью HAProxy

Балансировка ICAP с помощью балансировщика нагрузки HAProxy позволяет подключить один сервис Squid одновременно к нескольким узлам кластера и распределить нагрузку обработки трафика между ними.

По умолчанию ICAP-трафик не шифруется. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между HAProxy-сервером и Kaspersky Web Traffic Security, а также между сервисом Squid и HAProxy-сервером с помощью туннелирования трафика или средствами iptables.

В этом разделе

Изменение IP-адреса ICAP-сервера

► *Чтобы изменить IP-адрес, на который ICAP-сервер принимает трафик, выполните следующие действия:*

1. В главном окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **ICAP-сервер**.
2. В поле **Адрес ICAP-сервера** измените значение с `127.0.0.1` на `0.0.0.0`.

   Если вы используете IP-адрес в формате IPv6, то вам требуется изменить значение с `::1` на `::`.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

IP-адрес, на который ICAP-сервер принимает трафик, будет изменен.

Установка и настройка HAProxy

Для настройки и установки HAProxy учетная запись должна обладать правами суперпользователя.

Не рекомендуется устанавливать балансировщик нагрузки HAProxy на одном сервере с программой, так как HAProxy и Kaspersky Web Traffic Security используют один и тот же порт (1344) для взаимодействия с другими серверами локальной сети.

► *Чтобы установить и настроить HAProxy, выполните следующие действия:*

1. Откройте доступ к порту 1344. Для этого на Управляющем узле выполните следующие команды в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     firewall-cmd --add-port=1344/tcp --permanent
     firewall-cmd --reload
     ```

   - Ubuntu:

     ```
     ufw allow 1344
     ```

   - Debian:

     ```
     apt-get install iptables-persistent
     iptables -A INPUT -p tcp --dport 1344 -j ACCEPT
     ```

Если вы используете операционную систему SUSE Linux Enterprise Server, добавьте в файле /etc/sysconfig/SuSEfirewall2 порт 1344: `FW_SERVICES_EXT_TCP="1344"`.

1. На сервере, который вы хотите использовать для балансировки ICAP, установите пакет HAProxy. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:
   - CentOS или Red Hat Enterprise Linux:

     ```
     yum install haproxy
     ```

   - SUSE Linux Enterprise Server:

     ```
     zypper install haproxy
     ```

   - Ubuntu и Debian:

     ```
     apt-get install haproxy
     ```

2. На сервере, который вы хотите использовать для балансировки ICAP, добавьте в файл /etc/haproxy/haproxy.cfg следующие блоки параметров:

   ```
   frontend ICAP
       bind 0.0.0.0:1344
       mode tcp
       default_backend icap_pool

   backend icap_pool
       balance <схема балансировки, рекомендуется использовать roundrobin>
       mode tcp
   ```

```
    server <имя ICAP-сервера 1> <IP-адрес узла кластера>:<порт
ICAP-сервера> check

    server <имя ICAP-сервера 2> <IP-адрес узла кластера>:<порт
ICAP-сервера> check

    server <имя ICAP-сервера 3> <IP-адрес узла кластера>:<порт
ICAP-сервера> check
```

3. На сервере, который вы хотите использовать для балансировки ICAP, перезапустите службу HAProxy. Для этого выполните команду:

   ```
   service haproxy restart
   ```

Балансировщик нагрузки HAProxy будет настроен.

Настройка сервиса Squid для работы HAProxy

► *Чтобы настроить сервис Squid для работы HAProxy, выполните следующие действия:*

1. Измените параметры сервиса Squid. Для этого выполните команду:

   ```
   sed -i 's!icap://127.0.0.1:1344!icap://<IP-адрес сервера с
   HAProxy>:<порт>!g' /etc/squid/squid.conf
   ```

2. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   service squid restart
   ```

Настройка сервиса Squid для работы HAProxy завершится.

Приложение 4. MIME-типы объектов

Наиболее часто используются следующие MIME-типы объектов:

- application/font-woff;
- application/javascript;
- application/json;
- application/ocsp-response;
- application/octet-stream;
- application/x-javascript;
- audio/mp4;
- audio/mpeg;
- image/gif;
- image/jpeg;
- image/png;
- image/svg+xml;
- image/vnd.microsoft.icon;
- image/x-icon;
- text/css;
- text/html;
- text/javascript;
- text/plain;
- video/mpeg.

kaspersky

Приложение 5. Нормализация URL-адресов

Kaspersky Web Traffic Security поддерживает импорт URL-адресов, состоящих из четырех частей и представленных в следующем формате:

<протокол>://<домен>:<порт>/<путь>

Указание домена является обязательным. Остальные части URL-адреса могут быть опущены.

Пример:

`https://example.com:8080/path`

Здесь `https` – протокол, `example.com` – домен, `8080` – порт, `path` – путь.

Если в процессе нормализации URL-адреса произошла ошибка и адрес не был принят программой, рекомендуется выполнить следующие действия.

1. Определите, с какой частью URL-адреса возникла проблема. Для этого добавляйте части адреса последовательно по следующему алгоритму:
   a. <домен>.
   b. <протокол>://<домен>.
   c. <протокол>://<домен>:<порт>.
   d. <протокол>://<домен>:<порт>/<путь>.
2. Проверьте, соответствует ли значение части URL-адреса, с которой возникла проблема, требованиям, приведенным в таблице ниже.

Таблица 18. Требования к URL-адресу для успешного выполнения нормализации

Часть URL-адреса	Требования
Протокол	• Должен начинаться с буквы латинского алфавита (ASCII A–Z, a–z). • Может содержать в себе буквы латинского алфавита (ASCII A–Z, a–z), цифры от 0 до 9, а также знаки плюса, минуса и точку.
Домен	• Допускается указывать IPv4-, IPv6-адреса (в квадратных скобках), а также FQDN. • Допускается использование следующих символов: . _ ~ ! $ & ' ( ) * + , =
Порт	Допускается использовать цифровое значение в диапазоне от 1 до 65535.

Часть URL-адреса	Требования
Путь	• Допускается использование одного или нескольких сегментов, разделенных символом /. • В каждом сегменте допускается использование латинских букв (ASCII a-z), цифр (0-9), символов в кодировке UTF, %-encoded символов, а также следующих символов: - . _ ~ : @ ! $ & ' ( ) * , =

1. Если указанный URL-адрес содержит точку с запятой, укажите его без пути. Вы сможете указать путь позже в списке добавленных URL-адресов.

kaspersky

Приложение 6. Категории веб-ресурсов

Категории веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Порнография, эротика**.
- **Нудизм**.
- **Белье**.
- **Секс-образование**.
- **Знакомства для взрослых**.
- **ЛГБТ**.
- **Интим-магазины**.
- **Аборты**.

Алкоголь, табак, наркотические и психотропные вещества

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Наркотики**.
- **Алкоголь**.
- **Табак**.

Культура и общество

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Религии, религиозные объединения**.
- **Власть, политика, закон**.
- **Дом, семья**.
- **Новостные ресурсы**.
- **Вооруженные силы**.
- **Оружие, взрывчатые вещества, пиротехника**.
- **Поиск работы**.
- **Рестораны, еда, кафе**.

- **Астрология, эзотерика**.
- **Финансы, экономика**.
- **Бизнес**.

Программное обеспечение, аудио, видео

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Торренты**.
- **Файловые обменники**.
- **Аудио, видео**.

Информационные технологии

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Средства анонимного доступа**.
- **Поисковые машины, сервисы**.
- **Хостинг**.
- **Реклама, тизерные сети**.
- **Интернет-сервисы**.
- **Компьютерная техника, электроника**.
- **Информационная безопасность**.
- **Спам-сайты**.

Интернет-магазины, банки, платежные системы

Категория включает веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. Вы можете отдельно выбрать следующие подкатегории:

- **Интернет-магазины**.
- **Банки**.
- **Платежные системы**.
- **Криптовалюты и майнинг**.

Ненависть и дискриминация

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Насилие**.
- **Нецензурная лексика**.
- **Экстремизм, расизм**.
- **Самоповреждение, самоубийство**.

Общение в сети

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Веб почта**.
- **Социальные сети**.
- **Чаты, форумы**.
- **Блоги**.
- **Сайты знакомств**.

Образование

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Школы, университеты**.
- **Книги, писатели**.
- **Образовательные порталы, базы знаний**.

Хобби и развлечения

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Компьютерные игры**.
- **Охота, рыбалка**.
- **Путешествия, поездки**.
- **ТВ, радио** .
- **Дикие и домашние животные**.
- **Юмор**.
- **Музыка**.
- **Транспорт**.
- **Искусство**.

Красота, здоровье и спорт

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Спорт, спортивные игры**.
- **Здоровье**.
- **Мода, стиль**.
- **Медицина, фармацевтика**.

Азартные игры, лотереи, тотализаторы

Категория включает веб-ресурсы, предлагающие пользователям финансовое участие в игровой деятельности, даже если это не является обязательным условием использования веб-ресурса, а также информацию, способную вызвать желание участвовать в азартных играх, тотализаторах и лотереях. Вы можете отдельно выбрать следующие подкатегории:

- **Лотереи**.
- **Казино, карточные игры**.
- **Онлайн-тотализаторы**.

Другие

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Детский интернет**.
- **Недвижимость**.
- **Анорексия**.

Заблокировано законодательством Российской Федерации

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Защита детей (139-ФЗ, 436-ФЗ)**.
- **Федеральный список экстремистских материалов (114-ФЗ)**.
- **Единый реестр Роскомнадзора**.

Запрещено полицией

Категория включает подкатегорию **Запрещено полицией Японии**. В эту подкатегорию входят веб-ресурсы, предоставляемые по соглашению с японской полицией, только для японских клиентов.

kaspersky

Значения параметров программы в сертифицированном режиме

Этот раздел содержит перечень параметров программы, влияющих на сертифицированный режим работы программы. В таблице ниже приведены значения этих параметров в сертифицированном режиме работы программы.

Если вы меняете какие-либо из перечисленных значений параметров с их значений в сертифицированном режиме работы программы на другие значения, вы выводите программу из сертифицированного режима работы.

Таблица 19. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Название параметра	Значение параметра в сертифицированном режиме работы программы
KSN/KPSN	Использование KSN / KPSN	• **Не использовать KSN/KPSN** • **KPSN**
Защита: **Антивирус**	**Использовать эвристический анализ**	**Включено**
	Обнаруживать некоторые легальные программы	**Включено**
	Максимальная длительность проверки (сек.)	120
	Максимальная глубина проверки архивов	32
Защита: **Анти-Фишинг**	**Использовать эвристический анализ**	**Включено**
	Максимальная длительность проверки (сек.)	120

kaspersky

Глоссарий

I

ICAP-сервер

Сервер, реализующий ICAP-протокол. Этот протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером по ICAP-протоколу. Kaspersky Web Traffic Security получает данные с прокси-сервера организации после их обработки на ICAP-сервере.

K

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

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.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля Kerberos. Keytab-файлы используются в удаленных системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

M

MIB (Management Information Base)

Виртуальная база данных, используемая для управления объектами, которые передаются по протоколу SNMP.

N

NTLM-аутентификация

Механизм аутентификации, основанный на проверке подлинности запроса сервера и ответа клиента. Для шифрования запроса и ответа используются хеши пароля пользователя, которые передаются по сети. При захвате сетевого трафика злоумышленники могут получить доступ к хешам пароля, что делает этот механизм менее надежным, чем Kerberos-аутентификация.

P

PTR-запись

DNS-запись, связывающая IP-адрес компьютера с его доменным именем.

R

Replay cache

Кеш, используемый в технологии Kerberos для хранения записей о запросах пользователей на аутентификацию. Этот механизм помогает защитить инфраструктуру от атак повторного воспроизведения. Во время таких атак злоумышленники записывают трафик пользователя, чтобы воспроизвести ранее отправленные им сообщения и успешно пройти аутентификацию на прокси-сервере. При использовании replay cache сервер аутентификации обнаруживает дубликат запроса и отправляет в ответ сообщение об ошибке.

S

SELinux (Security-Enhanced Linux)

Система контроля доступа процессов к ресурсам операционной системы, основанная на применении политик безопасности.

SNI (Server Name Indication)

Расширение протокола TLS, передающее имя веб-сайта, с которым требуется установить соединение. SNI необходим в случаях, когда несколько сервисов, работающих по протоколу HTTPS, расположены на одном физическом сервере и используют один IP-адрес, но при этом у каждого сервиса есть свой сертификат безопасности.

SNMP-агент

Программный модуль сетевого управления Kaspersky Web Traffic Security, отслеживает информацию о

работе программы.

SNMP-ловушка

Уведомление о событиях работы программы, отправляемое SNMP-агентом.

Squid

Программный пакет, выполняющий функцию кеширующего прокси-сервера для протоколов HTTP(S) и FTP. Сервис Squid использует списки контроля доступа для распределения доступа к ресурсам.

SRV-запись

Стандарт в DNS, определяющий местоположение, то есть имя хоста и номер порта серверов для определенных служб.

SSL Bumping

Режим работы сервиса Squid, используемый для перехвата содержимого зашифрованных HTTPS-сеансов.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

Т

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Б

Базовая аутентификация

Механизм аутентификации, при котором имя пользователя и пароль передаются для проверки на сервер в незашифрованном виде.

В

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

И

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

Источник обновлений

Ресурс, содержащий обновления антивирусных баз программы Kaspersky Web Traffic Security. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

К

Кластер

Группа серверов с установленной программой Kaspersky Web Traffic Security, объединенных для централизованного управления через веб-интерфейс программы.

О

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Правило доступа

Список разрешений и запретов доступа пользователей к указанным веб-ресурсам и направлению трафика.

Правило защиты

Список проверок трафика на вирусы, фишинг, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. 132), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, проводимых при выполнении заданных условий.

Правило обработки трафика

Набор действий, которые программа выполняет над веб-ресурсом, удовлетворяющим заданным условиям.

Правило обхода

Набор критериев фильтрации трафика, согласно которым пользователям разрешается или запрещается доступ к веб-ресурсам без выполнения проверок по правилам доступа и правилам защиты.

Р

Рабочая область

Набор параметров и прав доступа, применимых к выделенной группе пользователей.

Репутационная фильтрация

Облачная служба, использующая технологии определения репутации сообщений. Информация о появлении новых видов спама в облачной службе появляется раньше, чем в базах модуля Анти-Спам, что дает возможность повысить скорость и точность обнаружения признаков спама в сообщении.

С

Сервис nginx

Программное обеспечение для UNIX-систем, используемое в качестве HTTP-сервера или почтового прокси-сервера.

Серийный номер лицензии

Уникальное сочетание букв и цифр, использующееся для однозначной идентификации приобретателя лицензии на программу.

Служба каталогов

Программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

Схема расположения графиков

Вид окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб некоторых графиков.

Т

Трассировка

Запись отладочной информации о работе программы.

kaspersky

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

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

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

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

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

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

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

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

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

Сайт "Лаборатории Касперского": https://www.kaspersky.ru

Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com (https://community.kaspersky.com/)

Информация о стороннем коде

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

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google Chrome – товарный знак Google, Inc.

z/VM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Microsoft, Windows, Windows Server, Active Directory, Hyper-V и Internet Explorer – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Oracle– зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

Parallels Desktop является зарегистрированным товарным знаком Parallels International GmbH в США и / или других странах.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat Enterprise Linux – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

VMware, VMware ESXi и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.