

Kaspersky Web Traffic Security

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.0

Сборка 6.0.0.1545

Уважаемый пользователь!

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

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

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

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

Документ может быть изменен без предварительного уведомления.

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

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

Дата редакции документа: 17.10.2018

Обозначение документа: 643.46856491.00047-03 90 01

© АО «Лаборатория Касперского», 2018.

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

Содержание

Об этом документе	8
Источники информации о программе	9
Kaspersky Web Traffic Security.....	11
О действиях программы над объектами.....	11
О задачах программы.....	12
Основные компоненты программы.....	13
Принцип работы программы.....	14
Об информационных X-заголовках.....	15
Требования.....	16
Аппаратные и программные требования.....	16
Указания по эксплуатации и требования к среде.....	17
Лицензирование программы.....	19
О Лицензионном соглашении.....	19
О лицензии.....	19
О лицензионном сертификате.....	20
О ключе.....	20
О коде активации.....	21
О предоставлении данных.....	21
Просмотр информации о лицензии и активации программы.....	26
Активация программы.....	26
Удаление ключа.....	27
Типовые схемы развертывания.....	28
Сценарий установки и настройки Управляющего и Обрабатывающего серверов на одном сервере ...	30
Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на одном сервере.....	31
Сценарий установки и настройки Управляющего и Обрабатывающего серверов на разных серверах.....	32
Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на разных серверах.....	33
Подготовка к установке программы.....	34
Отключение SELinux.....	35
Настройка портов для работы Управляющего и Резервного управляющего серверов.....	35
Настройка портов для работы Обрабатывающего сервера.....	36
Установка сервиса nginx.....	38
Настройка сервиса nginx при использовании ALT Linux.....	40
Установка и первоначальная настройка программы.....	41
Установка и настройка Управляющего и Резервного управляющего серверов.....	42
Установка пакета Управляющего и Резервного управляющего серверов.....	42
Установка пакета локализации.....	43
Настройка Управляющего сервера.....	43

Настройка Резервного управляющего сервера	45
Создание файла автоматической настройки Управляющего или Резервного управляющего сервера	46
Запуск автоматической настройки Управляющего или Резервного управляющего сервера	46
Удаление Управляющего или Резервного управляющего сервера	47
Установка и настройка Обрабатывающего сервера	49
Установка пакета Обрабатывающего сервера	49
Настройка Обрабатывающего сервера	49
Создание файла автоматической настройки Обрабатывающего сервера	50
Запуск автоматической настройки Обрабатывающего сервера	51
Удаление Обрабатывающего сервера	51
Сценарий повторной установки Управляющего сервера с добавлением Резервного управляющего сервера	52
Создание учетных записей пользователей	54
Процедура приемки	55
Безопасное состояние	55
Проверка работоспособности. Тестовый файл EICAR	55
Интерфейс Kaspersky Web Traffic Security	57
Мониторинг работы программы	58
Создание новой схемы расположения графиков	58
Выбор схемы расположения графиков из списка	59
Добавление графика на схему расположения графиков	59
Перемещение графика на схеме расположения графиков	60
Удаление графика со схемы расположения графиков	60
Назначение схемы расположения графиков для использования по умолчанию	61
Переименование схемы расположения графиков	61
Удаление схемы расположения графиков	61
Управление серверами	62
Настройка отображения таблицы серверов	62
Просмотр информации о сервере	62
Добавление сервера	65
Изменение параметров сервера	65
Удаление сервера	66
Изменение роли сервера	66
Проверка целостности данных	67
Работа программы в аварийном режиме	68
Работа с правилами обработки трафика	70
Сценарий настройки доступа к интернет-ресурсам	71
Добавление правила доступа	73
Добавление правила защиты	74
Настройка инициатора срабатывания правила	75
Настройка критериев фильтрации трафика	76

Добавление исключения для правила обработки трафика	78
Настройка расписания работы правила обработки трафика	80
Изменение правила обработки трафика	80
Удаление правила обработки трафика	81
Создание копии правила обработки трафика	82
Включение и отключение правила обработки трафика	82
Работа с группами правил обработки трафика	83
Создание группы правил обработки трафика	83
Изменение группы правил обработки трафика	84
Удаление группы правил обработки трафика	84
Изменение приоритета правила в рамках группы	85
Мониторинг работы правил обработки трафика	85
Обработка запросов пользователей о доступе к интернет-ресурсам	86
Получение статистики о доступе к интернет-ресурсам	86
Просмотр таблицы правил обработки трафика	87
Настройка отображения таблицы правил обработки трафика	88
Просмотр информации о правиле обработки трафика	88
Управление рабочими областями	90
Просмотр таблицы рабочих областей	90
Просмотр информации о рабочей области	90
Настройка отображения таблицы рабочих областей	91
Добавление рабочей области	91
Изменение параметров рабочей области	92
Удаление рабочей области	92
Работа с ролями и учетными записями пользователей	93
Настройка отображения таблицы ролей пользователей	93
Добавление роли	94
Изменение параметров роли	96
Удаление роли	96
Добавление учетной записи	97
Назначение роли	97
Изменение пароля учетной записи Administrator	97
Защита сетевого трафика	99
Настройка параметров защиты сетевого трафика	101
Настройка обработки архивов	102
Установка значений параметров защиты по умолчанию	102
Использование внешних служб «Лаборатории Касперского»	103
Настройка участия в Kaspersky Security Network	104
Настройка использования Kaspersky Private Security Network	105
Соединение с LDAP-сервером	106
Добавление соединения с LDAP-сервером	106

Удаление соединения с LDAP-сервером.....	107
Изменение параметров соединения с LDAP-сервером	107
Параметры ICAP-сервера	108
Настройка параметров подключения к ICAP-серверу.....	108
Настройка параметров обработки трафика на ICAP-сервере.....	109
Работа с программой по протоколу SNMP	111
Включение и отключение использования SNMP в программе	112
Настройка параметров подключения к SNMP-серверу.....	112
Настройка шифрования SNMP-соединений.....	113
Включение и отключение отправки SNMP-ловушек.....	114
Журнал событий Kaspersky Web Traffic Security	116
Просмотр журнала событий.....	116
Экспорт событий	117
Настройка отображения таблицы событий	118
Настройка параметров журнала событий	118
Настройка параметров Syslog	119
Экспорт и импорт параметров	120
Экспорт параметров Kaspersky Web Traffic Security.....	120
Импорт параметров Kaspersky Web Traffic Security.....	121
Настройка хранения экспортированных файлов	121
Настройка шаблона запрета доступа	122
Устранение уязвимостей и установка критических обновлений в программе	123
Действия после сбоя или неустранимой ошибки в работе программы	124
Обращение в Службу технической поддержки	125
Способы получения технической поддержки	125
Техническая поддержка по телефону.....	125
Техническая поддержка через Kaspersky CompanyAccount	126
Получение информации для Службы технической поддержки.....	127
Запуск трассировки.....	127
Изменение уровня трассировки	128
Просмотр журналов трассировки	128
Сохранение файла трассировки на компьютере	128
Приложения	130
Приложение. MIME-типы объектов	130
Значения параметров программы в сертифицированном режиме	131
Настройка интеграции сервиса Squid с Active Directory	132
Настройка Kerberos-аутентификации	132
Установка пакета Kerberos	132
Настройка синхронизации времени	133
Настройка DNS	134
Создание keytab-файла для сервиса Squid	135

Настройка клиентской части Kerberos	135
Настройка NTLM-аутентификации	137
Установка сервиса Samba	137
Настройка синхронизации времени	137
Настройка DNS	138
Настройка Samba на сервере с сервисом Squid	139
Проверка параметров Samba на сервере с сервисом Squid	141
Настройка сервиса Squid	141
Настройка клиентской части NTLM-аутентификации	141
Настройка NTLM-аутентификации хоста, не входящего в домен	142
Настройка Basic-аутентификации	142
Настройка балансировки ICAP с помощью HAProxy	144
Изменение IP-адреса ICAP-сервера	144
Установка и настройка HAProxy	144
Настройка сервиса Squid для работы HAProxy	146
Установка и настройка сервиса Squid	146
Установка сервиса Squid	146
Настройка сервиса Squid	147
Настройка SSL Bumping в сервисе Squid	147
Глоссарий	152
АО «Лаборатория Касперского»	157
Информация о стороннем коде	159
Уведомления о товарных знаках	160

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Web Traffic Security 6.0" (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.

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. 125).

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 на нашем форуме (<https://forum.kaspersky.com>).

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

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.....	11
О задачах программы.....	12
Основные компоненты программы.....	13
Принцип работы программы.....	14
Об информационных X-заголовках.....	15

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:
 - **Запретить**, 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:**
 - **Запретить, по возможности вылечить.**
 - **Пропустить проверку.**По умолчанию установлено значение **Запретить, по возможности вылечить.**
 - b. **Фишинг, Зашифрованный архив, Документ с макросом и Объект, для которого не удалось завершить проверку:**
 - **Запретить.**
 - **Пропустить проверку.**По умолчанию установлено значение **Запретить.**

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).
- SntpSender (ID=15).
- Snmp (ID=16).
- 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:

- *Обрабатывающий сервер.*

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

- *Управляющий сервер*

Позволяет администратору управлять параметрами программы через веб-интерфейс. Установленные значения параметров передаются на Обрабатывающие серверы.

- *Резервный управляющий сервер.*

Необходим для отказоустойчивого управления серверами. На сервер с этой ролью регулярно передаются актуальные значения параметров программы. При выходе из строя Управляющего сервера вы можете передать функции управления Резервному управляющему серверу для обеспечения бесперебойной работы программы.

Вы можете не устанавливать Резервный управляющий сервер, однако в этом случае не будет обеспечена отказоустойчивость программы.

Если Резервный управляющий сервер не установлен, а Управляющий сервер вышел из строя, вам потребуется установить программу заново (см. раздел «Сценарий повторной установки Управляющего сервера с добавлением Резервного управляющего сервера» на стр. [52](#)). Значения параметров программы на Обрабатывающих серверах будут потеряны. При наличии ранее экспортированного конфигурационного файла вы можете импортировать параметры программы (см. раздел «Импорт параметров Kaspersky Web Traffic Security» на стр. [121](#)) после повторной установки.

Принцип работы программы

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

Прокси-сервер передает все запросы пользователей по ICAP-протоколу на Обрабатывающий сервер. Kaspersky Web Traffic Security проверяет запрос по правилам обработки трафика, полученным от Управляющего сервера или Резервного управляющего сервера. После этого программа передает прокси-серверу результат проверки. Если доступ к интернет-ресурсу разрешен, то прокси-сервер отправляет запрос в интернет. Ответ на запрос также передается через прокси-сервер на Обрабатывающий сервер и проверяется правилами обработки трафика. По результатам проверки пользователю становится доступен запрошенный интернет-ресурс или отображается шаблон запрета доступа (см. раздел «Настройка шаблона запрета доступа» на стр. [122](#)).

Принцип работы программы показан на рис. ниже.

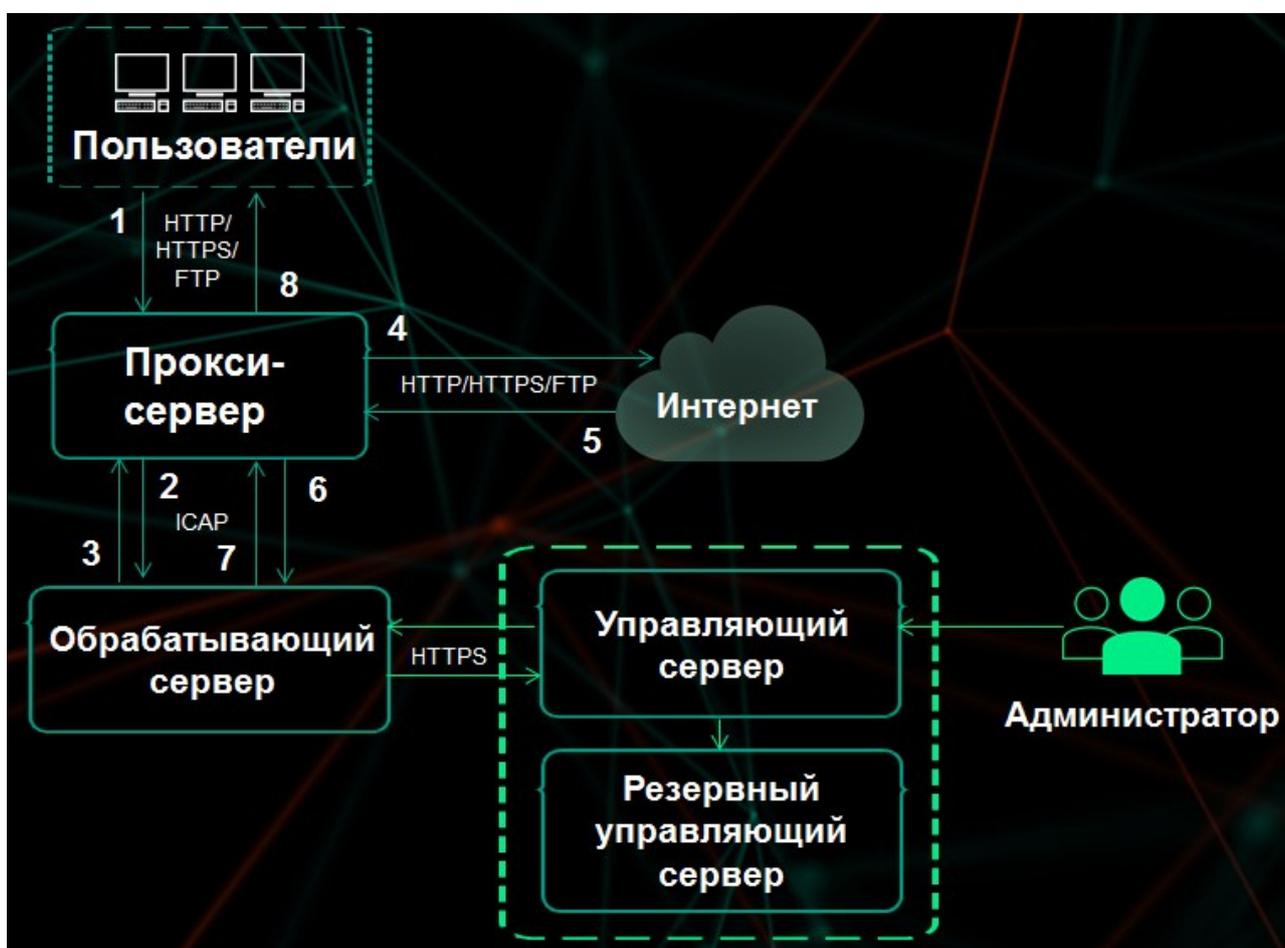


Рисунок 1. Принцип работы программы без балансировщика нагрузки

При наличии большого количества Обрабатывающих серверов рекомендуется использовать балансировщик нагрузки (см. раздел «Настройка балансировки ICAP с помощью NARProху» на стр. 144). Он определяет, какому Обрабатывающему серверу направить запрос на проверку, в соответствии с заданным способом балансировки. Далее механизм обработки трафика не отличается от работы программы без балансировщика нагрузки.

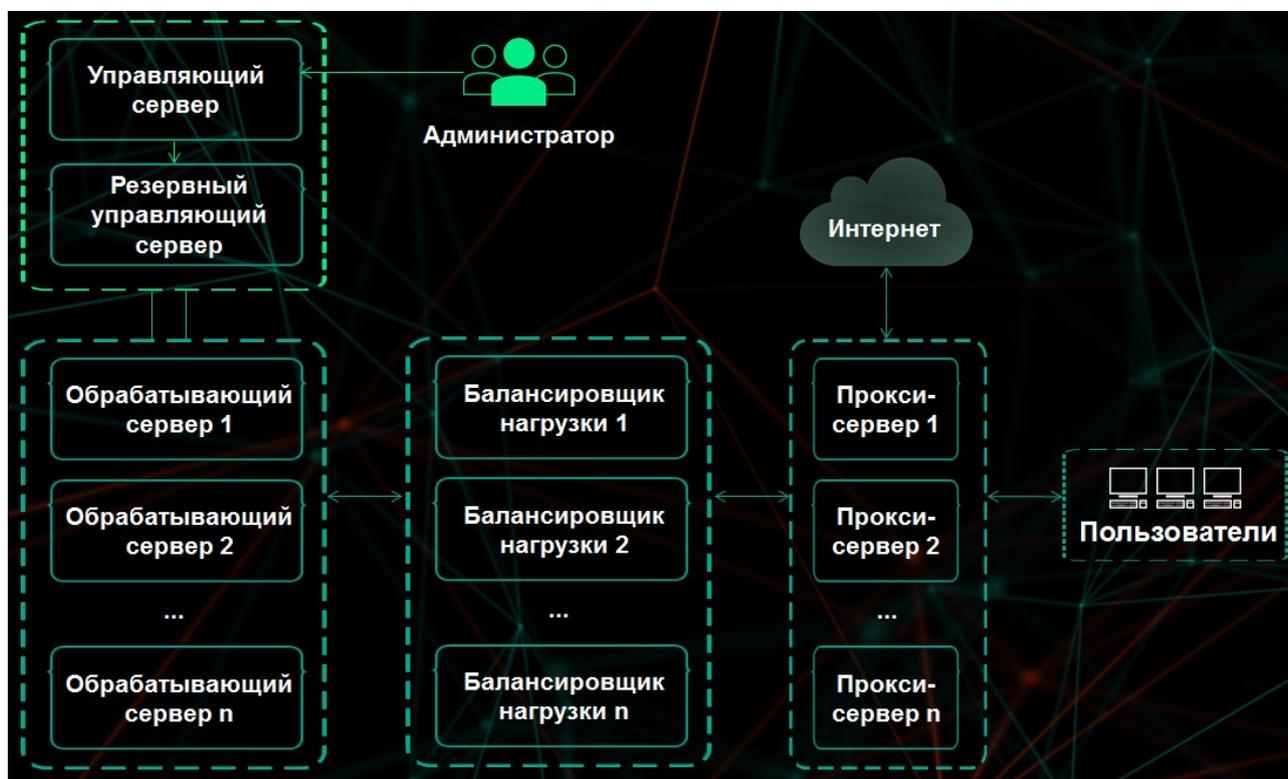


Рисунок 2. Принцип работы программы с балансировщиком нагрузки

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.

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	16
Указания по эксплуатации и требования к среде	17

Аппаратные и программные требования

Аппаратные требования к серверам для установки Kaspersky Web Traffic Security

Обрабатывающий сервер:

- процессор Intel® Xeon® E5606 (4 ядра) 1,86 ГГц;
- 8 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 100 ГБ на жестком диске, из которых:
 - 25 ГБ для хранения временных файлов;
 - 25 ГБ для хранения файлов журналов.

Управляющий сервер:

- процессор Intel® Xeon® E5606 (4 ядра) 1,86 ГГц;
- 8 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 100 ГБ на жестком диске.

При установке Управляющего и Обрабатывающего сервера на одном физическом сервере:

- 2 процессора Intel® Xeon® E5606 (8 ядер) 1,86 ГГц;
- 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.

Программные требования к серверам для установки Kaspersky Web Traffic Security

- Red Hat Enterprise Linux® версии 7.5 x64.
- Ubuntu 18.04.1 LTS.

- Debian 9.5.
- SUSE Linux® Enterprise Server 12 SP3.
- CentOS версии 7.5 x64.
- ALT Linux 7.0.5.
- Astra Linux Special Edition 1.6. Только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды.

Дополнительные требования

- Ngnix версий 1.10.3, 1.12.2, 1.14.0 и 1.14.2
- Nginx для балансировки нагрузки версии 1.5.
- Squid версии 3.5.20, если вы устанавливаете сервис Squid на Обрабатывающий сервер.
- В операционной системе должна быть установлена локализация en_US.UTF-8.

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 Обрабатывающий сервер 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 39.
- Internet Explorer® версии 11.
- Google Chrome™ версии 43.
- Microsoft® Edge версии 40.

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 контролируруемыми 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.

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении	19
О лицензии	19
О лицензионном сертификате	20
О ключе	20
О коде активации	21
О предоставлении данных	21
Просмотр информации о лицензии и активации программы	26
Активация программы	26
Удаление ключа	27

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:

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

О ключе

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

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 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. [125](#)).

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, перечисленную в Лицензионном соглашении в пункте Условия обработки данных. Эта информация требуется для повышения уровня защиты почтового сервера.
- 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.

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями и действующими правилами «Лаборатории Касперского».

«Лаборатория Касперского» использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

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

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	Срок хранения	Обеспечение защиты данных
<p>Информация из запросов доступа к интернет-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса пользователей. • Имя учетной записи и домен пользователей. • URL-адреса интернет-ресурсов, к которым запрашивается доступ. • Скачиваемые файлы. <p>Имена учетных записей пользователей веб-интерфейса программы.</p>	<ul style="list-style-type: none"> • Журналы и файлы трассировки. • Оперативная память. • Файлы дампов. 	<p>Журнал событий обработки трафика по умолчанию хранится трое суток. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Журнал событий программы по умолчанию хранится бессрочно и содержит 100 тыс. событий. По достижении заданного количества записей происходит ротация, старые записи начинают удаляться.</p> <p>Файлы трассировки хранятся бессрочно. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Срок хранения системного журнала определяется параметрами операционной системы.</p> <p>Информация в оперативной памяти хранится до перезапуска программы.</p> <p>Файлы дампов хранятся бессрочно.</p>	<p>По умолчанию доступ к персональным данным пользователей имеют только учетная запись суперпользователя операционных систем root и учетная запись администратора Kaspersky Web Traffic Security Administrator.</p> <p>Возможность ограничить права администраторов и других пользователей серверов и операционных систем, на которые установлена Kaspersky Web Traffic Security, средствами Kaspersky Web Traffic Security не предусмотрена.</p> <p>Администратору Kaspersky Web Traffic Security рекомендуется контролировать доступ администраторов и других пользователей серверов и</p>

Тип данных	Где используются данные	Срок хранения	Обеспечение защиты данных
<p>LDAP:</p> <ul style="list-style-type: none"> Имена учетных записей LDAP. DN. Принадлежность к группе пользователей. 	<ul style="list-style-type: none"> Журналы и файлы трассировки. Кеш LDAP. Оперативная память. Файлы дампов. 	<p>Журнал событий обработки трафика по умолчанию хранится трое суток. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Журнал событий программы по умолчанию хранится бессрочно и содержит 100 тыс. событий. По достижении заданного количества записей происходит ротация, старые записи начинают удаляться.</p> <p>Файлы трассировки хранятся бессрочно. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Срок хранения системного журнала определяется параметрами операционной системы.</p> <p>Кеш LDAP хранится бессрочно.</p> <p>Информация в оперативной памяти хранится до перезапуска программы.</p> <p>Файлы дампов хранятся бессрочно.</p>	<p>операционных систем, на которые установлена Kaspersky Web Traffic Security, к персональным данным других пользователей любыми системными средствами на его усмотрение.</p>
<p>Правила обработки трафика:</p> <ul style="list-style-type: none"> Имена учетных записей LDAP, DN, принадлежность к группе пользователей. IP-адреса пользователей. Комментарии. 	<ul style="list-style-type: none"> Файлы конфигурации. Оперативная память. Файлы дампов. 	<p>Файлы конфигурации хранятся бессрочно.</p> <p>Информация в оперативной памяти хранится до перезапуска программы.</p> <p>Файлы дампов хранятся бессрочно.</p>	

Тип данных	Где используются данные	Срок хранения	Обеспечение защиты данных
<p>Конфигурация программы:</p> <ul style="list-style-type: none"> Имена учетных записей администратора и пользователей программы. Права доступа учетных записей программы. Хеш пароля администратора. Имя учетной записи и пароль подключения программы к прокси-серверу. Keytab-файлы. 			
<p>Данные об обновлениях программы:</p> <ul style="list-style-type: none"> IP-адреса, используемые для скачивания обновлений. IP-адреса источников обновлений. Информация о скачиваемых IP-адреса пользователей. файл ах и скорости скачивания. 	<p>Журналы и файлы трассировки.</p>	<p>Журнал событий обработки трафика по умолчанию хранится трое суток. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться. Журнал событий программы по умолчанию хранится бессрочно и содержит 100 тыс. событий. По достижении заданного количества записей происходит ротация, старые записи начинают удаляться. Файлы трассировки хранятся бессрочно. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться. Срок хранения системного журнала определяется параметрами операционной системы.</p>	

Тип данных	Где используются данные	Срок хранения	Обеспечение защиты данных
<p>Данные в Хранилище</p>	<ul style="list-style-type: none"> • Журнал событий обработки трафика. • Журнал событий программы. • Файлы трассировки. • Системный журнал. • Оперативная память. • Файлы дампов. • Кеш LDAP. • Файлы конфигурации программы. • KSN-статистики. • Информация об установленной программе. 	<p>Журнал событий обработки трафика по умолчанию хранится трое суток. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Журнал событий программы по умолчанию хранится бессрочно и содержит 100 тыс. событий. По достижении заданного количества записей происходит ротация, старые записи начинают удаляться.</p> <p>Файлы трассировки хранятся бессрочно. По достижении объема 1 ГБ происходит ротация, старые записи начинают удаляться.</p> <p>Срок хранения системного журнала определяется параметрами операционной системы.</p> <p>Информация в оперативной памяти хранится до перезапуска программы.</p> <p>Файлы дампов хранятся бессрочно.</p> <p>Кеш LDAP хранится бессрочно.</p> <p>Файлы конфигурации хранятся бессрочно.</p> <p>KSN-статистики и информация об установленной программе хранятся на серверах «Лаборатории Касперского» бессрочно.</p>	

Работа с программой из консоли управления сервера, на котором установлен Kaspersky Web Traffic Security, 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 содержания сообщений электронной почты и 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 установлен Kaspersky Web Traffic Security, под учетной записью суперпользователя.

Администратору Kaspersky Web Traffic Security необходимо обеспечить безопасность этих данных 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 **Серверы**.
2. В блоке **Лицензия** перейдите по ссылке **Подробные сведения**.

Откроется окно **Лицензия**.

В окне отображается информация о лицензиях на Обрабатывающих серверах.

► 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 ключ, активирующий Kaspersky Web Traffic Security. Для добавления ключа необходимо ввести код активации.

► Чтобы ввести код активации, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **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 Обработывающих серверах**.

Удаление ключа

► *Чтобы удалить ключ, выполните следующие действия:*

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

2. В блоке **Лицензия** нажмите на кнопку **Удалить**.

Отобразится подтверждение удаления ключа.

3. Нажмите на кнопку **Да**.

Ключ будет удален.

Типовые схемы развертывания

Схема развертывания программы определяется планируемой нагрузкой на серверы программы.

Для оптимальной работы программы рекомендованы две типовые схемы развертывания:

- Схема развертывания на один сервер. На одном сервере устанавливаются Обрабатывающий сервер и Управляющий сервер.

Если вы не используете отдельный прокси-сервер, на этом же сервере Kaspersky Web Traffic Security установите сервис Squid (см. рис. ниже).



Рисунок 3. Схема развертывания на один сервер

- Схема развертывания на два и более серверов (см. рис. ниже). На одном сервере устанавливаются Обрабатывающий сервер и Управляющий сервер. На втором сервере устанавливаются Обрабатывающий сервер и Резервный управляющий сервер. На остальных серверах устанавливаются Обрабатывающие серверы.

Если вы не используете отдельный прокси-сервер, на Обрабатывающем сервере установите сервис Squid (см. рис. ниже).

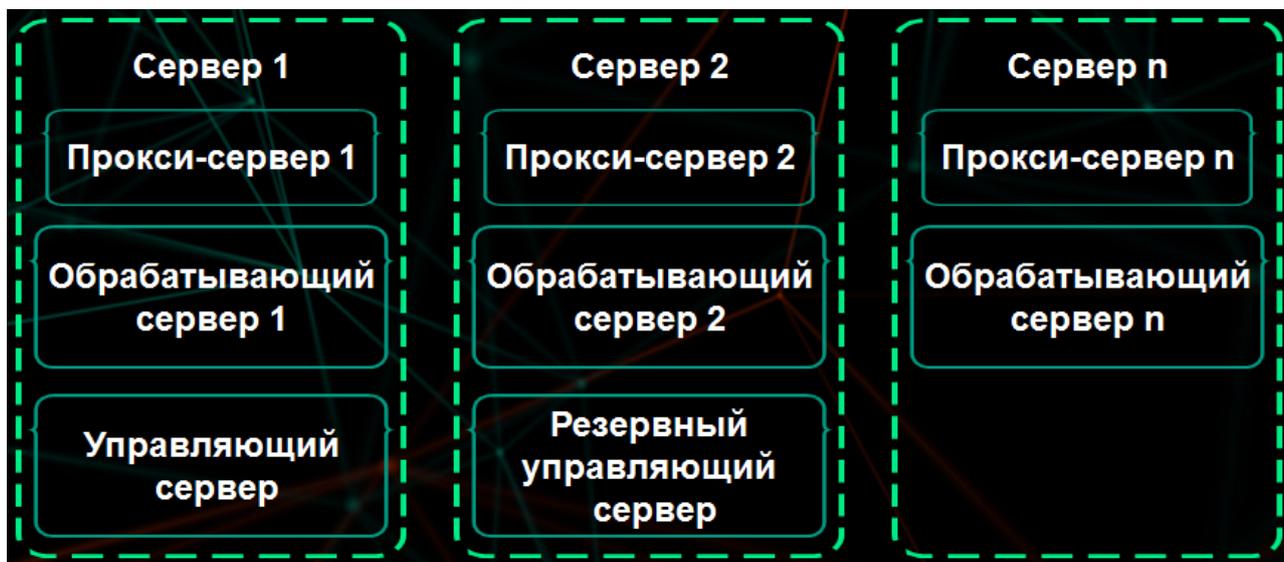


Рисунок 4. Схема развертывания на два и более серверов

В этом разделе

Сценарий установки и настройки Управляющего и Обрабатывающего серверов на одном сервере	30
Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на одном сервере	31
Сценарий установки и настройки Управляющего и Обрабатывающего серверов на разных серверах	32
Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на разных серверах	33

Сценарий установки и настройки Управляющего и Обрабатывающего серверов на одном сервере

Сценарий установки и настройки Управляющего сервера и Обрабатывающего сервера на одном сервере состоит из следующих этапов:

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Управляющего и Резервного управляющего серверов.
4. Настройка портов для работы Обрабатывающего сервера.
5. Установка пакета Управляющего и Резервного управляющего серверов.
6. Установка пакета локализации.
7. Настройка Управляющего сервера.
8. Установка сервиса Squid, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid.
9. Установка пакета Обрабатывающего сервера.
10. Настройка Обрабатывающего сервера.
11. Настройка сервиса Squid, если вы установили сервис Squid.
12. Настройка SSL Bumping в сервисе Squid, если вы установили сервис Squid.

Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на одном сервере

Сценарий установки и настройки Резервного управляющего сервера и Обрабатывающего сервера на одном сервере состоит из следующих этапов:

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Управляющего и Резервного управляющего серверов.
4. Настройка портов для работы Обрабатывающего Сервера.
5. Установка пакета Управляющего и Резервного управляющего серверов.
6. Установка пакета локализации.
7. Настройка Резервного управляющего сервера.
8. Установка сервиса Squid, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid.
9. Установка пакета Обрабатывающего сервера.
10. Настройка Обрабатывающего сервера.
11. Настройка сервиса Squid, если вы установили сервис Squid.
12. Настройка SSL Bumping в сервисе Squid, если вы установили сервис Squid.

Сценарий установки и настройки Управляющего и Обработывающего серверов на разных серверах

Сценарий установки и настройки Управляющего сервера и Обработывающего сервера на разных серверах состоит из следующих этапов:

На Управляющем сервере

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Управляющего и Резервного управляющего серверов.
4. Установка пакета Управляющего и Резервного управляющего серверов.
5. Установка пакета локализации.
6. Настройка Управляющего сервера.

На Обработывающем сервере

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Обработывающего Сервера.
4. Установка сервиса Squid, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid.
5. Установка пакета Обработывающего сервера.
6. Настройка Обработывающего сервера.
7. Настройка сервиса Squid, если вы установили сервис Squid.
8. Настройка SSL Bumping в сервисе Squid, если вы установили сервис Squid.
9. Настройка интеграции сервиса Squid с Active Directory® (на стр. [132](#)), если вы установили сервис Squid.

Сценарий установки и настройки Резервного управляющего и Обрабатывающего серверов на разных серверах

Сценарий установки и настройки Резервного управляющего сервера и Обрабатывающего сервера на разных серверах состоит из следующих этапов:

На Управляющем сервере

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Управляющего и Резервного управляющего серверов.
4. Установка пакета Управляющего и Резервного управляющего серверов.
5. Установка пакета локализации.
6. Настройка Резервного управляющего сервера.

На Обрабатывающем сервере

1. Отключение SELinux.
2. Установка сервиса nginx.
3. Настройка портов для работы Обрабатывающего Сервера.
4. Установка сервиса Squid, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid.
5. Установка пакета Обрабатывающего сервера.
6. Настройка Обрабатывающего сервера.
7. Настройка сервиса Squid, если вы установили сервис Squid.
8. Настройка SSL Bumping в сервисе Squid, если вы установили сервис Squid.
9. Настройка интеграции сервиса Squid с Active Directory (на стр. [132](#)), если вы установили сервис Squid.

Подготовка к установке программы

Этот раздел содержит инструкции по подготовке к установке Управляющего сервера, Резервного управляющего сервера и Обрабатывающего сервера.

Выполняйте действия по подготовке к установке на том сервере, который вы хотите использовать для Управляющего сервера, Резервного управляющего сервера или Обрабатывающего сервера. Учетная запись должна обладать правами суперпользователя.

Перед установкой пакета Kaspersky Web Traffic Security вам нужно выполнить следующие действия:

- убедиться, что сервер удовлетворяет аппаратным и программным требованиям;
- загрузить пакет установки Kaspersky Web Traffic Security формата TXZ, DEB или RPM с сайта интернет-магазина на сервер.

Перед установкой Kaspersky Web Traffic Security на сервер, работающий под управлением операционной системы Debian или Ubuntu, требуется выполнить следующую команду: `# locale-gen en_US.UTF-8`.

Установка пакета веб-интерфейса Kaspersky Web Traffic Security требуется, только если вы хотите управлять программой через браузер.

Перед установкой пакета веб-интерфейса Kaspersky Web Traffic Security вам нужно выполнить следующие действия:

- убедиться, что сервер удовлетворяет аппаратным и программным требованиям;
- загрузить пакет установки веб-интерфейса Kaspersky Web Traffic Security формата DEB или RPM с сайта интернет-магазина на сервер.

Для корректного функционирования пакетов локализации необходимо наличие в системе соответствующей локализации.

Пример:

Если необходимо установить в Debian GNU / Linux 6.0 пакет русской локализации `klms-110n-ru_<номер_версии>_i386.deb`, то перед установкой пакета необходимо убедиться, что в системе присутствует поддержка русского языка.

► Чтобы просмотреть список поддерживаемых языков, выполните следующую команду:

```
# locale -a
```

Если в этом списке нет русского языка, то вам нужно его установить.

► Чтобы установить русский язык, выполните следующую команду:

```
# dpkg-reconfigure locales
```

Теперь вы можете перейти к установке пакета `klms-110n-ru_<номер_версии>_i386.deb`.

Аналогичные действия необходимо производить для любой локализации.

В этом разделе

Отключение SELinux.....	35
Настройка портов для работы Управляющего и Резервного управляющего серверов.....	35
Настройка портов для работы Обрабатывающего сервера.....	36
Установка сервиса nginx.....	38
Настройка сервиса nginx при использовании ALT Linux.....	40

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.

Настройка портов для работы Управляющего и Резервного управляющего серверов

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

► *Чтобы настроить порты для работы Управляющего сервера или Резервного управляющего сервера, выполните следующие действия:*

1. Откройте доступ к портам 80, 443 и 9045. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux:

```
firewall-cmd --add-port=80/tcp --permanent
```

```
firewall-cmd --add-port=443/tcp --permanent
firewall-cmd --add-port=9045/tcp --permanent
firewall-cmd --add-port=705/tcp --permanent
```

- **Ubuntu:**

```
ufw allow 80
ufw allow 443
ufw allow 9045
ufw allow 705
```

- **Debian:**

```
apt-get install iptables-persistent
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp --dport 9045 -j ACCEPT
iptables -A INPUT -p tcp --dport 705 -j ACCEPT
```

- Если вы используете операционную систему SUSE Linux Enterprise Server, укажите в файле `/etc/sysconfig/SuSEfirewall2` параметр `FW_SERVICES_EXT_TCP=«80 443 9045 705»`.

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 Управляющего сервера или Резервного управляющего сервера.

Настройка портов для работы Обработывающего сервера

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

► Чтобы настроить порты для работы Обрабатывающего сервера, выполните следующие действия

1. Откройте доступ к портам 3128 и 9046. Для этого выполните следующие команды в зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux:

```
firewall-cmd --add-port=3128/tcp --permanent
firewall-cmd --add-port=9046/tcp --permanent
firewall-cmd --add-port=705/tcp --permanent
```

- Ubuntu:

```
ufw allow 3128
ufw allow 9046
ufw allow 705
```

- Debian:

```
apt-get install iptables-persistent
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
iptables -A INPUT -p tcp --dport 9046 -j ACCEPT
iptables -A INPUT -p tcp --dport 705 -j ACCEPT
```

- Если вы используете операционную систему SUSE Linux Enterprise Server, укажите в файле `/etc/sysconfig/SuSEfirewall2` параметр `FW_SERVICES_EXT_TCP=«3128 9046 705»`.

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 Обрабатывающего сервера.

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:

а. 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`.

б. 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`.

- Если вы используете CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server, включите поддержку репозитория 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
```

- 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
```

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

```
systemctl enable nginx
```

- Запустите сервис nginx. Для этого выполните команду:

```
service nginx start
```

- Проверьте статус сервиса nginx. Для этого выполните команду:

```
service nginx status
```

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

Сервис nginx будет установлен.

Настройка сервиса nginx при использовании ALT Linux

В сертифицированной версии ALT Linux 7.0.5 СПТ поставляется nginx версии 1.4.7, в котором недоступны некоторые конфигурационные директивы. При отсутствии возможности обновить nginx до версии не ниже 1.10.1, необходимо выполнить предварительную настройку сервиса nginx.

Настройку сервиса nginx необходимо выполнять после установки пакета формата RPM перед началом установки программы.

► Чтобы настроить сервис nginx, выполните следующие действия:

1. Если вы хотите выполнить настройку вручную, отредактируйте следующие конфигурационные файлы:

- /opt/kaspersky/kwts-control/share/configs/management/nginx.conf.template
- /opt/kaspersky/kwts-control/share/configs/backend/nginx.conf
- /opt/kaspersky/kwts-worker/share/configs/management/nginx.conf.template

В каждом из указанных файлов необходимо выполнить следующие действия:

- В директиве `add_header` удалите параметр `always`.
- Удалите директиву `expires` (строку целиком).

2. Если вы хотите выполнить настройку автоматически, запустите следующий скрипт:

```
find /opt/kaspersky/ -iname "*nginx.conf*" -exec sed -i -e 's/\<always\>//g' -e '/\<expires\>/d' {} \;
```

Настройка сервиса nginx будет завершена. Вы можете приступить к установке программы.

Установка и первоначальная настройка программы

В этом разделе

Установка и настройка Управляющего и Резервного управляющего серверов	42
Установка и настройка Обработывающего сервера.....	49
Сценарий повторной установки Управляющего сервера с добавлением Резервного управляющего сервера	52

Установка и настройка Управляющего и Резервного управляющего серверов

Этот раздел содержит пошаговые инструкции по установке и предварительной настройке Управляющего сервера или Резервного управляющего сервера на отдельном сервере.

Управляющий сервер и Резервный управляющий сервер должны удовлетворять аппаратным и программным требованиям.

Выполняйте действия по установке на том сервере, который вы хотите использовать для Управляющего сервера или Резервного управляющего сервера. Учетная запись должна обладать правами суперпользователя.

В этом разделе

Установка пакета Управляющего и Резервного управляющего серверов	42
Установка пакета локализации	43
Настройка Управляющего сервера	43
Настройка Резервного управляющего сервера	45
Создание файла автоматической настройки Управляющего или Резервного управляющего сервера	46
Запуск автоматической настройки Управляющего или Резервного управляющего сервера	46
Удаление Управляющего или Резервного управляющего сервера	47

Установка пакета Управляющего и Резервного управляющего серверов

► Чтобы установить пакет Управляющего сервера или Резервного управляющего сервера, выполните следующие действия:

1. Скопируйте пакет `kwts-control`, 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-control_6.0.0-<версия пакета>.rpm
```
 - Ubuntu или Debian:


```
dpkg -i kwts-control_6.0.0-<версия пакета>.deb
```
3. Ожидайте окончания установки.

После окончания установки в командной строке появится сообщение о необходимости запуска скрипта настройки сервера.

Установка пакета локализации

Установка пакета английской локализации не требуется.

- ▶ Чтобы установить пакет локализации формата RPM на 64-битную операционную систему, выполните следующую команду:

```
rpm -i kwts-control_xx-<номер_версии>.noarch.rpm
```

Здесь xx – двухбуквенное обозначение языка, например, ru.

- ▶ Чтобы установить пакет локализации из пакета формата DEB на 64-битную операционную систему, выполните следующие действия:

1. Убедитесь, что необходимый пакет локализации доступен в формате UTF-8. Для этого выполните следующую команду:

```
locale -a | grep utf8
```

2. Скомпилируйте необходимые пакеты локализации. Для этого выполните следующую команду:

```
dpkg-reconfigure locales
```

3. Выполните следующую команду:

```
dpkg -i kwts-control-ll10n-xx_<номер_версии>_all.deb
```

Здесь xx – двухбуквенное обозначение языка, например, ru.

Настройка Управляющего сервера

- ▶ Чтобы настроить Управляющий сервер, выполните следующие действия:

1. Запустите скрипт настройки Управляющего сервера. Для этого выполните команду:

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

2. Выберите язык просмотра Лицензионного соглашения, Политики конфиденциальности, Положения о Kaspersky Security Network и Дополнительного Положения о Kaspersky Security Network. Для этого введите число, расположенное рядом с языком, который вы хотите выбрать, и нажмите на клавишу **ENTER**.
3. Ознакомьтесь с Лицензионным соглашением. Для этого нажмите на клавишу **ENTER**.
4. Нажмите на клавишу **Q** для выхода из режима просмотра.
5. Выполните одно из следующих действий:
 - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.
 - Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.
6. Нажмите на клавишу **ENTER**.

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

7. Ознакомьтесь с текстом Политики конфиденциальности. Для этого нажмите на клавишу **ENTER**.
8. Нажмите на клавишу **Q** для выхода из режима просмотра.
9. Выполните одно из следующих действий:
 - Если вы хотите принять условия Политики конфиденциальности, введите `yes`.
 - Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.
10. Нажмите на клавишу **ENTER**.

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

11. Назначьте этому серверу роль Управляющий сервер (`master`). Для этого введите `1` и нажмите на клавишу **ENTER**.
12. Ознакомьтесь с Положением о Kaspersky Security Network. Для этого нажмите на клавишу **ENTER**.
13. Нажмите на клавишу **Q** для выхода из режима просмотра.
14. Выполните одно из следующих действий:
 - Если вы хотите участвовать в Kaspersky Security Network, введите `yes` и нажмите на клавишу **ENTER**.
 - Если вы хотите отказаться от участия в Kaspersky Security Network, введите `no` и нажмите на клавишу **ENTER**.

Вы можете изменить свой выбор в веб-интерфейсе программы.

15. Если вы выбрали участие в Kaspersky Security Network, ознакомьтесь с текстом Дополнительного Положения о Kaspersky Security Network. Для этого нажмите на клавишу **ENTER**.
16. Нажмите на клавишу **Q** для выхода из режима просмотра.
17. Выберите один из следующих вариантов:
 - Если вы хотите отправлять KSN-статистику в «Лабораторию Касперского», введите `yes` и нажмите на клавишу **ENTER**.
 - Если вы не хотите отправлять KSN-статистику в «Лабораторию Касперского», введите `no` и нажмите на клавишу **ENTER**.

Вы можете изменить свой выбор в веб-интерфейсе программы.

18. Введите IP-адрес сетевого интерфейса для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.

По умолчанию используется текущий активный IP-адрес.

19. Введите порт для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.

Рекомендуется использовать значение по умолчанию: 9045.

20. Введите пароль учетной записи Administrator, и нажмите на клавишу **ENTER**.

21. Повторно введите пароль учетной записи Administrator, и нажмите на клавишу **ENTER**.

Настройка Управляющего сервера будет завершена.

Настройка Резервного управляющего сервера

Вы можете назначить роль Резервный управляющий сервер любому количеству серверов, в том числе вы можете вообще не использовать Резервный управляющий сервер.

► Чтобы настроить Резервный управляющий сервер, выполните следующие действия:

1. Запустите скрипт настройки Резервного управляющего сервера. Для этого выполните команду:

```
/opt/kaspersky/kwts-control/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. Ознакомьтесь с Лицензионным соглашением. Для этого нажмите на клавишу **ENTER**.

4. Нажмите на клавишу **Q** для выхода из режима просмотра.

5. Выполните одно из следующих действий:

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

6. Нажмите на клавишу **ENTER**.

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

7. Ознакомьтесь с текстом Политики конфиденциальности. Для этого нажмите на клавишу **ENTER**.

8. Нажмите на клавишу **Q** для выхода из режима просмотра.

9. Выполните одно из следующих действий:

- Если вы хотите принять условия Политики конфиденциальности, введите `yes`.
- Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.

10. Нажмите на клавишу **ENTER**.

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

11. Назначьте этому Управляющему серверу роль Резервный управляющий сервер (`slave`). Для этого введите `2` и нажмите на клавишу **ENTER**.

12. Введите IP-адрес сетевого интерфейса для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.

По умолчанию используется текущий активный IP-адрес.

13. Введите порт для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.

Рекомендуется использовать значение по умолчанию: 9045.

Настройка Резервного управляющего сервера будет завершена.

Создание файла автоматической настройки Управляющего или Резервного управляющего сервера

Вы можете создать файл автоматической настройки, содержащий параметры сервера. Вы можете использовать этот файл для автоматической настройки других серверов с такой же ролью.

► Чтобы создать файл автоматической настройки, выполните команду:

```
/opt/kaspersky/kwts-control/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 Управляющего или Резервного управляющего сервера

Вы можете выполнить автоматическую настройку Управляющего сервера или Резервного управляющего сервера с помощью файла автоматической настройки.

Файл автоматической настройки может содержать пароль администратора. Убедитесь, что этот файл защищен от несанкционированного доступа.

► Чтобы запустить автоматическую настройку Управляющего сервера или Резервного управляющего сервера, выполните следующую команду:

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

Параметры файла автоматической настройки Управляющего сервера или Резервного управляющего сервера приведены в таблице ниже.

Таблица 2. Параметры файла автоматической настройки Управляющего сервера или Резервного управляющего сервера

Параметр	Описание	Возможные значения
eula	Согласие с условиями Лицензионного соглашения.	yes

Параметр	Описание	Возможные значения
privacy_policy	Согласие с условиями Политики конфиденциальности.	yes
ksn_eula	Только для Управляющего сервера. Согласие с условиями Положения о Kaspersky Security Network.	yes no
ksn_stat_eula	Только для Управляющего сервера. Согласие с условиями Дополнительного Положения о Kaspersky Security Network.	yes no
noderole	Только для Резервного управляющего сервера. Выбор Управляющего или Обрабатывающего сервера.	control
nodeip	Выбор IP-адреса Управляющего сервера.	<IP-адрес>
nodeport	Выбор порта для взаимодействия с другими серверами локальной сети. Рекомендуется использовать значение по умолчанию: 9045.	<порт>
nodesubrole	Выбор роли сервера.	master slave
adminpassword	Только для Управляющего сервера. Указание пароля учетной записи Administrator.	<пароль>

Удаление Управляющего или Резервного управляющего сервера

► Чтобы удалить Управляющий сервер или Резервный управляющий сервер, выполните следующие действия на том сервере, на котором он установлен:

1. Проверьте наличие пакетов локализации. Для этого выполните одну из следующих команд в зависимости от используемой операционной системы:

- CentOS, Red Hat Enterprise Linux или SUSE Linux Enterprise Server:

```
rpm -qa | grep kwts
```

- Ubuntu или Debian:

```
dpkg -l | grep kwts
```

2. Если у вас установлены пакеты локализации, удалите их. Для этого выполните следующие действия в зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux.

Выполните команду:

```
rpm -e kwts-control_xx-<номер_версии>.noarch
```

- SUSE Linux Enterprise Server:

a. Выполните команду:

```
rpm -e kwts-control_xx
```

b. Введите **Y** и нажмите на клавишу **ENTER**.

- Ubuntu или Debian.

Выполните команды:

```
dpkg -r kwts-control-l10n-xx
```

```
dpkg -P kwts-control-l10n-xx
```

Здесь **xx** – двухбуквенное обозначение языка, например, **ru**.

3. Удалите пакет Управляющего или Резервного управляющего сервера. Для этого выполните следующие действия в зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux.

Выполните команду:

```
rpm -e kwts-control
```

- SUSE Linux Enterprise Server:

a. Выполните команду:

```
rpm -e kwts-control
```

b. Подтвердите удаление пакета. Для этого введите **Y** и нажмите на клавишу **ENTER**.

- Ubuntu или Debian.

Выполните команду:

```
dpkg -r kwts-control
```

4. Запустите скрипт для удаления всех файлов и директорий. Для этого выполните команду:

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

Отобразится запрос подтверждения удаления всех файлов и директорий.

5. Введите **yes** и нажмите на клавишу **ENTER**.

6. Если вы используете Ubuntu или Debian, выполните следующую команду:

```
dpkg -P kwts-control
```

Удаление завершится.

Установка и настройка Обрабатывающего сервера

Этот раздел содержит пошаговые инструкции по установке и предварительной настройке Обрабатывающего сервера на отдельном сервере.

Обрабатывающий сервер должен удовлетворять аппаратным и программным требованиям.

Выполняйте действия по установке на том сервере, который вы хотите использовать для Обрабатывающего сервера. Учетная запись должна обладать правами суперпользователя.

В этом разделе

Установка пакета Обрабатывающего сервера	49
Настройка Обрабатывающего сервера	49
Создание файла автоматической настройки Обрабатывающего сервера	50
Запуск автоматической настройки Обрабатывающего сервера	51
Удаление Обрабатывающего сервера	51

Установка пакета Обрабатывающего сервера

► Чтобы установить пакет Обрабатывающего сервера, выполните следующие действия:

1. Скопируйте пакет `kwts-worker`, входящий в комплект поставки, в домашнюю директорию.
2. Запустите установку пакета Обрабатывающего сервера. 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-worker_6.0.0-<версия пакета>.rpm
```

- Ubuntu или Debian:

```
dpkg -i kwts-worker_6.0.0-<версия пакета>.deb
```

3. Ожидайте окончания установки.

После окончания установки в командной строке появится сообщение о необходимости запуска скрипта настройки Обрабатывающего сервера.

Настройка Обрабатывающего сервера

► Чтобы настроить Обрабатывающий сервер, выполните следующие действия:

1. Запустите скрипт настройки Обрабатывающего сервера. Для этого выполните команду:

```
/opt/kaspersky/kwts-worker/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. Ознакомьтесь с Лицензионным соглашением. Для этого нажмите на клавишу **ENTER**.
4. Нажмите на клавишу **Q** для выхода из режима просмотра.
5. Выполните одно из следующих действий:
 - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.
 - Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.
6. Нажмите на клавишу **ENTER**.

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

7. Ознакомьтесь с текстом Политики конфиденциальности. Для этого нажмите на клавишу **ENTER**.
8. Нажмите на клавишу **Q** для выхода из режима просмотра.
9. Выполните одно из следующих действий:
 - Если вы хотите принять условия Политики конфиденциальности, введите `yes`.
 - Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.
10. Нажмите на клавишу **ENTER**.

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

11. Введите IP-адрес сетевого интерфейса для приема входящего соединения для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.
По умолчанию используется текущий активный IP-адрес.
12. Укажите порт для взаимодействия с другими серверами локальной сети и нажмите на клавишу **ENTER**.
Рекомендуется использовать значение по умолчанию: 9046.
13. Перезагрузите сервис `nginx`. Для этого выполните команду:

```
service nginx restart
```

Настройка Обрабатывающего сервера будет завершена.

Создание файла автоматической настройки Обрабатывающего сервера

Вы можете создать файл автоматической настройки, содержащий параметры сервера. Вы можете использовать этот файл для автоматической настройки других серверов с такой же ролью.

- Чтобы создать файл автоматической настройки, выполните команду:

```
/opt/kaspersky/kwts-worker/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 Обрабатывающего сервера

Вы можете выполнить автоматическую настройку Обрабатывающего сервера с помощью файла автоматической настройки.

Файл автоматической настройки может содержать пароль администратора. Убедитесь, что этот файл защищен от несанкционированного доступа.

- Чтобы запустить автоматическую настройку Обрабатывающего сервера, выполните следующую команду:

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

Параметры файла автоматической настройки Обрабатывающего сервера приведены в таблице ниже.

Таблица 3. Параметры файла автоматической настройки Обрабатывающего сервера

Параметр	Описание	Возможные значения
eula	Согласие с условиями Лицензионного соглашения.	yes
privacy_policy	Согласие с условиями Политики конфиденциальности.	yes
noderole	Назначение серверу роли Обрабатывающий сервер.	worker
nodeip	Выбор IP-адреса Обрабатывающего сервера.	<IP-адрес>
nodeport	Выбор порта для взаимодействия с другими серверами локальной сети. Рекомендуется использовать значение по умолчанию: 9046.	<порт>

Удаление Обрабатывающего сервера

- Чтобы удалить Обрабатывающий сервер, выполните следующие действия:

1. Удалите пакет Обрабатывающего сервера. Для этого выполните следующие действия в

зависимости от используемой операционной системы:

- CentOS или Red Hat Enterprise Linux.

Выполните команду:

```
rpm -e kwts-worker
```

- SUSE Linux Enterprise Server:

a. Выполните команду:

```
rpm -e kwts-worker
```

b. Подтвердите удаление пакета. Для этого введите `Y` и нажмите на клавишу **ENTER**.

- Ubuntu или Debian.

Выполните команду:

```
dpkg -r kwts-worker
```

2. Запустите скрипт для удаления всех файлов и директорий Обрабатывающего сервера:

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

Отобразится запрос подтверждения удаления всех файлов и директорий Обрабатывающего сервера.

3. Введите `yes` и нажмите на клавишу **ENTER**.

4. Если вы используете Ubuntu или Debian, выполните следующую команду:

```
dpkg -P kwts-worker
```

Обрабатывающий сервер будет удален.

Сценарий повторной установки Управляющего сервера с добавлением Резервного управляющего сервера

Если Резервный управляющий сервер не был настроен, а Управляющий сервер вышел из строя, необходимо повторно установить программу. Повторная установка состоит из следующих этапов:

- a. Удаление Управляющего или Резервного управляющего сервера (на стр. [47](#))
- b. Установка пакета Управляющего и Резервного управляющего серверов
- c. Установка пакета локализации, если требуется
- d. Настройка Управляющего сервера

Для обеспечения отказоустойчивости рекомендуется настроить Резервный управляющий сервер. Вы можете пропустить следующие шаги, однако в этом случае отказоустойчивость продукта не гарантируется.

Установку и настройку Резервного управляющего сервера необходимо выполнять на отдельном сервере в следующей последовательности:

1. Установка пакета Управляющего и Резервного управляющего сервера (см. раздел «Установка пакета Управляющего и Резервного управляющего серверов» на стр. [42](#)).
2. Установка пакетов локализации (см. раздел «Установка пакета локализации» на стр. [43](#)), если требуется.
3. Настройка Резервного управляющего сервера (на стр. [45](#)).
4. Добавление сервера (на стр. [65](#)) с помощью веб-интерфейса программы.

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 **Administrator с правами суперпользователя**.

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

- Администратор сервера.
- Администратор безопасности.

Администратору сервера рекомендуется назначить следующие права:

- **Создавать/изменять/удалять серверы.**
- **Просматривать журналы трассировки.**

Администратору безопасности рекомендуется назначить следующие права:

- **Создавать/изменять/удалять серверы.**
- **Просматривать журналы трассировки.**
- **Проверять целостность данных.**
- **Просматривать информацию о серверах.**
- **Создавать/изменять рабочие области.**
- **Просматривать рабочие области.**
- **Удалять рабочие области.**
- **Создавать/изменять глобальные роли.**
- **Просматривать глобальные роли.**
- **Удалять глобальные роли.**
- **Создавать/изменять глобальные правила.**
- **Просматривать глобальные правила.**
- **Удалять глобальные правила.**
- **Просматривать глобальные события.**
- **Экспортировать глобальные события.**
- **Просматривать раздел Мониторинг.**
- **Изменять параметры.**
- **Просматривать параметры.**

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	55
Проверка работоспособности. Тестовый файл EICAR	55

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.

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.
- **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.
- **Серверы.** Позволяет управлять серверами с Kaspersky Web Traffic Security.
- **Параметры.** Содержит разделы **Защита**, **Внешние службы**, **Обновление баз**, **Лицензирование**, **Соединение с прокси-сервером**, **Соединение с LDAP-сервером**, **Шаблоны страниц запрета доступа**, **События**, **Syslog**, **ICAP-сервер**, **Соединение с SNMP-сервером**, **Вход с помощью службы единого входа** и **Administrator с правами суперпользователя**, 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.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков. Вы можете настраивать схему расположения графиков, добавлять, удалять, перемещать графики и выбирать период отображения данных.

В окне веб-интерфейса программы в разделе **Мониторинг** отображаются следующие графики:

- **Общая информация:**
 - **Обнаружения по категории.** Отображение обнаруженной активности по категории информации, к которой обращались пользователи.
 - **Работа серверов.** Отображение работоспособности серверов.
 - **Обработка данных.** Отображение состояния обработки трафика программой.
 - **Антивирус.** Отображение состояния обработки трафика модулем Антивирус.
 - **Анти-Фишинг.** Отображение состояния обработки трафика модулем Анти-Фишинг.
- **Последние 10:**
 - **Последние 10 угроз.** 10 угроз, обнаруженных программой за последнее время.
 - **Последние 10 заблокированных URL-адресов.** 10 заблокированных URL-адресов, обнаруженных программой за последнее время.
 - **Последние 10 пользователей с заблокированными запросами.** 10 пользователей с заблокированными запросами, обнаруженных программой за последнее время.

В этом разделе

Создание новой схемы расположения графиков	58
Выбор схемы расположения графиков из списка	59
Добавление графика на схему расположения графиков	59
Перемещение графика на схеме расположения графиков	60
Удаление графика со схемы расположения графиков.....	60
Назначение схемы расположения графиков для использования по умолчанию	61
Переименование схемы расположения графиков	61
Удаление схемы расположения графиков	61

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 на новую схему расположения графиков, нажмите на кнопку **Графики** и выполните следующие действия:
 - а. В появившемся окне **Добавить график** включите переключатели рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
 - б. Нажмите на кнопку .Выбранные графики будут добавлены в схему расположения графиков.
 6. Нажмите на кнопку **Сохранить**.
- Новая схема расположения графиков будет добавлена в список схем расположения графиков в разделе **Графики**.

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.

Добавление графика на схему расположения графиков

- *Чтобы добавить график на схему расположения графиков, выполните следующие действия*
1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
 2. В списке схем расположения графиков выберите схему, на которую вы хотите добавить график.
 3. В верхней части окна нажмите на кнопку .
 4. В раскрывающемся списке выберите **Изменить**.
 5. Нажмите на кнопку **Графики**.
 6. В появившемся окне **Добавить график** включите переключатель рядом с графиком, который вы хотите добавить на схему расположения графиков.
 7. Нажмите на кнопку .

8. Нажмите на кнопку **Сохранить**.

График будет добавлен на текущую схему расположения графиков.

Перемещение графика на схеме расположения графиков

- *Чтобы переместить график на схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, на которой вы хотите переместить график.
3. В верхней части окна нажмите на кнопку .
4. В раскрывающемся списке выберите **Изменить**.
5. Выберите график, который вы хотите переместить на схеме расположения графиков.
6. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.
7. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков будет сохранена.

Удаление графика со схемы расположения графиков

- *Чтобы удалить график со схемы расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, с которой вы хотите удалить график.
3. В верхней части окна нажмите на кнопку .
4. В раскрывающемся списке выберите **Изменить**.
5. Нажмите на значок  в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Назначение схемы расположения графиков для использования по умолчанию

► Чтобы назначить схему расположения графиков для использования 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 расположения графиков, которую вы хотите назначить для использования по умолчанию.
4. Нажмите на значок ☆ слева от названия схемы расположения графиков.

Выбранная схема расположения графиков будет отмечена значком ★ и будет использоваться по умолчанию.

Переименование схемы расположения графиков

► Чтобы переименовать 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 переименовать.
3. В верхней части окна нажмите на кнопку .
4. В раскрывающемся списке выберите **Изменить**.
5. В поле с именем текущей схемы расположения графиков введите новое имя схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет переименована.

Удаление схемы расположения графиков

► 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.

Управление серверами

В веб-интерфейсе вы можете управлять Управляющим, Резервным управляющим и обрабатывающим серверами.

В разделе **Серверы** окна веб-интерфейса программы отображается таблица серверов, а также следующая информация о серверах с установленными компонентами программы:

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

В этом разделе

Настройка отображения таблицы серверов.....	62
Просмотр информации о сервере	62
Добавление сервера.....	65
Изменение параметров сервера	65
Удаление сервера.....	66
Изменение роли сервера	66
Проверка целостности данных	67

Настройка отображения таблицы серверов

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

1. В окне веб-интерфейса программы выберите раздел **Серверы**.
Откроется таблица серверов.
2. По кнопке  откройте меню отображения таблицы.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

Должен быть установлен хотя бы один флажок.

Отображение таблицы серверов будет настроено.

Просмотр информации о сервере

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

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

2. Выберите сервер, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о сервере.

Окно содержит следующую информацию в зависимости от типа сервера:

1. Для Управляющего сервера:

- **Роль текущего сервера** – роль текущего сервера.
- **Состояние кеша LDAP** – дата и время последнего успешного обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Статус отображается для каждого домена Active Directory, с которым была настроена интеграция.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Последнее обновление кеша LDAP** – время и результат последнего обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Если обновление кеша завершилось с ошибкой, то отображается дата и время последней попытки обновления. Если первое выполнение обновления завершилось с ошибкой, то кеш-файл будет пустым, а в информации о сервере отобразится статус *Кеш LDAP пуст*.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Состояние keytab-файла Kerberos** – статус keytab-файла, используемого для Kerberos-аутентификации. Поле доступно, если в разделе **Параметры**, в подразделе **Вход с помощью службы единого входа** включена Kerberos-аутентификация и загружен keytab-файл.
- **Отпечаток сертификата** – отпечаток сертификата сервера.
- **Комментарий** – дополнительная информация о сервере. Необязательный параметр.

Если не установлен Резервный управляющий сервер, то в строке с Управляющим сервером появляется значок  и предупреждение о необходимости обеспечить отказоустойчивость серверов.

2. Для Резервного управляющего сервера:

- **Роль текущего сервера** – роль текущего сервера.
- **Синхронизация серверов** – результат синхронизации с Управляющим сервером.
- **Последнее обновление параметров** – время последней успешной синхронизации с Управляющим сервером, когда были обновлены параметры программы.
- **Состояние кеша LDAP** – дата и время последнего успешного обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Статус отображается для каждого домена Active Directory, с которым была настроена интеграция.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Последнее обновление кеша LDAP** – время и результат последнего обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Если обновление кеша завершилось с ошибкой, то отображается дата и время последней попытки обновления. Если первое выполнение обновления завершилось с ошибкой, то кеш-файл будет пустым, а в информации о сервере отобразится статус *Кеш LDAP пуст*.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Синхронизация времени** – состояние синхронизации времени с сервером, на котором установлен Управляющий сервер.
- **Состояние keytab-файла Kerberos** - статус keytab-файла, используемого для Kerberos-аутентификации. Поле доступно, если в разделе **Параметры**, в подразделе **Вход с помощью службы единого входа** включена Kerberos-аутентификация и загружен keytab-файл.
- **Отпечаток сертификата** – отпечаток сертификата сервера.
- **Комментарий** – дополнительная информация о сервере. Необязательный параметр.

3. Для Обрабатывающего сервера:

- **Роль текущего сервера** – роль текущего сервера.
- **Синхронизация серверов** – результат синхронизации с Управляющим сервером.
- **Последнее обновление параметров** – время последней успешной синхронизации с Управляющим сервером, когда были обновлены параметры программы.
- **Дата окончания срока действия лицензии** – дата, когда истекает срок 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** – доступность внешних служб KSN / KPSN.
- **Антивирус:** – состояние модуля Антивирус.
- **Анти-Фишинг:** – состояние модуля Анти-Фишинг.
- **Последнее обновление баз** – состояние баз программы, а также результат и время их последнего успешного обновления.
- **Состояние кеша LDAP** – дата и время последнего успешного обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Статус отображается для каждого домена Active Directory, с которым была настроена интеграция.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Последнее обновление кеша LDAP** – время и результат последнего обновления информации об учетных записях пользователей в Active Directory, сохраняемой в кеш-файле на сервере. Если обновление кеша завершилось с ошибкой, то отображается дата и время последней попытки обновления. Если первое выполнение обновления завершилось с ошибкой, то кеш-файл будет пустым, а в информации о сервере отобразится статус *Кеш LDAP пуст*.

Поле доступно, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)).

- **Синхронизация времени** – состояние синхронизации времени с сервером, на котором установлен Управляющий сервер.
- **Отпечаток сертификата** – отпечаток сертификата сервера.
- **Комментарий** – дополнительная информация о сервере. Необязательный параметр.
- **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.

Добавление сервера

► Чтобы добавить сервер, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Серверы**.
2. Нажмите на кнопку **Добавить сервер**.
Откроется окно **Добавить сервер**.
3. В поля **IP-адрес** и **Порт** введите IP-адрес и порт сервера, который вы хотите добавить.
4. Если требуется, в поле **Комментарий (необязательно)** укажите дополнительную информацию о сервере.
5. Нажмите на кнопку **Далее**.
6. Сравните отпечатки сертификата в окне **Подтвердить сервер** и в файле сертификата в папке сервиса nginx (/etc/nginx/kwts-control/management.crt для Управляющего сервера или Резервного управляющего сервера или /etc/nginx/kwts-worker/management.crt для Обрабатывающего сервера). Если отпечаток совпадает, нажмите на кнопку **Подтвердить**.

Вы можете получить отпечаток сертификата сервера с помощью следующей команды:

- для Управляющего сервера или Резервного управляющего сервера:

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

- для Обрабатывающего сервера:

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

Сервер будет добавлен и отобразится в таблице серверов на странице **Серверы**.

Изменение параметров сервера

► Чтобы изменить параметры сервера, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Серверы**.
2. В таблице серверов выберите сервер, параметры которого вы хотите изменить.
Откроется окно параметров сервера.
3. В правом нижнем углу окна параметров сервера нажмите на кнопку **Изменить**.
Откроется окно **Изменить сервер**.
4. Если требуется, измените следующие параметры:
 - Дополнительную информацию о сервере в поле **Комментарий (необязательно)**.
 - Количество одновременных потоков обработки трафика ICAP-сервером в поле **Количество потоков проверки**.

Вы можете указать значение от 4 до 1024. Этот параметр доступен только для Обрабатывающих серверов.

Вы не можете изменить IP-адрес и порт сервера. При необходимости удалите этот сервер (см. раздел «Удаление сервера» на стр. 66) и добавьте новый сервер (см. раздел «Добавление сервера» на стр. 65) с нужным адресом.

5. Нажмите на кнопку **Сохранить**.

Удаление сервера

Вы можете удалить Резервный управляющий сервер или Обработывающий сервер через веб-интерфейс программы. Удаление Управляющего сервера через веб-интерфейс программы не предусмотрено.

► *Чтобы удалить сервер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы**.
2. В таблице серверов выберите сервер, параметры которого вы хотите удалить.
Откроется окно параметров сервера.
3. В левом нижнем углу окна параметров сервера нажмите на кнопку **Удалить**.
Сервер будет удален из таблицы серверов.

Изменение роли сервера

Вы можете назначить Управляющему серверу роль Резервный управляющий сервер или назначить Резервному управляющему серверу роль Управляющий сервер. Например, это может понадобиться при выходе из строя Управляющего сервера или при необходимости удалить программу с этого сервера. Для Обработывающих серверов изменение роли не предусмотрено.

► *Чтобы назначить Управляющему серверу роль Резервный управляющий сервер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы**.
2. В таблице серверов выберите Управляющий сервер.
Откроется окно параметров сервера.
3. Нажмите на кнопку **Изменить роль**.
Управляющий сервер станет Резервным управляющим сервером.

► *Чтобы назначить Резервному управляющему серверу роль Управляющий сервер, выполните следующие действия:*

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

2. В таблице серверов выберите Резервный управляющий сервер.
Откроется окно параметров сервера.
3. Нажмите на кнопку **Перейти к управлению сервером**.
В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль администратора программы.
Откроется окно с информацией о Резервном управляющем сервере.
5. Нажмите на кнопку **Назначить роль Управляющий сервер**.
Откроется окно подтверждения.
6. Нажмите на кнопку **Да**.
Резервный управляющий сервер станет Управляющим сервером.

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 **Серверы**.
2. По кнопке  откройте меню раздела **Серверы**.
3. Выберите пункт **Проверить целостность данных**.
Откроется окно **Выбор серверов для проверки целостности данных**.
4. В таблице серверов установите флажки напротив тех серверов, для которых вы хотите запустить проверку целостности.
5. Нажмите на кнопку **Запустить**.
После окончания проверки отобразится таблица с результатами. Вы можете загрузить список исполняемых файлов, в которых обнаружено нарушение целостности.

Работа программы в аварийном режиме

Kaspersky Web Traffic Security переходит в аварийный режим, если в системе два и более Управляющих серверов. Например, Управляющий сервер стал недоступен, и эта роль была назначена Резервному управляющему серверу. Через некоторое время первый Управляющий сервер снова стал доступен, и в системе оказалось два Управляющих сервера.

Аварийный режим программы не влияет на работоспособность Обработывающих серверов. Они продолжают обрабатывать сетевой трафик в соответствии с последними значениями параметров, полученными от Управляющего сервера до перехода программы в аварийный режим.

Управляющий сервер

В окне аварийного режима на Управляющем сервере отображается следующая информация:

- IP-адрес текущего сервера.
- Роль текущего сервера.
- Таблица Управляющих и Резервных управляющих серверов.

Таблица Управляющих и Резервных управляющих серверов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к серверу.
- **Роль** – роль текущего сервера в программе.
- **Управляющий сервер** – IP-адрес Управляющего сервера.
Доступно только для Резервного управляющего сервера.
- **Последнее обновление параметров** – время последней синхронизации параметров.
- **Состояние соединения с Управляющим сервером** – доступность Управляющего сервера по сети.

Значок  в строке таблицы означает, что в работе этого сервера возникла проблема. Например, Резервный управляющий сервер ошибочно стал основным, или сервер недоступен по сети.

Если вы хотите передать управление программой другому серверу, вы можете назначить текущему Управляющему серверу роль Резервного управляющего сервера с помощью кнопки **Назначить роль Резервный управляющий сервер**.

Резервный управляющий сервер

В окне аварийного режима на Резервном управляющем сервере отображается следующая информация:

- IP-адрес текущего сервера.
- Роль текущего сервера.
- IP-адрес и доступность Управляющего сервера.
- Дата и время последней синхронизации параметров.
- Таблица Резервных управляющих серверов.

Таблица Резервных управляющих серверов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к серверу.
- **Роль** – роль сервера в программе.

Если вы хотите управлять параметрами программы на этом сервере, вы можете назначить ему роль Управляющего сервера с помощью кнопки **Назначить роль Управляющий сервер**.

Работа с правилами обработки трафика

Вы можете регулировать доступ пользователей к интернет-ресурсам с помощью правил обработки трафика. Все правила делятся на правила доступа и правила защиты. Вы можете создавать группы правил доступа и группы правил защиты. В рамках группы правила проверяются в порядке расположения в таблице сверху вниз.

Kaspersky Web Traffic Security начинает обработку трафика с проверки правил доступа. Если доступ к интернет-ресурсу разрешен, программа переходит к проверке трафика с помощью правил защиты.

Kaspersky Web Traffic Security обрабатывает трафик, начиная с правила с наивысшим приоритетом. Если заданные условия не выполняются, программа проверяет условия правила со следующим приоритетом. Как только заданные в очередном правиле условия выполняются, к трафику применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается.

Порядок определения приоритета зависит от наличия рабочей области (см. раздел «Управление рабочими областями» на стр. [90](#)).

Определение приоритета правил при наличии рабочих областей

Если вы добавили рабочую область, Kaspersky Web Traffic Security классифицирует все правила обработки трафика как *глобальные правила* (действующие для всех рабочих областей) и *правила рабочей области* (созданные для одной рабочей области).

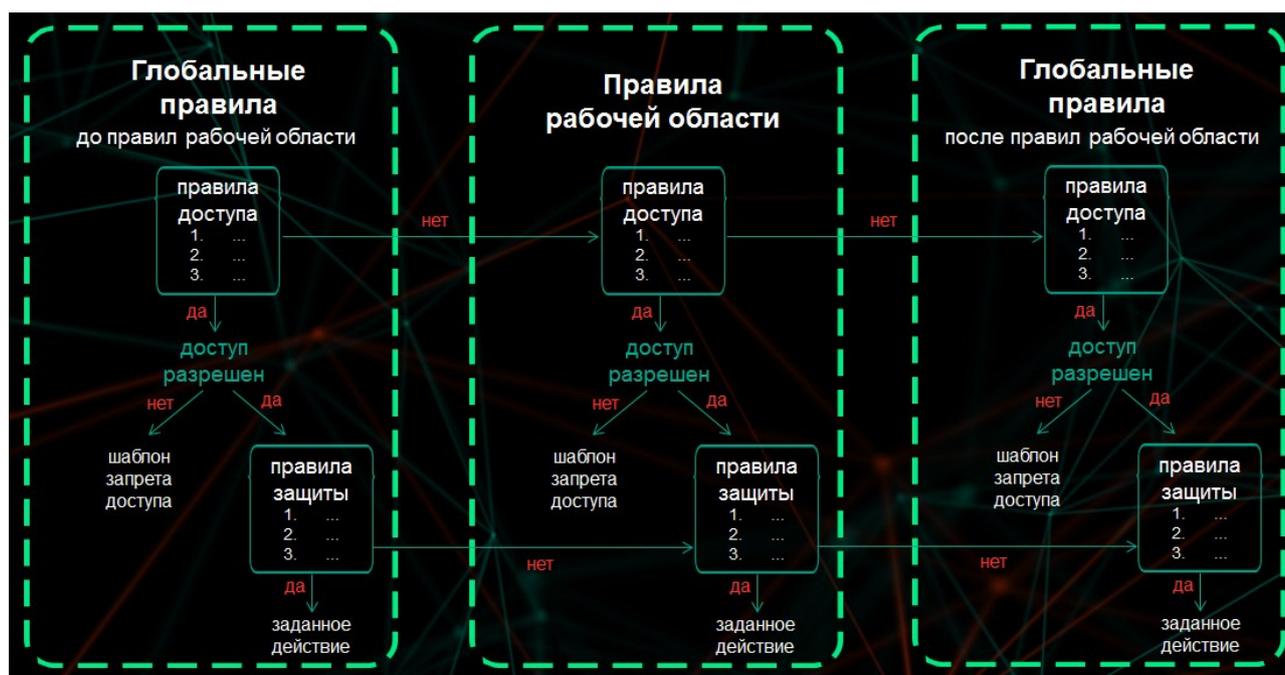


Рисунок 5. Алгоритм срабатывания правил обработки трафика при наличии рабочих областей

В первую очередь программа проверяет глобальные правила наивысшего приоритета. Они отображаются в разделе **Правила** на закладке **До правил рабочей области**.

Правила рабочей области применяются в том случае, если обрабатываемый интернет-ресурс не удовлетворяет условиям ни одного глобального правила наивысшего приоритета. Правила рабочей

области отображаются и настраиваются в разделе **Рабочие области** при выборе рабочей области.

После правил рабочей области программа переходит к проверке глобальных правил более низкого приоритета. Они отображаются в разделе **Правила** на закладке **После правил рабочей области**.

Если ни одно правило низкого приоритета не содержит условий, подходящих для данного интернет-ресурса, трафик обрабатывается согласно правилам по умолчанию – **Default Access Rule** и **Default Protection Rule**. В этом случае программа разрешает доступ ко всем интернет-ресурсам, которые не запрещены в результате проверки на вирусы, фишинг, некоторые легальные программы, которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу. Правила по умолчанию создаются во время установки Kaspersky Web Traffic Security и отображаются в разделе **Правила** на закладке **После правил рабочей области**. Вы не можете изменить или удалить правила по умолчанию.

Определение приоритета правил при отсутствии рабочих областей

Если вы не добавили ни одну рабочую область, то сетевой трафик обрабатывается в соответствии с глобальными правилами от верхнего к нижнему правилу списка до первого совпадения условий. Если ни одно правило не содержит условий, подходящих для данного интернет-ресурса, применяются правила по умолчанию.

В этом разделе

Сценарий настройки доступа к интернет-ресурсам.....	71
Добавление правила доступа	73
Добавление правила защиты	74
Настройка инициатора срабатывания правила	75
Настройка критериев фильтрации трафика	76
Добавление исключения для правила обработки трафика	78
Настройка расписания работы правила обработки трафика	80
Изменение правила обработки трафика	80
Удаление правила обработки трафика.....	81
Создание копии правила обработки трафика	82
Включение и отключение правила обработки трафика	82
Работа с группами правил обработки трафика.....	83
Мониторинг работы правил обработки трафика	85

Сценарий настройки доступа к интернет-ресурсам

Совокупность правил обработки трафика позволяет выполнять следующие задачи:

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

Для этого вы можете использовать существующие доменные группы, если настроена интеграция с Active Directory (см. раздел «Настройка интеграции сервиса Squid с Active Directory» на стр. [132](#)). Например, вы можете разрешить доступ ко всем интернет-ресурсам для группы Администраторы и

запретить категории **Социальные сети** или **Программное обеспечение, аудио, видео (S0)** для остальных сотрудников.

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

Для этого вы можете создать глобальные правила самого высокого приоритета, распространяющиеся на всех пользователей.

- Контролировать объем трафика.

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

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

Если в правиле обработки трафика выбрано действие **Разрешить**, то пользователь получает доступ к интернет-ресурсу, но информация об этом запросе сохраняется в журнал событий (см. раздел «Журнал событий Kaspersky Web Traffic Security» на стр. [116](#)). 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. [90](#)) и / или групп правил обработки трафика (см. раздел «Работа с группами правил обработки трафика» на стр. [83](#)).**

Правила обработки трафика проверяются в соответствии с их приоритетом (см. раздел «Работа с правилами обработки трафика» на стр. [70](#)). 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 правила обработки трафика.**

В рамках каждой рабочей области или группы вы можете добавлять правила доступа (см. раздел «Добавление правила доступа» на стр. [73](#)) и правила защиты (см. раздел «Добавление правила защиты» на стр. [74](#)).

3. **Настройка инициатора срабатывания правила (на стр. [75](#)).**

Для каждого добавленного правила доступа и правила защиты требуется указать пользователя или программу, сетевые соединения которых будет контролировать Kaspersky Web Traffic Security.

4. **Настройка критериев фильтрации трафика (на стр. [76](#)).**

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

5. **Добавление исключения для правила (см. раздел «Добавление исключения для правила обработки трафика» на стр. [78](#)), если требуется.**

Вы можете добавить в исключения инициатора срабатывания правила или критерий фильтрации. Например, вы можете запретить доступ к категории **Программное обеспечение, аудио, видео (S0)** 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.

6. **Настройка расписания работы правила (см. раздел «Настройка расписания работы правила обработки трафика» на стр. [80](#)), 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.

Добавление правила доступа

► Чтобы добавить правило доступа, выполните следующие действия:

1. В окне веб-интерфейса программы выберите один из следующих разделов:
 - для глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. В списке **Группы доступа** выберите одну из групп правил доступа.
Откроется таблица правил обработки трафика.
4. Нажмите на кнопку **Добавить правило доступа**.
Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. Если вы хотите применить правило сразу после добавления, установите флажок **Включить правило**.
7. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
 - **Запретить**, 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.
8. Если вы выбрали вариант **Запретить** и хотите, чтобы при попытке открыть ресурс, доступ к которому запрещен, отображалось сообщение, выполните следующие действия:
 - a. Установите флажок **Введите текст для отображения в шаблоне блокировки**.
 - b. Введите текст сообщения.
 - c. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из вариантов:
 - **%URL%**, если вы хотите добавить URL-адрес веб-сайта, доступ к которому запрещен.
 - **%RULE_NAME%**, если вы хотите добавить название правила доступа.
 - **%APPLICATION%**, если вы хотите добавить название программы.
 - **%DATE%**, если вы хотите добавить дату и время начала действия правила доступа.
9. Если вы выбрали вариант **Разрешить** и хотите удалять HTTP-заголовков *Range*, установите флажок **Удалять HTTP-заголовков 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.
10. Если вы выбрали вариант **Перенаправить**, в поле **URL-адрес перенаправления** укажите URL-адрес, на который будет перенаправлен исходный запрос.

11. В поле **Название правила** введите название правила доступа.
12. В поле **Комментарий (необязательно)** введите комментарий.
Необязательный параметр.
13. Нажмите на кнопку **Добавить**.
Правило доступа будет добавлено.

Добавление правила защиты

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

1. В окне веб-интерфейса программы выберите один из следующих разделов:
 - для глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. В списке **Группы защиты** выберите одну из групп правил защиты.
Откроется таблица правил обработки трафика.
4. Нажмите на кнопку **Добавить правило защиты**.
Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. Если вы хотите применить правило сразу после добавления, установите флажок **Включить правило**.
7. В блоке параметров **Действия** в раскрывающихся списках выберите одно из действий для каждого из следующих параметров:
 - a. **Вредоносная программа**:
 - **Запретить, по возможности вылечить**.
 - **Пропустить проверку**.По умолчанию установлено значение **Запретить, по возможности вылечить**.
 - b. **Фишинг, Зашифрованный архив, Документ с макросом и Объект, для которого не удалось завершить проверку**:
 - **Запретить**.
 - **Пропустить проверку**.По умолчанию установлено значение **Запретить**.
8. Если вы хотите, чтобы при попытке открыть ресурс, доступ к которому запрещен, отображалось сообщение, выполните следующие действия:
 - a. Установите флажок **Введите текст для отображения в шаблоне блокировки**.

- b. Введите текст сообщения.
- c. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из вариантов:
 - **%URL%**, если вы хотите добавить URL-адрес веб-сайта, доступ к которому запрещен.
 - **%RULE_NAME%**, если вы хотите добавить название правила доступа.
 - **%APPLICATION%**, если вы хотите добавить название программы.
 - **%DATE%**, если вы хотите добавить дату и время начала действия правила доступа.
9. В поле **Название правила** введите название правила защиты.
10. В поле **Комментарий (необязательно)** введите комментарий.
Необязательный параметр.
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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. Выберите группу правил обработки трафика.
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` с помощью кнопки **Добавить запись в список**.
 - **Группа пользователей.**
Вы можете выбрать доменную группу из Active Directory или добавить название группы в формате `domain.com/groups/groupname` с помощью кнопки **Добавить запись в список**.

- **DN пользователя.**

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` с помощью кнопки **Добавить запись в список**.

- **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 почтового клиента или программы, сетевую активность которой вы хотите контролировать (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 **любое 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 критериев фильтрации трафика

► *Чтобы настроить критерии фильтрации трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:

- для глобальных правил раздел **Правила**;
- для правил рабочих областей раздел **Рабочие области**.

2. Если вы добавили рабочую область, выберите одну из следующих закладок:

- **До правил рабочей области.**
- **После правил рабочей области.**

3. Выберите группу правил обработки трафика.

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 интернет-ресурсам какой-либо тематики. Например, вы можете запретить доступ к социальным сетям, выбрав категорию **Социальные сети**.

- **URL.**

Вы можете добавить в критерии фильтрации не только URL-адрес, но и протокол или порт сетевых соединений.

- Если вы хотите добавить в критерии фильтрации URL-адрес, введите его в поле в окне **URL**.
- 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 интернет-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.**

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.

При указании `multipart/*` общий заголовок `Content-Type` объекта не учитывается. Объекты MIME-типа `multipart` обрабатываются по частям в соответствии с заголовком `Content-Type` каждой составной части объекта. Если по результатам проверки хотя бы одна составная часть объекта оказывается запрещенной, то действие **Запретить** применяется ко всему объекту.

- **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.

- **SHA2.**

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.
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 **любое из**.
 - Если вы хотите, чтобы правило срабатывало только при одновременном соблюдении всех добавленных условий, выберите **все из**.
 10. Нажмите на кнопку **Сохранить**.
- Критерии фильтрации трафика будут настроены.

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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
 2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области.**
 - **После правил рабочей области.**
 3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите добавить исключение для правила доступа.
 - **Группы защиты**, если вы хотите добавить исключение для правила защиты.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.**
- **Группа пользователей.**
- **DN пользователя.**
- **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 фильтр 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.**
- **MD5.**
- **SHA2.**
- **Направление трафика.**

b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.

c. Если вы хотите добавить новый фильтр трафика, повторите действия по добавлению фильтра трафика.

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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите настроить расписание работы правила доступа.
 - **Группы защиты**, если вы хотите настроить расписание работы правила защиты.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.

Изменение правила обработки трафика

► Чтобы изменить правило обработки трафика, выполните следующие действия:

1. В окне веб-интерфейса программы выберите один из следующих разделов:
 - для глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.

2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области.**
 - **После правил рабочей области.**
 3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите изменить правило доступа.
 - **Группы защиты**, если вы хотите изменить правило защиты.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 **Изменить правило доступа**.
 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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
 2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области.**
 - **После правил рабочей области.**
 3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите удалить правило доступа.
 - **Группы защиты**, если вы хотите удалить правило защиты.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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите скопировать правило доступа.
 - **Группы защиты**, если вы хотите скопировать правило защиты.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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите включить или отключить правило доступа.
 - **Группы защиты**, если вы хотите включить или отключить правило защиты.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.

Работа с группами правил обработки трафика

Вы можете объединять правила обработки трафика в группы правил доступа и группы правил защиты, чтобы задать порядок их проверки.

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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
 2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
 3. Создайте новую группу правил. Для этого в раскрывающемся списке **Добавить группу** выберите один из следующих вариантов:
 - **Группа правил доступа**, если вы хотите создать группу правил доступа.
 - **Группа правил защиты**, если вы хотите создать группу правил защиты.Откроется окно создания группы правил.
 4. В поле **Название** введите название новой группы правил.
 5. 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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
 2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
 3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите изменить группу правил доступа.
 - **Группы защиты**, если вы хотите изменить группу правил защиты.
 4. По кнопке  откройте меню группы правил обработки трафика.
 5. Если вы хотите изменить название группы правил, выполните следующие действия:
 - a. Выберите пункт **Изменить**.
Откроется окно с информацией о группе правил.
 - b. Внесите необходимые изменения.
 - c. Нажмите на кнопку **Сохранить**.
 6. Если вы хотите переместить группу правил выше по списку групп правил, выберите пункт **Вверх**.
 7. Если вы хотите переместить группу правил ниже по списку групп правил, выберите пункт **Вниз**.
- 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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области**.
 - **После правил рабочей области**.
3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите удалить группу правил доступа.
 - **Группы защиты**, если вы хотите удалить группу правил защиты.
4. По кнопке  откройте меню группы правил обработки трафика.

5. Выберите пункт **Удалить**.

Отобразится окно подтверждения удаления группы правил обработки трафика.

6. Нажмите на кнопку **Да**.

Группа правил обработки трафика будет удалена.

Изменение приоритета правила в рамках группы

В рамках группы правила проверяются в порядке расположения в таблице правил обработки трафика сверху вниз. Чем выше правило располагается в таблице правил обработки трафика, тем выше его приоритет. Изменение приоритета правила выполняется с помощью перемещения в таблице правил обработки трафика.

► *Чтобы изменить приоритет правила в рамках группы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:

- для глобальных правил раздел **Правила**;
- для правил рабочих областей раздел **Рабочие области**.

2. Если вы добавили рабочую область, выберите одну из следующих закладок:

- **До правил рабочей области**.
- **После правил рабочей области**.

3. Выберите группу правил обработки трафика из следующих списков:

- **Группы доступа**, если вы хотите настроить отображение таблицы правил доступа.
- **Группы защиты**, если вы хотите настроить отображение таблицы правил защиты.

Откроется таблица правил обработки трафика.

4. Если вы хотите переместить правило обработки трафика выше по списку правил, выполните следующие действия:

- a. Установите флажок рядом с правилом, которое вы хотите переместить.
- b. Нажмите на кнопку **Переместить вверх**.

Правило обработки трафика будет перемещено выше по списку правил.

5. Если вы хотите переместить правило обработки трафика ниже по списку правил, выполните следующие действия:

- a. Установите флажок рядом с правилом, которое вы хотите переместить.
- b. Нажмите на кнопку **Переместить вниз**.

Правило обработки трафика будет перемещено ниже по списку правил.

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 интернет-ресурсам

Если блокировка доступа к интернет-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 интернет-ресурсу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите закладку **Трафик**.
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 интернет-ресурса:
 - a. В левом раскрывающемся списке выберите **URL**.
 - b. В центральном раскрывающемся списке выберите **Равняется**.
 - c. В правом поле введите веб-адрес заблокированного интернет-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 интернет-ресурсу.

Получение статистики о доступе к интернет-ресурсам

В целях мониторинга сетевой активности пользователей вам может потребоваться получить статистику о посещении определенного интернет-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 интернет-ресурсам, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите закладку **Трафик**.
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 глобальных правил обработки трафика отображается в разделе **Правила** для каждой из групп правил обработки трафика на вкладках **До правил рабочей области** и **После правил рабочей области**.

Таблица правил рабочих областей отображается в разделе **Рабочие области** при выборе рабочей области.

В таблице правил обработки трафика содержится следующая информация:

1. **Действие.** Действие, которое выполняет правило обработки трафика.

В правилах доступа возможны следующие действия:

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

В правилах защиты возможны следующие действия:

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

2. **Название.** Название правила обработки трафика.

3. **Статус.** Состояние правила обработки трафика.

Правило обработки трафика может находиться в одном из следующих состояний:

- **Выключено.**
 - **Включено.**
4. **Комментарий.** Комментарий к правилу обработки трафика.

Настройка отображения таблицы правил обработки трафика

► *Чтобы настроить отображение таблицы правил обработки трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите один из следующих разделов:
 - для глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области.**
 - **После правил рабочей области.**
3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите настроить отображение таблицы правил доступа.
 - **Группы защиты**, если вы хотите настроить отображение таблицы правил защиты.
 Откроется таблица правил обработки трафика.
4. По кнопке  откройте меню отображения таблицы правил обработки трафика.
5. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице правил обработки трафика.

Должен быть установлен хотя бы один флажок.

Отображение таблицы правил обработки трафика будет настроено.

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 глобальных правил раздел **Правила**;
 - для правил рабочих областей раздел **Рабочие области**.
2. Если вы добавили рабочую область, выберите одну из следующих закладок:
 - **До правил рабочей области.**
 - **После правил рабочей области.**

3. Выберите группу правил обработки трафика из следующих списков:
 - **Группы доступа**, если вы хотите просмотреть информацию о правиле доступа.
 - **Группы защиты**, если вы хотите просмотреть информацию о правиле защиты.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.
На закладке **Общие параметры** отображаются следующие параметры:
 - a. **Статус** – статус правила обработки трафика.
 - b. **Действие** – действие, которое выполняет правило обработки трафика.
 - c. **Название правила** – название правила обработки трафика.
 - d. **Комментарий** – комментарий к правилу обработки трафика.
2. **Исключения.** Исключение для правила обработки трафика.
На закладке **Исключения** отображаются блоки параметров **Исключение**. В каждом блоке **Исключение** отображаются следующие параметры:
 - a. **Инициатор** – инициатор соединения.
 - b. **Фильтрация трафика** – фильтр трафика.
3. **Расписание.** Расписание работы правила обработки трафика.
На закладке **Расписание** отображается дата отключения правила, а также дни недели и периоды работы правила.

Управление рабочими областями

Вы можете создавать рабочие области, чтобы использовать локальные правила обработки трафика (см. раздел «Работа с правилами обработки трафика» на стр. 70) для каждой рабочей области, например, для подразделений организаций или управляемых организаций (для интернет-провайдеров).

В этом разделе

Просмотр таблицы рабочих областей	90
Просмотр информации о рабочей области	90
Настройка отображения таблицы рабочих областей	91
Добавление рабочей области.....	91
Изменение параметров рабочей области	92
Удаление рабочей области.....	92

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:

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

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 (необязательно)** 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:
 - **Группа пользователей.**
 - **DN пользователя.**
 - **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**.
2. В строке с рабочей областью, параметры которой вы хотите изменить, нажмите на кнопку **Просмотреть**.

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**.
2. В строке с рабочей областью, которую вы хотите удалить, нажмите на кнопку **Просмотреть**.

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.

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 на закладке **Роли**.

Каждой учетной записи пользователя вы можете назначить несколько ролей. Таблица учетных записей пользователей отображается в разделе **Пользователи** окна веб-интерфейса программы на закладке **Учетные записи**.

Для каждой роли вы можете задать набор прав, которыми будет обладать роль. Например, вы можете создать роль *Администратор* с полным набором прав и роль *Специалист Технической поддержки*, обладающую правами только на просмотр информации в веб-интерфейсе программы.

В этом разделе

Настройка отображения таблицы ролей пользователей	93
Добавление роли	94
Изменение параметров роли	96
Удаление роли	96
Добавление учетной записи.....	97
Назначение роли.....	97
Изменение пароля учетной записи Administrator	97

Настройка отображения таблицы ролей пользователей

- ▶ *Чтобы настроить отображение таблицы ролей пользователей, выполните следующие действия:*
 1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Учетные записи**.
Откроется список учетных записей и таблица ролей пользователей.
 2. По кнопке  откройте меню отображения таблицы ролей пользователей.
 3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице ролей пользователей.

Должен быть установлен хотя бы один флажок.

Отображение таблицы ролей пользователей будет настроено.

Добавление роли

► Чтобы добавить роль, выполните следующие действия:

1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Роли**.
2. Нажмите на кнопку **Добавить роль**.
Откроется окно добавления роли.
3. В поле **Имя** введите имя роли.
4. В списке **Разрешения** установите флажки рядом с теми правами, которыми должна обладать роль:

- **Создавать/изменять/удалять серверы.**

Это право позволяет пользователю добавлять (см. раздел «Добавление сервера» на стр. [65](#)) и удалять серверы (см. раздел «Удаление сервера» на стр. [66](#)), а также изменять их параметры (см. раздел «Изменение параметров сервера» на стр. [65](#)) в разделе **Серверы**.

При назначении этого права пользователь сможет также просматривать информацию о серверах.

- **Просматривать журналы трассировки.**

Это право позволяет пользователю просматривать журналы трассировки (см. раздел «Просмотр журналов трассировки» на стр. [128](#)) управляемых серверов.

При назначении этого права пользователь сможет также просматривать информацию о серверах, добавлять и удалять серверы, а также изменять их параметры.

- **Проверять целостность данных.**

Это право позволяет пользователю проверять целостность данных (см. раздел «Проверка целостности данных» на стр. [67](#)) на управляемых серверах.

При назначении этого права пользователь сможет также просматривать информацию о серверах, добавлять и удалять серверы, а также изменять их параметры.

- **Просматривать информацию о серверах.**

Это право позволяет пользователю только просматривать информацию о серверах (см. раздел «Просмотр информации о сервере» на стр. [62](#)) в разделе **Серверы**. Пользователь не сможет добавлять и удалять серверы, а также изменять их параметры.

- **Создавать/изменять рабочие области.**

Это право позволяет пользователю добавлять рабочие области (см. раздел «Добавление рабочей области» на стр. [91](#)) и изменять параметры рабочих областей (см. раздел «Изменение параметров рабочей области» на стр. [92](#)) в разделе **Рабочие области**.

При назначении этого права пользователь сможет также просматривать информацию о рабочих областях.

- **Просматривать рабочие области.**

Это право позволяет пользователю только просматривать таблицу рабочих областей (см. раздел «Просмотр таблицы рабочих областей» на стр. [90](#)) в разделе **Рабочие области**. Пользователь не сможет добавлять и удалять рабочие области, а также изменять их параметры.

- **Удалять рабочие области.**

Это право позволяет пользователю удалять рабочие области в разделе **Рабочие области**.

При назначении этого права пользователь сможет также просматривать информацию о рабочих областях.

- **Создавать/изменять глобальные роли.**

Это право позволяет пользователю добавлять роли и изменять их параметры (см. раздел «Изменение параметров роли» на стр. [96](#)) в разделе **Пользователи**.

При назначении этого права пользователь сможет также просматривать список ролей.

- **Просматривать глобальные роли.**

Это право позволяет пользователю только просматривать список ролей в разделе **Пользователи**. Пользователь не сможет добавлять или удалять роли, а также изменять их параметры.

- **Удалять глобальные роли.**

Это право позволяет пользователю удалять роли (см. раздел «Удаление роли» на стр. [96](#)) в разделе **Пользователи**.

При назначении этого права пользователь сможет также просматривать список ролей.

- **Создавать/изменять глобальные правила.**

Это право позволяет пользователю добавлять правила доступа (см. раздел «Добавление правила доступа» на стр. [73](#)) и правила защиты (см. раздел «Добавление правила защиты» на стр. [74](#)), а также изменять их параметры (см. раздел «Изменение правила обработки трафика» на стр. [80](#)) в разделах **Правила** и **Рабочие области**.

При назначении этого права пользователь сможет также просматривать все правила обработки трафика.

- **Просматривать глобальные правила.**

Это право позволяет пользователю только просматривать таблицу правил обработки трафика (см. раздел «Просмотр таблицы правил обработки трафика» на стр. [87](#)) в разделах **Правила** и **Рабочие области**. Пользователь не сможет добавлять или удалять правила, а также изменять их параметры.

- **Удалять глобальные правила.**

Это право позволяет пользователю удалять правила обработки трафика (см. раздел «Удаление правила обработки трафика» на стр. [81](#)) в разделах **Правила** и **Рабочие области**.

При назначении этого права пользователь сможет также просматривать все правила обработки трафика.

- **Просматривать глобальные события.**

Это право позволяет пользователю просматривать журнал событий (см. раздел «Просмотр журнала событий» на стр. [116](#)) программы в разделе **События**.

- **Экспортировать глобальные события.**

Это право позволяет пользователю сохранять файл с экспортированными событиями (см. раздел «Экспорт событий» на стр. [117](#)) на жестком диске компьютера.

При назначении этого права пользователь сможет также просматривать журнал событий программы.

- **Просматривать раздел Мониторинг.**

Это право позволяет пользователю просматривать информацию в разделе **Мониторинг** (см. раздел **«Мониторинг работы программы»** на стр. [58](#)).

- **Изменять параметры.**

Это право позволяет пользователю изменять параметры программы в разделе **Параметры**.

При назначении этого права пользователь сможет также просматривать параметры программы.

- **Просматривать параметры.**

При назначении этого права пользователь сможет только просматривать параметры программы в разделе **Параметры**, но не сможет изменять их.

5. Нажмите на кнопку **Добавить**.

Роль будет добавлена.

Изменение параметров роли

Вы можете изменить название роли, а также состав прав, которыми она обладает.

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

1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Роли**.
2. В блоке параметров **Роли** выберите роль, параметры которой вы хотите изменить, и нажмите на кнопку **Разрешения**.
Откроется окно **Просмотреть роль**.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.
Откроется окно **Изменить роль**.
4. Если требуется, измените название роли в поле **Имя**.
5. Если требуется, изменить состав прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Разрешения**.
6. Нажмите на кнопку **Сохранить**.

Параметры роли будут изменены.

Удаление роли

► *Чтобы удалить роль, выполните следующие действия:*

1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Роли**.
2. В списке **Роли** выберите роль, которую вы хотите удалить.
3. Нажмите на кнопку **Разрешения**.
Откроется окно с информацией о роли.
4. Нажмите на кнопку **Удалить**.

Отобразится окно подтверждения удаления роли.

5. Нажмите на кнопку **Да**.

Роль будет удалена.

Добавление учетной записи

► Чтобы добавить учетную запись, выполните следующие действия:

1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Учетные записи**.
2. Нажмите на кнопку **Добавить учетную запись**.
Откроется окно добавления учетной записи.
3. В поле **Учетная запись (домен/имя для NTLM или user@REALM для Kerberos)** введите имя учетной записи.
4. В списке ролей установите флажки рядом с теми ролями, которыми должна обладать учетная запись.
5. Нажмите на кнопку **Добавить**.

Учетная запись будет добавлена.

Назначение роли

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

1. В окне веб-интерфейса программы в разделе **Пользователи** выберите закладку **Роли**.
2. В списке **Роли** выберите роль, которую вы хотите назначить для учетной записи.
3. Нажмите на кнопку **Назначить роль**.
Откроется окно **Назначить роль**.
4. В поле **Учетная запись (домен/имя для NTLM или user@REALM для Kerberos)** введите имя учетной записи, которой вы хотите назначить роль.
5. Нажмите на кнопку **Сохранить**.

Роль будет назначена выбранной учетной записи.

Изменение пароля учетной записи Administrator

Учетная запись Administrator с правами суперпользователя позволяет входить в систему без использования внешних служб и доменов аутентификации. Пароль данной учетной записи действует в течение одного года. После этого администратору требуется сменить пароль.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Administrator с правами суперпользователя**.

2. В поле **Старый пароль** введите пароль учетной записи Administrator, указанный 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**.

Защита сетевого трафика

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

- Проверяет сетевой трафик на вирусы, фишинг, некоторые легальные программы (на стр. 99), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу.
- Лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

В этом разделе

Настройка параметров защиты сетевого трафика	101
Настройка обработки архивов	102
Установка значений параметров защиты по умолчанию	102

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 получают доступ к таким программам или внедряют 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 4. 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).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры злоумышленники.

Тип	Название	Описание
RemoteAdmin	Программы удаленного администрирования	<p>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.</p> <p>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.</p>
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.
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 защиты сетевого трафика

► Чтобы настроить параметры защиты сетевого трафика, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Защита**.
2. В блоке параметров **Антивирус** выполните следующие действия:
 - Включите переключатель рядом с названием параметра **Использовать эвристический анализ**, если вы хотите использовать эвристический анализ при антивирусной проверке сетевого трафика.
 - Отключите переключатель рядом с названием параметра **Использовать эвристический анализ**, если вы не хотите использовать эвристический анализ при антивирусной проверке сетевого трафика.
3. Если вы включили использование эвристического анализа, в списке **Уровень эвристического анализа** выберите один из следующих уровней эвристического анализа:
 - **Поверхностный**, если вы хотите использовать максимально быстрый эвристический анализ проверяемых объектов.
 - **Средний**, если вы хотите использовать эвристический анализ проверяемых объектов средней скорости и глубины.
 - **Глубокий**, если вы хотите использовать максимально глубокий эвристический анализ проверяемых объектов.По умолчанию выбран уровень эвристического анализа **Средний**.
4. Для параметра **Включить обнаружение некоторых легальных программ** выполните одно из следующих действий:
 - Установите флажок **Включить обнаружение некоторых легальных программ**, если вы считаете, что такие программы при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации.
 - Снимите флажок **Включить обнаружение некоторых легальных программ**, если вы не считаете, что такие программы при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации.

К таким легальным программам относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями. В случае обнаружения таких программ, они будут обработаны согласно правилам для зараженных объектов.

5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности антивирусной проверки объектов сетевого трафика в секундах.
6. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности проверяемых архивов.
7. В блоке параметров **Анти-Фишинг** выполните следующие действия:
 - Включите переключатель рядом с названием параметра **Использовать эвристический анализ**, если вы хотите использовать эвристический анализ при проверке сетевого трафика на фишинг.

- Отключите переключатель рядом с названием параметра **Использовать эвристический анализ**, если вы не хотите использовать эвристический анализ при проверке сетевого трафика на фишинг.
8. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности проверки объектов сетевого трафика на фишинг в секундах.
 9. Нажмите на кнопку **Сохранить**.
- Значения параметров защиты сетевого трафика будут сохранены.

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/kwts-workertmp`. 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 Обрабатывающем сервере.
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.

Установка значений параметров защиты по умолчанию

► *Чтобы установить значения параметров защиты сетевого трафика по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Защита**.
2. В нижней части окна **Параметры** перейдите по ссылке **Установить значения по умолчанию**.
3. Нажмите на кнопку **Сохранить**.

Параметры защиты сетевого трафика примут значения по умолчанию.

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.

В этом разделе

Настройка участия в Kaspersky Security Network	104
Настройка использования Kaspersky Private Security Network	105

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 **Внешние службы**.
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**, подраздел **Внешние службы**.
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.
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.

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. [70](#));
- создавать учетные записи пользователей (см. раздел «Работа с ролями и учетными записями пользователей» на стр. [93](#)) для работы с Kaspersky Web Traffic Security.

В этом разделе

Добавление соединения с LDAP-сервером.....	106
Удаление соединения с LDAP-сервером.....	107
Изменение параметров соединения с LDAP-сервером	107

Добавление соединения с LDAP-сервером

Вы можете добавить соединение с одним или несколькими LDAP-серверами.

► *Чтобы добавить соединение с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **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**, подраздел **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**, подраздел **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.
Откроется окно **Просмотреть параметры соединения**.
3. Если требуется, измените следующие параметры:
 - Имя LDAP-сервера, которое отображается в веб-интерфейсе программы, в поле **Имя**.
 - Keytab-файл, нажав на кнопку **Изменить**.
 - Каталог, начиная с которого программа осуществляет поиск записей, в поле **База поиска**.
4. Нажмите на кнопку **Сохранить**.
Параметры соединения с LDAP-сервером будут изменены.

Параметры ICAP-сервера

Чтобы выполнять проверку трафика, а также регулировать доступ пользователей вашей сети к интернет-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	108
Настройка параметров обработки трафика на ICAP-сервере	109

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 подключение к ICAP-серверу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **ICAP-сервер**.
2. В списке **Адрес ICAP-сервера** выберите одно из следующих значений:
 - 127.0.0.1 (адрес IPv4), если прокси-сервер и Обрабатывающий сервер установлены на одном хосте. Kaspersky Web Traffic Security будет обрабатывать трафик только с текущего хоста.
 - 0.0.0.0 (адрес IPv4), если вы используете отдельный прокси-сервер. Kaspersky Web Traffic Security будет обрабатывать трафик с любых хостов.
 - ::1 (адрес IPv6, аналог адреса 127.0.0.1), если прокси-сервер и Обрабатывающий сервер

установлены на одном хосте. Kaspersky Web Traffic Security будет обрабатывать трафик только с текущего хоста.

- :: (адрес IPv6, аналог адреса 0.0.0.0), если вы используете отдельный прокси-сервер. Kaspersky Web Traffic Security будет обрабатывать трафик с любых хостов.

3. Введите порт подключения к ICAP-серверу.
4. В поле **Максимальное количество соединений по 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 Обрабатывающих серверах.

- *Чтобы настроить параметры обработки трафика на ICAP-сервере, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **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, установите флажок **Начинать**

передачу HTTP-сообщений до окончания их проверки.

Если этот параметр включен, а проверка объекта не успела завершиться до истечения времени ожидания, 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.

8. Если вы хотите обрабатывать HTTP-сообщения с методом CONNECT, снимите флажок **Не использовать HTTP-метод CONNECT при проверке**.

Рекомендуется снять этот флажок, если вы не настроили SSL Bumping на вашем прокси-сервере (см. раздел «Настройка SSL Bumping в сервисе Squid» на стр. [147](#)).

9. Нажмите на кнопку **Сохранить**.

Параметры обработки трафика на ICAP-сервере будут настроены.

Работа с программой по протоколу SNMP

SNMP (Simple Network Management Protocol – простой протокол сетевого управления) – протокол управления сетевыми устройствами.

В Kaspersky Web Traffic Security протокол SNMP используется следующим образом:

1. *SNMP-агент* – программный модуль сетевого управления Kaspersky Web Traffic Security, который отслеживает информацию о работе Kaspersky Web Traffic Security.
2. Kaspersky Web Traffic Security может отправлять эту информацию в виде *SNMP-ловушек* – уведомлений о событиях работы программы.

По протоколу SNMP вы можете получить доступ к следующей информации о Kaspersky Web Traffic Security:

- общим сведениям;
- статистике работы Kaspersky Web Traffic Security с момента установки программы;
- данным о событиях, возникающих в ходе работы Kaspersky Web Traffic Security.

Например, Kaspersky Web Traffic Security отправляет SNMP-ловушки в следующих случаях:

- Лицензия обновлена.
SNMP-ловушка содержит номер лицензии, тип лицензии, доступную функциональность, дату окончания срока действия лицензии.
- Льготный период действия лицензии.
SNMP-ловушка содержит номер лицензии и количество дней до истечения льготного периода.
SNMP-ловушка отправляется в начале действия льготного периода, далее один раз в сутки и при перезагрузке Kaspersky Web Traffic Security.

Доступ предоставляется только на чтение информации.

В этом разделе

Включение и отключение использования SNMP в программе	112
Настройка параметров подключения к SNMP-серверу	112
Настройка шифрования SNMP-соединений.....	113
Включение и отключение отправки SNMP-ловушек.....	114

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**, подраздел **Соединение с SNMP-сервером**.
 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**, подраздел **Соединение с SNMP-сервером**.
 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.

► 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. Запустите службу snmpd. Для этого выполните команду:

```
service snmpd start
```

- e. 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 отpravку SNMP-ловушек событий, возникающих в ходе работы программы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Соединение с SNMP-сервером**.

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.

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 Обрабатывающем сервере. Файлы журнала событий автоматически ротируются по достижении максимально разрешенного размера файлов или по истечении максимального срока их хранения.

Вы можете настроить запись событий в журнал операционной системы по протоколу Syslog для последующего импорта событий в стороннюю SIEM-систему.

Программа распределяет события по следующим уровням:

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

В этом разделе

Просмотр журнала событий.....	116
Экспорт событий.....	117
Настройка отображения таблицы событий.....	118
Настройка параметров журнала событий.....	118
Настройка параметров Syslog.....	119

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.**
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. [116](#)) 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.

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.

Настройка параметров журнала событий

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

Параметры журнала событий не влияют на параметры записи событий по протоколу Syslog (см. раздел «Настройка параметров Syslog» на стр. [119](#)).

► 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 Запретить/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 **Период записи событий в журнал (сут.)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на Обрабатывающем сервере.

3. 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.

Настройка параметров Syslog

Для удаленной записи событий по протоколу Syslog по сети рекомендуется использовать протокол TCP. Сетевые порты, используемые сервером Syslog, должны быть открыты.

При настройке параметров Kaspersky Web Traffic Security рекомендуется учитывать параметры Syslog, установленные на сервере.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Syslog**.
2. В раскрывающемся списке **Категория журнала** выберите категорию системного журнала, в который будет записываться информация о событиях.
3. В раскрывающемся списке **Уровень события** выберите уровень важности событий, которые будут записываться по протоколу Syslog.

Запись событий по протоколу Syslog будет настроена.

Экспорт и импорт параметров

Вы можете экспортировать параметры Kaspersky Web Traffic Security для их последующего импорта. Эта функциональность может быть использована для резервного копирования параметров программы. Если Управляющий сервер выйдет из строя, вы сможете перенести ранее экспортированные параметры после повторной установки программы.

Вы также можете использовать экспорт и импорт параметров для создания одинаковой конфигурации программы на разных серверах (например, для быстрого развертывания Kaspersky Web Traffic Security на новом сервере).

При экспорте параметров создается конфигурационный файл со следующей информацией:

- Глобальные параметры программы:
 - правила защиты и доступа, не относящиеся к рабочим областям;
 - роли и права пользователей;
 - учетные записи пользователей, имеющих глобальные роли;
 - шаблоны страниц запрета доступа;
 - параметры защиты.
- Параметры рабочих областей:
 - критерии принадлежности трафика к рабочей области;
 - правила защиты и доступа, созданные в рамках рабочей области;
 - роли пользователей, относящиеся ко всем рабочим областям.

При импорте конфигурационного файла вы можете выбрать, какие из указанных параметров должны быть применены. Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров Kaspersky Web Traffic Security.....	120
Импорт параметров Kaspersky Web Traffic Security.....	121
Настройка хранения экспортированных файлов	121

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**, подраздел **Параметры конфигурации**.
2. 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.

3. Нажмите на значок  в нужной строке.

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.

Версии программы и импортируемых параметров должны совпадать.

- ▶ *Чтобы импортировать параметры Kaspersky Web Traffic Security, выполните следующие действия:*
 1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Параметры конфигурации**.
 2. Нажмите на кнопку **Импортировать**.
Откроется окно **Импортировать конфигурацию**.
 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**, подраздел **Параметры конфигурации**.
 2. В поле **Ограничить число экспортированных конфигурационных файлов до** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.
Количество экспортированных файлов будет ограничено заданным значением.

Настройка шаблона запрета доступа

Если по результатам проверки интернет-ресурса по правилам обработки трафика доступ запрещен, пользователю отображается страница запрета доступа. Вы можете изменить текст шаблона этой страницы.

► *Чтобы настроить шаблон запрета доступа, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Шаблоны страниц запрета доступа**.
2. Если требуется, измените текст шаблона в поле **Макрос %ТЕХТ%**.
3. Если требуется, измените разметку страницы в поле **HTML-код**.
4. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
5. Нажмите на кнопку **Сохранить**.

Шаблон запрета доступа будет настроен.

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.
- На форуме «Лаборатории Касперского» (<https://forum.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. [125](#)).

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки	125
Техническая поддержка по телефону	125
Техническая поддержка через Kaspersky CompanyAccount	126
Получение информации для Службы технической поддержки	127

Способы получения технической поддержки

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

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/b2c>) ;
- 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/b2c>).

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).

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).

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.

В этом разделе

Запуск трассировки.....	127
Изменение уровня трассировки.....	128
Просмотр журналов трассировки	128
Сохранение файла трассировки на компьютере	128

Запуск трассировки

► Чтобы запустить трассировку, выполните следующие действия:

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



2. По кнопке  откройте меню раздела **Серверы**.

3. Выберите пункт **Запустить трассировку**.

Откроется окно **Выбор серверов 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 **Серверы**.

2. По кнопке  откройте меню раздела **Серверы**.

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**.

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 **Серверы**.

2. По кнопке  откройте меню раздела **Серверы**.

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 **Серверы**.

2. По кнопке  откройте меню раздела **Серверы**.
 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.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

Приложение. MIME-типы объектов	130
Значения параметров программы в сертифицированном режиме	131
Настройка интеграции сервиса Squid с Active Directory	132
Настройка балансировки ICAP с помощью HAProxy	144
Установка и настройка сервиса Squid	146

Приложение. 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.

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 5. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Название параметра	Значение параметра в сертифицированном режиме работы программы
Внешние службы	Использование KSN / KPSN	<ul style="list-style-type: none"> • Не использовать KSN/KPSN • KPSN
Защита: Антивирус	Использовать эвристический анализ	Включено
	Включить обнаружение некоторых легальных программ	Включено
	Максимальная длительность проверки (сек.)	120
	Максимальная глубина проверки архивов	32
Защита: Анти-Фишинг	Использовать эвристический анализ	Включено
	Максимальная длительность проверки (сек.)	120

Настройка интеграции сервиса Squid с Active Directory

Чтобы иметь возможность управлять доступом пользователей к сетевым и веб-ресурсам на основе доменных политик безопасности, необходимо настроить интеграцию сервиса Squid с Active Directory. Это позволит использовать единую точку входа (SSO, Single Sign-On) для аутентификации пользователей.

Вы можете использовать следующие механизмы аутентификации:

- Kerberos-аутентификация.
- NTLM-аутентификация.
- Basic-аутентификация.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм проверки подлинности является самым надежным. При NTLM- и Basic-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

В этом разделе

Настройка Kerberos-аутентификации	132
Настройка NTLM-аутентификации	137
Настройка Basic-аутентификации	142

Настройка Kerberos-аутентификации

Выполняйте действия по настройке Kerberos-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись должна обладать правами суперпользователя.

В этом разделе

Установка пакета Kerberos	132
Настройка синхронизации времени	133
Настройка DNS	134
Создание keytab-файла для сервиса Squid	135
Настройка клиентской части Kerberos	135

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 команду:
`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 команду:
`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 с Управляющим сервером и NTP-серверами 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 подключена правильно. 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>
```

Имя сервера с сервисом Squid должно совпадать с именем этого сервера на DNS-сервере.

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 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.

6. 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> /mapuser <LDAP-пользователь сервиса Squid>@<realm Active Directory> /crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> /ptype KRB5_NT_PRINCIPAL /pass <пароль LDAP-пользователя сервиса Squid> /out C:\squid.keytab
```

Keytab-файл для сервиса Squid будет создан.

Настройка клиентской части Kerberos

► 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 squidCA.pem
```

- Ubuntu или Debian:

```
chown proxy:proxy squidCA.pem
```

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>
```

```
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>
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>
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>

```

- **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.....	137
Настройка синхронизации времени	137
Настройка DNS.....	138
Настройка Samba на сервере с сервисом Squid	139
Проверка параметров Samba на сервере с сервисом Squid	141
Настройка сервиса Squid	141
Настройка клиентской части NTLM-аутентификации	141
Настройка NTLM-аутентификации хоста, не входящего в домен	142

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
```

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 команду:

```
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 команду:

```
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 с Управляющим сервером и NTP-серверами 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.

- 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.

- Укажите имя сервера с сервисом Squid. Для этого выполните команду:

```
hostnamectl set-hostname <имя сервера с сервисом Squid>
```

- 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.

- Убедитесь, что имя сервера с сервисом Squid совпадает с именем этого сервера на DNS-сервере Active Directory.
- 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.

- 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.

Настройка Samba на сервере с сервисом Squid

► Чтобы настроить сервис Samba, выполните следующие действия:

- 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 домена Active Directory>
```

```
realm = <realm Active Directory>
```

```
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 проху в группу winbindd_priv. Для этого выполните команду:

```
usermod -a -G winbindd_priv proxy
```

Настройка NTLM-авторизации будет завершена. Перейдите к проверке работы NTLM-авторизации.

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 Suid 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
```

- 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.

- 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.

- Введите `^]` и нажмите на клавишу **ENTER**.
- 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.

- 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,

на компьютерах локальной сети организации в параметрах браузера укажите FQDN-адрес сервера с сервисом Squid в качестве прокси-сервера.

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:

- 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.

Настройка балансировки ICAP с помощью HAProxy

Балансировка ICAP с помощью балансировщика нагрузки HAProxy позволяет подключить один сервис Squid одновременно к нескольким обрабатывающим серверам 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	144
Установка и настройка HAProxy	144
Настройка сервиса Squid для работы HAProxy.....	146

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 в дереве консоли управления выберите раздел **Параметры**, подраздел **ICAP-сервер**.
2. В поле **Адрес ICAP-сервера** измените значение с `localhost` на `0.0.0.0`.
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 обрабатывающим сервером, так как HAProxy и Обрабатывающий сервер 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 на Обрабатывающем сервере. Для этого на сервере с обрабатывающим сервером 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=«3128 9046 705 1344»`.

2. 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
```

3. 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 Обрабатывающего сервера>:<порт ICAP-сервера> check
    server <имя ICAP-сервера 2> <IP-адрес Обрабатывающего сервера>:<порт ICAP-сервера> check
    server <имя ICAP-сервера 3> <IP-адрес Обрабатывающего сервера>:<порт ICAP-сервера> check
```

4. 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.

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 установить сервис Squid на один или несколько Обрабатывающих серверов, если вы не хотите использовать отдельный прокси-сервер.

В этом разделе

Установка сервиса Squid	146
Настройка сервиса Squid	147
Настройка SSL Bumping в сервисе Squid	147

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-crt` 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_crt -c -s /var/lib/squid/ssl_db
```

```
chown -R squid:squid /var/lib/squid
```

- Ubuntu:

```
mkdir -p /var/lib/squid
```

```
/usr/lib/squid/ssl_crt -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_crt -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_crted -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_crted -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_crted -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_crted -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_crted -s /var/lib/squid/ssl_db -M 4MB
```

```
sslcrtd_children 5
```

```
ssl_bump server-first all
```

```
sslproxy_cert_error deny all
```

с. 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.

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.

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.

S

SELinux (Security-Enhanced Linux)

Система контроля доступа процессов к ресурсам операционной системы, основанная на применении политик безопасности.

SNMP-агент

Программный модуль сетевого управления Kaspersky Web Traffic Security, отслеживает информацию о работе Kaspersky Web Traffic Security.

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.

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.

T

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Б

Базовая аутентификация

Способ 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.

О

Обрабатывающий сервер

Компонент программы, который проверяет сетевой трафик пользователей согласно правилам обработки трафика. Обрабатывающий сервер получает заданные администратором параметры от Управляющего сервера.

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 интернет-ресурсам и направлению трафика.

Правило защиты

Список проверок трафика на вирусы, фишинг, некоторые легальные программы (на стр. [99](#)), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, проводимых при выполнении заданных условий.

Правило обработки трафика

Набор действий, которые программа выполняет над интернет-ресурсом, удовлетворяющим заданным

условиям.

Р

Резервный управляющий сервер

Компонент программы, на котором хранится копия параметров, заданных на Управляющем сервере. Необходим для отказоустойчивой работы программы.

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 графиков.

Т

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

Управляющий сервер

Компонент программы, который позволяет администратору управлять параметрами программы через

веб-интерфейс. Управляющий сервер следит за состоянием обрабатывающих серверов, передает им заданные параметры и установленные ключи.

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.

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/>

Вирусная лаборатория:

<https://virusdesk.kaspersky.ru/> (для проверки подозрительных файлов и сайтов)

Веб-форум «Лаборатории Касперского»:

<https://forum.kaspersky.com>

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Google Chrome – товарный знак Google, Inc.

Intel и Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Microsoft, Windows, Active Directory 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.

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.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.