

kaspersky

Программное изделие «Kaspersky Web Traffic Security 6.1»

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.1

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: 20.05.2020

Обозначение документа:
643.46856491.00047-05 90 02

© АО "Лаборатория Касперского", 2020.

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

Содержание

Об этом документе.....	10
Источники информации о программе.....	11
Kaspersky Web Traffic Security	13
О действиях программы над объектами	13
О задачах программы	14
Основные компоненты программы	15
Принцип работы программы_cert_appliance	16
Об информационных X-заголовках	17
Требования	18
Аппаратные и программные требования	18
Указания по эксплуатации и требования к среде.....	19
Лицензирование программы.....	21
О Лицензионном соглашении	21
О лицензии	21
О лицензионном сертификате	22
О ключе	22
О коде активации	23
О предоставлении данных.....	23
Просмотр информации о лицензии и активации программы.....	36
Активация программы.....	36
Удаление лицензионного ключа	37
Установка и первоначальная настройка программы	38
Развертывание виртуальной машины в консоли управления гипервизора VMware ESXi.....	39
Загрузка iso-файла.....	39
Создание виртуальной машины в консоли управления гипервизора VMware ESXi	40
Подключение к виртуальной машине	42
Развертывание виртуальной машины в веб-интерфейсе VMware vSphere.....	42
Загрузка iso-файла.....	42
Создание виртуальной машины в веб-интерфейсе VMware vSphere	43
Подключение к виртуальной машине	45
Развертывание виртуальной машины в консоли управления гипервизора Microsoft Hyper-V Manager.....	45
Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager	46
Изменение количества процессоров виртуальной машины	48
Подключение к виртуальной машине	48
Развертывание виртуальной машины с помощью программы Microsoft SCVMM.....	49
Загрузка iso-файла.....	49
Создание виртуальной машины с помощью программы Microsoft SCVMM	50
Подключение к виртуальной машине	52

Установка программы	53
Подготовка и первоначальная настройка операционной системы	53
Установка сервиса nginx	54
Установка сервиса Squid	54
Установка дополнительных пакетов	55
Установка пакетов программы	55
Первоначальная настройка программы	56
Удаление программы, развернутой из ISO-файла	58
Подготовка к удалению программы	58
Удаление программы с физического сервера	58
Удаление виртуальной машины в консоли управления гипервизора VMware ESXi	60
Удаление виртуальной машины в веб-интерфейсе VMware vSphere	60
Удаление виртуальной машины в консоли управления гипервизора Microsoft Hyper-V	60
Удаление виртуальной машины с помощью Microsoft SCVMM	61
Создание учетных записей пользователей	62
Процедура приемки	63
Безопасное состояние	63
Проверка работоспособности. Тестовый файл EICAR	63
Интерфейс Kaspersky Web Traffic Security	65
Начало работы с программой	66
Настройка сетевых доступов	66
Подключение к веб-интерфейсу программы	69
Проверка работы Kaspersky Web Traffic Security в веб-интерфейсе	69
Мониторинг работы программы	71
Создание новой схемы расположения графиков	72
Изменение схемы расположения графиков	73
Удаление схемы расположения графиков	73
Выбор схемы расположения графиков из списка	74
Выбор схемы расположения графиков, отображаемой по умолчанию	74
Фильтрация данных мониторинга	74
Отчеты	76
Создание отчета	76
Удаление отчета	77
Скачивание отчета на компьютер	77
Просмотр содержимого отчета	77
Журнал событий Kaspersky Web Traffic Security	79
Просмотр журнала событий	79
Экспорт событий	80
Настройка отображения таблицы событий	81
Фильтрация системных событий	81

Настройка параметров журнала событий	82
Работа с правилами обработки трафика	84
Сценарий настройки доступа к веб-ресурсам	85
Добавление правила обхода	87
Добавление правила доступа	88
Добавление правила защиты	90
Настройка инициатора срабатывания правила	91
Настройка фильтрации трафика	92
Добавление исключения для правила обработки трафика	95
Настройка расписания работы правила обработки трафика	97
Изменение правила обработки трафика	97
Удаление правила обработки трафика	98
Создание копии правила обработки трафика	99
Включение и отключение правила обработки трафика	99
Изменение порядка применения правил	100
Работа с группами правил обработки трафика	101
Создание группы правил обработки трафика	101
Изменение группы правил обработки трафика	102
Удаление группы правил обработки трафика	103
Настройка политики защиты по умолчанию	103
Мониторинг работы правил обработки трафика	104
Обработка запросов пользователей о доступе к веб-ресурсам	104
Получение статистики о доступе к веб-ресурсам	105
Просмотр таблицы правил обработки трафика	106
Просмотр информации о правиле обработки трафика	107
Управление рабочими областями	108
Сценарий настройки рабочей области	108
Просмотр таблицы рабочих областей	109
Просмотр информации о рабочей области	109
Настройка отображения таблицы рабочих областей	109
Добавление рабочей области	110
Изменение параметров рабочей области	111
Удаление рабочей области	111
Переключение между рабочими областями в веб-интерфейсе программы	112
Работа с ролями и учетными записями пользователей	114
Ролевое разграничение доступа к функциям программы	114
Набор прав для ролей по умолчанию	123
Добавление роли	125
Просмотр информации о роли	125
Изменение параметров роли	126

Удаление роли	127
Назначение роли	127
Отзыв роли	128
Изменение пароля учетной записи Administrator	128
Управление кластером	130
Создание нового кластера	130
Настройка отображения таблицы узлов кластера	131
Просмотр информации об узле кластера	131
Добавление узла в кластер	133
Изменение параметров узла	134
Удаление узла из кластера	134
Изменение роли узла в кластере	135
Удаление кластера	136
Проверка целостности данных	136
Подключение к узлам кластера по протоколу SSH	137
Перезагрузка узла кластера	137
Работа программы в аварийном режиме	139
Защита сетевого трафика	141
О защите трафика от некоторых легальных программ	141
Настройка параметров модуля Антивирус	143
Настройка параметров модуля Анти-Фишинг	144
Настройка обработки архивов	145
Параметры ICAP-сервера	146
Настройка параметров подключения к ICAP-серверу	146
Настройка параметров обработки трафика на ICAP-сервере	147
Страница блокировки	149
Список поддерживаемых макросов	149
Настройка страницы блокировки по умолчанию	151
Настройка страницы блокировки для рабочей области	151
Настройка страницы блокировки для правила обработки трафика	152
Экспорт и импорт параметров	154
Экспорт параметров Kaspersky Web Traffic Security	155
Импорт параметров Kaspersky Web Traffic Security	155
Настройка хранения экспортированных файлов	156
Обновление программы	157
Настройка времени сервера	158
Настройка параметров соединения с прокси-сервером	159
Обновление баз Kaspersky Web Traffic Security	160
Выбор источника обновлений баз	160
Настройка расписания и параметров обновления баз	161

Запуск обновления баз вручную	162
Использование внешних служб "Лаборатории Касперского"	163
Настройка участия в Kaspersky Security Network	164
Настройка использования Kaspersky Private Security Network	165
Соединение с LDAP-сервером	166
Добавление соединения с LDAP-сервером	166
Удаление соединения с LDAP-сервером	167
Изменение параметров соединения с LDAP-сервером	167
Запуск синхронизации с контроллером домена Active Directory вручную	168
Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform	169
Сценарий настройки интеграции с программой KATA	171
Добавление сервера KATA	171
Изменение сервера KATA	172
Удаление сервера KATA	172
Выбор режима интеграции	173
Пересоздание сертификата KWTS	173
Настройка параметров кеша KATA	174
Мониторинг интеграции KATA	174
Настройка отправки HTML-файлов в KATA	176
Журнал событий Syslog	178
Настройка параметров Syslog	178
Содержание syslog-сообщений о событиях обработки трафика	179
Содержание syslog-сообщений о системных событиях программы	187
Содержание syslog-сообщений о событиях отправки файлов на сервер KATA	190
Работа с программой по протоколу SNMP	193
Настройка службы snmpd в операционной системе	193
Включение и отключение использования SNMP в программе	194
Настройка параметров подключения к SNMP-серверу	194
Настройка шифрования SNMP-соединений	195
Включение и отключение отправки SNMP-ловушек	197
Описание объектов MIB Kaspersky Web Traffic Security	197
Аутентификация с помощью технологии единого входа	200
Создание keytab-файла	200
Настройка Kerberos-аутентификации	201
Настройка NTLM-аутентификации	202
Управление параметрами встроенного прокси-сервера в веб-интерфейсе программы	204
Изменение порта подключения к прокси-серверу	204
Настройка фильтра доступа	205
Настройка балансировки нагрузки	206
Аутентификация пользователей	207

Настройка Kerberos-аутентификации	207
Создание keytab-файла	208
Настройка NTLM-аутентификации.....	210
Настройка проверки имен доменов.....	211
Добавление исключений аутентификации	218
Настройка формата журнала доступа	220
Восстановление параметров до значений по умолчанию	221
Расшифровка TLS/SSL-соединений	222
Обработка CONNECT-запросов	223
Настройка исключений в правилах обработки трафика	227
Создание правила обхода	228
О TLS-соединениях.....	229
Работа с сертификатами для перехвата SSL-соединений	234
Добавление самоподписанного сертификата	235
Добавление сертификата на основе CSR.....	236
Создание файла запроса.....	236
Формирование сертификата в центре сертификации.....	237
Загрузка сертификата в веб-интерфейсе программы.....	238
Добавление сертификата в формате PFX	238
Формирование сертификата в центре сертификации.....	238
Экспорт сертификата в файл.....	239
Загрузка сертификата в веб-интерфейсе программы.....	240
Просмотр информации о сертификате.....	241
Назначение сертификата активным	241
Скачивание сертификата	242
Удаление сертификата	242
Импорт сертификата на компьютеры пользователей	242
Включение и отключение расшифровки SSL-соединений.....	244
Выбор действия над SSL-соединениями по умолчанию	245
Работа с SSL-правилами	245
Создание SSL-правила	246
Просмотр информации об SSL-правиле	249
Изменение SSL-правила.....	249
Включение и отключение SSL-правила.....	250
Изменение порядка применения SSL-правил.....	250
Удаление SSL-правила	250
Работа с доверенными сертификатами	251
Добавление доверенного сертификата.....	251
Просмотр информации о доверенном сертификате.....	252
Изменение доверенного сертификата.....	252

Включение и отключение использования доверенного сертификата	253
Удаление доверенного сертификата	253
Источники информации о программе	254
Устранение уязвимостей и установка критических обновлений в программе	255
Действия после сбоя или неустранимой ошибки в работе программы	256
Обращение в Службу технической поддержки	257
Способы получения технической поддержки	257
Техническая поддержка по телефону	257
Техническая поддержка через Kaspersky CompanyAccount	258
Получение информации для Службы технической поддержки	259
Запуск трассировки	259
Изменение уровня трассировки	260
Просмотр журналов трассировки	260
Сохранение файла трассировки на компьютере	261
Приложение 1. MIME-типы объектов	262
Приложение 2. Нормализация URL-адресов	263
Приложение 3. Категории веб-ресурсов	265
Значения параметров программы в сертифицированном режиме	269
Глоссарий	270
АО "Лаборатория Касперского"	276
Информация о стороннем коде	278
Уведомления о товарных знаках	279

Об этом документе

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

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

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

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. 257).

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

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

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

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

Страница Kaspersky Web Traffic Security в Базе знаний

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

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

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

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

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

"веб-интерфейс").

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе (<https://community.kaspersky.com>).

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

Kaspersky 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	13
О задачах программы	14
Основные компоненты программы	15
Принцип работы программы_cert_appliance	16
Об информационных X-заголовках	17

О действиях программы над объектами

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

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

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

- Для правил доступа:
 - **Заблокировать**, если вы хотите добавить правило запрета доступа.
 - **Разрешить**, если вы хотите добавить правило разрешения доступа.
 - **К следующей группе**, если вы хотите добавить переход к следующей группе правил.
 - **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.
- Для правил защиты:
 - a. **Вредоносная программа:**
 - **Заблокировать.**
 - **Заблокировать, по возможности вылечить.**
 - **Пропустить проверку.**По умолчанию установлено значение **Заблокировать, по возможности вылечить.**
 - b. **Объекты, обнаруженные КАТА, Фишинг, Вредоносная ссылка, Зашифрованный объект и Документ с макросом:**
 - **Заблокировать.**
 - **Пропустить проверку.**По умолчанию установлено значение **Заблокировать.**

О задачах программы

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

В состав Kaspersky Web Traffic Security входят следующие задачи:

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

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

Большинство задач являются системными и не предназначены для настройки администратором.

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

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

Основные компоненты программы

В состав Kaspersky Web Traffic Security входят следующие компоненты:

- *Подчиненный узел.*
Выполняет проверку интернет-ресурсов согласно правилам обработки трафика, полученным от Управляющего узла.
- *Управляющий узел.*
Позволяет администратору управлять параметрами программы через веб-интерфейс. Установленные значения параметров передаются на Подчиненные узлы.

Принцип работы программы_cert_appliance

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

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

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

Работа программы без балансировщика нагрузки

При развертывании программы из ISO-образа на каждом узле кластера устанавливается встроенный прокси-сервер. Обмен данными между встроенным прокси-сервером и ICAP-сервером программы осуществляется локально на сервере с установленной программой по протоколу ICAP.

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

Обработка трафика осуществляется по следующему алгоритму:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на сервер с установленной программой.
2. Встроенный прокси-сервер принимает запрос и передает его ICAP-серверу на проверку по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. [84](#)). Если по результатам проверки доступ к веб-ресурсу разрешен, прокси-сервер отправляет запрос на веб-сервер в интернет.
3. Прокси-сервер получает ответ от веб-сервера, на котором располагается запрашиваемый веб-ресурс, и направляет его ICAP-серверу для проверки по правилам обработки трафика. Результат проверки возвращается на прокси-сервер.
4. Прокси-сервер передает ответ пользователю. В зависимости от заданных в программе действий пользователю могут отобразиться следующие страницы:
 - Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
 - Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. [149](#)).
 - Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

Работа программы с балансировщиком нагрузки

При наличии большого количества серверов с установленной программой рекомендуется использовать балансировщик нагрузки NARoxy. В этом случае NARoxy определяет, какому серверу направить запрос на проверку, в соответствии с заданным способом балансировки.

Обработка трафика осуществляется по следующему алгоритму:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается балансировщику

нагрузки.

2. Балансировщик нагрузки выбирает узел кластера согласно заданному способу балансировки и передает этому узлу запрос пользователя.
3. Встроенный прокси-сервер выбранного узла принимает запрос и передает его ICAP-серверу на проверку по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. [84](#)). Если по результатам проверки доступ к веб-ресурсу разрешен, прокси-сервер отправляет запрос на веб-сервер в интернет.
4. Прокси-сервер получает ответ от веб-сервера, на котором располагается запрашиваемый веб-ресурс, и направляет его ICAP-серверу для проверки по правилам обработки трафика. Результат проверки возвращается на прокси-сервер.
5. Прокси-сервер передает ответ балансировщику нагрузки. В зависимости от заданных в программе действий пользователю могут отобразиться следующие страницы:
 - Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
 - Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. [149](#)).
 - Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

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	18
Указания по эксплуатации и требования к среде	19

Аппаратные и программные требования

Программные требования для создания виртуальной машины из бинарных компонентов

Перед началом работы вам нужно создать виртуальную машину с установленными файлами программы.

На виртуальной машине должна быть установлена операционная система CentOS 7.7.

Объем дискового пространства в каталоге /boot – не менее 500 МБ. Объем раздела подкачки должен составлять размер оперативной памяти, умноженный на два.

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

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

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

Программные требования к гипервизору для развертывания виртуальной машины

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

Программные требования к компьютерам локальной сети организации

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

Программные требования для настройки интеграции с LDAP-сервером

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

- Windows Server 2019 Standard.

Дополнительные требования

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

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

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

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

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

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с 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	21
О лицензии	21
О лицензионном сертификате	22
О ключе	22
О коде активации	23
О предоставлении данных.....	23
Просмотр информации о лицензии и активации программы	36
Активация программы.....	36
Удаление лицензионного ключа	37

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

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

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.
Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Web Traffic Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.
Вы можете активировать программу по пробной лицензии только один раз.
- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.
По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Web Traffic Security). Чтобы продолжить использование Kaspersky Web Traffic Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

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

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О ключе

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

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

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

О коде активации

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

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

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. [257](#)).

О предоставлении данных

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

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

- В Лицензионном соглашении.

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

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

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

Дополнительном Положении о Kaspersky Security Network:

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

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

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

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

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

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

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

Тип данных	Где используются данные	Место хранения	Срок хранения
Основная функциональность программы			
<ul style="list-style-type: none"> Имена учетных записей администратора и пользователей программы. Права доступа учетных записей программы. Хеш пароля Локального администратора. IP-адреса пользователей. Имя учетной записи и пароль подключения программы к прокси-серверу. Keutab-файлы для подключения к LDAP-серверу. Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. 	Конфигурация программы	/var/opt/kaspersky	Бессрочно.
<ul style="list-style-type: none"> Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. IP-адреса пользователей. Комментарии. 	Правила обработки трафика	/var/opt/kaspersky	Бессрочно.

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. 	<p>Статистика работы программы</p>	<p>/var/opt/kaspersky</p>	<p>Бессрочно.</p>
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса и User Agent пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. <p>Информация о LDAP-атрибутах пользователей:</p> <ul style="list-style-type: none"> • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. 	<p>Журнал событий обработки трафика</p>	<ul style="list-style-type: none"> • /var/opt/kaspersky • журнал событий Syslog (настраивается администратором) 	<p>Согласно параметрам, заданным пользователем программы.</p> <p>По умолчанию устанавливается срок хранения 3 дня или максимальный размер журнала 1 ГБ.</p> <p>При достижении этого ограничения более старые записи удаляются.</p>
<ul style="list-style-type: none"> • Имя учетной записи пользователя, инициировавшего событие. • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. 	<p>Журнал системных событий</p>	<ul style="list-style-type: none"> • /var/opt/kaspersky • журнал событий Syslog (настраивается администратором) 	<p>Согласно параметрам, заданным пользователем программы.</p> <p>По умолчанию хранится 100 тысяч записей.</p> <p>При достижении этого ограничения более старые записи удаляются.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. <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 файлах и скорости скачивания. <p>Информация об учетных записях пользователей:</p> <ul style="list-style-type: none"> • Имена учетных записей пользователей, осуществивших вход в программу через веб-интерфейс. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. 	<p>Файлы трассировки</p>	<p>/var/log/kaspersky</p>	<p>Бессрочно. При достижении объема 150 МБ для каждого потока трассировки более старые записи удаляются.</p>
		<p>/var/log/kaspersky/extra</p>	<p>Бессрочно. При достижении объема 400 МБ для каждого потока трассировки более старые записи удаляются.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Тела HTTP-сообщений, содержащих cookies и скачиваемые файлы. 	Временные файлы	/tmp/kwtstmp	До перезагрузки программы.
Интеграция с программой Kaspersky Anti Targeted Attack Platform (KATA)			
Файлы пользователей	Отправка файлов на сервер KATA	/tmp/kwtstmp	<p>До перезагрузки программы.</p> <p>Максимально допустимый размер очереди составляет 5 тысяч файлов. При достижении этого ограничения файлы перестают помещаться в очередь.</p>
<p>Информация из обнаружений KATA:</p> <ul style="list-style-type: none"> • MD5- или SHA256-хеш файла. • URL-адреса. 	Получение объектов, обнаруженных программой KATA	/var/opt/kaspersky/kwts/detects.cache	<p>Согласно параметру Срок хранения кеша (часы), заданному пользователем программы.</p> <p>По умолчанию установлено значение 48 часов.</p>
Интеграция с Active Directory®			

Тип данных	Где используются данные	Место хранения	Срок хранения
<ul style="list-style-type: none"> • DN пользователя. • CN пользователя. • sAMAccountName. • UPN-суффикс. • objectSID. 	<ul style="list-style-type: none"> • Правила обработки трафика. • Аутентификация с помощью технологии единого входа. • Автозаполнение учетных записей при работе с ролями и правами пользователей, а также при настройке правил обработки трафика. 	<p>/var/opt/kaspersky/kwts/ldap/cache.dbm</p>	<p>Бессрочно. Данные регулярно обновляются. При отключении интеграции программы с Active Directory данные удаляются.</p>
<p>Использование Kaspersky Security Network (KSN)</p>			

Тип данных	Где используются данные	Место хранения	Срок хранения
<ul style="list-style-type: none"> • MD5- или SHA256-хеш проверяемого файла. • Идентификаторы типа и формата проверяемого файла. • Название обнаруженной угрозы согласно классификации "Лаборатории Касперского". • Идентификаторы антивирусных баз и записи в антивирусных базах, которые использовались для проверки файла. • Дата и время выпуска антивирусных баз. • URL-адрес, с которого был загружен проверяемый файл. • Имя файла процесса, выполнившего загрузку проверяемого объекта, сообщения или ссылки. • Нормализованные URL-адреса запрашиваемых веб-ресурсов, содержащие тип протокола и номер порта. • Отпечаток сертификата и SHA256-хеш открытого ключа сертификата для подписанных файлов. 	<p>Отправка KSN-запросов</p>	<p>/var/opt/kaspersky</p>	<p>Бессрочно.</p> <p>Максимальное количество хранимых записей составляет 360 тысяч. При достижении этого ограничения удаляются записи, к которым дольше всего не было обращений.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
<ul style="list-style-type: none"> • IP-адрес пользователя. <p>Информация о программе и компьютере:</p> <ul style="list-style-type: none"> • Уникальный идентификатор компьютера, на котором установлена программа. • Уникальный идентификатор установки программы. • Полная версия установленной программы. • Идентификатор типа программы. • Тип, версия, редакция, разрядность и параметры режима работы операционной системы. • Информация об установленных пакетах обновлений. <p>Информация о проверке URL-адресов модулями Антивирус и Анти-Фишинг:</p> <ul style="list-style-type: none"> • URL-адрес веб-ресурса, в котором обнаружена угроза. • URL-адрес исходной страницы или страницы, с которой пользователь был перенаправлен на данный URL-адрес. • Дата и время выпуска баз программы. • Название организации и веб-ресурса, на которые была произведена атака. • Результат проверки (уровень доверия, вес и статус решения). • Время события. <p>Информация о проверяемых файлах:</p> <ul style="list-style-type: none"> • Имя, размер, MD5-код, SHA256-код 	<p>KSN-статистика</p>	<p>/var/opt/kaspersky</p>	<p>До отправки статистики в KSN.</p> <p>После отключения отправки KSN-статистики в параметрах программы данные удаляются при следующей попытке отправки.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
Функциональность, доступная только при развертывании программы из ISO-файла			
<p>Расшифровка TLS/SSL-соединений:</p> <ul style="list-style-type: none"> • Сертификаты для перехвата SSL-соединений. • Поля Common name и Organization из CSR-запроса. • SHA1- или SHA256-отпечатки доверенных сертификатов. • Файлы частных ключей сертификатов¹. <p>Параметры Kerberos-аутентификации:</p> <ul style="list-style-type: none"> • Keytab-файлы. • Токены (хеш-строки) пользователей. • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей. <p>Параметры NTLM-аутентификации:</p> <ul style="list-style-type: none"> • Адрес сервера Active Directory. • Сертификат сервера Active Directory. 	<p>Параметры встроенного прокси-сервера</p>	<p>/etc/squid/ /var/opt/kaspersky/</p>	<p>Бессрочно.</p> <p>Данные удаляются при удалении соответствующих параметров в веб-интерфейсе программы.</p> <p>Файлы сертификатов могут быть перезаписаны при замене сертификата.</p>

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

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • URL-адреса веб-ресурсов, к которым запрашивается доступ. • IP-адреса и DNS-имена веб-серверов. • IP-адреса доверенных балансировщиков нагрузки. • IP-адрес ICAP-сервера. • IP-адреса пользователей. • HTTP-заголовки обрабатываемых HTTP-сообщений. 	<p>Журнал событий прокси-сервера</p>	<p>/var/log/squid/icap.log /var/log/squid/ssl.log /var/log/squid/squid.out /var/log/squid/access.log /var/log/squid/cache.log</p>	<p>Бессрочно. При достижении объема 3 ГБ для каждого потока трассировки более старые записи удаляются.</p>
<p>Параметры Kerberos-аутентификации:</p> <ul style="list-style-type: none"> • Keytab-файлы. • Токены (хеш-строки) пользователей. • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей. 	<p>Журнал событий прокси-сервера</p>	<p>/var/log/squid/cache.log</p>	<p>Бессрочно. При достижении объема 10 ГБ для каждого потока трассировки более старые записи удаляются.</p>
<p>Параметры NTLM-аутентификации:</p> <ul style="list-style-type: none"> • Идентификаторы домена (SID) пользователей. • Имена учетных записей пользователей. • Тела NTLM-сообщений в кодировке Base-64. • Кодированные LDAP-сообщения. 	<p>Журнал событий прокси-сервера</p>	<p>/var/log/squid/cache.log</p>	<p>Бессрочно. При достижении объема 10 ГБ для каждого потока трассировки более старые записи удаляются.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Подключение по протоколу SSH:</p> <ul style="list-style-type: none"> • IP-адрес пользователя. • Имя учетной записи пользователя. • Отпечаток ключа SSH. <p>Подключение через веб-интерфейс:</p> <ul style="list-style-type: none"> • IP-адрес пользователя. • Имя учетной записи пользователя. 	<p>Журнал событий авторизации</p>	<p>/var/log/secure</p>	<p>Не более 5 недель. Выполняется еженедельная ротация файлов.</p>

Тип данных	Где используются данные	Место хранения	Срок хранения
<p>Информация из запросов доступа к веб-ресурсам:</p> <ul style="list-style-type: none"> • IP-адреса и User Agent пользователей. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. <p>Информация о LDAP-атрибутах пользователей:</p> <ul style="list-style-type: none"> • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. <p>Информация о системных событиях:</p> <ul style="list-style-type: none"> • Имя учетной записи пользователя, инициировавшего событие. • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. 	<p>Журнал системных событий и событий обработки трафика</p>	<p>/var/log/kwts-messages</p>	<p>Не более 5 недель. Выполняется еженедельная ротация файлов.</p>

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

По умолчанию формирование дампа в Kaspersky Web Traffic Security отключено.

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

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

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

Просмотр информации о лицензии и активации программы

► Чтобы просмотреть информацию о лицензии, выполните следующие действия:

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

Откроется окно **Лицензия**.

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

► Чтобы просмотреть информацию об активации программы,

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

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

Активация программы

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

► Чтобы ввести код активации, выполните следующие действия:

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

3. Нажмите на кнопку **Активировать**.

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

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

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

Удаление лицензионного ключа

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

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Лицензирование**.

2. Нажмите на кнопку **Удалить**.

Отобразится подтверждение удаления лицензионного ключа.

3. Нажмите на кнопку **Да**.

Лицензионный ключ будет удален.

Установка и первоначальная настройка программы

Вы можете установить программу на физическом сервере или на виртуальной машине. Поддерживается развертывание виртуальной машины на следующих гипервизорах:

- VMware ESXi.

Вы можете выполнять все действия по развертыванию виртуальной машины в следующих интерфейсах:

- в веб-интерфейсе VMware vSphere™;
- в консоли управления гипервизора VMware ESXi.

- Microsoft Hyper-V.

Вы можете выполнять все действия по развертыванию виртуальной машины в следующих интерфейсах:

- в интерфейсе программы Microsoft System Center Virtual Machine Manager (далее также Microsoft SCVMM);
- в консоли управления Microsoft Hyper-V Manager.

Убедитесь, что версия гипервизора и аппаратные ресурсы, выделенные для виртуальной машины, удовлетворяют аппаратным и программным требованиям.

После развертывания виртуальной машины вы можете перейти к установке программы (см. раздел "Установка программы" на стр. [53](#)). Для этого вам потребуются следующие файлы:

- Дистрибутив (rpm-пакеты) программы:
 - ram-0.4.9-4762.noarch.rpm;
 - kwts-6.1.0-4762.x86_64.rpm;
 - kwts-appliance-addon-6.1.0-4762.noarch.rpm;
 - kwts-appliance-addon_ru-6.1.0.4762-1.noarch.rpm.
- ISO-образ установочного диска операционной системы CentOS Linux® 7.7 (1908) Minimal.

Дополнительные пакеты будут загружены автоматически из публичных репозиториях в сети Интернет в процессе установки.

В этом разделе

Развертывание виртуальной машины в консоли управления гипервизора VMware ESXi	39
Развертывание виртуальной машины в веб-интерфейсе VMware vSphere.....	42
Развертывание виртуальной машины в консоли управления гипервизора Microsoft Hyper-V Manager	45
Развертывание виртуальной машины с помощью программы Microsoft SCVMM.....	49
Установка программы	53
Удаление программы, развернутой из ISO-файла	58

Развертывание виртуальной машины в консоли управления гипервизора VMware ESXi

Развертывание образа виртуальной машины состоит из следующих этапов:

1. Загрузка iso-файла в виртуальное хранилище данных (см. раздел "Загрузка iso-файла" на стр. [39](#))
Для установки операционной системы на виртуальной машине вам требуется загрузить ISO-образ установочного диска CentOS Linux.
2. Создание виртуальной машины (см. раздел "Создание виртуальной машины в консоли управления гипервизора VMware ESXi" на стр. [40](#))
Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Web Traffic Security.
3. Подключение к виртуальной машине (на стр. [42](#))

В этом разделе

Загрузка iso-файла.....	39
Создание виртуальной машины в консоли управления гипервизора VMware ESXi.....	40
Подключение к виртуальной машине	42

Загрузка iso-файла

Прежде чем запустить мастер создания виртуальной машины, необходимо загрузить iso-файл в виртуальное хранилище данных хоста.

► *Чтобы загрузить iso-файл в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Storage**.

3. Выберите закладку **Datastores**.
4. Нажмите на кнопку **Datastore browser**.
Откроется окно **Datastore browser**.
5. Выберите хранилище данных и папку, в которую вы хотите загрузить iso-файл.
6. Нажмите на кнопку **Upload**.
Откроется окно выбора файла.
7. Выберите файл и нажмите **Open**.

Дождитесь загрузки файла. После завершения загрузки имя iso-файла отобразится в таблице файлов виртуального хранилища данных хоста. Убедитесь, что указанный размер загруженного файла совпадает с размером исходного файла.

Создание виртуальной машины в консоли управления гипервизора VMware ESXi

► Чтобы создать виртуальную машину в консоли управления гипервизора VMware ESXi, выполните следующие действия:

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Virtual Machines**.
3. Нажмите на кнопку **Create/Register VM**.

Откроется мастер создания виртуальной машины.

4. Следуйте шагам мастера:

a. Выберите способ создания виртуальной машины.

1. Выберите вариант **Create a new virtual machine**.

Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

b. Укажите имя виртуальной машины и выберите гостевую операционную систему.

1. В поле **Name** введите имя виртуальной машины.

Имя должно быть уникальным среди используемых виртуальных машин.

2. В раскрывающемся списке **Compatibility** выберите **ESXi 6.5 and later**.
3. В раскрывающемся списке **Guest OS Family** выберите **Linux**.
4. В раскрывающемся списке **Guest OS Version** выберите **CentOS 7 (64-bit)**.
5. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

c. Выберите виртуальное хранилище данных.

1. Выберите виртуальное хранилище данных из списка доступных хранилищ.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

d. Настройте аппаратную конфигурацию виртуальной машины.

1. На закладке **Virtual Hardware** выберите блок параметров **CPU**.
2. В раскрывающемся списке **CPU** укажите количество виртуальных процессоров.

Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

3. В раскрывающемся списке **Cores per Socket** выберите максимальное доступное значение.

Набор доступных значений зависит от возможностей гипервизора.

4. В блоке параметров **Memory** в поле **RAM** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

Минимальное рекомендуемое значение 16 GB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

5. Установите флажок **Reserve all guest memory**.
6. В блоке параметров **Hard Disk 1** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

7. В раскрывающемся списке **Disk Provisioning** выберите тип размещения файлов виртуальной машины.
8. В блоке параметров **SCSI controller 0** выберите **VMwareParavirtual**.
9. В блоке параметров **Network Adapter 1** выберите виртуальную сеть, к которой будет подключена виртуальная машина.
10. В блоке параметров **CD/DVD Drive 1** выберите тип привода **Datastore ISO File**.
11. Нажмите на кнопку **Browse...** справа от поля **CD/DVD Media**.

Откроется окно выбора файлов.

12. Выберите iso-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.
13. В блоке параметров **CD/DVD Drive 1** установите флажок **Connect at power on**.
14. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

e. Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана.

Подключение к виртуальной машине

► Чтобы подключиться к виртуальной машине в консоли управления гипервизора VMware ESXi, выполните следующие действия:

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** в разделе **Virtual Machines** выберите виртуальную машину, которую вы хотите запустить.
3. Нажмите на кнопку **Power on**.
Виртуальная машина запустится.
4. Нажмите на кнопку **Console** и в раскрывающемся списке выберите требуемый формат запуска консоли:
 - **Open browser console**.
 - **Launch remote console**.

Откроется консоль управления виртуальной машины.

После подключения к виртуальной машине вы можете начинать установку программы (см. раздел "Установка программы" на стр. [53](#)).

Развертывание виртуальной машины в веб-интерфейсе VMware vSphere

Развертывание образа виртуальной машины состоит из следующих этапов:

1. Загрузка iso-файла в виртуальное хранилище данных (см. раздел "Загрузка iso-файла" на стр. [42](#))
Для установки операционной системы на виртуальной машине вам требуется загрузить ISO-образ установочного диска CentOS Linux.
2. Создание виртуальной машины (см. раздел "Создание виртуальной машины в веб-интерфейсе VMware vSphere" на стр. [43](#))
Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Web Traffic Security.
3. Подключение к виртуальной машине (на стр. [45](#))

Загрузка iso-файла

► Чтобы загрузить iso-файл в виртуальное хранилище через веб-интерфейс VMware vSphere, выполните следующие действия:

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В панели **Navigator** выберите центр обработки данных и хранилище, в котором вы хотите создать виртуальную машину.
В рабочей области отобразится окно свойств выбранного хранилища.
3. Выберите закладку **Files**.

4. Нажмите на кнопку  .

Откроется окно выбора файла.

5. Выберите iso-файл и нажмите на кнопку **Open**.

Дождитесь загрузки файла. После завершения загрузки имя iso-файла отобразится в таблице файлов виртуального хранилища данных хоста. Убедитесь, что указанный размер загруженного файла совпадает с размером исходного файла.

Создание виртуальной машины в веб-интерфейсе VMware vSphere

- Чтобы создать виртуальную машину в веб-интерфейсе VMware vSphere, выполните следующие действия:

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В панели **Navigator** выберите центр обработки данных и хранилище, в котором вы хотите создать виртуальную машину.

В рабочей области отобразится окно свойств выбранного хранилища.

3. В панели управления в раскрывающемся списке **Actions** выберите **New Virtual Machine** → **New Virtual Machine....**

Откроется мастер создания виртуальной машины.

4. Следуйте шагам мастера:

a. Выберите способ создания виртуальной машины.

1. Выберите вариант **Create a new virtual machine**.

Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

b. Укажите имя и расположение виртуальной машины.

1. В поле ввода введите имя виртуальной машины.

Имя должно быть уникальным среди используемых виртуальных машин.

2. В дереве папок под полем ввода выберите папку в виртуальном хранилище хоста, в которой должна храниться виртуальная машина.

3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

c. Выберите вычислительные ресурсы.

1. В правой части окна мастера выберите кластер и ресурсный пул.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- d. Выберите виртуальное хранилище данных.
 - 1. Выберите виртуальное хранилище данных из списка доступных хранилищ.
 - 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- e. Настройте совместимость с виртуальной инфраструктурой.
 - 1. В раскрывающемся списке **Compatible with** выберите **ESXi 6.5 and later**.
 - 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- f. Выберите гостевую операционную систему.
 - 1. В раскрывающемся списке **Guest OS Family** выберите **Linux**.
 - 2. В раскрывающемся списке **Guest OS Version** выберите **CentOS 7 (64-bit)**.
 - 3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- g. Настройте аппаратную конфигурацию виртуальной машины.
 - 1. На закладке **Virtual Hardware** выберите блок параметров **CPU**.
 - 2. В раскрывающемся списке **CPU** укажите количество виртуальных процессоров.

Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

- 3. В раскрывающемся списке **Cores per Socket** выберите максимальное доступное значение.

Набор доступных значений зависит от возможностей гипервизора.

- 4. В блоке параметров **Memory** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

Минимальное рекомендуемое значение 16 GB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

- 5. Установите флажок **Reserve all guest memory**.
 - 6. В блоке параметров **New Hard Disk** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

- 7. В раскрывающемся списке **Disk Provisioning** выберите тип размещения файлов виртуальной машины.
 - 8. В блоке параметров **New SCSI controller** в раскрывающемся списке **Change Type** выберите **VMwareParavirtual**.
 - 9. В блоке параметров **New Network** выберите виртуальную сеть, к которой будет подключена виртуальная машина.
 - 10. В блоке параметров **New CD/DVD Drive** в раскрывающемся списке выберите тип привода **Datastore ISO File**.

11. Нажмите на кнопку **Browse...**

Откроется окно выбора файлов.

12. Выберите iso-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.

13. В поле **Status** установите флажок **Connect At Power On**.

14. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

h. Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.

2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана.

Подключение к виртуальной машине

► Чтобы подключиться к виртуальной машине в веб-интерфейсе VMware vSphere, выполните следующие действия:

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.

2. В панели **Navigator** на закладке **Hosts and clusters** щелкните правой клавишей мыши по виртуальной машине, которую вы хотите запустить.

3. В контекстном меню выберите **Power** → **Power On**.

Виртуальная машина запустится.

4. В панели управления в раскрывающемся списке **Actions** выберите **Open console**.

Откроется консоль управления виртуальной машины.

После подключения к виртуальной машине вы можете начинать установку программы (см. раздел "Установка программы" на стр. [53](#)).

Развертывание виртуальной машины в консоли управления гипервизора Microsoft Hyper-V Manager

Развертывание образа виртуальной машины состоит из следующих этапов:

1. Создание виртуальной машины (см. раздел "Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager" на стр. [46](#))

2. Изменение количества процессоров виртуальной машины (на стр. [48](#))

В мастере создания виртуальной машины нет возможности задать требуемое количество процессоров. Поэтому требуется изменить этот параметр в уже созданной виртуальной машине.

3. Подключение к виртуальной машине (на стр. [48](#))

В этом разделе

Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager.....	46
Изменение количества процессоров виртуальной машины.....	48
Подключение к виртуальной машине.....	48

Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager

Перед созданием виртуальной машины необходимо разместить iso-файл в любой сетевой папке, доступной для сервера с гипервизором. Если вы открываете консоль Microsoft Hyper-V Manager на том же сервере, на котором установлен гипервизор, вы можете разместить iso-файл на локальном жестком диске.

► Чтобы создать виртуальную машину, выполните следующие действия:

1. Откройте консоль управления Microsoft Hyper-V Manager.
2. В левой части окна выберите для подключения гипервизор, на котором вы хотите развернуть образ виртуальной машины.
3. В контекстном меню выберите пункт **New** → **Virtual Machine**.
Откроется мастер создания виртуальной машины.
4. Следуйте шагам мастера:
 - a. Выберите имя и расположение виртуальной машины.
 1. Введите имя новой виртуальной машины в поле **Name**.

Имя должно быть уникальным среди используемых виртуальных машин.

2. Если вы хотите изменить папку для сохранения виртуальной машины, выполните следующие действия:
 - (i) Установите флажок **Store the virtual machine in a different location**.
 - (ii) В поле **Location** укажите путь к папке, в которой вы хотите сохранить виртуальную машину.
По умолчанию выбрана папка <диск>:\Virtual Machines.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- b. Выберите поколение виртуальной машины.
 1. Выберите вариант **Generation 1**.
 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

с. Выделите память для виртуальной машины.

1. В поле **Startup memory** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

Минимальное рекомендуемое значение 16384 MB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

2. Снимите флажок **Use Dynamic Memory for this virtual machine**.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

d. Настройте сетевое подключение.

1. В раскрывающемся списке **Connection** выберите виртуальную сеть, к которой будет подключена виртуальная машина.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

e. Подключите виртуальный жесткий диск.

1. Выберите пункт **Create a virtual hard disk**.
2. В поле **Size** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

f. Выберите диск для развертывания образа виртуальной машины.

1. В списке действий выберите **Install an operating system from a bootable CD / DVD-ROM**.
2. В блоке параметров **Media** выберите вариант **Image file (.iso)**.
3. Укажите путь к установочному ISO-образу виртуальной машины.
4. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

g. Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана. Убедитесь, что она отображается в списке **Virtual Machines** на выбранном гипервизоре.

Виртуальная машина создается с количеством процессоров, установленным по умолчанию. Вам требуется изменить этот параметр в свойствах виртуальной машины (см. раздел "Изменение количества процессоров виртуальной машины" на стр. [48](#)) после ее создания.

Изменение количества процессоров виртуальной машины

Перед выполнением этой инструкции убедитесь, что виртуальная машина выключена.

- ▶ *Чтобы изменить количество процессоров виртуальной машины, выполните следующие действия:*
 1. Запустите программу Hyper-V Manager.
 2. В главном окне программы в таблице **Virtual Machines** выберите виртуальную машину, развернутую из iso-файла.
 3. По правой кнопке мыши откройте контекстное меню и выберите пункт **Settings**.
Откроется окно свойств виртуальной машины.
 4. В блоке параметров **Hardware** выберите раздел **Processor**.
 5. В поле **Number of virtual processors** укажите количество виртуальных процессоров.
Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.
 6. Нажмите на кнопку **OK**.Количество процессоров виртуальной машины будет изменено.

Подключение к виртуальной машине

- ▶ *Чтобы подключиться к виртуальной машине в консоли управления Microsoft Hyper-V Manager, выполните следующие действия:*
 1. Откройте консоль управления Microsoft Hyper-V Manager
 2. В левой части окна выберите гипервизор, на котором развернута виртуальная машина.
 3. В рабочей области щелкните правой клавишей мыши по виртуальной машине, которую вы хотите запустить.
 4. В контекстном меню выберите команду **Start**.
Виртуальная машина запустится.
 5. В контекстном меню виртуальной машины выберите команду **Connect**.
Откроется консоль управления виртуальной машины.После подключения к виртуальной машине вы можете начинать установку программы (см. раздел "Установка программы" на стр. [53](#)).

Развертывание виртуальной машины с помощью программы Microsoft SCVMM

Развертывание образа виртуальной машины состоит из следующих этапов:

1. Загрузка iso-файла в библиотеку сервера Microsoft SCVMM (см. раздел "Загрузка iso-файла" на стр. [49](#))
Для установки операционной системы на виртуальной машине вам требуется загрузить ISO-образ установочного диска CentOS Linux.
2. Создание виртуальной машины (см. раздел "Создание виртуальной машины с помощью программы Microsoft SCVMM" на стр. [50](#))
Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Web Traffic Security.
3. Подключение к виртуальной машине

В этом разделе

Загрузка iso-файла.....	49
Создание виртуальной машины с помощью программы Microsoft SCVMM.....	50
Подключение к виртуальной машине.....	52

Загрузка iso-файла

Для загрузки iso-файла в библиотеку сервера Microsoft SCVMM необходимо разместить его на локальном жестком диске того компьютера, на котором запускается программа Microsoft SCVMM.

► Чтобы загрузить iso-файл в библиотеку сервера Microsoft SCVMM, выполните следующие действия:

1. Запустите программу Virtual Machine Manager (VMM).
2. В левой нижней части окна выберите раздел **Library**.
3. В панели управления нажмите на кнопку **Import Physical Resource**.
Откроется окно **Import Library Resources**.
4. Нажмите на кнопку **Browse....**
Откроется окно **Select Destination Folder**.
5. Выберите библиотеку ресурсов и папку, в которую будет загружен iso-файл, и нажмите на кнопку **OK**.
6. В окне **Import Library Resources** нажмите на кнопку **Add resource....**

Откроется окно **Select resource items**.

7. Выберите iso-файл и нажмите на кнопку **Open**.
8. Нажмите на кнопку **Import**.

Iso-файл будет загружен в библиотеку сервера Microsoft SCVMM и отобразится в таблице **Physical Library Objects**.

Создание виртуальной машины с помощью программы Microsoft SCVMM

Если гипервизор Microsoft Hyper-V подключен к инфраструктуре Microsoft System Center, то вы можете создать виртуальную машину с помощью программы Microsoft SCVMM.

► *Чтобы создать виртуальную машину, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левом нижнем углу окна выберите раздел **VMs and Services**.
3. В панели инструментов нажмите на кнопку **Create Virtual Machine** и в раскрывающемся списке выберите пункт **Create Virtual Machine**.

Откроется мастер создания виртуальной машины.

4. Следуйте шагам мастера:
 - a. Выберите способ создания виртуальной машины.
 1. Выберите вариант **Create the new virtual machine with a blank virtual hard disk**.

Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.
 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- b. Укажите имя и поколение виртуальной машины.
 1. В поле **Virtual machine name** введите имя виртуальной машины.

Имя должно быть уникальным среди используемых виртуальных машин.

2. В раскрывающемся списке **Generation** выберите **Generation 1**.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- c. Настройте аппаратную конфигурацию виртуальной машины.
 1. В разделе **Compatibility** установите флажок **Hyper-V**.
 2. В блоке параметров **General** в разделе **Processor** укажите количество виртуальных процессоров в поле **Number of processors**.

Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

3. В блоке параметров **General** в разделе **Memory** выполните следующие действия:
 - (i) Выберите вариант **Static**.
 - (ii) В поле **Virtual machine memory** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

Минимальное рекомендуемое значение 16384 MB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

4. В блоке параметров **Bus configuration** в разделе **IDE Devices** → **<название диска>** выполните следующие действия:
 - (i) В раскрывающемся списке **Type** выберите тип виртуального диска **Fixed**.
 - (ii) В поле **Size** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

5. В блоке параметров **Bus configuration** в разделе **IDE Devices** → **Virtual DVD Drive** выберите тип носителя виртуального диска. Для этого выполните следующие действия:

- (i) Выберите вариант **Existing ISO image**.
- (ii) Нажмите на кнопку **Browse....**
Откроется окно **Select ISO**.
- (iii) Выберите iso-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.

6. В блоке параметров **Network Adapters** в разделе **Network Adapter 1** выполните следующие действия:

- (i) Выберите режим подключения сетевого адаптера **Connected to a VM network**.
- (ii) Справа от поля **VM network** нажмите на кнопку **Browse....**
Откроется окно **Select a VM Network**.
- (iii) Выберите виртуальную сеть, к которой будет подключена виртуальная машина, и нажмите на кнопку **OK**.

7. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- d. Выберите тип размещения виртуальной машины.

1. Выберите вариант **Place the virtual machine on a host**.
2. В раскрывающемся списке **Destination** выберите группу хостов для создания виртуальной машины.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера

- e. Выберите гипервизор, на котором будет создана виртуальная машина.

1. В таблице гипервизоров группы, выбранной на предыдущем шаге, выберите гипервизор, на котором будет размещена виртуальная машина.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- f. Проверьте правильность заданных значений параметров.
 - 1. Проверьте параметры виртуальной машины, заданные на предыдущих шагах мастера.

После выбора гипервизора заданные ранее параметры могут измениться.

- 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- g. Выберите операционную систему.
 - 1. В блоке параметров **Operating system** в раскрывающемся списке выберите **CentOS Linux 7 (64 bit)**.
 - 2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

- h. Подтвердите создание виртуальной машины.
 - 1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
 - 2. Если все параметры установлены правильно, нажмите на кнопку **Create**.

Запустится процесс создания виртуальной машины с заданными параметрами. Убедитесь, что процесс завершен корректно и виртуальная машина отображается в списке виртуальных машин выбранного гипервизора.

Подключение к виртуальной машине

- Чтобы подключиться к виртуальной машине с помощью программы Microsoft SCVMM, выполните следующие действия:

1. Запустите программу Virtual Machine Manager (VMM).
2. В левой нижней части окна выберите раздел **VMs and Services**.
3. В левой верхней части окна в дереве выберите гипервизор, на котором была создана виртуальная машина.
4. В рабочей области окна выберите виртуальную машину, которую вы хотите запустить.
5. В панели инструментов нажмите на кнопку **Power On**.

Виртуальная машина запустится.

6. В панели инструментов нажмите на кнопку **Connect or View** и в раскрывающемся списке выберите пункт **Connect via Console**.

Откроется консоль управления виртуальной машины.

После подключения к виртуальной машине вы можете начинать установку программы (см. раздел "Установка программы" на стр. [53](#)).

Установка программы

Для выполнения всех действий, описанных в этом разделе, учетная запись должна обладать правами суперпользователя.

Установка программы включает следующие этапы.

1. Подготовка и первоначальная настройка операционной системы (на стр. [53](#))
2. Установка сервиса nginx (на стр. [54](#))
3. Установка сервиса Squid (на стр. [54](#))
4. Установка дополнительных пакетов (на стр. [55](#))
5. Установка пакетов программы (на стр. [55](#))
6. Первоначальная настройка программы (на стр. [56](#))

В этом разделе

Подготовка и первоначальная настройка операционной системы.....	53
Установка сервиса nginx.....	54
Установка сервиса Squid.....	54
Установка дополнительных пакетов.....	55
Установка пакетов программы.....	55
Первоначальная настройка программы.....	56

Подготовка и первоначальная настройка операционной системы

Установка операционной системы

После подключения к развернутой виртуальной машине требуется выполнить установку операционной системы в минимальной конфигурации. Во время установки вам нужно провести разметку жесткого диска. При этом рекомендуется создать на жестком диске разделы, описанные в таблице ниже.

Таблица 2. Рекомендуемая разметка жесткого диска

Раздел	Размер	Файловая система
Загрузочный раздел /boot	500 МБ	ext2
Раздел подкачки swap	Размер оперативной памяти, умноженный на два	swap
Корневой раздел /	Все оставшееся дисковое пространство	ext4

После завершения установки вы можете перейти к первоначальной настройке операционной системы.

Первоначальная настройка операционной системы

► *Выполните следующие действия для подготовки операционной системы к установке программы:*

1. Настройте на виртуальной машине сетевое подключение для доступа в интернет.
Доступ в интернет потребуется для загрузки дополнительных пакетов.
2. Отключите SELinux. Для этого в конфигурационном файле `/etc/selinux/config` установите значение параметра `SELINUX=disabled`.
3. Отключите встроенный сетевой экран. Для этого выполните команду:

```
systemctl disable firewalld
```
4. Перезагрузите операционную систему.
Операционная система готова к установке программы.

Установка сервиса nginx

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

1. Создайте файл `/etc/yum.repos.d/nginx.repo`. Файл должен содержать следующие строки:

```
[nginx-stable]
name=nginx stable repo
baseurl=http://nginx.org/packages/centos/$releasever/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```
2. Установите пакет nginx версии 1.16.1. Для этого выполните команду:

```
yum -y install nginx-1.16.1
```
3. Разрешите автоматический запуск сервиса nginx. Для этого выполните команду:

```
systemctl enable nginx
```


Сервис nginx будет установлен.

Установка сервиса Squid

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

1. Создайте файл `/etc/yum.repos.d/squid.repo`. Файл должен содержать следующие строки:

```
[squid]
name=squid4 repo
```

```
baseurl=http://www1.ngtech.co.il/repo/centos/$releasever/$basearch/  
failovermethod=priority  
enabled=1  
gpgcheck=0
```

2. Установите пакеты squid-4.8 и squid-helpers-4.8. Для этого выполните команду:

```
yum -y install squid-4.8 squid-helpers-4.8
```

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

```
systemctl enable squid
```

Сервис Squid будет установлен.

Установка дополнительных пакетов

- Чтобы установить дополнительные пакеты, выполните следующие команды:

```
yum -y install libtool-ltdl  
yum -y install open-vm-tools  
yum -y install pyOpenSSL  
yum -y install libuser-python cracklib-python python-dateutil  
python-inotify
```

Установка пакетов программы

- Чтобы установить пакеты программы, выполните следующие действия:

1. Скопируйте rpm-пакеты, входящие в дистрибутив программы, на виртуальную машину.
2. Выполните следующие команды:

```
rpm -i ram-0.4.9-*.rpm  
rpm -i kwts-6.1.0-*.rpm  
rpm -i kwts-appliance-addon-6.1.0-*.rpm --excludepath  
/usr/lib/systemd/system/getty@.service.d  
rpm -i kwts-appliance-addon_ru-6.1.0-*.rpm
```

Пакеты программы будут установлены.

Первоначальная настройка программы

Перед выполнением первоначальной настройки программы вы можете создать шаблон виртуальной машины для развертывания программы на последующих узлах. Перед созданием шаблона необходимо выключить виртуальную машину.

► Чтобы провести первоначальную настройку программы, выполните следующие действия:

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

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

2. Выберите язык просмотра Лицензионного соглашения и Политики конфиденциальности. Для этого введите число, расположенное рядом с языком, который вы хотите выбрать, и нажмите на клавишу **ENTER**.
3. Выразите свое согласие или несогласие с Лицензионным соглашением. Для этого выполните следующие действия:
 - a. Нажмите на клавишу **ENTER**, чтобы ознакомиться с текстом Лицензионного соглашения.
 - b. Нажмите на клавишу **Q** для выхода из режима просмотра.
 - c. Выполните одно из следующих действий:
 - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.
 - Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.
 - d. Нажмите на клавишу **ENTER**.

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

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

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

5. Выразите свое согласие или несогласие со значениями параметров защиты, устанавливаемыми по умолчанию. Для этого выполните следующие действия:
 - a. Нажмите на клавишу **ENTER**, чтобы ознакомиться с описанием параметров защиты по умолчанию.

- b. Нажмите на клавишу **Q** для выхода из режима просмотра.
- c. Выполните одно из следующих действий:
 - Если вы хотите принять параметры защиты по умолчанию, введите `yes`.
 - Если вы хотите отклонить параметры защиты по умолчанию, введите `no`.
- d. Нажмите на клавишу **ENTER**.

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

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

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

По умолчанию используется текущий активный IP-адрес.

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

Рекомендуется использовать значение по умолчанию: 9045.

- 8. Задайте пароль Локального администратора.

Пароль должен содержать:

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

Вы можете изменить пароль Локального администратора (см. раздел "Изменение пароля учетной записи Administrator" на стр. [128](#)) после установки в веб-интерфейсе программы в разделе **Локальный администратор**.

Настройка программы будет завершена. После этого вам нужно добавить сервер в кластер (см. раздел "Добавление узла в кластер" на стр. [133](#)) для управления параметрами программы через веб-интерфейс.

Удаление программы, развернутой из ISO-файла

После удаления программы вся информация, связанная с ней, будет потеряна.

Для программы, развернутой из ISO-файла, не предусмотрено стандартной процедуры удаления.

Если вы развернули программу на виртуальной машине, вы можете удалить всю виртуальную машину, в том числе файлы виртуальных дисков и файлы снимков состояния системы. Для этого следуйте указаниям одной из инструкций этого раздела в зависимости от используемого гипервизора.

Если вы развернули программу на физическом сервере, для удаления программы вам потребуется перезаписать данные жесткого диска (см. раздел "Удаление программы с физического сервера" на стр. [58](#)) сервера.

В этом разделе

Подготовка к удалению программы.....	58
Удаление программы с физического сервера	58
Удаление виртуальной машины в консоли управления гипервизора VMware ESXi.....	60
Удаление виртуальной машины в веб-интерфейсе VMware vSphere	60
Удаление виртуальной машины в консоли управления гипервизора Microsoft Hyper-V	60
Удаление виртуальной машины с помощью Microsoft SCVMM	61

Подготовка к удалению программы

Перед удалением программы с физического сервера или виртуальной машины требуется выполнить следующие действия:

1. Отключить балансировку нагрузки (см. раздел "Настройка балансировки нагрузки" на стр. [206](#)) для удаляемого узла кластера
2. Остановить поступление запросов на обработку трафика
Для этого убедитесь, что браузеры пользователей настроены на передачу трафика балансировщику нагрузки или другому узлу кластера.
3. Удалить узел из кластера (см. раздел "Удаление узла из кластера" на стр. [134](#))

Удаление программы с физического сервера

Перед удалением программы требуется выполнить подготовительные действия (см. раздел "Подготовка к удалению программы" на стр. [58](#)).

Для полного удаления программы с физического сервера рекомендуется выполнить многократную перезапись текущих данных произвольными.

► Чтобы удалить программу с физического сервера, выполните следующие действия:

1. Скачайте загрузочный образ LiveCD <https://wiki.centos.org/Download> (LiveKDE или LiveGNOME) дистрибутива CentOS.

В этой инструкции описана работа с LiveCD LiveGNOME.

2. Разверните образ LiveCD на USB-накопителе. Для этого воспользуйтесь инструкцией из базы знаний CentOS <https://wiki.centos.org/HowTos/InstallFromUSBkey>.
3. Подключите USB-накопитель к серверу с Kaspersky Web Traffic Security.
4. Укажите подключенный USB-накопитель в параметрах BIOS/UEFI в качестве загрузочного устройства и выполните загрузку.
5. Запустите программу Terminal. Для этого выберите в меню **Applications** раздел **System Tools** → **Terminal**.

Откроется консоль программы Terminal.

6. Определите название жесткого диска. Для этого выполните команду:

```
lsblk
```

7. В открывшейся таблице в графе **TYPE** найдите значение **disk**. Имя жесткого диска указано в этой же строке в графе **NAME**.
8. Если вы хотите перезаписать данные диска однократно, выполните следующие действия:

- Для перезаписи диска символами 0 выполните команду:

```
sudo dd if=/dev/zero of=<название жесткого диска> bs=1M
```

- Для перезаписи диска произвольными данными выполните команду:

```
sudo dd if=/dev/urandom of=<название жесткого диска> bs=1M
```

9. Если вы хотите перезаписать данные диска многократно, выполните следующие действия:

- a. Подготовьте файл скрипта. Для этого выполните команду:

```
echo "for n in `seq 7` ; do dd if=/dev/urandom of=/dev/sda bs=1M conv=notrunc ; done" > wipe
```

- b. Сделайте файл скрипта исполняемым. Для этого выполните команду:

```
chmod a+x wipe
```

- c. Запустите скрипт. Для этого выполните команду:

```
sudo ./wipe
```

10. Дождитесь завершения операции. После выполнения перезаписи отобразится уведомление о том, что на диске не осталось свободного места.

11. Извлеките USB-носитель.

12. Перезагрузите сервер и выполните попытку загрузки с жесткого диска.

В случае успешного удаления данных загрузка программы будет невозможен.

Удаление виртуальной машины в консоли управления гипервизора VMware ESXi

Перед удалением программы требуется выполнить подготовительные действия (см. раздел "Подготовка к удалению программы" на стр. [58](#)).

► *Чтобы удалить виртуальную машину в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Virtual Machines**.
3. В рабочей области выберите виртуальную машину, которую вы хотите удалить.
4. Если виртуальная машина включена, отключите ее. Для этого нажмите на кнопку **Shut down**. Дождитесь отключения машины.
5. В панели управления в раскрывающемся списке **Actions** выберите **Delete from Disk**.
6. В окне подтверждения нажмите на кнопку **Delete**.

Виртуальная машина с установленной программой Kaspersky Web Traffic Security будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины в веб-интерфейсе VMware vSphere

Перед удалением программы требуется выполнить подготовительные действия (см. раздел "Подготовка к удалению программы" на стр. [58](#)).

► *Чтобы удалить виртуальную машину в веб-интерфейсе VMware vSphere, выполните следующие действия:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В панели **Navigator** выберите закладку **Hosts and Clusters**.
3. Выберите виртуальную машину, которую вы хотите удалить.
В рабочей области отобразится окно свойств выбранной виртуальной машины.
4. Если виртуальная машина включена, отключите ее. Для этого в панели управления в раскрывающемся списке **Actions** выберите **Power** → **Shut Down Guest OS**.
5. В окне подтверждения нажмите на кнопку **Yes**. Дождитесь отключения машины.
6. В панели управления в раскрывающемся списке **Actions** выберите **Delete from Disk**.
7. В окне подтверждения нажмите на кнопку **Yes**.

Виртуальная машина с установленной программой Kaspersky Web Traffic Security будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины в консоли управления гипервизора Microsoft Hyper-V

Перед удалением программы требуется выполнить подготовительные действия (см. раздел "Подготовка к удалению программы" на стр. [58](#)).

удалению программы" на стр. [58](#)).

► *Чтобы удалить виртуальную машину в консоли управления гипервизора Microsoft Hyper-V, выполните следующие действия:*

1. Запустите программу Hyper-V Manager.
2. В главном окне программы в списке виртуальных машин гипервизора в таблице **Virtual Machines** выберите виртуальную машину, которую вы хотите удалить.
3. Если виртуальная машина включена, отключите ее. Для этого по правой кнопке мыши откройте контекстное меню и выберите пункт **Shut Down**. Дождитесь отключения машины.
4. В контекстном меню виртуальной машины выберите пункт **Delete**.
5. В окне подтверждения нажмите на кнопку **Delete**.

Виртуальная машина с установленной программой Kaspersky Web Traffic Security будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины с помощью Microsoft SCVMM

Перед удалением программы требуется выполнить подготовительные действия (см. раздел "Подготовка к удалению программы" на стр. [58](#)).

► *Чтобы удалить виртуальную машину с помощью Microsoft SCVMM, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левом нижнем углу окна выберите раздел **VMs and Services**.
3. В дереве в левой верхней панели выберите гипервизор, на котором была создана виртуальная машина.
4. В рабочей области выберите виртуальную машину, которую вы хотите удалить.
5. Если виртуальная машина включена, отключите ее. Для этого в панели инструментов нажмите на кнопку **Shut Down**.
6. В окне подтверждения нажмите на кнопку **Yes**. Дождитесь отключения машины.
7. В панели инструментов нажмите на кнопку **Delete**.
8. В окне подтверждения нажмите на кнопку **Yes**.

Виртуальная машина с установленной программой Kaspersky Web Traffic Security будет удалена и перестанет отображаться в списке виртуальных машин.

Создание учетных записей пользователей

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

При первоначальной настройке программы после установки для соответствия требованиям ИТ.СAB3.Б2.ПЗ рекомендуется создать следующие роли:

- Администратор сервера.
- Администратор безопасности.

Администратору сервера рекомендуется назначить следующие права:

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

Администратору безопасности рекомендуется назначить следующие права:

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

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	63
Проверка работоспособности. Тестовый файл EICAR.....	63

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.
- **Отчеты.** Позволяет формировать отчеты о работе программы.
- **События.** Содержит информацию о событиях, обнаруженных в сетевом трафике.
- **Правила.** Позволяет работать с правилами обработки трафика.
- **Рабочие области.** Позволяет работать с рабочими областями и распределять сетевой трафик.
- **Пользователи.** Позволяет управлять пользователями программы.
- **Узлы.** Позволяет управлять узлами кластера.
- **Параметры.** Содержит разделы **Общие**, **Внешние службы**, **Журналы и события**, **Доступ к программе** и **Встроенный прокси-сервер**, 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.

Начало работы с программой

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

Администратору Kaspersky Web Traffic Security требуется самостоятельно обеспечить защиту передачи данных между браузером и Управляющим узлом. Для обеспечения безопасности также рекомендуется настроить Kerberos-аутентификацию с использованием технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. [201](#)).

Для того, чтобы управлять параметрами программы, вам требуется подключиться к Управляющему узлу. При подключении к Подчиненным узлам вам доступно изменение роли сервера (см. раздел "Изменение роли узла в кластере" на стр. [135](#)) и просмотр состояния других подключенных серверов.

В этом разделе

Настройка сетевых доступов	66
Подключение к веб-интерфейсу программы.....	69
Проверка работы Kaspersky Web Traffic Security в веб-интерфейсе.....	69

Настройка сетевых доступов

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

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

Таблица 3. Сетевые доступы, необходимые для работы программы

Функциональность	Протокол	Порт	Направление	Назначение соединения
Работа с программой через веб-интерфейс	TCP	443	Входящее	Компьютер администратора программы
Technical Support Mode (см. раздел "Подключение к узлам кластера по протоколу SSH" на стр. 137)	TCP	22	Входящее	Компьютер администратора программы

Функциональность	Протокол	Порт	Направление	Назначение соединения
Взаимодействие между узлами кластера (см. раздел "Управление кластером" на стр. 130)	TCP	По умолчанию 9045 (возможно изменить в веб-интерфейсе программы)	Входящее и исходящее	Другие узлы кластера
Соединение с ICAP-сервером (см. раздел "Параметры ICAP-сервера" на стр. 146)	TCP	По умолчанию 1344 (возможно изменить в веб-интерфейсе программы)	Входящее	ICAP-клиенты и балансировщики нагрузки
DNS-запросы	UDP	53	Исходящее	DNS-серверы
Соединение с внешним прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 159)	TCP	По умолчанию 8080 (возможно изменить в веб-интерфейсе программы)	Исходящее	Внешний прокси-сервер
Активация программы (на стр. 36)	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
Обновление баз программы (см. раздел "Обновление баз Kaspersky Web Traffic Security" на стр. 160)	TCP	80, 443	Исходящее	Серверы "Лаборатории Касперского"
KSN	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
KPSN (см. раздел "Настройка использования Kaspersky Private Security Network" на стр. 165)	TCP	443	Исходящее	Сервер KPSN
Соединение с LDAP-сервером (на стр. 166)	TCP	389	Исходящее	Серверы Active Directory
Kerberos-аутентификация в Active Directory (см. раздел "Добавление соединения с LDAP-сервером" на стр. 166)	UDP, TCP	88	Исходящее	Серверы Active Directory

Функциональность	Протокол	Порт	Направление	Назначение соединения
NTLM-аутентификация с помощью технологии единого входа (см. раздел "Настройка NTLM-аутентификации" на стр. 202)	TCP	445	Исходящее	Серверы Active Directory
Интеграция с программой KATA (см. раздел "Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform" на стр. 169)	TCP	По умолчанию 443 (возможно изменить в веб-интерфейсе программы)	Исходящее	Сервер KATA
Работа службы snmpd (см. раздел "Настройка службы snmpd в операционной системе" на стр. 193)	TCP	По умолчанию 705 (возможно изменить в веб-интерфейсе программы)	Исходящее	SNMP-сервер
SNMP-статистика	UDP, TCP	161	Входящее	Внешняя система мониторинга
SNMP-ловушки (см. раздел "Включение и отключение отправки SNMP-ловушек" на стр. 197)	UDP, TCP	162	Исходящее	Внешняя система мониторинга
Доступ в интернет при использовании встроенного прокси-сервера	TCP	Любой	Исходящее	Интернет, интранет
Соединение пользователей с встроенным прокси-сервером (см. раздел "Изменение порта подключения к прокси-серверу" на стр. 204)	TCP	По умолчанию 3128 (возможно изменить в веб-интерфейсе программы)	Входящее	Компьютеры локальной сети организации
NTLM-аутентификация на встроенном прокси-сервере (см. раздел "Настройка NTLM-аутентификации" на стр. 210)	TCP	389, 636	Исходящее	Серверы Active Directory

Функциональность	Протокол	Порт	Направление	Назначение соединения
Синхронизация времени сервера (см. раздел "Настройка времени сервера" на стр. 158)	UDP	123	Исходящее	NTP-серверы

Подключение к веб-интерфейсу программы

Если вы подключаетесь к веб-интерфейсу впервые после установки программы, перед началом работы вам потребуется создать новый кластер (см. раздел "Создание нового кластера" на стр. [130](#)).

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

1. В браузере введите следующий адрес:

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

Откроется страница авторизации веб-интерфейса с запросом имени и пароля пользователя.

2. В поле **Имя пользователя** введите `Administrator`.
3. В поле **Пароль** введите пароль администратора.

Если вы введете неверный пароль пять раз, возможность авторизации будет заблокирована на пять минут.

4. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса программы.

Проверка работы Kaspersky Web Traffic Security в веб-интерфейсе

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

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

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

- <https://www.eicar.org/download/eicar.com>.

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

Если программа настроена верно и в параметрах сервиса Squid выключен SSL Bumping, отобразится сообщение о запрете доступа только к первому ресурсу (<http://www.eicar.org/download/eicar.com>).

4. Откройте веб-сайт, доступ к которому не запрещен, например, <https://www.kaspersky.ru>.

Если программа настроена верно, веб-сайт откроется.

Мониторинг работы программы

В статистике обработанного трафика не учитываются веб-ресурсы, к которым были применены правила обхода (см. раздел "Добавление правила обхода" на стр. 87) или действия **Tunnel** и **Tunnel with SNI check** в рамках обработки SSL-соединений (см. раздел "Расшифровка TLS/SSL-соединений" на стр. 222).

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

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

Недоступно в веб-интерфейсе рабочей области.

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

В общем веб-интерфейсе программы вы можете фильтровать данные мониторинга (см. раздел "Фильтрация данных мониторинга" на стр. 74) по следующим критериям:

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

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

Вы можете создавать новые схемы расположения графиков (см. раздел "Создание новой схемы расположения графиков" на стр. [72](#)), переключаться между сохраненными схемами (см. раздел "Выбор схемы расположения графиков из списка" на стр. [74](#)), а также устанавливать схему, отображаемую по умолчанию (см. раздел "Выбор схемы расположения графиков, отображаемой по умолчанию" на стр. [74](#)).

В этом разделе

Создание новой схемы расположения графиков	72
Изменение схемы расположения графиков	73
Удаление схемы расположения графиков	73
Выбор схемы расположения графиков из списка	74
Выбор схемы расположения графиков, отображаемой по умолчанию	74
Фильтрация данных мониторинга	74

Создание новой схемы расположения графиков

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

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

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

Изменение схемы расположения графиков

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

► Чтобы изменить схему расположения графиков, выполните следующие действия:

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

Схема расположения графиков будет изменена.

Удаление схемы расположения графиков

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

► Чтобы удалить схему расположения графиков, выполните следующие действия:

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

Отобразится подтверждение удаления схемы расположения графиков.

5. Нажмите на кнопку **Удалить**.

Схема расположения графиков будет удалена.

Выбор схемы расположения графиков из списка

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

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

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

Выбор схемы расположения графиков, отображаемой по умолчанию

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

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

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

Фильтрация данных мониторинга

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

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

- Прошедший месяц.
- Прошедший год.

По умолчанию отображаются сведения за последний час.

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

По умолчанию отображаются сведения обо всех узлах.

Недоступно в веб-интерфейсе рабочих областей.

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

По умолчанию отображаются сведения обо всех рабочих областях.

Недоступно в веб-интерфейсе рабочих областей.

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

Отчеты

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

Вы можете создать отчет (см. раздел "Создание отчета" на стр. [76](#)) по заданным критериям на основе статистики из раздела **Мониторинг**. Отчет содержит данные об обработанном трафике выбранной рабочей области за указанный период времени.

После создания отчет доступен для скачивания (см. раздел "Скачивание отчета на компьютер" на стр. [77](#)) в формате PDF.

В этом разделе

Создание отчета	76
Удаление отчета	77
Скачивание отчета на компьютер	77
Просмотр содержимого отчета	77

Создание отчета

► *Чтобы создать отчет, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Отчеты**.
2. Нажмите на кнопку **Создать отчет**.
Откроется окно **Новый отчет**.
3. В раскрывающемся списке **Период** выберите один из следующих периодов, за который вы хотите сформировать отчет:
 - **Прошедшие сутки**.
 - **Прошедшая неделя**.
 - **Прошедший месяц**.
 - **Прошедший год**.
4. В раскрывающемся списке **Рабочая область** выберите рабочую область, данные о которой вы хотите включить в отчет.
Если вы хотите получить данные обо всех рабочих областях, выберите **Глобальная**.
5. В раскрывающемся списке **Язык** выберите язык отчета.
6. Нажмите на кнопку **Добавить**.

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

отчет (см. раздел "Скачивание отчета на компьютер" на стр. [77](#)) на жесткий диск компьютера.

Удаление отчета

► Чтобы удалить отчет, выполните следующие действия:

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

Отчет будет удален.

Скачивание отчета на компьютер

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

► Чтобы скачать отчет на компьютер, выполните следующие действия:

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

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

Просмотр содержимого отчета

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

В заголовке отчета содержится следующая информация:

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

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

- Язык отчета.

Тело отчета включает в себя следующие блоки информации:

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

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

Журнал событий Kaspersky Web Traffic Security

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

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

Программа распределяет записи о событиях по следующим уровням:

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

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

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

В этом разделе

Просмотр журнала событий.....	79
Экспорт событий	80
Настройка отображения таблицы событий	81
Фильтрация системных событий	81
Настройка параметров журнала событий	82

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**;
 - **КАТА**.

3. В раскрываемом 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 раскрываемых списков:
 - a. В левом раскрываемом списке выберите критерий фильтрации.
 - b. В центральном раскрываемом 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 раскрываемом 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. [79](#)) 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 раскрываемом 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 раскрываемых 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.

Фильтрация системных событий

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

Таблица 4. Детали системных событий на русском и английском языках

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

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

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

1. В окне веб-интерфейса программы выберите раздел **События**.
 2. Выберите закладку **Система**.
 3. Нажмите на кнопку **Добавить условие**.
 4. В раскрывающемся списке слева выберите **Сведения**.
 5. В поле ввода справа укажите описание события или фрагмент описания на английском языке.
Например, если вы хотите просмотреть только события запуска обновления, введите `Update started`.
 6. Нажмите на кнопку **Найти**.
- Отобразится таблица событий, удовлетворяющих условиям фильтрации.

Настройка параметров журнала событий

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

Параметры журнала событий не влияют на параметры записи событий по протоколу Syslog (см. раздел "Настройка параметров Syslog" на стр. [178](#)).

► Чтобы настроить параметры журнала событий, выполните следующие действия:

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

- **все события;**
 - **после действий Заблокировать/Перенаправить;**
 - **не записывать.**
- b. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.
 - c. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на сервере.
3. В блоке **КАТА** выполните следующие действия:
- a. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.
 - b. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на сервере.
4. В блоке **Система** в поле **Максимальное количество событий** укажите количество записей о событиях Kaspersky Web Traffic Security, при превышении которого более старые записи будут удалены.

Параметры журнала событий будут настроены.

Работа с правилами обработки трафика

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

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



Kaspersky Web Traffic Security применяет правила в порядке их расположения в таблице правил (см. раздел "Просмотр таблицы правил обработки трафика" на стр. [106](#)) сверху вниз. Если заданные в правиле условия не выполняются, программа переходит к следующему правилу. Как только заданные в очередном правиле условия выполняются, к трафику применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается.

При наличии рабочей области (см. раздел "Управление рабочими областями" на стр. [108](#)) приоритет правил рабочей области определяется положением строки **Правила рабочей области** в таблице общих правил. В этом случае правила также применяются в порядке расположения в таблице сверху вниз. Правила рабочей области будут применены после проверки трафика по всем правилам, расположенным в таблице выше. Если ни одно из правил рабочей области не сработало, программа переходит к проверке трафика по правилам, расположенным в таблице под строкой **Правила рабочей области**.

При установке программы создается *правило обхода по умолчанию*. Согласно этому правилу, доступ к веб-ресурсам, для которых значение HTTP-заголовка Content-Length превышает 10240 КБ, разрешается всем пользователям без выполнения проверки модулями Антивирус и Анти-Фишинг. Это значение обеспечивает баланс между производительностью программы и безопасностью сетевого трафика. Вы можете изменить (см. раздел "Изменение правила обработки трафика" на стр. [97](#)), отключить (см. раздел "Включение и отключение правила обработки трафика" на стр. [99](#)) или удалить (см. раздел "Удаление правила обработки трафика" на стр. [98](#)) правило обхода по умолчанию.

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

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

В этом разделе

Сценарий настройки доступа к веб-ресурсам	85
Добавление правила обхода	87
Добавление правила доступа	88
Добавление правила защиты	90
Настройка инициатора срабатывания правила	91
Настройка фильтрации трафика	92
Добавление исключения для правила обработки трафика	95
Настройка расписания работы правила обработки трафика	97
Изменение правила обработки трафика	97
Удаление правила обработки трафика	98
Создание копии правила обработки трафика	99
Включение и отключение правила обработки трафика	99
Изменение порядка применения правил	100
Работа с группами правил обработки трафика	101
Настройка политики защиты по умолчанию	103
Мониторинг работы правил обработки трафика	104

Сценарий настройки доступа к веб-ресурсам

Совокупность правил обработки трафика позволяет выполнять следующие задачи:

- Разграничивать доступ к веб-ресурсам для сотрудников разных подразделений.
Для этого вы можете использовать существующие доменные группы, если настроена интеграция с Active Directory. Например, вы можете разрешить доступ ко всем веб-ресурсам для группы Администраторы и запретить категории **Социальные сети** или **Программное обеспечение, аудио, видео** для остальных сотрудников.
- Блокировать доступ к веб-ресурсам, запрещенным законами вашей страны.
Для этого вы можете создать правила для всех рабочих областей, распространяющиеся на всех пользователей.
- Контролировать объем трафика.
В целях экономии трафика вы можете запретить или ограничить загрузку мультимедийных файлов, а также доступ к веб-ресурсам, не связанным с работой.
- Получать статистику о запрошенных веб-ресурсах в вашей организации.

Если в правиле обработки трафика выбрано действие **Разрешить**, то пользователь получает доступ к веб-ресурсу, но информация об этом запросе сохраняется в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. [79](#)). 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. [108](#)) и / или групп правил обработки трафика (см. раздел "Работа с группами правил обработки трафика" на стр. [101](#)), если требуется

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

2. Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. [87](#)), если требуется

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

3. Добавление правил доступа и правил защиты

Вы можете добавлять правила доступа (см. раздел "Добавление правила доступа" на стр. [88](#)) и правила защиты (см. раздел "Добавление правила защиты" на стр. [90](#)) как для отдельной рабочей области, так и для всех рабочих областей. Кроме того, правила можно объединять в группы или добавлять их вне групп.

4. Настройка инициатора срабатывания правила (на стр. [91](#))

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

5. Настройка критериев фильтрации трафика

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

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

6. Добавление исключения для правила (см. раздел "Добавление исключения для правила обработки трафика" на стр. [95](#)), если требуется

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

7. Настройка расписания работы правила (см. раздел "Настройка расписания работы правила обработки трафика" на стр. [97](#)), если требуется

Расписание позволяет автоматически отключать правило в заданные часы. Например, вы можете настроить работу правил только в рабочие часы организации или отключить правило в

определенный день.

8. Настройка политики защиты по умолчанию (на стр. [103](#))

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

Добавление правила обхода

Создание правил обхода для отдельных рабочих областей недоступно.

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

► Чтобы добавить правило обхода, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите закладку **Обход**.
Откроется таблица правил обхода.
4. Нажмите на кнопку **Добавить правило**.
Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
 - **Разрешить без проверки**, если вы хотите добавить правило разрешения.

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

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

По умолчанию установлено значение **Заблокировать**.

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

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

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

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

Добавление правила доступа

► Чтобы добавить правило доступа, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите закладку **Доступ**.
Откроется таблица правил доступа.
4. Выполните одно из следующих действий:
 - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
 - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
 - **Заблокировать**, если вы хотите запрещать доступ к веб-ресурсам.

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

Программа будет выполнять проверку по правилам, которые расположены в таблице после этой группы.

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

По умолчанию установлено значение **Заблокировать**.

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

7. Если вы выбрали вариант **Заблокировать** и хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. [151](#)), выполните следующие действия:
 - a. Установите флажок **Введите текст для отображения на странице блокировки**.
 - b. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. [149](#)). Если вы выбрали вариант **Разрешить** и хотите удалять HTTP-заголовки Range, установите флажок **Удалять HTTP-заголовки Range**.

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

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

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

Правило доступа будет добавлено.

Добавление правила защиты

► Чтобы добавить правило защиты, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите закладку **Защита**.
Откроется таблица правил защиты.
4. Выполните одно из следующих действий:
 - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
 - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.Откроется окно добавления правила.
5. Выберите закладку **Общие параметры**.
6. В блоке параметров **Действия** в раскрывающихся списках выберите одно из действий для каждого из следующих параметров:

a. **Вредоносная программа:**

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

По умолчанию установлено значение **Заблокировать, по возможности вылечить**.

b. **Объекты, обнаруженные КАТА, Фишинг, Вредоносная ссылка, Зашифрованный объект и Документ с макросом:**

- **Заблокировать.**
- **Пропустить проверку.**

По умолчанию установлено значение **Заблокировать**.

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

7. Если вы хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. [151](#)), выполните следующие действия:
 - a. Установите флажок **Введите текст для отображения на странице блокировки**.
 - b. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. [149](#)). В поле **Название правила** введите название правила защиты.

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

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

Настройка инициатора срабатывания правила

► Чтобы настроить инициатора срабатывания правила, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
 - **Обход**.
 - **Доступ**.
 - **Защита**.Откроется таблица правил обработки трафика.
4. Выберите правило, для которого вы хотите настроить инициатора срабатывания правила. Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.

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

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

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

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

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

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

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

Настройка фильтрации трафика

Для корректной обработки HTTPS-трафика требуется настроить перехват SSL-соединений на внешнем прокси-сервере (при установке программы из rpm- или deb-пакета) или на встроенном прокси-сервере (см. раздел "Расшифровка TLS/SSL-соединений" на стр. [222](#)) (при развертывании программы из ISO-файла). Если перехват SSL-соединений не настроен, критерии фильтрации трафика не будут применены и проверка веб-ресурса модулями Антивирус и Анти-Фишинг не будет выполняться.

► Чтобы настроить фильтрацию трафика, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

4. Выберите правило, для которого вы хотите настроить критерии фильтрации.
Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Нажмите на кнопку  в блоке **Фильтрация трафика**.
7. В появившемся раскрывающемся списке выберите один из следующих вариантов:

- **Категория.**

С помощью этого критерия вы можете контролировать доступ пользователей к веб-ресурсам какой-либо тематики. Например, вы можете запретить доступ к социальным сетям, выбрав категорию **Социальные сети**. Список веб-категорий, поддерживаемых программой, см. в Приложении 3.

- **URL.**

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

- Если вы хотите добавить в критерии фильтрации URL-адреса, введите их в поле в окне **URL** и нажмите на кнопку **Добавить**.

Если URL-адрес не прошел процесс нормализации, он не будет добавлен в список.

- Если вы хотите добавить в критерии фильтрации протокол или порт сетевых соединений, то в окне **URL** введите в поле любое значение и нажмите на кнопку **Добавить**. В появившихся ниже полях **Протокол** и **Порт** укажите необходимые значения.

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

- **Имя файла.**

Вы можете добавить в критерии фильтрации название конкретного файла или использовать регулярные выражения. Например, вы можете запретить загрузку исполняемых файлов с

расширением exe, указав значение * .exe.

- **Тип файла.**

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

- **Размер файла, КБ.**

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

- **MIME-тип части HTTP-сообщения.**

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

- **MIME-тип HTTP-сообщения.**

С помощью этого критерия вы можете контролировать доступ к объектам в соответствии с их содержимым. Например, вы можете запретить воспроизведение потокового видео-контента, указав значение video/* . Примеры указания MIME-типов объектов см. в Приложении 4.

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

- **MD5.**

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

- **SHA256.**

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

- **Направление трафика.**

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

- **HTTP-метод.**

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

- **HTTP Content-Length, КБ.**

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

заголовок отсутствует, то значение Content-Length считается пустым и не учитывается при обработке трафика.

Доступно только для правил обхода.

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

Добавление исключения для правила обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

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

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

7. Нажмите на кнопку **+ Добавить исключение**.

Появится блок параметров исключения **Исключение**.

8. Добавьте инициатора соединения. Для этого нажмите на кнопку .

9. Укажите следующие параметры:

a. В раскрывающемся списке **Инициатор** выберите один из следующих вариантов:

- **Имя пользователя.**
- **LDAP: group canonicalName.**
- **LDAP: user distinguishedName.**
- **IP-адрес.**
- **User agent.**

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

c. Если вы хотите добавить нового инициатора соединения, повторите действия по добавлению инициатора соединения.

10. Добавьте критерий фильтрации трафика. Для этого нажмите на кнопку .

11. Укажите следующие параметры:

a. В раскрывающемся списке **Фильтрация трафика** выберите один из следующих вариантов:

- **Категория.**
- **URL.**
- **Имя файла.**
- **Тип файла.**
- **Размер файла, КБ.**
- **MIME-тип HTTP-сообщения.**
- **MIME-тип части HTTP-сообщения.**
- **MD5.**
- **SHA256.**
- **Направление трафика.**
- **HTTP-метод.**

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

c. Если вы хотите добавить новый критерий фильтрации, повторите действия по добавлению критерия.

12. Нажмите на кнопку **Сохранить**.

Исключение для правила обработки трафика будет добавлено.

Настройка расписания работы правила обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
 3. Выберите одну из следующих закладок:
 - **Обход**.
 - **Доступ**.
 - **Защита**.Откроется таблица правил обработки трафика.
 4. Выберите правило обработки трафика, расписание работы которого вы хотите настроить. Откроется окно с информацией о правиле.
 5. Нажмите на кнопку **Изменить**.
 6. Выберите закладку **Расписание**.
 7. Если вы хотите отключить правило после наступления запланированной даты, установите флажок **Отключить правило** и во всплывающем календаре укажите дату и время завершения действия правила.
 8. Если вы хотите, чтобы правило действовало в определенные дни недели и часы, выполните следующие действия:
 - a. Установите флажок **Задать расписание действия правила**.
 - b. Установите флажки рядом с названиями дней недели, в которые будет действовать правило.
 - c. Укажите период действия правила.
 9. Нажмите на кнопку **Сохранить**.
- Расписание работы правила обработки трафика будет настроено.

Изменение правила обработки трафика

► Чтобы изменить правило обработки трафика, выполните следующие действия:

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

- для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
- для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

4. Выберите правило обработки трафика, которое вы хотите изменить.
Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.
Откроется окно изменения правила.
6. Внесите необходимые изменения.
7. Нажмите на кнопку **Сохранить**.

Правило обработки трафика будет изменено.

Удаление правила обработки трафика

► Чтобы удалить правило обработки трафика, выполните следующие действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

4. Выберите правило, которое вы хотите удалить.

Откроется окно с информацией о правиле.

5. Нажмите на кнопку **Удалить**.

Отобразится окно подтверждения удаления правила обработки трафика.

6. Нажмите на кнопку **Да**.

Правило обработки трафика будет удалено.

Создание копии правила обработки трафика

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

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

- для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
- для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.

3. Выберите одну из следующих закладок:

- **Обход**.
- **Доступ**.
- **Защита**.

Откроется таблица правил обработки трафика.

4. Выберите правило обработки трафика, которое вы хотите скопировать.

Откроется окно с информацией о правиле обработки трафика.

5. Нажмите на кнопку **Копировать**.

Откроется окно создания правила обработки трафика. Все параметры правила обработки трафика будут скопированы.

6. Измените имя копии правила обработки трафика.

7. Нажмите на кнопку **Добавить**.

Будет создана копия правила обработки трафика.

Включение и отключение правила обработки трафика

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

действия:

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

4. Выберите правило, которое вы хотите включить или отключить.

Откроется окно с информацией о правиле.

5. Выполните одно из следующих действий:
 - Если вы хотите включить правило, нажмите на кнопку **Включить**.
Правило будет включено.
 - Если вы хотите отключить правило, нажмите на кнопку **Отключить**.
Правило будет отключено.

Изменение порядка применения правил

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

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

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

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

5. Нажмите на кнопку **Сохранить**.

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

Работа с группами правил обработки трафика

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

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

Создание группы правил обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

4. Нажмите на кнопку **Добавить группу**.
Откроется окно создания группы правил.
5. В поле **Название** введите название новой группы правил.

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

6. Нажмите на кнопку **Добавить**.
Группа правил обработки трафика будет создана.

Изменение группы правил обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
 - **Доступ**.
 - **Защита**.
4. Выберите группу правил, которую вы хотите изменить.
Откроется окно с информацией о группе правил.
5. Нажмите на кнопку **Изменить**.
6. В поле **Название** введите новое название группы правил.

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

7. Нажмите на кнопку **Сохранить**.
Группа правил обработки трафика будет изменена.

Удаление группы правил обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
 - **Доступ**.
 - **Защита**.
4. Выберите группу правил, которую вы хотите удалить.
Откроется окно с информацией о группе правил.
5. Нажмите на кнопку **Удалить**.
Отобразится окно подтверждения удаления группы правил обработки трафика.
6. Нажмите на кнопку **Да**.
Группа правил обработки трафика будет удалена.

Настройка политики защиты по умолчанию

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

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

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

- Пропустить проверку.
- Фишинг:
 - Заблокировать.
 - Пропустить проверку.
- Вредоносная ссылка:
 - Заблокировать.
 - Пропустить проверку.
- Зашифрованный объект:
 - Заблокировать.
 - Пропустить проверку.
- Документ с макросом:
 - Заблокировать.
 - Пропустить проверку.

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

3. Нажмите на кнопку **Сохранить**.

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

Мониторинг работы правил обработки трафика

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

Обработка запросов пользователей о доступе к веб-ресурсам

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

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

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выберите закладку **Трафик** при ее наличии.
3. Нажмите на кнопку **Добавить условие**.
4. Настройте фильтр по имени обратившегося пользователя:

- a. В левом раскрывающемся списке выберите **Пользователь**.
 - b. В центральном раскрывающемся списке выберите **Равняется**.
 - c. В правом поле введите имя пользователя.
5. Нажмите на кнопку **Добавить условие**.
 6. Настройте фильтр по веб-адресу заблокированного веб-ресурса:
 - a. В левом раскрывающемся списке выберите **URL**.
 - b. В центральном раскрывающемся списке выберите **Равняется**.
 - c. В правом поле введите веб-адрес заблокированного веб-ресурса.
 7. Нажмите на кнопку **Найти**.

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

Получение статистики о доступе к веб-ресурсам

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

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

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

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

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

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

5. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации.
6. Нажмите на кнопку **Экспортировать**.

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

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

Просмотр таблицы правил обработки трафика

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

В таблице правил обработки трафика содержится следующая информация:

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

В правилах обхода возможны следующие действия:

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

В правилах доступа возможны следующие действия:

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

В правилах защиты возможны следующие действия:

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

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

Правило обработки трафика может находиться в одном из следующих состояний:

- **Выключено.**
- **Включено.**

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

Просмотр информации о правиле обработки трафика

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

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
 - **Обход**.
 - **Доступ**.
 - **Защита**.Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, информацию о котором вы хотите просмотреть. Откроется окно с информацией о правиле.

Окно содержит следующие закладки:

1. Общие параметры.

Общие параметры правила обработки трафика:

- a. **Статус** – использование правила обработки трафика при проверке веб-ресурсов.
- b. **Действие** – действие, которое выполняет правило обработки трафика.
- c. **Название правила** – название правила обработки трафика.
- d. **Комментарий** – комментарий к правилу обработки трафика.

2. Исключения.

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

- a. **Инициатор** – инициатор соединения.
- b. **Фильтрация трафика** – фильтр трафика.

3. Расписание.

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

Управление рабочими областями

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

Использование рабочих областей предоставляет следующие возможности:

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

В этом разделе

Сценарий настройки рабочей области.....	108
Просмотр таблицы рабочих областей.....	109
Просмотр информации о рабочей области.....	109
Настройка отображения таблицы рабочих областей	109
Добавление рабочей области	110
Изменение параметров рабочей области	111
Удаление рабочей области	111
Переключение между рабочими областями в веб-интерфейсе программы.....	112

Сценарий настройки рабочей области

Настройка рабочей области включает в себя следующие этапы.

1. Добавление рабочей области (на стр. [110](#))
2. Добавление роли администратора рабочей области (см. раздел "Добавление роли" на стр. [125](#)), если требуется

В программе доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. [123](#)). Вы можете назначить учетной записи администратора одну из этих ролей. Если набор прав для ролей по умолчанию вам не подходит, вы можете добавить новую роль.
3. Назначение роли администратора рабочей области (см. раздел "Назначение роли" на стр. [127](#))

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

Вы можете добавлять несколько администраторов для одной рабочей области или создавать другие роли с нужным вам набором прав доступа.
4. Создание правил обработки трафика для этой рабочей области (см. раздел "Сценарий настройки доступа к веб-ресурсам" на стр. [85](#))

5. Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. [151](#)), если требуется

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

Просмотр таблицы рабочих областей

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

В таблице рабочих областей содержится следующая информация:

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

Просмотр информации о рабочей области

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

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

Окно содержит следующую информацию:

- Закладка **Общие**:
 - **Название** – название рабочей области.
 - **Комментарий** – комментарий к рабочей области.
 - **Закрепить клиентские лицензии за рабочей областью** – количество лицензий, выделенных для этой рабочей области.
 - **Критерии** – критерии для определения трафика рабочей области.
- Закладка **Страница блокировки** – параметры страницы блокировки для рабочей области (см. раздел "Настройка страницы блокировки для рабочей области" на стр. [151](#)).

Настройка отображения таблицы рабочих областей

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

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

Откроется таблица рабочих областей.

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

Должен быть установлен хотя бы один флажок.

4. Если вы хотите обновить информацию о рабочих областях, нажмите на кнопку **Обновить**.
Информация о рабочих областях будет обновлена.
Отображение таблицы рабочих областей будет настроено.

Добавление рабочей области

► Чтобы добавить рабочую область, выполните следующие действия:

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

Критерии вы можете выбрать один из следующих вариантов:

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

9. Нажмите на кнопку **Добавить**.

Рабочая область будет добавлена.

Изменение параметров рабочей области

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

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.
Откроется таблица рабочих областей.
2. Выберите рабочую область, параметры которой вы хотите изменить.
Откроется окно **Просмотреть рабочую область**.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.
Откроется окно **Изменить рабочую область**.
4. Внесите необходимые изменения в параметры рабочей области.
5. Нажмите на кнопку **Сохранить**.

Параметры рабочей области будут изменены.

Удаление рабочей области

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

1. В окне веб-интерфейса программы выберите раздел **Рабочие области**.
Откроется таблица рабочих областей.
2. Выберите рабочую область, которую вы хотите удалить.
Откроется окно с информацией о рабочей области.
3. Нажмите на кнопку **Удалить**.
Отобразится окно подтверждения удаления рабочей области.
4. Нажмите на кнопку **Да**.

Рабочая область будет удалена.

Переключение между рабочими областями в веб-интерфейсе программы

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

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

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

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

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

► Чтобы переключиться между рабочими областями, выполните следующие действия:

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

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

Работа с ролями и учетными записями пользователей

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

Для каждой роли вы можете задать набор прав, которыми будет обладать роль. Кроме того, в программе доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. [123](#)), создаваемые во время установки программы:

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

Удаление и изменение роли по умолчанию недоступно.

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

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

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

В этом разделе

Ролевое разграничение доступа к функциям программы	114
Набор прав для ролей по умолчанию	123
Добавление роли	125
Просмотр информации о роли	125
Изменение параметров роли	126
Удаление роли	127
Назначение роли.....	127
Отзыв роли.....	128
Изменение пароля учетной записи Administrator	128

Ролевое разграничение доступа к функциям программы

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

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

ниже.

Таблица 6. Операции, доступные при назначении прав

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать разделы Мониторинг и Отчеты	Просмотр всей информации в разделах Мониторинг (см. раздел " Мониторинг работы программы " на стр. 71) и Отчеты (см. раздел " Отчеты " на стр. 76).	Да	<p>Просмотр информации в разделе Мониторинг со следующими ограничениями:</p> <ul style="list-style-type: none"> • не отображается график Работоспособность системы; • отсутствует возможность фильтрации по узлам и по рабочим областям. <p>Просмотр, скачивание (см. раздел "Скачивание отчета на компьютер" на стр. 77) и удаление (см. раздел "Удаление отчета" на стр. 77) всех ранее созданных отчетов, а также создание новых отчетов (см. раздел "Создание отчета" на стр. 76) только для текущей рабочей области.</p>
Просматривать события обработки трафика	Просмотр журнала событий (на стр. 79) обработки трафика рабочих областей и вне рабочих областей, а также экспорт событий обработки трафика в разделе События .	Да	Просмотр журнала событий (на стр. 79) обработки трафика рабочих областей, а также экспорт событий обработки трафика в разделе События .

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать системные события	Просмотр журнала системных событий (см. раздел "Просмотр журнала событий" на стр. 79) программы, а также экспорт системных событий программы в разделе События .	Нет	Функциональность отсутствует.
Создавать/изменять правила	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 87), правил доступа (см. раздел "Добавление правила доступа" на стр. 88) и правил защиты (см. раздел "Добавление правила защиты" на стр. 90) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 97) в разделе Правила .	Да	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 87), правил доступа (см. раздел "Добавление правила доступа" на стр. 88) и правил защиты (см. раздел "Добавление правила защиты" на стр. 90) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 97) в разделе Правила .

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать правила	<p>Просмотр таблицы правил обработки трафика (на стр. 106) для рабочих областей и вне рабочих областей в разделе Правила.</p> <p>При назначении этого права пользователь не сможет добавлять или удалять правила, а также изменять их параметры.</p>	Да	<p>Просмотр таблицы правил обработки трафика (на стр. 106) для текущей рабочей области в разделе Правила.</p> <p>При назначении этого разрешения пользователь не сможет добавлять или удалять правила, а также изменять их параметры.</p>
Удалять правила	<p>Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 98) для рабочих областей и вне рабочих областей в разделе Правила.</p>	Да	<p>Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 98) для текущей рабочей области в разделе Правила.</p>
Создавать/изменять рабочие области	<p>Добавление рабочих областей (см. раздел "Добавление рабочей области" на стр. 110) и изменение параметров рабочих областей (см. раздел "Изменение параметров рабочей области" на стр. 111) в разделе Рабочие области.</p>	Да	<p>Функциональность отсутствует.</p>

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать рабочие области	<p>Просмотр таблицы рабочих областей (на стр. 109) в разделе Рабочие области.</p> <p>При назначении этого права пользователь не сможет добавлять и удалять рабочие области, а также изменять их параметры.</p>	Да	Функциональность отсутствует.
Удалять рабочие области	<p>Удаление рабочих областей (см. раздел "Удаление рабочей области" на стр. 111) в разделе Рабочие области.</p>	Да	Функциональность отсутствует.
Создавать/изменять роли	<p>Добавление ролей (см. раздел "Добавление роли" на стр. 125) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 126) в разделе Пользователи.</p>	Да	<p>Добавление ролей (см. раздел "Добавление роли" на стр. 125) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 126) в разделе Пользователи.</p>

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать роли	<p>Просмотр списка ролей для рабочих областей и вне рабочих областей в разделе Пользователи.</p> <p>При назначении этого права пользователь не сможет добавлять или удалять роли, а также изменять их параметры.</p>	Да	<p>Просмотр списка ролей для текущей рабочей области в разделе Пользователи.</p> <p>При назначении этого разрешения пользователь не сможет добавлять или удалять роли, а также изменять их параметры.</p>
Удалять роли	<p>Удаление ролей (см. раздел "Удаление роли" на стр. 127) для рабочих областей и вне рабочих областей в разделе Пользователи.</p>	Да	<p>Удаление ролей (см. раздел "Удаление роли" на стр. 127) для текущей рабочей области в разделе Пользователи.</p>
Создавать/изменять/удалять узлы	<p>Добавление (см. раздел "Добавление узла в кластер" на стр. 133) и удаление узлов кластера (см. раздел "Удаление узла из кластера" на стр. 134), а также изменение их параметров (см. раздел "Изменение параметров узла" на стр. 134) в разделе Узлы.</p>	Нет	<p>Функциональность отсутствует.</p>

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Получать диагностическую информацию	<p>Запуск трассировки (на стр. 259), изменение уровня трассировки (на стр. 260), а также просмотр журналов трассировки (на стр. 260) узлов кластера.</p> <p>При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.</p>	Нет	Функциональность отсутствует.
Проверять целостность данных	<p>Проверка целостности данных (на стр. 136) на узлах кластера.</p> <p>При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.</p>	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать информацию об узлах	<p>Просмотр информации об узлах (см. раздел "Просмотр информации об узле кластера" на стр. 131) в разделе Узлы.</p> <p>При назначении этого права пользователь не сможет добавлять и удалять узлы, а также изменять их параметры.</p>	Нет	Функциональность отсутствует.
Изменять параметры	<p>Изменение параметров программы в разделе Параметры.</p>	Нет	Функциональность отсутствует.
Просматривать параметры	<p>Просмотр параметров программы в разделе Параметры.</p> <p>При назначении этого права пользователь не сможет изменять параметры программы.</p>	Нет	Функциональность отсутствует.
Управлять доступом SSH	<p>Добавление и удаление открытого ключа SSH (см. раздел "Подключение к узлам кластера по протоколу SSH" на стр. 137).</p>	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Создавать/изменять страницу блокировки	Функциональность отсутствует.	Нет	Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 151) для текущей рабочей области.
Просматривать страницу блокировки	Функциональность отсутствует.	Нет	Просмотр страницы блокировки для текущей рабочей области.

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

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

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

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

Набор прав для ролей по умолчанию

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

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

Таблица 8. Набор прав для ролей по умолчанию

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

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

Добавление роли

► Чтобы добавить роль, выполните следующие действия:

1. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
 - Название рабочей области, если вы хотите добавить роль для одной рабочей области.
 - **Глобальная**, если вы хотите добавить роль вне рабочих областей.
2. Выберите раздел **Пользователи**.
3. Откроется список ролей и учетных записей.
4. Нажмите на кнопку **Добавить**.
Откроется окно добавления роли.
5. В поле **Имя** введите имя роли.
6. В списке **Права** установите флажки рядом с теми правами, которыми должна обладать роль (см. раздел "Ролевое разграничение доступа к функциям программы" на стр. [114](#)):
7. Нажмите на кнопку **Добавить**.
Роль будет добавлена.

Просмотр информации о роли

► Чтобы просмотреть информацию о роли, выполните следующие действия:

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

2. Выберите раздел **Пользователи**.

Откроется список ролей и учетных записей.

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

Отобразится следующая информация:

- На закладке **Учетные записи** отображается список учетных записей пользователей, которым назначена выбранная роль. Вы можете отзывать роль (см. раздел "Отзыв роли" на стр. [128](#)) или назначать ее (см. раздел "Назначение роли" на стр. [127](#)) новым пользователям.
- На закладке **Права** отображается набор прав, которые получает пользователь при назначении ему этой роли. Вы можете изменять список прав (см. раздел "Изменение параметров роли" на стр. [126](#)) для выбранной роли.

Изменение параметров роли

Изменение роли Superuser недоступно.

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

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

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
 - Название рабочей области, если вы хотите изменить параметры роли для одной рабочей области
 - **Глобальная**, если вы хотите изменить параметры роли вне рабочих областей.
2. Выберите раздел **Пользователи**.
Откроется список ролей и учетных записей.
3. В блоке параметров **Роли** выберите роль, параметры которой вы хотите изменить, и нажмите на кнопку .
кнопку .
4. В раскрывающемся списке выберите вариант **Изменить**.
Откроется окно **Изменить роль**.
5. Если требуется, измените название роли в поле **Имя**.
6. Если требуется, измените набор прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Права**.
7. Нажмите на кнопку **Сохранить**.
Параметры роли будут изменены.

Удаление роли

Удаление роли Superuser недоступно.

► Чтобы удалить роль, выполните следующие действия:

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
 - Название рабочей области, если вы хотите удалить роль для одной рабочей области.
 - **Глобальная**, если вы хотите удалить роль вне рабочих областей.
2. Выберите раздел **Пользователи**.
Откроется список ролей и учетных записей.
3. В списке **Роли** выберите роль, которую вы хотите удалить.
4. Нажмите на кнопку .
5. В раскрывающемся списке выберите вариант **Удалить**.
Отобразится окно подтверждения удаления роли.
6. Нажмите на кнопку **Да**.
Роль будет удалена.

Назначение роли

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

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
 - Название рабочей области, если вы хотите предоставить пользователю разрешения на параметры одной рабочей области.
 - **Глобальная**, если вы хотите предоставить пользователю разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.
Откроется список ролей и учетных записей.
3. В списке **Роли** выберите роль, которую вы хотите назначить для учетной записи.
4. Нажмите на кнопку **Назначить роль**.
Откроется окно **Назначить роль**.
5. В поле **Учетная запись (домен\имя для NTLM или user@REALM для Kerberos; значение чувствительно к регистру)** введите доменное имя учетной записи, которой вы хотите назначить роль.

6. Нажмите на кнопку **Сохранить**.

Роль будет назначена выбранной учетной записи.

Отзыв роли

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

1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите один из следующих вариантов:
 - Название рабочей области, если вы хотите отозвать у пользователя разрешения на параметры одной рабочей области.
 - **Глобальная**, если вы хотите отозвать у пользователя разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.
Откроется список ролей и учетных записей.
3. В левой части окна выберите роль, которую вы хотите отозвать.
4. На закладке **Учетные записи** установите флажки напротив тех пользователей, у которых вы хотите отозвать роль.
5. Нажмите на кнопку **Отозвать роль**.
6. В окне подтверждения нажмите на кнопку **Да**.

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

Изменение пароля учетной записи Administrator

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

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

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

В первый раз этот пароль задается во время установки программы.

3. В поле **Новый пароль** введите новый пароль, удовлетворяющий требованиям к паролю.
Требования к паролю приведены ниже под полем **Подтвердите пароль**.

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

Управление кластером

После установки и первоначальной настройки вы можете настраивать параметры в веб-интерфейсе программы. Для этого требуется объединить все узлы с установленной программой Kaspersky Web Traffic Security в кластер. Вы можете добавлять узлы в кластер (см. раздел "Добавление узла в кластер" на стр. [133](#)) и удалять узлы из кластера (см. раздел "Удаление узла из кластера" на стр. [134](#)). Вы можете назначить роль Управляющего узла (см. раздел "Изменение роли узла в кластере" на стр. [135](#)) любому из узлов, входящих в кластер. Остальные серверы в кластере получают роль Подчиненный узел. Независимо от роли все узлы кластера будут осуществлять обработку трафика.

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

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

В этом разделе

Создание нового кластера.....	130
Настройка отображения таблицы узлов кластера	131
Просмотр информации об узле кластера	131
Добавление узла в кластер	133
Изменение параметров узла	134
Удаление узла из кластера.....	134
Изменение роли узла в кластере	135
Удаление кластера	136
Проверка целостности данных	136
Подключение к узлам кластера по протоколу SSH.....	137
Перезагрузка узла кластера	137
Работа программы в аварийном режиме	139

Создание нового кластера

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

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

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

2. Через несколько минут обновите страницу браузера.

Откроется веб-интерфейс Управляющего узла.

Кластер будет создан. После этого вы можете добавлять в кластер Подчиненные узлы (см. раздел "Добавление узла в кластер" на стр. [133](#)).

Настройка отображения таблицы узлов кластера

- Чтобы настроить отображение таблицы узлов кластера, выполните следующие действия:

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

Должен быть установлен хотя бы один флажок.

Отображение таблицы узлов кластера будет настроено.

Просмотр информации об узле кластера

- Чтобы просмотреть информацию об узле кластера, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. Выберите узел, информацию о котором вы хотите просмотреть.
Откроется окно с информацией об узле.

Окно содержит следующую информацию в зависимости от типа сервера:

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

Возможны следующие значения:

- **ACRN**.
- **bhyve (гипервизор FreeBSD™)**.
- **Bochs Emulator**.
- **Linux KVM**.
- **Microsoft Hyper-V**.
- **Не используется** – программа установлена на физическом сервере.

- Oracle® VM VirtualBox.
- Parallels Desktop® или Server.
- QEMU.
- QNX.
- UML (user-mode Linux).
- VMware™ Workstation или Server.
- Xen.
- z/VM.

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

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

2. Блок параметров **Обработка трафика**:

- **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.
- **Дата окончания срока действия лицензии**.
- **Лицензия** – информация о лицензии и количестве дней до окончания срока действия лицензии.
- **Тип лицензии** – тип лицензии (пробная или коммерческая).
- **Серийный номер** – серийный номер лицензии.
- **Состояние подключения к KSN/KPSN** – состояние соединения со службами KSN / KPSN.
- **Антивирус** – состояние баз модуля Антивирус.
- **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
- **Отправка файлов в KATA** – наличие или отсутствие ошибок при отправке файлов в KATA (отображается только при включенном режиме **Отправлять файлы** (см. раздел "**Выбор режима интеграции**" на стр. [173](#))).
- **Получение объектов из KATA** – наличие или отсутствие ошибок при получении объектов, обнаруженных KATA (отображается только при включенном режиме **Получать объекты** (см. раздел "**Выбор режима интеграции**" на стр. [173](#))).
- **Обновление баз** – состояние баз программы, а также результат и время их последнего успешного обновления.

3. Блок параметров **Кеш LDAP** (отображается только при настроенной интеграции с доменом Active Directory):

- **Подключение** – дата и время последнего успешного подключения к контроллеру домена Active Directory.
- **Данные для подбора правил** – дата и время последнего успешного обновления данных об учетных записях, используемых для подбора правил обработки трафика.

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

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

4. Блок параметров **Параметры**:

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

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

Добавление узла в кластер

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

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

Вы можете получить отпечаток сертификата с помощью следующей команды:

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

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

Изменение параметров узла

Вы не можете изменить IP-адрес и порт сервера, на котором установлена программа. При необходимости удалите узел из кластера (см. раздел "Удаление узла из кластера" на стр. [134](#)) и добавьте в кластер новый узел (см. раздел "Добавление узла в кластер" на стр. [133](#)) с нужным адресом.

► Чтобы изменить параметры узла, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите узел, параметры которого вы хотите изменить.
Откроется окно параметров узла.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.
Откроется окно **Изменить узел**.
4. Если требуется, измените следующие параметры:
 - Дополнительную информацию об узле в поле **Комментарий**.
 - Количество одновременных потоков обработки трафика ICAP-сервером в поле **Количество потоков проверки**.
Максимально допустимое значение: количество ядер процессора плюс один.
5. Нажмите на кнопку **Сохранить**.

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

Параметры узла будут изменены.

Удаление узла из кластера

Удаление Управляющего узла недоступно.

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

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

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
 2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите удалить из кластера.
Откроется окно параметров узла.
 3. В левом нижнем углу окна нажмите на кнопку **Удалить**.
Отобразится окно подтверждения удаления узла из кластера.
 4. Нажмите на кнопку **Да**.
- Узел будет удален из кластера. Информация об узле не будет отображаться в таблице узлов кластера.

Изменение роли узла в кластере

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

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

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.
Откроется окно параметров узла.
3. Нажмите на кнопку **Назначить роль Подчиненный узел**.
Управляющий узел станет Подчиненным узлом. Откроется веб-интерфейс Подчиненного узла.

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

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел.
Откроется окно параметров узла.
3. Нажмите на кнопку **Перейти к управлению узлом**.
В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль администратора программы.
Откроется веб-интерфейс Подчиненного узла.
5. Нажмите на кнопку **Назначить роль Управляющий узел**.
6. В окне подтверждения нажмите на кнопку **Да**.

Подчиненный узел станет Управляющим узлом.

Удаление кластера

Удаление кластера возможно только при отсутствии Подчиненных узлов.

► Чтобы удалить кластер, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.
Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить кластер**.
Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **Да**.

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

Проверка целостности данных

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

► Чтобы проверить целостность данных, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Проверить целостность данных**.
Откроется окно **Выбор узлов для проверки целостности данных**.
4. В таблице узлов кластера установите флажки напротив тех узлов, для которых вы хотите запустить проверку целостности.
5. Нажмите на кнопку **Запустить**.

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

Подключение к узлам кластера по протоколу SSH

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

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

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

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

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

► Чтобы удалить открытый ключ SSH, выполните следующие действия:

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

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

Перезагрузка узла кластера

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

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

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

следующие действия:

1. В веб-интерфейсе программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.
Откроется окно с информацией об узле.
3. Нажмите на кнопку **Перезагрузить**.
4. В окне подтверждения нажмите на кнопку **Да**.

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

До завершения перезагрузки обработка трафика будет остановлена.

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

1. В веб-интерфейсе программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите перезагрузить.
Откроется окно с информацией об узле.
3. По ссылке **Перейти к управлению узлом** перейдите к веб-интерфейсу Подчиненного узла.
Страница подключения к веб-интерфейсу откроется в новой закладке браузера.
4. Введите учетные данные и подключитесь к Подчиненному узлу.
5. Нажмите на кнопку **Перезагрузить**.
6. В окне подтверждения нажмите на кнопку **Да**.

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

До завершения перезагрузки обработка трафика будет остановлена.

Работа программы в аварийном режиме

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

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

Управляющий узел

В окне аварийного режима на Управляющем узле отображается следующая информация:

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

Таблица узлов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу.
- **Роль** – роль текущего узла в программе.
- **Управляющий узел** – IP-адрес Управляющего узла.
Доступно только для Подчиненного узла.
- **Синхронизированы** – время последней синхронизации значений параметров.
- **Состояние соединения с Управляющим узлом** – доступность Управляющего узла по сети.

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

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

Подчиненный узел

В окне аварийного режима на Подчиненном узле отображается следующая информация:

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

Таблица узлов содержит следующие графы:

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

- **Роль** – роль узла в программе.

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

Защита сетевого трафика

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

- Проверяет сетевой трафик на вирусы, фишинг, вредоносные ссылки, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. [141](#)), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу.
- Лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

В этом разделе

О защите трафика от некоторых легальных программ.....	141
Настройка параметров модуля Антивирус.....	143
Настройка параметров модуля Анти-Фишинг.....	144
Настройка обработки архивов.....	145

О защите трафика от некоторых легальных программ

Легальные программы – программы, разрешенные к установке и использованию на компьютерах пользователей и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред компьютеру пользователя или компьютерной сети организации. Если злоумышленники 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 9. Легальные программы

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

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

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

Настройка параметров модуля Антивирус

► Чтобы настроить параметры модуля Антивирус, выполните следующие действия:

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

По умолчанию выбран уровень эвристического анализа **Средний**.

4. Включите или отключите блокировку объектов, во время проверки которых произошли ошибки, с помощью переключателя **Блокировать объекты с ошибками проверки**.
5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности антивирусной проверки объектов сетевого трафика в секундах.
По умолчанию установлено значение 120.
6. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности проверяемых архивов.
По умолчанию установлено значение 32.
7. Если требуется, установите флажок **Блокировать архивы при превышении уровня вложенности**.

Если флажок снят, архив будет пропущен без выполнения антивирусной проверки. В журнал событий для этого объекта будет записан статус *Проверка не завершена*.

8. Включите или отключите обнаружение некоторых легальных программ с помощью переключателя **Обнаруживать некоторые легальные программы**.

К таким легальным программам (см. раздел "О защите трафика от некоторых легальных программ" на стр. 141) относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями.

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

9. Нажмите на кнопку **Сохранить**.

Параметры модуля Антивирус будут настроены.

Настройка параметров модуля Анти-Фишинг

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

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

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

Если переключатель включен, программа отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.

4. Включите или отключите обнаружение ссылок, связанных с некоторыми легальными программами (см. раздел "О защите трафика от некоторых легальных программ" на стр. 141), с помощью переключателя **Отмечать ссылки, связанные с некоторыми легальными программами, как вредоносные**.

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

Если переключатель включен, программа отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.

5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности проверки объектов сетевого трафика на фишинг в секундах.

По умолчанию установлено значение 120.

6. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Фишинг будут настроены.

Настройка обработки архивов

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

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

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

Пример:

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

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

3. Перезапустите Kaspersky Web Traffic Security.
Архивы будут распаковываться в указанную директорию.

Параметры ICAP-сервера

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

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

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

В этом разделе

Настройка параметров подключения к ICAP-серверу	146
Настройка параметров обработки трафика на ICAP-сервере	147

Настройка параметров подключения к ICAP-серверу

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

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

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

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

обрабатывать трафик с любых серверов.

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

3. Введите порт подключения к ICAP-серверу.

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

4. В поле **Максимальное количество соединений 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 серверах с установленной программой.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **ICAP-сервер**.
2. В поле **Заголовок, содержащий IP-адрес клиента** введите заголовок, который прокси-сервер использует для передачи IP-адреса пользователя прокси-сервера.

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

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

3. В поле **Заголовок, содержащий имя пользователя** введите заголовок, который прокси-сервер использует для передачи имени пользователя прокси-сервера.

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

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

4. Если прокси-сервер передает имена пользователей в кодировке Base64, установите флажок **Имя пользователя в кодировке Base64**.

5. В поле **Путь службы модификации запросов** укажите путь службы Request Modification (REQMOD), которая обрабатывает исходящий трафик.
6. В поле **Путь службы модификации ответов** укажите путь службы Response Modification (RESPMOD), которая обрабатывает входящий трафик.
7. Если вы хотите, чтобы браузер пользователя не прерывал соединение с ошибкой превышения времени ожидания при загрузке объектов большого размера, выполните следующие действия:
 - a. Переведите переключатель **Начинать передачу HTTP-сообщений до окончания их проверки** в положение **Включено**.

Если этот параметр включен, а проверка объекта занимает продолжительное время, Kaspersky Web Traffic Security передает часть объекта браузеру, не дожидаясь завершения проверки. Kaspersky Web Traffic Security продолжает проверять объект по правилам обработки трафика. Если по результатам проверки доступ к объекту разрешен, то объект передается браузеру полностью. Если доступ к объекту запрещен, то сессия браузера прерывается и оставшаяся часть объекта не передается. В этом случае загрузка запрещенного объекта прерывается без объяснения причин. Пользователю не выводится сообщение о запрете загрузки, и не производится перенаправление на другую страницу.
 - b. В поле **Скорость передачи данных (КБ/с)** укажите количество байт, которое будет передаваться браузеру каждую секунду до завершения проверки HTTP-сообщения программой.

Вы можете указать целое число от 1 до 1024.
 - c. В поле **Задержка отправки (сек.)** укажите время задержки в секундах. Программа начнет передавать объект браузеру через указанное количество секунд.

Вы можете указать целое число от 1 до 3600.
8. Нажмите на кнопку **Сохранить**.

Параметры обработки трафика на ICAP-сервере будут настроены.

Страница блокировки

Если в результате проверки веб-ресурса по правилам обработки трафика доступ заблокирован, пользователю отображается страница блокировки.

Вы можете использовать следующие шаблоны страницы блокировки:

- по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. [151](#));
- для рабочих областей (см. раздел "Настройка страницы блокировки для рабочей области" на стр. [151](#));
- для правил обработки трафика (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. [152](#)).

Алгоритм выбора страницы блокировки представлен на рисунке ниже.

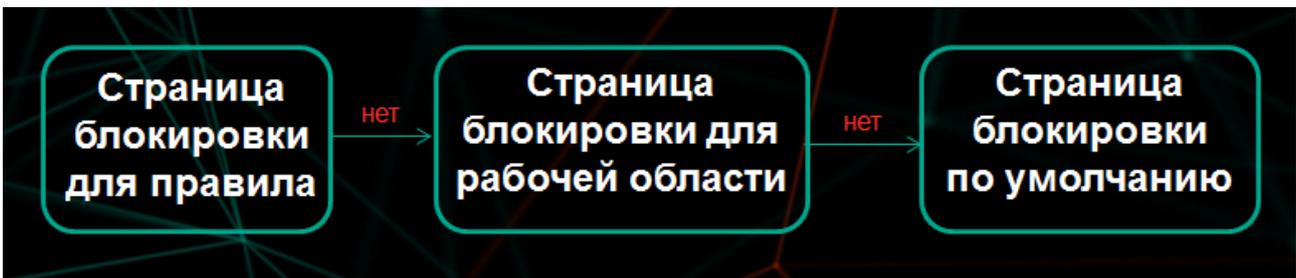


Рисунок 1. Алгоритм применения шаблона для страницы запрета доступа

Если веб-ресурс заблокирован по правилу обработки трафика, в параметрах которого настроена страница блокировки, то пользователю отображается текст, заданный на странице блокировки для этого правила. Если страница блокировки для правила не настроена, то программа проверяет наличие страницы блокировки для рабочей области. Если страница блокировки для рабочей области настроена, то программа использует ее. Если не настроена ни одна страница блокировки, то будет использована страница блокировки по умолчанию.

В этом разделе

Список поддерживаемых макросов	149
Настройка страницы блокировки по умолчанию	151
Настройка страницы блокировки для рабочей области	151
Настройка страницы блокировки для правила обработки трафика	152

Список поддерживаемых макросов

Вы можете использовать следующие макросы в тексте страницы блокировки:

- %DATE% – дата и время события.
- %APPLICATION% – название программы.

- %BUILD% – номер сборки программы.
- %SERVER_NAME% – имя компьютера, на котором был обработан HTTP-запрос.
- %TYPE% – тип HTTP-сообщению (Request или Response).
- %METHOD% – метод HTTP-сообщения.
- %RULE_NAME% – название правила обработки трафика, согласно которому веб-ресурс был заблокирован.
- %THREAT% – имя обнаруженного вредоносного объекта.
- %CURED_LIST% – список угроз, которые были вылечены.
- %SCAN_RESULT% – тип обнаруженной угрозы, которая представляет наибольшую опасность среди всех угроз, обнаруженных в данном объекте.

Например, если в одном объекте обнаружены вирус и фишинговая ссылка (`av_status="detected"` и `ap_status="detected"`), то в качестве значения макроса будет указан вирус.

- %CATEGORY% – категория обработанного веб-ресурса по тематике его содержания.
- %PROCESSING_TIME% – продолжительность обработки HTTP-сообщения.
- %WORKSPACE_NAME% – имя рабочей области, к которой относится обработанный трафик.
- %USER_NAME% – имя учетной записи пользователя, который является источником HTTP-запроса.
- %USER_AGENT% – программа на компьютере пользователя, инициировавшая HTTP-запрос (User Agent).
- %CLIENT_IP% – IP-адрес компьютера, с которого был направлен HTTP-запрос.
- %URL% – URL-адрес веб-сайта, доступ к которому запрещен.
- %MIME_TYPE% – MIME-тип HTTP-сообщения и его частей.
- %FILE_NAME% – имена заблокированных файлов.
- %FILE_TYPE% – тип заблокированных файлов.

Настройка страницы блокировки по умолчанию

► Чтобы настроить страницу блокировки по умолчанию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Страница блокировки по умолчанию**.
2. Если требуется, измените текст страницы в поле **Макрос %ТЕХТ%** и / или разметку страницы в поле **HTML-код**.
3. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. [149](#)).

Вы также можете использовать макрос %ТЕХТ% – содержимое поля **Макрос %ТЕХТ%** (доступен только для поля **HTML-код**).

При наличии нескольких значений в одном макросе эти значения отображаются через запятую.

4. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
5. Нажмите на кнопку **Сохранить**.

Страница блокировки по умолчанию будет настроена. Эта страница будет отображаться, если не настроены страницы блокировки для рабочей области и для сработавшего правила обработки трафика.

Настройка страницы блокировки для рабочей области

Настройка страницы блокировки для рабочей области доступна в общем веб-интерфейсе, а также в веб-интерфейсе рабочей области.

► Чтобы настроить страницу блокировки для рабочей области, выполните следующие действия:

1. Перейдите в раздел настройки страницы блокировки в общем веб-интерфейсе или в веб-интерфейсе рабочей области. Для этого выполните следующие действия:
 - В общем веб-интерфейсе.
2. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите общие параметры.
3. Выберите раздел **Рабочие области**.
4. Выберите рабочую область, для которой вы хотите настроить отдельную страницу блокировки. Откроется окно с информацией о рабочей области.
5. Выберите закладку **Страница блокировки**.
6. В правом нижнем углу нажмите на кнопку **Изменить**.
 - В веб-интерфейсе рабочей области.
7. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите

название нужной рабочей области.

8. Выберите раздел **Параметры рабочей области**.
9. Выберите вариант **Создать индивидуальную страницу блокировки**.
10. Если вы хотите скопировать текст и разметку страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. [151](#)), заданной в общих параметрах, нажмите на ссылку **Скопировать из страницы блокировки по умолчанию** в правом нижнем углу окна.
11. Измените текст страницы в поле **Макрос %ТЕХТ%** и / или разметку страницы в поле **HTML-код**.
12. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. [149](#)).

Вы также можете использовать макрос %ТЕХТ% – содержимое поля **Макрос %ТЕХТ%** (доступен только для поля **HTML-код**).

При наличии нескольких значений в одном макросе эти значения отображаются через запятую.

13. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
14. Нажмите на кнопку **Сохранить**.

Страница блокировки для рабочей области будет настроена. Пользователям, входящим в эту рабочую область, будет отображаться заданный текст. Остальным пользователям будет отображаться страница блокировки по умолчанию.

Если сработало правило, в котором настроена страница блокировки, то используется страница блокировки для правила (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. [152](#)), а не страница для рабочей области или страница по умолчанию.

Настройка страницы блокировки для правила обработки трафика

Вы можете изменить только текст страницы блокировки для отдельного правила обработки трафика. Разметка страницы определяется параметрами страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. [151](#)).

► *Чтобы изменить текст страницы блокировки для правила обработки трафика, выполните следующие действия:*

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

Применимо только при наличии прав доступа к нескольким рабочим областям.

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

Откроется таблица правил обработки трафика.

4. Выберите правило обработки трафика, для которого вы хотите настроить страницу блокировки.
Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.
Откроется окно **Изменить правило**.
6. Установите флажок **Введите текст для отображения на странице блокировки**.
7. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. [149](#)).
При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
9. Нажмите на кнопку **Сохранить**.

Страница блокировки для правила обработки трафика будет настроена.

Экспорт и импорт параметров

Функциональность доступна при наличии у пользователя права **Изменять параметры**.

Экспорт и импорт параметров Kaspersky Web Traffic Security может быть использован для следующих целей:

- Резервное копирование параметров программы.
Если Управляющий узел выйдет из строя, вы сможете импортировать ранее экспортированные параметры после повторной установки программы.
- Развертывание программы на новом сервере.
Вы можете настроить параметры на одном сервере, затем экспортировать их и создать одинаковую конфигурацию программы на всех серверах.
- Миграция программы на новую версию.
Перед обновлением программы вы можете экспортировать параметры из старой версии и импортировать их в новую версию.

Миграция с более новой на более старую версию не поддерживается.

При экспорте параметров (см. раздел "Экспорт параметров Kaspersky Web Traffic Security" на стр. [155](#)) создается конфигурационный файл со следующей информацией:

- Версия программы.
- Параметры программы вне рабочих областей:
 - правила защиты и доступа, не относящиеся к рабочим областям;
 - роли и права пользователей;
 - учетные записи пользователей, имеющих роли вне рабочих областей;
 - страницы блокировки;
 - параметры защиты.
- Параметры рабочих областей:
 - критерии принадлежности трафика к рабочей области;
 - правила защиты и доступа, созданные в рамках рабочей области;
 - роли и права пользователей, относящиеся ко всем рабочим областям.

Созданный конфигурационный файл сохраняется локально на Управляющем узле.

При импорте конфигурационного файла (см. раздел "Импорт параметров Kaspersky Web Traffic Security" на стр. [155](#)) вы можете выбрать, какие параметры должны быть применены:

- отдельные параметры программы вне рабочих областей;
- рабочие области, для которых будут применены все параметры.

При импорте правил защиты из версии 6.0 в версию 6.1 для типа объектов **Вредоносная ссылка** устанавливается действие **Заблокировать**.

Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров Kaspersky Web Traffic Security	155
Импорт параметров Kaspersky Web Traffic Security	155
Настройка хранения экспортированных файлов	156

Экспорт параметров Kaspersky Web Traffic Security

► *Чтобы экспортировать параметры Kaspersky Web Traffic Security, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Экспорт**.
3. Нажмите на кнопку **Экспортировать**.

В блоке **Последние операции экспорта конфигурации** отобразится текущее состояние операции экспорта. После успешного завершения операции отобразится строка с датой и временем экспорта.

4. Нажмите на значок  в нужной строке.

Конфигурационный файл с экспортированными параметрами будет сохранен в папке загрузки браузера.

Импорт параметров Kaspersky Web Traffic Security

Не рекомендуется импортировать несколько конфигурационных файлов одновременно. В этом случае будут применены параметры только из одного файла.

► *Чтобы импортировать параметры Kaspersky Web Traffic Security, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Импорт**.
3. Нажмите на кнопку **Загрузить**.

Откроется окно выбора файлов.

4. Выберите файл с ранее экспортированными параметрами.

Откроется окно **Выберите параметры для импорта**.

5. Установите флажки напротив тех параметров, которые вы хотите импортировать.
6. Установите флажок под таблицей параметров, подтверждающий согласие на импорт.
7. Нажмите на кнопку **Импортировать**.

Отобразится сообщение о результате запуска операции импорта.

Настройка хранения экспортированных файлов

Вы можете ограничить количество экспортированных конфигурационных файлов, которые хранятся на сервере. В случае превышения установленного ограничения ранее экспортированные файлы будут удалены.

► *Чтобы настроить хранение экспортированных файлов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите закладку **Экспорт**.
3. В поле **Максимальное количество хранимых конфигурационных файлов** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.

Количество экспортированных файлов будет ограничено заданным значением.

Обновление программы

Функциональность доступна только при развертывании программы из ISO-образа.

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Web Traffic Security. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, или плановые обновления, добавляющие новые или улучшающие существующие функции программы.

Службы Kaspersky Web Traffic Security могут быть приостановлены на время установки обновления. Процесс обновления может занять несколько минут. После запуска не следует прерывать процесс обновления или выключать сервер. После установки обновлений может потребоваться перезапуск программы.

- ▶ *Чтобы запустить обновление системы на Управляющем узле, выполните следующие действия:*
 1. В веб-интерфейсе программы выберите раздел **Параметры** → **Общие** → **Обновление системы**.
 2. Справа от поля ввода нажмите на кнопку **Обзор**.
Откроется окно выбора файлов.
 3. Выберите архив, содержащий пакет обновлений, и нажмите на кнопку **Отрп**.
Название выбранного архива отобразится в поле ввода.
 4. Нажмите на кнопку **Загрузить файл**.
Запустится мастер установки пакета обновлений. Следуйте указаниям мастера.
- ▶ *Чтобы запустить обновление системы на Подчиненном узле, выполните следующие действия:*
 1. Войдите в веб-интерфейс Подчиненного узла под учетной записью администратора.
 2. В правом верхнем углу нажмите на кнопку **Установить обновление**.
Откроется страница **Установить обновление**.
 3. Справа от поля ввода нажмите на кнопку **Обзор**.
Откроется окно выбора файлов.
 4. Выберите архив, содержащий пакет обновлений, и нажмите на кнопку **Отрп**.
Название выбранного архива отобразится в поле ввода.
 5. Нажмите на кнопку **Загрузить файл**.
Запустится мастер установки пакета обновлений. Следуйте указаниям мастера.

Настройка времени сервера

Функциональность доступна только при развертывании программы из ISO-образа.

Вы можете настроить время сервера, используемое в параметрах программы. Обновления баз и правила обработки трафика, для которых задано расписание, будут применяться согласно установленному времени.

► Чтобы настроить время сервера, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Общие** → **Дата и время**.
2. В блоке параметров **Часовой пояс** выполните следующие действия:
 - a. В раскрывающемся списке **Страна** выберите страну, к которой относится нужный часовой пояс.
 - b. В раскрывающемся списке **Часовой пояс** выберите часовой пояс.Выбранный часовой пояс будет выделен на карте под раскрывающимся списком.
3. В блоке параметров **Синхронизация времени** включите или отключите синхронизацию с NTP-сервером с помощью переключателя **Синхронизировать с NTP-сервером**.

Если вы развернули программу из ISO-образа на виртуальной машине VMware, то при включении синхронизации с NTP-сервером синхронизация времени с гипервизором будет отключена автоматически. Если вы используете другой гипервизор, вам требуется самостоятельно отключить синхронизацию в параметрах гипервизора.

4. Если вы включили синхронизацию с NTP-сервером, в поле **NTP-сервер** введите полное доменное имя (FQDN) или IP-адрес NTP-сервера в формате IPv4 или IPv6.
5. Если вы хотите добавить еще один NTP-сервер для синхронизации, нажмите на кнопку  и в появившемся поле ввода укажите его адрес.
6. Нажмите на кнопку **Сохранить**.

Время сервера будет настроено. Внесенные изменения будут сохранены на Управляющем узле и распространены на все узлы кластера. Состояние синхронизации времени будет отображаться в информации о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. [131](#)).

Настройка параметров соединения с прокси-сервером

Заданные параметры прокси-сервера будут использованы для обновления баз, активации программы и работы внешних служб.

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с прокси-сервером**.
2. Включите переключатель рядом с параметром **Использовать прокси-сервер**.
3. В блоке параметров **Адрес прокси-сервера** введите адрес и порт прокси-сервера.
4. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси для локальных адресов**.
5. Если вы хотите использовать аутентификацию при подключении к прокси-серверу, в полях **Имя пользователя (необязательно)** и **Пароль (необязательно)** введите имя пользователя и пароль подключения к прокси-серверу.
6. Нажмите на кнопку **Сохранить**.

Обновление баз Kaspersky Web Traffic Security

Базы модулей *Антивирус* и *Анти-Фишинг* (далее также "базы") представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Эти записи содержат информацию о контрольных участках вредоносного кода и алгоритмы лечения объектов, в которых содержатся угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Чтобы свести риск заражения защищаемого сервера к минимуму, рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений, загружая их с веб-сайта "Лаборатории Касперского".

Во время установки Kaspersky Web Traffic Security получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". Это специальные интернет-сайты, на которые выкладываются обновления баз и программных модулей для всех программ "Лаборатории Касперского". Если для доступа в интернет вы используете прокси-сервер, вам нужно настроить параметры соединения с прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. [159](#)).

Чтобы уменьшить интернет-трафик, вы можете выбрать *пользовательский источник обновлений* (см. раздел "Выбор источника обновлений баз" на стр. [160](#)). Это могут быть указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

В этом разделе

Выбор источника обновлений баз	160
Настройка расписания и параметров обновления баз	161
Запуск обновления баз вручную	162

Выбор источника обновлений баз

► Чтобы выбрать источник обновлений баз, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В раскрывающемся списке **Источник обновлений** выберите один из следующих источников обновлений:
 - Серверы "Лаборатории Касперского" (безопасное соединение).
 - Серверы "Лаборатории Касперского" (небезопасное соединение).
 - Пользовательский.

3. Если на предыдущем шаге вы выбрали **Пользовательский**, в поле **Пользовательский источник** укажите URL-адрес пользовательского источника, из которого вы хотите получать пакеты обновлений.

Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории Касперского"**, если вы хотите получать пакеты обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен.

4. Нажмите на кнопку **Сохранить**.

Настройка расписания и параметров обновления баз

Программа загружает обновления баз из выбранного источника обновлений на все узлы кластера.

► *Чтобы настроить расписание и параметры обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В блоке параметров **Расписание** в раскрывающемся списке выберите один из вариантов и выполните следующие действия:
 - **Вручную**.
 - **Один раз**. В появившемся поле укажите дату и время запуска обновления баз.
 - **Ежедневно**. В появившемся поле укажите время ежедневного запуска обновления баз.
 - **Еженедельно**. В появившихся полях укажите день недели и время запуска обновления баз.
 - **Ежемесячно**. В появившихся полях укажите день месяца и время запуска обновления баз.
 - **Запускать каждые**. В появившихся полях укажите периодичность запуска обновления баз в минутах, часах или днях.

Первое обновление баз запустится сразу после сохранения внесенных изменений.

3. В поле **Случайное отклонение (мин)** укажите интервал отклонения от заданного расписанием времени в минутах. Программа будет запускать обновление баз не на всех узлах одновременно, а случайным образом в течение заданного интервала. Рекомендуется использовать эту опцию для распределения нагрузки на сеть при большом количестве узлов в кластере.
4. В поле **Максимальная длительность (мин)** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.
5. Переведите переключатель **Запускать пропущенные задачи** в положение **Включено**, если вы хотите запускать пропущенные задачи обновления баз при последующем запуске программы.

Если запуск пропущенных задач выключен, то пропущенные задачи обновления баз не будут запущены при последующем запуске программы. Следующий запуск обновления баз будет выполнен согласно расписанию.
6. Нажмите на кнопку **Сохранить**.

Запуск обновления баз вручную

- Чтобы запустить обновление баз вручную, выполните следующие действия:
1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
 2. В верхней части окна **Параметры** нажмите на кнопку **Обновить базы**.
Появится сообщение о запуске обновления баз.

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	164
Настройка использования Kaspersky Private Security Network	165

Настройка участия в Kaspersky Security Network

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network.

► Чтобы настроить участие в Kaspersky Security Network, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **KSN/KPSN**.
2. Выберите один из следующих вариантов:
 - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
 - **Kaspersky Security Network (KSN)**, если вы хотите участвовать в Kaspersky Security Network.
3. Если вы выбрали участие в Kaspersky Security Network, в блоке **Положение о KSN** просмотрите Положение о Kaspersky Security Network и выполните следующие действия:
 - Если вы согласны с условиями, установите флажок **Я согласен участвовать в KSN**.
 - Если вы не согласны с условиями, снимите флажок **Я согласен участвовать в KSN**.
4. Если вы хотите участвовать в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", установите флажок **Отправлять KSN-статистику для повышения уровня обнаружения угроз**.
5. Если вы выбрали участие в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", в блоке **Дополнительное Положение о KSN** просмотрите Дополнительное Положение о Kaspersky Security Network и выполните следующие действия:
 - Если вы согласны с условиями, установите флажок **Я согласен отправлять KSN-статистику**.
 - Если вы не согласны с условиями, снимите флажок **Я согласен отправлять KSN-статистику**.
6. Нажмите на кнопку **Сохранить**.

Участие в Kaspersky Security Network будет настроено.

Настройка использования Kaspersky Private Security Network

► Чтобы настроить использование Kaspersky Private Security Network, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите один из следующих вариантов:
 - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
 - **KPSN**, если вы хотите использовать Kaspersky Private Security Network.
3. Если вы выбрали использование Kaspersky Private Security Network, в блоке **Конфигурационный файл KPSN** загрузите конфигурационный файл KPSN. Для этого выполните следующие действия:
 - a. Нажмите на кнопку **Загрузить**.
Откроется окно выбора файлов.
 - b. Выберите конфигурационный файл KPSN, который вы хотите добавить.
Для получения конфигурационного файла необходимо включить компонент Additional Services в программе KPSN, а затем отправить запрос в "Лабораторию Касперского". Более подробную информацию вы можете найти в *Руководстве администратора Kaspersky Private Security Network*.
Конфигурационный файл KPSN должен быть в формате ZIP-архива.
4. Нажмите на кнопку **Open**.
Окно выбора файлов закроется.
5. Нажмите на кнопку **Сохранить**.
Использование Kaspersky Private Security Network будет настроено.

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. [84](#));
- создавать учетные записи пользователей (см. раздел "Работа с ролями и учетными записями пользователей" на стр. [114](#)) для работы с Kaspersky Web Traffic Security.

В этом разделе

Добавление соединения с LDAP-сервером	166
Удаление соединения с LDAP-сервером	167
Изменение параметров соединения с LDAP-сервером	167
Запуск синхронизации с контроллером домена Active Directory вручную	168

Добавление соединения с LDAP-сервером

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

Если вы настраиваете интеграцию с доменом, в названии которого содержится корневой домен `.local`, то для успешного соединения с LDAP-сервером требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы `avahi-daemon`. Для этого выполните команду:

```
systemctl status avahi-daemon
```

2. Если служба запущена, остановите ее. Для этого выполните команду:

```
systemctl stop avahi-daemon
```

3. Отключите автоматический запуск службы. Для этого выполните команду:

```
systemctl disable avahi-daemon
```

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

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Добавить**.
Откроется окно **Добавить соединение**.
3. В поле **Имя** введите имя LDAP-сервера, которое будет отображаться в веб-интерфейсе Kaspersky Web Traffic Security.

4. В блоке параметров **Keytab-файл** нажмите на кнопку **Загрузить**, чтобы загрузить keytab-файл.
Откроется окно выбора файла.
5. Выберите keytab-файл и нажмите на кнопку **Open**.
6. В поле **База поиска** введите *DN (Distinguished Name – уникальное имя)* объекта каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей.

Вводите суффикс каталога в формате `ou=<название подразделения>` (если требуется), `dc=<имя домена>`, `dc=<имя родительского домена>`.

Например, вы можете ввести `ou=people`, `dc=example`, `dc=com`.

Здесь `people` – уровень в схеме каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей (поиск осуществляется на уровне `people` и ниже. Объекты, расположенные выше этого уровня, исключаются из поиска), `example` – доменное имя каталога, в котором Kaspersky Web Traffic Security осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

7. Нажмите на кнопку **Добавить**.

Соединение с LDAP-сервером будет добавлено.

Удаление соединения с LDAP-сервером

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

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, который вы хотите удалить.
Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Удалить**.
Откроется окно подтверждения.
4. Нажмите на кнопку **Да**.

Соединение с LDAP-сервером будет удалено.

Изменение параметров соединения с LDAP-сервером

► *Чтобы изменить параметры соединения с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.
Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Изменить**.

4. Если требуется, измените следующие параметры:
 - Имя LDAP-сервера, которое отображается в веб-интерфейсе программы, в поле **Имя**.
 - Keytab-файл, нажав на кнопку **Заменить**.
 - Каталог, начиная с которого программа осуществляет поиск записей, в поле **База поиска**.
5. Нажмите на кнопку **Сохранить**.

Параметры соединения с LDAP-сервером будут изменены.

Запуск синхронизации с контроллером домена Active Directory вручную

Программа выполняет автоматическую синхронизацию данных с контроллером домена Active Directory каждые 30 минут. Если вам требуется обновить данные об учетных записях пользователей немедленно (например, при добавлении нового пользователя), вы можете запустить синхронизацию вручную.

► *Чтобы запустить синхронизацию с контроллером домена Active Directory вручную, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Синхронизировать**.

Синхронизация данных с контроллером домена будет запущена. В результате будут обновлены данные об учетных записях пользователей, используемые при подборе правил и при автозаполнении имен пользователей в веб-интерфейсе программы.

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. [131](#)).

Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform

Настройка интеграции с программой Kaspersky Anti Targeted Attack Platform (далее также "КАТА") доступна только при наличии у пользователя права **Изменять параметры**.

Kaspersky Anti Targeted Attack Platform – решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats.

Программа КАТА позволяет интегрироваться с другими программами "Лаборатории Касперского", чтобы получать и обрабатывать проверяемые ими объекты. В качестве такой программы может выступать Kaspersky Web Traffic Security.

Администратору Kaspersky Web Traffic Security требуется выполнить настройку интеграции КАТА (см. раздел "Сценарий настройки интеграции с программой КАТА" на стр. [171](#)) на Управляющем узле. После этого параметры интеграции отправляются на все Подчиненные узлы, входящие в кластер. Далее каждый узел кластера взаимодействует с сервером КАТА самостоятельно, независимо от других узлов.

При интеграции с программой КАТА доступно два режима: отправка файлов на сервер КАТА и получение объектов, обнаруженных программой КАТА.

Отправка файлов на сервер КАТА

Kaspersky Web Traffic Security отправляет на сервер КАТА объекты, которые не были заблокированы правилами обработки трафика или политикой защиты по умолчанию. При этом программа не ожидает от сервера КАТА результатов проверки этих объектов.

При обработке каждого файла программа проверяет необходимость отправки его на сервер КАТА. По результатам в журнал событий программы (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. [79](#)) записывается статус проверки. Возможны следующие статусы:

- *Неприменимо. Нет файла для проверки* – HTTP-сообщение не содержит файлов для проверки.
- *Отключено согласно параметрам программы* – режим отправки файлов на сервер КАТА отключен в параметрах программы.
- *Пропущено согласно действию правила* – HTTP-сообщение было заблокировано программой (применены действия **Заблокировать** или **Перенаправить**) или пропущено по правилу обхода без проверки.
- *Отклонено фильтром КАТА* – файл не удовлетворяет условиям отправки на сервер КАТА.
- *Запланировано* – отправка файла запланирована.
- *Завершено с ошибкой* – запланировать отставку файла не удалось.

Для файлов со статусами *Запланировано* и *Завершено с ошибкой* в журнал также записывается подробная информация о результате отправки файла.

Все события, связанные с отправкой файлов на сервер КАТА, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на

сервер KATA" на стр. [190](#)).

Получение объектов, обнаруженных программой KATA

Kaspersky Web Traffic Security получает от сервера KATA информацию об объектах, обнаруженных программой KATA с помощью технологий Sandbox и YARA. Подробнее об этих технологиях см. *Справку Kaspersky Anti Targeted Attack Platform*.

Информация о полученных объектах сохраняется в кеш KATA. Каждый узел кластера хранит свой кеш KATA и получает объекты, обнаруженные программой KATA, независимо от других узлов. По истечении времени хранения информация об объектах удаляется из кеша. Эти объекты больше не учитываются при применении правил защиты (см. раздел "Добавление правила защиты" на стр. [90](#)) и политики защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. [103](#)).

В правилах защиты и в политике защиты по умолчанию вы можете настроить действия над объектами, информация о которых была получена с сервера KATA. При обнаружении в трафике пользователя таких объектов Kaspersky Web Traffic Security будет обрабатывать их согласно заданным в правилах параметрам. Это позволяет блокировать потенциально опасные объекты до того, как информация о них была добавлена в репутационные базы KSN, а также в локальные базы программы.

Результат проверки каждого объекта записывается в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. [79](#)). Возможны следующие статусы проверки:

- *Не обнаружено* – соответствий в кеше KATA не обнаружено.
- *Обнаружено* – обнаружены угрозы.
- *Не проверен* – проверка не выполнялась согласно параметрам программы.
- *Ошибка проверки* – проверка завершилась с ошибкой.

Все события, связанные с проверкой трафика на соответствие объектам KATA, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. [179](#)).

В этом разделе

Сценарий настройки интеграции с программой KATA.....	171
Добавление сервера KATA.....	171
Изменение сервера KATA.....	172
Удаление сервера KATA.....	172
Выбор режима интеграции	173
Пересоздание сертификата KWTS.....	173
Настройка параметров кеша KATA	174
Мониторинг интеграции KATA	174
Настройка отправки HTML-файлов в KATA	176

Сценарий настройки интеграции с программой КАТА

Настройка интеграции Kaspersky Web Traffic Security с программой КАТА состоит из следующих этапов.

1. Добавление сервера КАТА (на стр. [171](#))

При добавлении сервера КАТА требуется сверить отпечатки сертификата, отображаемые в веб-интерфейсах KWTS и КАТА. Если отпечатки совпадают, администратор подтверждает добавление сервера. После этого Управляющий узел отправляет адрес и сертификат сервера КАТА на все узлы кластера, не дожидаясь подтверждения авторизации.

2. Выбор режима интеграции (на стр. [173](#))

В Kaspersky Web Traffic Security доступно два режима интеграции с программой КАТА. Вы можете отправлять файлы на проверку в КАТА (в этом случае KWTS выступает в качестве внешней системы для программы КАТА) и/или получать информацию об объектах, обнаруженных программой КАТА. Эти режимы работают независимо друг от друга.

3. Настройка параметров кеша КАТА (на стр. [174](#))

При применении правил защиты и политики по умолчанию Kaspersky Web Traffic Security учитывает объекты, информация о которых хранится в кеше КАТА. Вы можете настраивать период их хранения в кеше, по истечении которого эти объекты перестают учитываться при обработке трафика.

4. Авторизация Kaspersky Web Traffic Security в веб-интерфейсе программы КАТА

Во время добавления сервера КАТА отправляется запрос на авторизацию внешней системы. Администратору КАТА требуется подтвердить этот запрос в веб-интерфейсе КАТА. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

Добавление сервера КАТА

Вы можете настроить интеграцию только с одним сервером КАТА.

► Чтобы добавить сервер КАТА, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция КАТА**.
2. В блоке параметров **Сервер КАТА** нажмите на кнопку **Добавить**.
Откроется окно **Добавление сервера КАТА**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес сервера КАТА, на котором установлен компонент Central Node.
4. В поле **Порт** введите порт подключения к серверу КАТА.
По умолчанию указано значение 443.
5. Нажмите на кнопку **Далее**.
Откроется окно **Подтверждение сервера КАТА**.
6. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера КАТА. Если отпечатки совпадают,

нажмите на кнопку **Подтвердить**.

Сервер KATA будет добавлен. Информация о сервере отобразится в разделе **Интеграция KATA**, в блоке параметров **Сервер KATA**.

Изменение сервера KATA

В программе доступна интеграция только с одним сервером KATA. Если вы хотите настроить интеграцию с другим сервером, вы можете изменить сервер KATA.

► *Чтобы изменить сервер KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Заменить**.
Откроется окно **Изменение сервера KATA**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес нового сервера KATA, на котором установлен компонент Central Node.
4. Нажмите на кнопку **Далее**.
Откроется окно **Подтверждение сервера KATA**.
5. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет изменен.

Удаление сервера KATA

► *Чтобы удалить сервер KATA, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Удалить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Сервер KATA будет удален. Информационные панели об интеграции с программой KATA в разделах **Мониторинг** и **Узлы** перестанут отображаться. Записи об обработанных ранее объектах в журнале событий программы и в журнале Syslog не будут удалены.

Выбор режима интеграции

Выбор режима интеграции доступен только при добавленном сервере KATA (см. раздел "Добавление сервера KATA" на стр. [171](#)).

► Чтобы выбрать режим интеграции с программой KATA, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Режим интеграции KATA** включите нужный режим интеграции с помощью следующих переключателей:

- **Получать объекты.**

Kaspersky Web Traffic Security будет получать объекты, обнаруженные программой KATA, и использовать информацию об этих объектах в правилах защиты и в политике защиты по умолчанию.

- **Отправлять файлы.**

Kaspersky Web Traffic Security будет авторизован в программе KATA в качестве внешней системы. Файлы из проверяемого трафика пользователей, удовлетворяющие заданным в программе критериям, будут отправляться в KATA. Kaspersky Web Traffic Security не будет ожидать результатов проверки отправленных файлов.

Эти режимы работают независимо друг от друга. Вы можете включить один из режимов или оба режима одновременно.

3. Нажмите на кнопку **Сохранить**.

Режим интеграции с программой KATA будет выбран. В зависимости от выбранного режима в разделе **Узлы** отобразятся информационные панели о состоянии интеграции (см. раздел "Мониторинг интеграции KATA" на стр. [174](#)).

Пересоздание сертификата KWTS

При компрометации сертификата Kaspersky Web Traffic Security администратор программы KATA может отменить авторизацию KWTS как внешней системы. В этом случае вам требуется создать новый сертификат в веб-интерфейсе KWTS и пройти процедуру авторизации в программе KATA повторно (см. раздел "Сценарий настройки интеграции с программой KATA" на стр. [171](#)).

► Чтобы пересоздать сертификат для авторизации KWTS в программе KATA, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Учетные данные KWTS** нажмите на кнопку **Создать новый сертификат**.
3. В окне подтверждения нажмите на кнопку **Да**.

Новый сертификат KWTS будет создан. В блоке параметров **Учетные данные KWTS** отобразятся SensorID и отпечаток нового сертификата.

Настройка параметров кеша КАТА

Если включен режим **Получать объекты**, то Kaspersky Web Traffic Security сохраняет информацию об объектах, обнаруженных программой КАТА, на всех узлах кластера в кеше КАТА. При применении правил защиты и политики по умолчанию учитываются объекты, информация о которых хранится в кеше КАТА.

► *Чтобы настроить параметры кеша КАТА, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Интеграция КАТА**.
2. В блоке параметров **Кеш КАТА** в поле **Срок хранения кеша (часы)** введите время хранения информации об объектах, обнаруженных программой КАТА, в часах.
Допустимые значения – от 1 до 48. По умолчанию установлено значение 48.
3. Если вы хотите очистить кеш КАТА, нажмите на кнопку **Очистить кеш** и в окне подтверждения нажмите на кнопку **Да**.

Информация об этой операции записывается в журнал событий программы (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 79), а также в журнал операционной системы по протоколу Syslog (см. раздел "Журнал событий Syslog" на стр. 178).

Параметры кеша КАТА будут настроены.

Мониторинг интеграции КАТА

► *Чтобы проверить состояние интеграции Kaspersky Web Traffic Security с программой КАТА, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Узлы**.

Откроется страница с информацией об узлах кластера. На странице отображаются следующие информационные панели об интеграции с программой КАТА:

- **Отправка файлов в КАТА.** Количество узлов кластера со статусами отправки файлов на сервер КАТА:
 - *Без ошибок.* Все файлы успешно отправлены на сервер КАТА.
 - *Отключено.* Режим интеграции **Отправлять файлы** отключен.
 - *С ошибкой.* Во время отправки файлов на сервер КАТА за последний час произошли ошибки.
- **Получение объектов из КАТА.** Количество узлов кластера со статусами получения объектов, обнаруженных программой КАТА:
 - *Без ошибок.* Все объекты, обнаруженные программой КАТА, получены успешно.

- *Отключено.* Режим интеграции **Получать объекты** отключен.
 - *С ошибкой.* Во время получения объектов, обнаруженных программой KATA, произошли ошибки.
2. Перейдите по ссылке **Подробные сведения** в одной из информационных панелей об интеграции с программой KATA.
Откроется страница **Интеграция KATA**.
 3. В правом верхнем углу в раскрывающихся списках выберите период отображения данных, а также узлы кластера, статистику о которых вы хотите посмотреть.

На странице **Интеграция KATA** отобразится следующая информация:

- График **Отправка файлов в KATA**.

Отображается только при включенном режиме **Отправлять файлы**.

График показывает, какое количество файлов было отправлено на сервер KATA за выбранный период времени. Линии графиков представляют следующие статусы отправки файлов:

- *Успешно.*
- *Не удалось отправить файлы на сервер KATA из-за переполнения буфера.*
- *Ошибка.*
- Диаграмма **Детальная информация об ошибках**.

Отображается только при включенном режиме **Отправлять файлы**.

Детальная информация о типах ошибок, возникших при отправке файлов на сервер KATA, представлена в виде круговой и столбчатой диаграмм. Круговая диаграмма показывает соотношение количества ошибок определенного типа к общему количеству всех ошибок. Столбчатая диаграмма показывает количество ошибок определенного типа в заданном интервале времени.

Возможны следующие типы ошибок:

- Не удалось установить соединение с сервером KATA.
- SSL-сертификат сервера KATA не совпадает с доверенным.
- Требуется авторизация на сервере KATA.
- Превышено время ожидания соединения с сервером KATA.
- HTTP-код 4xx: ошибка клиента.
- HTTP-код 5xx: ошибка сервера.
- Внутренняя ошибка.
- Таблица **Состояние интеграции KATA**.

В таблице представлена сводная информация об обработанных объектах по узлам кластера. Таблица содержит следующие графы:

- **IP-адрес:порт.**

IP-адрес и порт узла кластера, который интегрирован с программой KATA.

- **Отправка файлов в KATA.**

Статус отправки файлов из трафика этого узла кластера на сервер KATA. Возможны следующие значения:

- *ОК.*
- *Ошибка.*
- *Выключено.*

- **Получение объектов из KATA.**

Статус получения объектов, обнаруженных программой KATA, на этом узле кластера. Возможны следующие значения:

- *ОК.*
- *Ошибка.*
- *Выключено.*

- **Количество объектов в кеше KATA.**

Количество объектов, обнаруженных программой KATA, которые были сохранены на всех узлах кластера в кеше KATA.

Если включен только один из режимов интеграции KATA, отображаются только графы, относящиеся к этому режиму.

Настройка отправки HTML-файлов в KATA

Действия, описанные в этом разделе, требуется выполнить на каждом узле кластера.

По умолчанию файлы формата HTML не отправляются в KATA. Вы можете настроить фильтр для отправки HTML-файлов в KATA по формату файла или по регулярным выражениям.

► *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по формату файла, выполните следующие действия:*

1. В файле с параметрами фильтра KATA `/var/opt/kaspersky/kwts/kata-filters.json` добавьте в секцию `includeFormats` новую строку следующего формата:

```
{"contentFormat": "<формат файла>", "nameMask": "<маска имени файла>"}
```

Возможные значения ключа `contentFormat`:

- `GeneralHtml`;

- `GeneralHtmlStrict`.

Возможные значения ключа `nameMask`:

- `*.html;`
- `*.htm;`
- `*.xhtml;`
- `*.xht;`
- `*.xml.`
- `*`.

Если вы хотите добавить несколько значений, то для каждого значения требуется добавить отдельную строку.

2. Перезагрузите компьютер с установленной программой Kaspersky Web Traffic Security.

Изменения, внесенные в конфигурационный файл фильтра KATA, будут применены. Программа будет отправлять в KATA все HTML-файлы, формат и имя которых соответствуют записям в конфигурационном файле.

- *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по регулярным выражениям, выполните следующие действия:*

1. Убедитесь, что в файле с параметрами фильтра KATA `/var/opt/kaspersky/kwts/kata-filters.json` в секции `includeFormats` отсутствуют записи об HTML-файлах.
2. Переименуйте файл с регулярными выражениями для фильтра KATA, расположенный по пути `/var/opt/kaspersky/kwts/kata-html-regex_sample.txt`, в `kata-html-regex.txt`.
3. Перезагрузите компьютер с установленной программой Kaspersky Web Traffic Security.

Программа будет отправлять в KATA только те HTML-файлы, которые удовлетворяют регулярным выражениям, указанным в файле `kata-html-regex.txt`.

Журнал событий Syslog

Вы можете настроить запись событий обработки трафика (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. [179](#)), системных событий программы (см. раздел "Содержание syslog-сообщений о системных событиях программы" на стр. [187](#)) и событий отправки файлов на сервер KATA (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на сервер KATA" на стр. [190](#)) в журнал событий по протоколу Syslog (далее также "журнал событий Syslog"). Это позволит импортировать события в стороннюю SIEM-систему.

Информация о событиях записывается в отдельной категории журнала, установленной в параметрах Syslog (см. раздел "Настройка параметров Syslog" на стр. [178](#)). Сведения о каждом событии отправляются как отдельное syslog-сообщение. Текст syslog-сообщения соответствует информации о событии, отображающейся в веб-интерфейсе программы в разделе **События**.

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

В этом разделе

Настройка параметров Syslog	178
Содержание syslog-сообщений о событиях обработки трафика	179
Содержание syslog-сообщений о системных событиях программы	187
Содержание syslog-сообщений о событиях отправки файлов на сервер KATA	190

Настройка параметров Syslog

При настройке параметров Kaspersky Web Traffic Security рекомендуется учитывать параметры Syslog, установленные в операционной системе.

► Чтобы настроить параметры Syslog, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **Syslog**.
2. В раскрывающемся списке **Категория журнала** выберите категорию журнала, в который будет записываться информация о событиях.

По умолчанию установлено значение Local1.

При развертывании программы из iso-файла изменение параметра недоступно.

3. В раскрывающемся списке **Уровень события** выберите уровень важности событий, которые будут записываться по протоколу Syslog.

- **Ошибка** – сообщения об ошибках в работе программы.
События обработки трафика не будут записаны в журнал Syslog.
 - **Информация** – сообщения об ошибках в работе программы, а также события обработки трафика.
4. Если специалисты Службы технической поддержки попросили вас включить запись информации об объеме и параметрах потока трафика, обрабатываемого программой, в журнал событий Syslog, переведите переключатель **Записывать информацию о профиле трафика** в положение **Включено**.

Включение этой опции увеличивает требования к дисковому пространству сервера с установленной программой, а также снижает производительность программы. Не рекомендуется включать эту опцию без запроса специалистов Службы технической поддержки.

Запись событий по протоколу Syslog будет настроена.

Содержание syslog-сообщений о событиях обработки трафика

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение KWTS).

Поля syslog-сообщения о событии обработки трафика, определяемые параметрами программы, представлены в формате `<ключ>=<значение>`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

```
Oct 9 10:13:06 localhost KWTS: type="Response": method="GET": action="Block":  
blocked_by_rule="protection_rules [Workspace1/-/Rule2]":  
processing_time="952": scan_result="Malware": workspace="Workspace1":  
http_user_name="example@test.local": http_user_agent="curl/7.29.0":  
http_user_ip="192.0.2.0": url="http://example.com/eicar.com":  
kata-alert="NotDetected": "eicar.com", filesize="69",  
kata_upload="SkippedByAction", guid="", rules="access_rules  
[Workspace1/Group1/Rule1], protection_rules [Workspace1/-/Rule2]",  
av-status="Detected", threats="EICAR-Test-File/Block",  
ap-status="NotDetected", mlf-status="NotDetected", encrypted="NotDetected",  
macros="NotDetected", kata-alert="NotDetected"
```

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 10. Информация о событиях обработки трафика в syslog-сообщении

Ключ	Описание и возможные значения
type	Тип HTTP-сообщения. Может принимать значения Request (запрос) или Response (ответ).
method	Метод HTTP-запроса.
action	Действие над обнаруженным объектом. Может принимать одно из следующих значений: <ul style="list-style-type: none"> • Allow – Разрешить. • Block – Заблокировать. • Redirect – Перенаправить.
blocked_by_rule	Название правила обработки трафика, по которому веб-ресурс был заблокирован. Отображается в следующем формате: <ul style="list-style-type: none"> • Для правил обхода: "[<Название правила>]". • Для правил защиты и правил доступа: "[<Название рабочей области>/<Название группы правил>/<Название правила>]".
redirected_by_rule	Название правила обработки трафика, по которому пользователь был перенаправлен на указанный URL-адрес. Отображается в следующем формате: <ul style="list-style-type: none"> • Для правил обхода: "[<Название правила>]". • Для правил доступа: "[<Название рабочей области>/<Название группы правил>/<Название правила>]".
processing_time	Продолжительность обработки HTTP-сообщения в миллисекундах. Учитывается время с начала обработки заголовка HTTP-сообщения до сохранения записи о выполненной проверке в журнале событий программы и в журнале событий Syslog.
scan_result	Результат проверки HTTP-сообщения. Если обнаружено несколько угроз, отображается название угрозы с наибольшим приоритетом. Если угрозы устранены или не обнаружены, отображается результат проверки с наибольшим приоритетом (<i>Вылечен, Не обнаружено, Не проверен</i>).
workspace	Название рабочей области, к которой относится событие обработки трафика. При отсутствии рабочей области отображается прочерк.
http_user_name	Имя учетной записи пользователя, инициировавшего HTTP-запрос.
http_user_agent	Клиентское приложение, инициировавшее HTTP-запрос.
http_user_ip	IP-адрес компьютера, с которого был отправлен HTTP-запрос.

Ключ	Описание и возможные значения
url	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.
kata-alert	<p>Результат проверки URL-адреса на соответствие объектам, обнаруженным программой KATA.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>NotDetected</code> – URL-адрес проверен, угрозы не обнаружены. • <code>Detected</code> – обнаружено соответствие с объектом в кеше KATA. Указывается ID объекта, критерий совпадения и технология. Например, <code>kata-alert="Detected/128563/Url/Sb"</code>. • <code>NotScanned/AccessRuleSettings</code> – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • <code>NotScanned/ProtectionRuleSettings</code> – проверка не выполнена, так как в правиле защиты для типа объектов Объекты, обнаруженные KATA задано действие Пропустить проверку. • <code>NotScanned/ApplicationSettings</code> – проверка не выполнена, так как режим получения объектов, обнаруженных KATA или интеграция KATA отключены согласно параметрам программы. • <code>ScanError/InternalServerError</code> – проверка завершилась с ошибкой.
<p>Для объекта MIME-типа <code>multipart</code> указывается информация обо всех составных частях. Для каждой составной части используется ключ <code>part</code> с порядковым номером, после которого передаются все атрибуты этой составной части (ключи <code>filename</code>, <code>filesize</code>, <code>part_mimetype</code>, <code>kata_upload</code>, <code>guid</code>, <code>rules</code>, <code>av_status</code>, <code>ap_status</code>, <code>mlf-status</code>, <code>encrypted</code>, <code>macros</code> и <code>kata-alert</code>).</p> <p>Например, <code>part1 "news.html", <атрибуты составной части 1>: part2 <атрибуты составной части 2></code>.</p>	
filename	<p>Имя проверяемого объекта.</p> <p>Если HTTP-сообщение не содержит объектов, указывается <code>"nofile"</code>. В этом случае все последующие поля относятся к проверяемому URL-адресу.</p>

Ключ	Описание и возможные значения
filesize	<p>Размер проверяемого объекта.</p> <p>Если HTTP-сообщение не содержит объектов или для применения правил не требуется вычисление размера файла, указывается "NotApplicable".</p>
part_mimetype	<p>MIME-тип составной части multipart-объекта. Используется значение заголовка Content-Type.</p> <p>Если HTTP-сообщение не содержит объектов или для применения правил не требуется определение MIME-типа, указывается "NotApplicable".</p>
kata_upload	<p>Результат проверки объекта на необходимость отправки на сервер KATA. Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>NotApplicable</code> – HTTP-сообщение не содержит файлов. • <code>Scheduled</code> – отправка файла запланирована. • <code>DisabledBySettings</code> – режим отправки файлов на сервер KATA или интеграция KATA отключены в параметрах программы. • <code>SkippedByAction</code> – HTTP-сообщение пропущено по правилу обхода без проверки или к нему применены действия Заблокировать или Перенаправить. • <code>RejectedByFilter</code> – файл не удовлетворяет условиям отправки на сервер KATA. • <code>Failed/QueueOverflowed</code> – файл должен быть отправлен на сервер KATA, но запланировать отставку не удалось из-за переполнения очереди. • <code>Failed/InternalError</code> – файл должен быть отправлен на сервер KATA, но запланировать отставку не удалось из-за внутренней ошибки программы.
guid	<p>Идентификатор, присвоенный объекту программой.</p> <p>Идентификатор передается, только если при проверке необходимости отправки на сервер KATA был присвоен один из следующих статусов:</p> <ul style="list-style-type: none"> • <code>Scheduled</code>. • <code>Failed/QueueOverflowed</code>. • <code>Failed/InternalError</code>. <p>Для других статусов поле <code>guid</code> передается с пустым значением.</p>

Ключ	Описание и возможные значения
rules	<p>Названия сработавших правил обработки трафика в следующем формате:</p> <pre>"bypass_rule [<Название правила>], access_rules [<Название рабочей области>/<Название группы правил>/<Название правила>], protection_rules [<Название рабочей области>/<Название группы правил>/<Название правила>]"</pre> <p>Если правило не относится к рабочей области, вместо названия рабочей области отображается прочерк.</p> <p>Если правило не входит в группу правил, вместо названия группы отображается прочерк.</p> <p>Если не было применено ни одно правило обработки трафика, применяется политика защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. 103). Отображается значение "default_policy [Default Policy]".</p>
av_status	<p>Результаты проверки веб-ресурса модулем Антивирус.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>Detected</code> – в объекте найдены вирусы или другие программы, представляющие угрозу. Через запятую указываются имена обнаруженных угроз и действие программы над объектом. Например, <code>av-status="Detected", threats="EICAR-Test-File/Block"</code>. • <code>ScanError/Timeout</code> – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • <code>ScanError/InternalError</code> – проверка завершилась с внутренней ошибкой. • <code>ScanError/BasesNotLoaded</code> – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • <code>IncompleteScan/MaxNestingLevelReached</code> – проверка не была выполнена, так как уровень вложенности проверяемого архива превышает максимально допустимый. • <code>IncompleteScan/EncryptedArchive</code> – проверка не была выполнена, так как объект зашифрован. • <code>Disinfected</code> – обнаружены угрозы, все угрозы вылечены. • <code>NotDetected</code> – объект проверен, угрозы не обнаружены. • <code>NotScanned/AccessRuleSettings</code> – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – объект не проходил проверку, так как к нему было применено правило обхода. • <code>NotScanned/ProtectionRuleSettings</code> – объект не проходил проверку согласно действию, заданному в правиле защиты. • <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
ap_status	<p>Результаты проверки веб-ресурса модулем Анти-Фишинг.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>Detected (local bases)</code> – ссылка признана фишинговой на основе записей в локальных базах программы. • <code>Detected (KSN)</code> – ссылка признана фишинговой на основе проверки репутации в KSN. • <code>Detected (heuristics)</code> – ссылка признана фишинговой на основе данных эвристического анализа. • <code>ScanError/Timeout</code> – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • <code>ScanError/InternalServerError</code> – проверка завершилась с внутренней ошибкой. • <code>ScanError/BasesNotLoaded</code> – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • <code>NotDetected</code> – объект проверен, угрозы не обнаружены. • <code>NotScanned/AccessRuleSettings</code> – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – объект не проходил проверку, так как к нему было применено правило обхода. • <code>NotScanned/ProtectionRuleSettings</code> – объект не проходил проверку согласно действию, заданному в правиле защиты. • <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
mlf-status	<p>Результаты проверки ссылок на наличие вредоносных объектов.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>Detected (local bases)</code> – ссылка признана вредоносной на основе записей в локальных антивирусных базах. • <code>Detected (KSN)</code> – ссылка признана вредоносной на основе проверки репутации в KSN. • <code>ScanError/Timeout</code> – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • <code>ScanError/InternalError</code> – проверка завершилась с внутренней ошибкой. • <code>ScanError/BasesNotLoaded</code> – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • <code>NotDetected</code> – ссылка проверена, угрозы не обнаружены. • <code>NotScanned/AccessRuleSettings</code> – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – объект не проходил проверку, так как к нему было применено правило обхода. • <code>NotScanned/ProtectionRuleSettings</code> – объект не проходил проверку согласно действию, заданному в правиле защиты. • <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
<p>encrypted</p>	<p>Информация о шифровании проверяемого объекта. Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>Detected</code> – обнаружены угрозы. • <code>ScanError/Timeout</code> – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • <code>ScanError/InternalError</code> – проверка завершилась с внутренней ошибкой. • <code>ScanError/BasesNotLoaded</code> – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • <code>NotDetected</code> – ссылка проверена, <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы. угрозы не обнаружены. • <code>NotScanned/AccessRuleSettings</code> – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – объект не проходил проверку, так как к нему было применено правило обхода. • <code>NotScanned/ProtectionRuleSettings</code> – объект не проходил проверку согласно действию, заданному в правиле защиты. • <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы.
<p>macros</p>	<p>Информация о наличии макросов в проверяемом объекте. Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>Detected</code> – обнаружены макросы. • <code>ScanError/Timeout</code> – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • <code>ScanError/InternalError</code> – проверка завершилась с внутренней ошибкой. • <code>ScanError/BasesNotLoaded</code> – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • <code>NotDetected</code> – объект проверен, макросы не обнаружены. • <code>NotScanned/AccessRuleSettings</code> – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – объект не проходил проверку, так как к нему было применено правило обхода. • <code>NotScanned/ProtectionRuleSettings</code> – объект не проходил проверку согласно действию, заданному в правиле защиты. • <code>NotScanned/ApplicationSettings</code> – объект не проходил проверку согласно заданным параметрам программы.

Ключ	Описание и возможные значения
kata-alert	<p>Результат проверки файла, содержащегося в HTTP-сообщении, или составной части (для multipart-объектов) на соответствие объектам, обнаруженным программой КАТА.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • <code>NotDetected</code> – URL-адрес проверен, угрозы не обнаружены. • <code>Detected</code> – обнаружено соответствие с объектом в кеше КАТА. Указывается ID объекта, критерий совпадения и технология. Например, <code>kata-alert="Detected/124567/Md5/Yara"</code>. • <code>NotScanned/AccessRuleSettings</code> – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • <code>NotScanned/BypassRuleSettings</code> – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • <code>NotScanned/ProtectionRuleSettings</code> – проверка не выполнена, так как в правиле защиты для типа объектов Объекты, обнаруженные КАТА задано действие Пропустить проверку. • <code>NotScanned/ApplicationSettings</code> – проверка не выполнена, так как режим получения объектов, обнаруженных КАТА или интеграция КАТА отключены согласно параметрам программы. • <code>ScanError/InternalError</code> – проверка завершилась с ошибкой.

Содержание syslog-сообщений о системных событиях программы

Системные события программы содержат информацию о состоянии узлов кластера, модулей программы и лицензии.

В каждом syslog-сообщении для всех типов событий передаются следующие поля, определяемые параметрами Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение KWTS).

Пример:

```
Jan 5 03:39:01 hostname KWTS: Anti-Phishing bases applied:
publishing-time="2019-01-05T03:08:00"
```

Содержание syslog-сообщений в зависимости от типа системного события приведено в таблице ниже.

Таблица 11. Содержание syslog-сообщений в зависимости от типа системного события

Тип события	Описание события	Сообщение
Запуск / остановка программы	Программа запущена	audit started
	Программа остановлена	audit stopped
Обновление баз модуля Антивирус	Ошибка загрузки баз	Anti-Virus bases loading error: <причина ошибки>
	Ошибка обновления баз	Anti-Virus bases update error: <причина ошибки>
	Базы успешно загружены	Anti-Virus bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>
	Базы успешно обновлены	Anti-Virus bases updated
Обновление баз модуля Анти-Фишинг	Ошибка загрузки баз	Anti-Phishing bases loading error: <причина ошибки>
	Ошибка обновления баз	Anti-Phishing bases update error: <причина ошибки>
	Базы успешно загружены	Anti-Phishing bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>
	Базы успешно обновлены	Anti-Phishing bases updated

Тип события	Описание события	Сообщение
Лицензирование	Срок действия лицензии истек	license key expired: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" expiration-date="<дата и время истечения срока действия лицензии>"
	Ошибка лицензии	license error: <описание ошибки>
	Лицензионный ключ помещен в черный список	license is blacklisted: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"
	Код активации заблокирован до активации программы	activation code cannot be installed as it is blocked
	Лицензия отсутствует	no license
	Код активации успешно добавлен	license installed: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"
	Статус лицензионного ключа успешно обновлен	license updated: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"
	Код активации успешно удален	license removed: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"

Тип события	Описание события	Сообщение
	Срок действия лицензии скоро истекает	license expires soon: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>
	Действует льготный период действия лицензии	license grace period: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>
	Лицензия действительна	license is ok: license-id="<серийный номер лицензии>" functionalityLevel="Full functionality"
Процессы	Процесс программы завершился аварийно (при многократных аварийных остановках указывается количество остановок и период, за который они произошли)	<имя процесса> crashed [<количество остановок> times during last <количество минут> minutes]
	Процесс программы перезапущен (при многократных перезапусках процесса указывается количество перезапусков и период, за который они произошли)	<имя процесса> restarted [<количество перезапусков> times during last <количество минут> minutes]

Содержание syslog-сообщений о событиях отправки файлов на сервер КАТА

Информация о помещении файла в очередь на отправку в КАТА, а также результаты отправки файла в КАТА записываются в журнал операционной системы по протоколу Syslog.

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение KWTS).

В зависимости от типа события передается поле `KATA upload scheduling` (помещение файла в очередь на отправку) или `KATA uploading` (отправка файла). Поля `syslog`-сообщения, определяемые параметрами программы, представлены в формате `<ключ>=<значение>`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

```
Oct 2 13:19:27 localhost KWTS: KATA uploading: result="Succeeded":  
type="Request": http_user_name="example@test.local":  
http_user_ip="192.0.2.0": url="http://example.com/TEST/test.pdf":  
guid="A485A9DD-A740-4ED3-9933-63ACAЕA964E4": filename="test.pdf":  
filetype="OfficePdf"
```

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 12. Информация о событиях отправки файлов на сервер KATA в syslog-сообщениях

Ключ	Описание и возможные значения
result	<p>Результат помещения файла в очередь на отправку или отправки файла.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • Succeeded – операция выполнена успешно. • Failed/<причина> – не удалось поместить файл в очередь на отправку по указанной причине.
type	<p>Тип HTTP-сообщения.</p> <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> • Request – запрос. • Response – ответ.
http_user_name	Имя учетной записи пользователя, от имени которого выполнена операция с файлом.
http_user_ip	IP-адрес компьютера, с которого был отправлен файл.
url	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.
guid	Идентификатор, который был присвоен файлу программой.
filename	Имя отправляемого файла.
filetype	Тип отправляемого файла.

Работа с программой по протоколу SNMP

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

В Kaspersky Web Traffic Security для работы по протоколу SNMP используется *SNMP-агент*, который отслеживает информацию о работе программы. Kaspersky Web Traffic Security может отправлять эту информацию в виде *SNMP-ловушек* – уведомлений о событиях работы программы.

Для работы по протоколу SNMP требуется предварительно настроить службу `snmpd` в операционной системе (см. раздел «Настройка службы `snmpd` в операционной системе» на стр. [193](#)).

По протоколу SNMP вы можете получить доступ к следующей информации о программе:

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

Доступ предоставляется только на чтение информации.

Информация об SNMP-ловушках и статистике, отправляемой по протоколу SNMP, хранится в базе данных MIB (см. раздел "Описание объектов MIB Kaspersky Web Traffic Security" на стр. [197](#)).

В этом разделе

Настройка службы <code>snmpd</code> в операционной системе	193
Включение и отключение использования SNMP в программе	194
Настройка параметров подключения к SNMP-серверу	194
Настройка шифрования SNMP-соединений.....	195
Включение и отключение отправки SNMP-ловушек	197
Описание объектов MIB Kaspersky Web Traffic Security	197

Настройка службы `snmpd` в операционной системе

► Чтобы настроить службу `snmpd`, выполните следующие действия:

1. Добавьте в файл `/etc/snmp/snmpd.conf` следующие строки для соединений через Unix-сокеты:

```
master agentx
agentXSocket unix:/var/run/agentx-master.socket
```

```
agentXPerms 770 770 kluser klusers
```

2. Перезапустите службу snmpd. Для этого выполните команду:

```
service snmpd restart
```

Служба snmpd будет настроена. Для работы с программой по протоколу SNMP вам требуется включить его использование (см. раздел "Включение и отключение использования SNMP в программе" на стр. [194](#)) в веб-интерфейсе программы.

Если служба snmpd была настроена до установки Kaspersky Web Traffic Security, передача данных программы по протоколу SNMP может осуществляться некорректно. В этом случае требуется повторно перезапустить службу snmpd.

Включение и отключение использования SNMP в программе

- ▶ Чтобы включить или отключить использование SNMP в работе программы, выполните следующие действия:
 1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
 2. Выполните одно из следующих действий:
 - Включите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите включить использование SNMP.
 - Выключите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите отключить использование SNMP.
 3. Нажмите на кнопку **Сохранить**.

Настройка параметров подключения к SNMP-серверу

- ▶ Чтобы настроить параметры подключения к SNMP-серверу, выполните следующие действия:
 1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
 2. В раскрывающемся списке **Тип сокета** выберите, какой сокет должен быть использован для подключения к SNMP-серверу.

Для безопасной передачи данных рекомендуется выбирать **UNIX**.

3. Если вы выбрали **UNIX**, в поле **Путь к UNIX-сокету**, укажите путь к файлу сокета.
4. Если вы выбрали **TCP**, в блоке параметров **Адрес SNMP-сервера** введите IP-адрес или имя хоста SNMP-сервера и порт подключения к SNMP-серверу.
5. В поле **Время ожидания ответа сервера (сек.)** укажите максимальное время ожидания ответа от

SNMP-сервера в секундах. Вы можете указать значение в интервале от 1 до 255 секунд.

Значение по умолчанию: 15 секунд.

6. Нажмите на кнопку **Сохранить**.

Соединение с SNMP-сервером будет настроено.

Настройка шифрования SNMP-соединений

Сторонние программы могут получать доступ к данным, отправляемым по протоколу SNMP, или заменять эти данные своими данными. Для безопасной передачи данных по протоколу SNMP рекомендуется настроить шифрование SNMP-соединений.

Перед настройкой убедитесь, что на всех серверах с программой Kaspersky Web Traffic Security установлены службы `snmpd` и `snmptrapd`.

► Чтобы настроить шифрование SNMP-соединений, выполните следующие действия:

1. Получите EngineID, необходимый для обработки SNMP-ловушек. Для этого на Управляющем сервере выполните команду:

```
snmpget -v2c -cpublic localhost SNMP-FRAMEWORK-MIB::snmpEngineID.0  
2>/dev/null | sed -ne 's/ //g; s/.*/0x/p'
```

2. На каждом сервере настройте службу `snmpd`. Для этого выполните следующие действия:

a. Остановите службу `snmpd`. Для этого выполните команду:

```
service snmpd stop
```

b. Добавьте строку `createUser kwts-snmp-user SHA "<password>" AES "<password>"` в конфигурационный файл `/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
```

```
trapssess -e <EngineID> -v3 -l authPriv -u kwts-snmp-user -a SHA -A  
<password> -x AES -X <password> udp:localhost:162
```

- d. Добавьте в конфигурационный файл `/etc/snmp/snmp.conf` следующие строки:

```
mibdirs +/opt/kaspersky/kwts/share/snmp-mibs/  
mibs all
```

- e. Запустите службу `snmpd`. Для этого выполните команду:

```
service snmpd start
```

- f. Проверьте SNMP-соединение. Для этого выполните следующие команды:

```
snmpwalk -mALL -v3 -l authPriv -u kwts-snmp-user -a SHA -A <password> -x  
AES -X <password> udp:localhost:161 .1.3.6.1.4.1.23668
```

```
snmpget -v3 -l authPriv -u kwts-snmp-user -a SHA -A <password> -x AES -X  
<password> udp:localhost:161 .1.3.6.1.4.1.23668.2022.2.8.1.0
```

3. На сервере, на котором вы хотите получать SNMP-ловушки, настройте службу `snmptrapd`. Для этого выполните следующие действия:

- a. Остановите службу `snmptrapd`. Для этого выполните команду:

```
service snmptrapd stop
```

- b. Добавьте строку `createUser -e <EngineID> kwts-snmp-user SHA "<password>" AES "<password>"` в конфигурационный файл `/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 отставку SNMP-ловушек событий, возникающих в ходе работы программы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
2. Включите переключатель рядом с названием блока **Использовать SNMP**, если он выключен.
3. Выполните одно из следующих действий:
 - Установите флажок **Отправлять SNMP-ловушки**, если вы хотите включить отставку SNMP-ловушек.
 - Снимите флажок **Отправлять SNMP-ловушки**, если вы хотите отключить отставку SNMP-ловушек.
4. Нажмите на кнопку **Сохранить**.

Отправка SNMP-ловушек будет настроена.

Описание объектов MIB Kaspersky Web Traffic Security

В таблицах ниже приведена информация об объектах MIB Kaspersky Web Traffic Security.

События управления кластером

Таблица 13. События управления кластером

Символьное имя	Описание	Параметры
clusterConsistencyErrorEvent	Ошибка состояния серверов. Например, нет ни одного сервера с ролью Управляющий узел.	<ul style="list-style-type: none"> • Имя Управляющего узла. • Сообщение об ошибке.
clusterEmergencyStateEvent	Программа перешла в аварийный режим.	<ul style="list-style-type: none"> • Имя Управляющего узла. • Сообщение об ошибке.
settingsSynchronizationErrorEvent	Ошибка синхронизации параметров между Управляющим и Подчиненными узлами.	<ul style="list-style-type: none"> • Имя Управляющего узла. • Сообщение об ошибке.

События обработки трафика

Таблица 14. События обработки трафика

Символьное имя	Описание	Параметры
productStartEvent	Программа запущена. Это событие возникает после того, как запускаются все службы, необходимые для работы Kaspersky Web Traffic Security.	Нет параметров.

Символьное имя	Описание	Параметры
taskCrashEvent	Процесс программы завершился аварийно.	Полный путь к бинарному файлу.
taskRestartEvent	Процесс программы перезапущен.	Полный путь к бинарному файлу.
licenseInstalledEvent	Код активации добавлен.	Серийный номер лицензии.
licenseUpdatedEvent	Статус лицензионного ключа изменен.	<ul style="list-style-type: none"> Серийный номер лицензии. Тип лицензии. Дата окончания срока действия лицензии.
licenseRevokedEvent	Код активации удален.	Серийный номер лицензии.
licenseExpiredEvent	Истек срок действия лицензии.	<ul style="list-style-type: none"> Серийный номер лицензии. Дата окончания срока действия лицензии.
licenseExpiresSoonEvent	Срок действия лицензии скоро истечет.	<ul style="list-style-type: none"> Серийный номер лицензии. Дата окончания срока действия лицензии.
licenseTrialPeriodIsOverEvent	Истек срок действия пробной лицензии.	<ul style="list-style-type: none"> Серийный номер лицензии. Дата окончания срока действия лицензии.
gracePeriodEvent	Начался льготный период действия лицензии.	<ul style="list-style-type: none"> Серийный номер лицензии. Количество дней до завершения льготного периода.
updateErrorEvent	Обновление баз программы завершилось ошибкой.	Причина ошибки.
avBasesOutdatedEvent	Базы модуля Антивирус устарели.	Нет параметров.
avBasesObsoletedEvent	Базы модуля Антивирус сильно устарели.	Нет параметров.
apBasesOutdatedEvent	Базы модуля Анти-Фишинг устарели.	Нет параметров.
apBasesObsoletedEvent	Базы модуля Анти-Фишинг сильно устарели.	Нет параметров.

Другие события программы

Таблица 15. Другие события программы

Символьное имя	Описание	Параметры
----------------	----------	-----------

Символьное имя	Описание	Параметры
KsnConnectionStatusEvent	Изменение состояния подключения к службам KSN.	Новое состояние подключения: <ul style="list-style-type: none"> • Ok. • Error. • KsnDisabled. • KsnRestrictedLicense.
LdapCacheUpdateEvent	Запуск синхронизации данных с Active Directory.	<ul style="list-style-type: none"> • Статус синхронизации LDAP-кэша. • Статус синхронизации данных для автозаполнения учетных записей.

Статистика программы

Таблица 16. Статистика программы

Символьное имя	Описание
productName	Название программы.
productVersion	Версия программы.
installDate	Дата установки программы.
licenseExpireDate	Дата окончания срока действия лицензии.
licenseStatus	Состояние кода активации.

Статистика модуля Антивирус

Таблица 17. Статистика модуля Антивирус

Символьное имя	Описание
cleanObjects	Количество объектов, в которых не обнаружены угрозы.
infectedObjects	Количество зараженных объектов.
passwordProtectedObjects	Количество объектов, защищенных паролем.
docsWithMacro	Количество документов, содержащих макросы.
scanErrors	Количество ошибок, связанных с превышением максимального допустимого времени проверки.
notScannedSettingsObjects	Количество объектов, не проверенных в соответствии с параметрами правила обработки трафика.
notScannedDueToNestingLevel	Количество объектов, не проверенных из-за превышения допустимой глубины проверки архивов.

Аутентификация с помощью технологии единого входа

При включении технологии единого входа пользователям не требуется вводить данные учетной записи программы для подключения к веб-интерфейсу. Аутентификация осуществляется с помощью доменной учетной записи пользователя.

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

В этом разделе

Создание keytab-файла	200
Настройка Kerberos-аутентификации	201
Настройка NTLM-аутентификации	202

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имя субъекта-службы* (далее также "SPN") для каждого из этих узлов.

► Чтобы создать keytab-файл, выполните следующие действия:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя с именем `control-ваше имя`.
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
 - a. Откройте свойства созданной учетной записи.
 - b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-ваше имя`. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-ваше имя@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-НМАС-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-ваше имя>> -out C:\control-ваше имя.keytab
```

Пример ввода имени узла: node01.test.local@TEST.LOCAL

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-<имя ранее созданного файла>.keytab -out C:\control-<новое имя>.keytab -setupn -setpass
```

Keytab-файл с именем C:\control-<новое имя>.keytab будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, при выполнении шага 3 вы создали файл под названием control-tmp1.keytab. Тогда для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp1.keytab -out C:\control-tmp2.keytab -setupn -setpass
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp2.keytab -out C:\control-tmp3.keytab -setupn -setpass
```

В результате будет создан файл с именем control-tmp3.keytab, содержащий все три добавленные SPN.

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS в зонах обратного просмотра присутствует PTR-запись для FQDN и URL (если URL отличается от FQDN) каждого узла кластера.

Если вы настраиваете аутентификацию с доменом, в названии которого содержится корневой домен `.local`, то для корректной работы Kerberos-аутентификации требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы `avahi-daemon`. Для этого выполните команду:

```
systemctl status avahi-daemon
```

2. Если служба запущена, остановите ее. Для этого выполните команду:

```
systemctl stop avahi-daemon
```

3. Отключите автоматический запуск службы. Для этого выполните команду:

```
systemctl disable avahi-daemon
```

► Чтобы настроить Kerberos-аутентификацию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **Kerberos-аутентификация** переведите переключатель **Использовать Kerberos** в положение **Включено**.
3. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. [200](#)).

Keytab-файл должен содержать SPN Управляющего узла и Подчиненных узлов.

Откроется окно выбора файла.

4. Выберите keytab-файл и нажмите на кнопку **Открыть**.
5. Нажмите на кнопку **Сохранить**.

Если в keytab-файле не найдено SPN Управляющего узла или SPN какого-либо из Подчиненных узлов, то для этого узла в разделе **Узлы** отображается статус *Отсутствует SPN-идентификатор для службы единого входа Kerberos*. Если в keytab-файле не найдено SPN ни одного из узлов, кнопка **Сохранить** недоступна.

Kerberos-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При отключении Kerberos-аутентификации ранее загруженный keytab-файл удаляется.

Настройка NTLM-аутентификации

► Чтобы настроить NTLM-аутентификацию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **NTLM-аутентификация** переведите переключатель **Использовать NTLM** в положение **Включено**.

3. В поле **IP-адрес/доменное имя контроллера домена** укажите IP-адрес или доменное имя доменного контроллера, с помощью которого будет осуществляться аутентификация.

Вы можете указать два доменных контроллера. Для добавления второго контроллера необходимо нажать на кнопку .

4. В поле **Порт** укажите порт для подключения к доменному контроллеру.

По умолчанию используется порт 445.

5. Нажмите на кнопку **Сохранить**.

NTLM-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При подключении с компьютеров, не входящих в домен, пользователю потребуется указать данные своей доменной учетной записи.

Управление параметрами встроенного прокси-сервера в веб-интерфейсе программы

При развертывании Kaspersky Web Traffic Security из iso-файла вы можете управлять параметрами встроенного прокси-сервера через веб-интерфейс программы.

В веб-интерфейсе программы вы можете настроить следующие параметры:

- Порт подключения компьютеров пользователей к прокси-серверу (см. раздел "Изменение порта подключения к прокси-серверу" на стр. [204](#)).
- Фильтр подключений к программе (см. раздел "Настройка фильтра доступа" на стр. [205](#)).
Программа будет обрабатывать трафик, поступающий только с указанных IP-адресов.
- Балансировку нагрузки (см. раздел "Настройка балансировки нагрузки" на стр. [206](#)).
Если вы установили программу на нескольких серверах, то для оптимизации распределения ресурсов вы можете использовать балансировщик нагрузки.
- Механизм аутентификации (см. раздел "Аутентификация пользователей" на стр. [207](#)).
- Формат журнала доступа (см. раздел "Настройка формата журнала доступа" на стр. [220](#)).

В этом разделе

Изменение порта подключения к прокси-серверу.....	204
Настройка фильтра доступа	205
Настройка балансировки нагрузки	206
Аутентификация пользователей	207
Настройка формата журнала доступа.....	220
Восстановление параметров до значений по умолчанию	221

Изменение порта подключения к прокси-серверу

По умолчанию для соединения между компьютерами пользователей и прокси-сервером используется порт 3128. Вы можете изменить это значение.

► *Чтобы изменить порт подключения к прокси-серверу, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Общие**.
2. В блоке параметров **Параметры подключения** в поле **Порт** укажите, по какому порту компьютеры пользователей будут подключаться к прокси-серверу.

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

3. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Порт подключения к прокси-серверу будет изменен.

Настройка фильтра доступа

Если вы хотите, чтобы программа, развернутая из iso-файла, обрабатывала запросы только заданных компьютеров, вы можете указать IP-адреса этих компьютеров в фильтре доступа.

► *Чтобы настроить фильтр доступа, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Общие**.
2. В блоке параметров **Фильтр доступа** переведите переключатель в положение **Включено**.
3. В поле **Разрешенные локальные IP-адреса** перейдите по ссылке **Изменить все** в правом нижнем углу.
Откроется окно **IP-адреса**.
4. В поле ввода укажите IP-адреса компьютеров, запросы от которых будут обрабатываться программой.

При указании нескольких адресов в качестве разделителя используйте точку с запятой.

Вы можете указать IP-адрес в одном из следующих форматов:

- IPv4-адрес (например, 172.16.5.6).
 - IPv4-адрес с маской в формате CIDR notation (например, 192.168.1.0/24).
 - IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
 - IPv6-адрес с маской в формате CIDR notation (например, fc00::/7).
5. Нажмите на кнопку **Добавить**.
- Если IP-адрес имеет недопустимый формат, слева от него отобразится значок . Вы можете удалить этот адрес с помощью кнопки  в правой части строки и добавить его заново, проверив правильность ввода.
6. Нажмите на кнопку **Сохранить**.

Фильтр доступа будет настроен. Программа будет обрабатывать запросы только от компьютеров с заданными IP-адресами.

Настройка балансировки нагрузки

► Чтобы настроить балансировку нагрузки, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Общие**.
2. В блоке параметров **Балансировка нагрузки** переведите переключатель в положение **Включено**.
3. Выберите один из следующих режимов в зависимости от протокола, поддерживаемого вашим балансировщиком нагрузки:
 - **Заголовок PROXY protocol.**
 - **Заголовок HTTP Forwarded.**
4. В поле **Доверенные балансировщики нагрузки** введите IP-адреса балансировщиков нагрузки, трафик с которых программа будет обрабатывать.

Убедитесь, что указанные балансировщики нагрузки передают реальные IP-адреса источников соединений. Эти IP-адреса будут использоваться при подборе правил обработки трафика.

При указании нескольких адресов в качестве разделителя используйте точку с запятой.

Вы можете указать IP-адрес в одном из следующих форматов:

- IPv4-адрес (например, 172.16.5.6).
 - IPv4-адрес с маской в формате CIDR notation (например, 192.168.1.0/24).
 - IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
 - IPv6-адрес с маской в формате CIDR notation (например, fc00::/7).
5. Нажмите на кнопку **Сохранить**.

Если вы изменили положение переключателя **Балансировка нагрузки** или режим балансировки, то при сохранении изменений прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Балансировка нагрузки будет настроена.

Аутентификация пользователей

В программе поддерживается настройка Kerberos- (см. раздел "Настройка Kerberos-аутентификации" на стр. [207](#)) и NTLM-аутентификации (см. раздел "Настройка NTLM-аутентификации" на стр. [210](#)). При использовании NTLM-аутентификации вы можете настроить проверку имен доменов (см. раздел "Настройка проверки имен доменов" на стр. [211](#)). Это позволит корректно обрабатывать разные форматы доменных имен пользователей, поддерживаемые протоколом NTLM.

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

Для обоих типов аутентификации доступно создание исключений (см. раздел "Добавление исключений аутентификации" на стр. [218](#)), позволяющих пользователям получить доступ к веб-ресурсам без аутентификации.

В этом разделе

Настройка Kerberos-аутентификации	207
Создание keytab-файла	208
Настройка NTLM-аутентификации	210
Настройка проверки имен доменов	211
Добавление исключений аутентификации	218

Настройка Kerberos-аутентификации

Вы можете создать один keytab-файл (см. раздел "Создание keytab-файла" на стр. [200](#)) и добавить в него SPN всех серверов с установленной программой. Это позволит пользователям проходить аутентификацию с использованием своих доменных учетных записей на всех узлах кластера.

► *Чтобы настроить Kerberos-аутентификацию на прокси-сервере, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Аутентификация**.
2. В поле **Kerberos** перейдите по ссылке **Настроить**.
Откроется окно **Параметры Kerberos-аутентификации**.
3. Переведите переключатель в положение **Включено**.
4. Нажмите на кнопку **Загрузить**, чтобы загрузить keytab-файл.

Если keytab-файл был загружен ранее, для его замены вам необходимо нажать на кнопку **Заменить**.

Откроется окно выбора файла.

5. Выберите файл и нажмите на кнопку **Open**.

Keytab-файл будет загружен.

6. Если вы хотите проверять запросы аутентификации на наличие дубликатов, включите переключатель **Использовать replay cache**.

Replay cache обеспечивает более надежную защиту, но может снижать производительность программы.

7. Нажмите на кнопку **Сохранить**.

Если вы изменили положение переключателя **Включено** или **Использовать replay cache**, то при сохранении изменений прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Kerberos-аутентификация будет настроена. Прокси-сервер будет обрабатывать запросы только от тех пользователей, которые пройдут процедуру аутентификации.

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имя субъекта-службы* (далее также "SPN") для каждого из этих узлов.

► Чтобы создать keytab-файл, выполните следующие действия:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя с именем `control-ваше имя`.
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
 - a. Откройте свойства созданной учетной записи.
 - b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-ваше имя`. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-ваше имя@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-HMAC-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-ваше имя>> -out
```

```
C:\control-<ваше имя>.keytab
```

Пример ввода имени узла: node01.test.local@TEST.LOCAL

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-НМАС-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-<имя ранее созданного файла>.keytab -out C:\control-<новое имя>.keytab -setupn -setpass
```

Keytab-файл с именем C:\control-<новое имя>.keytab будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, при выполнении шага 3 вы создали файл под названием control-tmp1.keytab. Тогда для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-НМАС-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp1.keytab -out C:\control-tmp2.keytab -setupn -setpass
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-<ваше имя>@<realm имя домена Active Directory в верхнем регистре> -crypto <тип шифрования, рекомендуется указать RC4-НМАС-NT> -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя control-<ваше имя>> -in C:\control-tmp2.keytab -out C:\control-tmp3.keytab -setupn -setpass
```

В результате будет создан файл с именем control-tmp3.keytab, содержащий все три добавленные SPN.

Настройка NTLM-аутентификации

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

► Чтобы настроить NTLM-аутентификацию на прокси-сервере, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Аутентификация**.
2. В поле **NTLM** перейдите по ссылке **Настроить**.
Откроется окно **Параметры NTLM-аутентификации**.
3. Переведите переключатель в положение **Включено**.
4. В поле **Имя домена** введите имя домена, для которого вы хотите настроить аутентификацию.

Поиск контроллера домена осуществляется по SRV-записям.

Для успешного поиска контроллера домена на DNS-сервере должны быть созданы SRV-записи для указанного домена. Обычно эти записи создаются автоматически при развертывании Active Directory. Однако при необходимости вы можете добавить их вручную.

Проверить наличие SRV-записей, а также правильность их полей вы можете с помощью следующих команд:

- Для операционных систем Linux вы можете использовать любую из следующих команд:
 - `host -t srv _ldap._tcp.<указанное имя домена>`
 - `dig _ldap._tcp.<указанное имя домена> srv`
 - `nslookup -type=srv _ldap._tcp.<указанное имя домена>`

Предварительно требуется настроить в DNS-клиенте использование DNS-сервера, ответственного за указанную DNS-зону.

- Для операционных систем Windows используйте команду:
`nslookup -type=srv _ldap._tcp.<указанное имя домена>`

Поиск контроллера домена осуществляется по следующему алгоритму:

- a. Программа получает список SRV-записей, найденных по строке `_ldap._tcp.<указанное имя домена>`.
- b. Все записи группируются по значению поля `priority` в очередности от более высокого приоритета к более низкому. Внутри каждой группы SRV-записи сортируются по значению поля `weight`.

Вы можете изменять поля SRV-записей (Priority и Weight) на DNS-сервере, чтобы задать порядок подключения к контроллерам домена.

- c. Программа пытается установить соединение последовательно с каждым сервером из списка до первого успешного подключения.
Если вы установили флажок **Использовать SSL**, то для соединения с контроллером домена используется протокол LDAPS и порт 636. Если флажок снят, то используется протокол LDAP и порт, указанный в SRV-записи.
- d. Если не удалось установить соединение ни с одним сервером из списка, алгоритм выполняется повторно.
1. Если вы хотите проверить соединение с контроллером домена по заданным параметрам, нажмите на кнопку **Проверить соединение**.
Результат проверки отобразится справа от кнопки.
2. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

NTLM-аутентификация будет настроена. Прокси-сервер будет обрабатывать запросы только от тех пользователей, которые пройдут процедуру аутентификации.

Настройка проверки имен доменов

Рекомендуется включить проверку имен доменов, чтобы обеспечить корректное применение правил обработки трафика, а также критериев принадлежности пользователей к рабочим областям. Вы можете отключить проверку имен доменов, если в вашей организации доменные имена пользователей сохранены в параметрах браузеров с пустой доменной частью или в формате, не поддерживаемом программой.

Разные форматы доменных имен получаются из комбинаций следующих элементов учетной записи:

- NETBIOS-имя – уникальное имя домена, представляющее собой 16-байтовый адрес для идентификации в локальной сети.
- DNS-имя – имя домена, которое включает в себя имена всех родительских доменов иерархии DNS, разделенные точкой.
- sAMAccountName – имя учетной записи пользователя в формате pre-Windows 2000.
- UPN-имя (User Principal Name) – имя учетной записи пользователя, которое состоит из UPN-префикса (имени входа) и UPN-суффикса (имени домена), разделенных символом @.

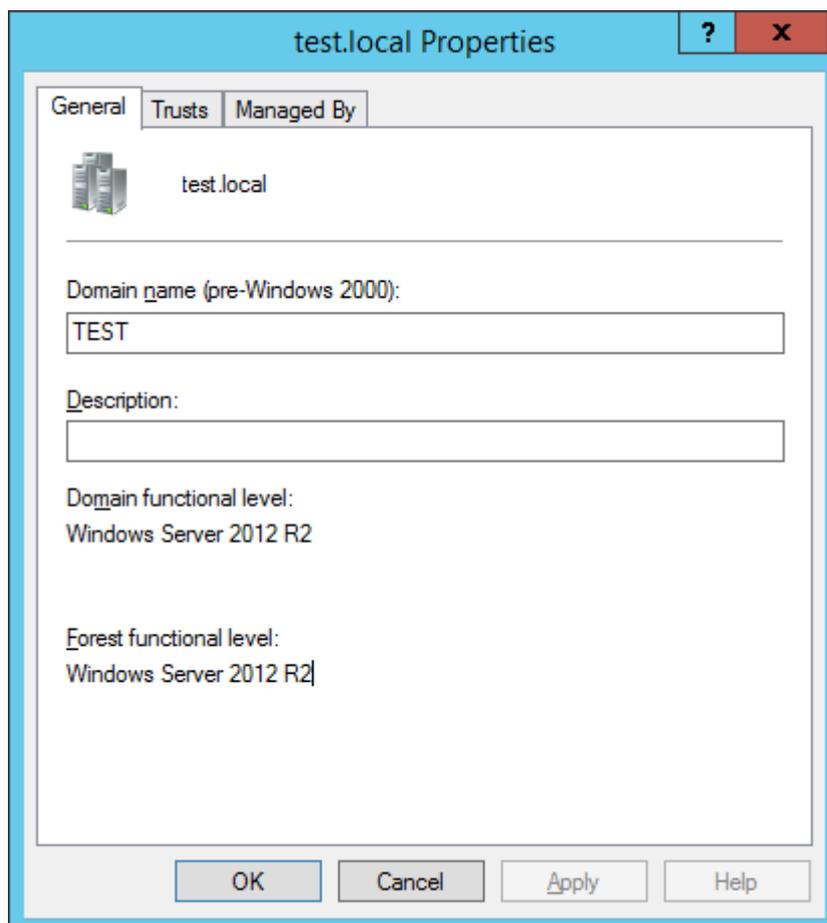
По умолчанию в качестве UPN-суффикса используется DNS-имя. Вы можете указать альтернативные UPN-суффиксы и выбрать их в свойствах учетной записи вместо DNS-имени.

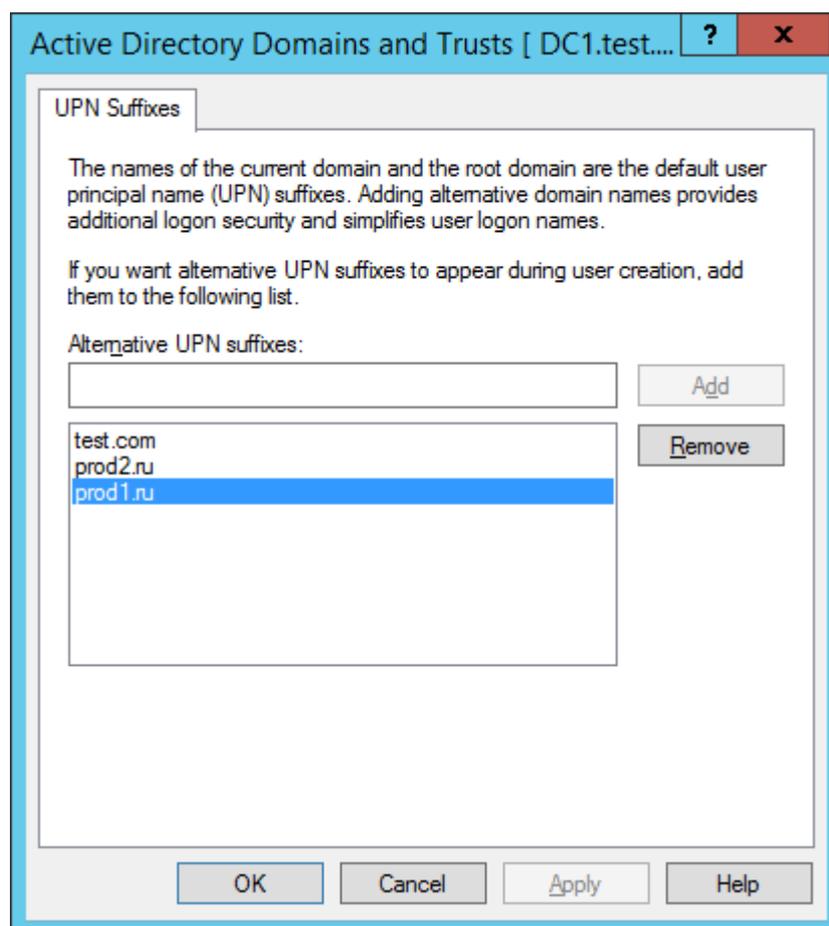
В оснастке Active Directory этим элементам соответствуют поля, представленные на примере ниже, где:

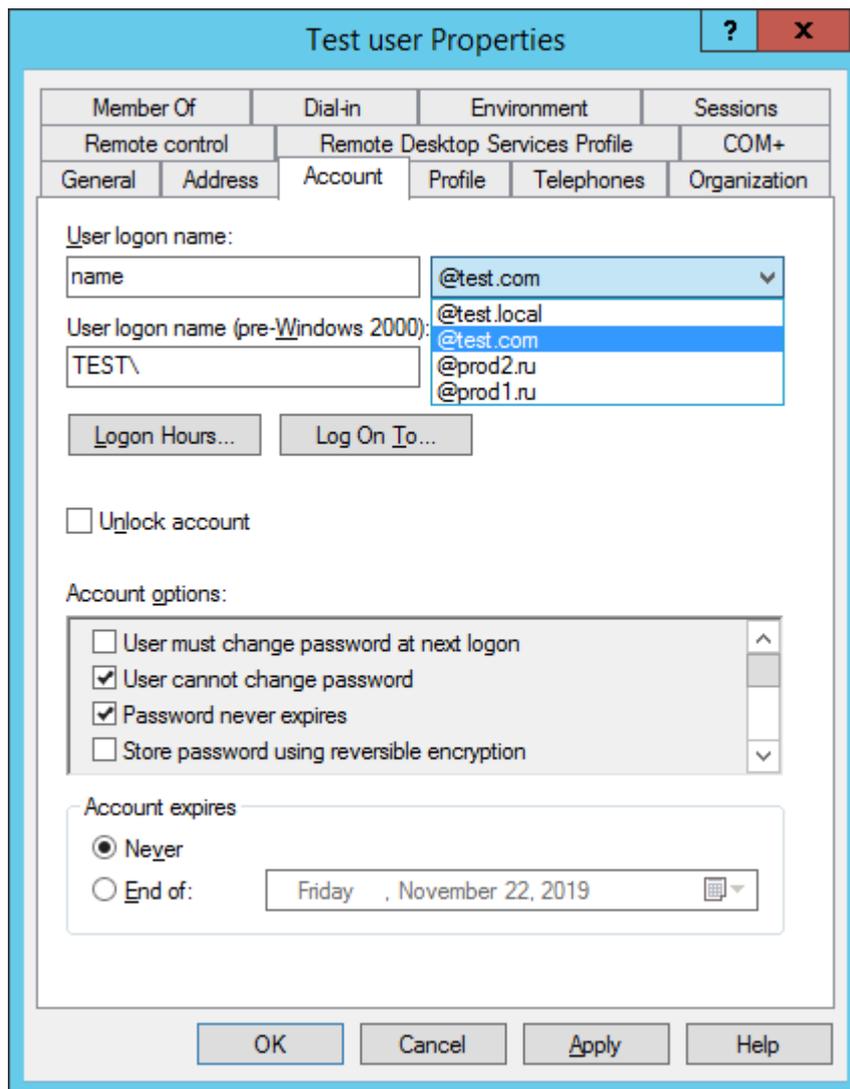
- name – UPN-Prefix;

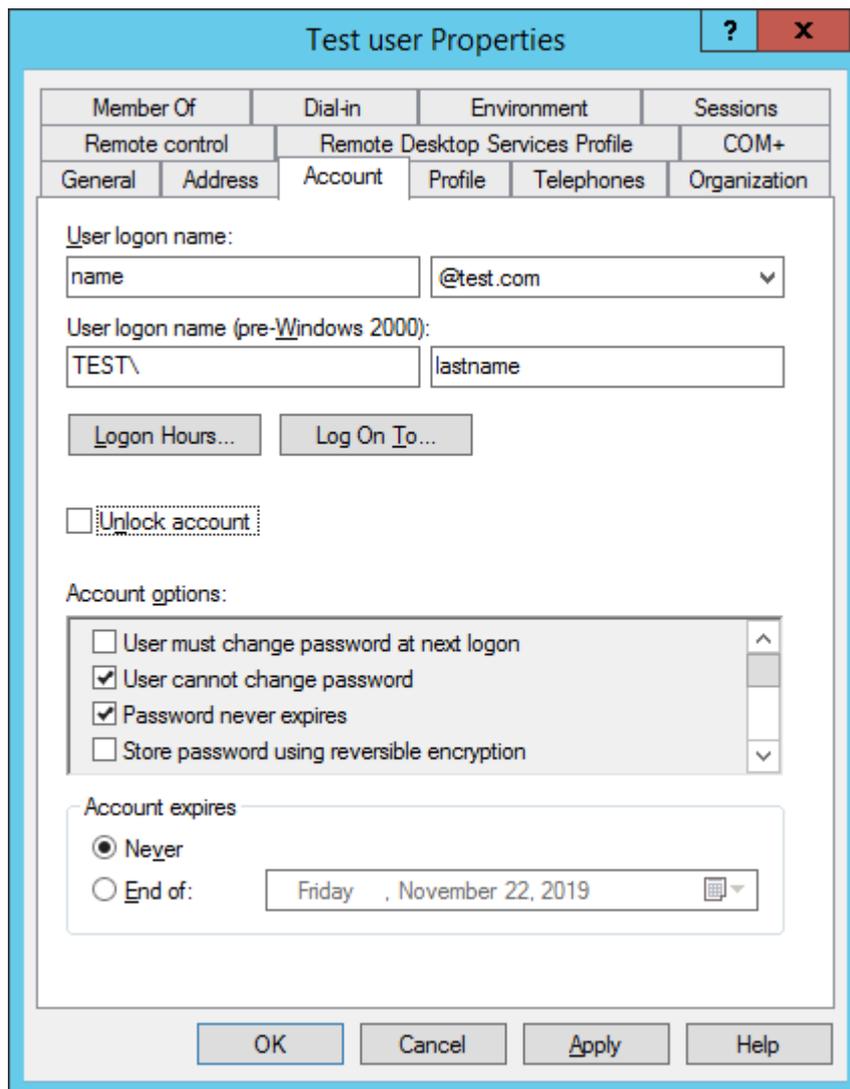
- `test.local` – DNS-имя;
- `TEST` – NETBIOS-имя;
- `lastname` – sAMAccountName.

- test.com – альтернативный UPN-суффикс.









Если проверка имен доменов отключена, аутентификация пользователей осуществляется согласно таблице, представленной ниже.

Таблица 18. Аутентификация при отключенной проверке имен доменов

Формат доменного имени	Пример	Аутентификация
DNS-Name\sAMAccountName	test.local\lastname	Выполняется.
NETBIOS-Name\sAMAccountName	test\lastname	Выполняется.
UPN-Suffix\sAMAccountName	test.com\lastname	Выполняется.
<любое значение> ² \sAMAccountName	<любое значение>\lastname	Выполняется.
DNS-Name\UPN-Prefix	test.local\name	Не выполняется.
NETBIOS-Name\UPN-Prefix	test\name	Не выполняется.
UPN-Suffix\UPN-Prefix	test.com\name	Не выполняется.
UPN-Prefix@DNS-Name	name@test.local	Выполняется, если в качестве UPN-префикса пользователя используется DNS-имя домена.
UPN-Prefix@NETBIOS-Name	name@test	Не выполняется.
UPN-Prefix@UPN-Suffix	name@test.com	Выполняется, если в качестве UPN-суффикса пользователя используется указанный UPN-суффикс.
sAMAccountName@DNS-Name	lastname@test.local	Выполняется.
sAMAccountName@NETBIOS-Name	lastname@test	Выполняется.
sAMAccountName@UPN-Suffix	lastname@test.com	Не выполняется.

Если проверка имен доменов включена, программа будет разрешать аутентификацию пользователей только при указании доменного имени в поддерживаемом формате. В этом случае программа сможет корректно распознать пользователя и применить заданные параметры правил обработки трафика и рабочих областей.

Форматы доменных имен, поддерживаемые программой в текущей версии, а также в версии 6.0, представлены в таблице ниже.

² Согласно спецификации протокола NTLM, контроллер домена пытается выполнить аутентификацию пользователя даже при некорректно указанной или пустой доменной части учетной записи.

Таблица 19. Форматы поддерживаемых доменных имен

Формат	Пример	Поддержка в версии 6.0
NETBIOS\sAMAccountName	TEST\lastname	Да
sAMAccountName@NETBIOS	lastname@TEST	Нет
sAMAccountName@DNS-Name	lastname@test.local	Да
DNS-Name\sAMAccountName	test.local\lastname	Нет
UPN-Prefix@UPN-Suffix	name@test.com	Нет

► Чтобы настроить проверку имен доменов, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Аутентификация**.
2. В поле **NTLM** перейдите по ссылке **Настроить**.
Откроется окно **Параметры NTLM-аутентификации**.
3. Переведите переключатель **Проверять имена доменов** в положение **Включено**.
4. В поле **Разрешенные DNS/NETBIOS-имена доменов** укажите разрешенное имя домена.
5. Если вы хотите добавить несколько имен, нажмите на значок  и укажите имя в появившемся поле ввода.
6. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Проверка имен доменов будет настроена. При попытке аутентификации с именем домена, не указанным в качестве разрешенного, прокси-сервер не будет передавать запрос на аутентификацию серверу Active Directory. Пользователю потребуется ввести учетные данные повторно.

Добавление исключений аутентификации

Вы можете добавить в исключения аутентификации компьютеры пользователей или веб-ресурсы. Если запрос отправлен с компьютера из списка исключений или запрашивается веб-ресурс из списка исключений, пользователю не потребуется проходить аутентификацию для соединения с прокси-сервером.

Исключения применяются и к Kerberos-, и к NTLM-аутентификации.

► Чтобы добавить исключения аутентификации, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Аутентификация**.

2. Если вы хотите разрешить некоторым компьютерам доступ ко всем веб-ресурсам без аутентификации на прокси-сервере, в блоке параметров **Источник** укажите их IP-адреса.

3. В поле **IP-адрес** перейдите по ссылке **Изменить все**.

Откроется окно **IP-адреса**.

4. Введите один или несколько IP-адресов.

Вы можете указывать IP-адреса в одном из следующих форматов:

- IPv4-адрес (например, 172.16.5.6).
- IPv4-подсеть с маской в формате CIDR notation (например, 192.168.1.0/24).
- IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6-подсеть с маской в формате CIDR notation (например, fc00::/7).

При указании нескольких IP-адресов используйте точку с запятой или новую строку в качестве разделителя.

5. Нажмите на кнопку **Добавить**.

Добавленные IP-адреса отобразятся в таблице под полем ввода. Если введенное значение имеет недопустимый формат, слева от него появится значок . Вы можете изменить этот адрес с помощью кнопки  в правой части строки.

6. Нажмите на кнопку **Сохранить**.

7. Если вы хотите разрешить всем компьютерам подключаться к заданным веб-ресурсам без аутентификации на прокси-сервере, в блоке параметров **Назначение** укажите один из следующих параметров:

- IP-адрес.

8. В поле **IP-адрес** перейдите по ссылке **Изменить все**.

Откроется окно **IP-адреса**.

9. Введите один или несколько IP-адресов.

Вы можете указывать IP-адреса в одном из следующих форматов:

- IPv4-адрес (например, 172.16.5.6).
- IPv4-подсеть с маской в формате CIDR notation (например, 192.168.1.0/24).
- IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6-подсеть с маской в формате CIDR notation (например, fc00::/7).

При указании нескольких IP-адресов используйте точку с запятой или новую строку в качестве разделителя.

10. Нажмите на кнопку **Добавить**.

Добавленные IP-адреса отобразятся в таблице под полем ввода. Если введенное значение имеет недопустимый формат, слева от него появится значок . Вы можете изменить этот адрес с помощью кнопки  в правой части строки.

11. Нажмите на кнопку **Сохранить**.

- Имя хоста.

12. В поле **Имя хоста** перейдите по ссылке **Изменить все**.

Откроется окно **Имена хостов**.

13. Введите одно или несколько имен хостов.

При указании нескольких имен используйте точку с запятой или новую строку в качестве разделителя.

Чтобы включить поддомены, используйте точку в начале значения. В этом случае недопустимо указывать поддомены в качестве отдельных записей, так как это может привести к ошибкам в работе прокси-сервера. Например, если вы указали `.example.org`, не следует добавлять запись `abc.example.org`.

14. Нажмите на кнопку **Добавить**.

Добавленные имена хостов отобразятся в таблице под полем ввода.

15. Если вы хотите, чтобы в фильтр попадали все поддомены указанного имени, установите флажок **Включить поддомены**.

Если вы ввели имя хоста с точкой в начале значения, флажок **Включить поддомены** будет установлен автоматически.

16. Нажмите на кнопку **Сохранить**.

17. Нажмите на кнопку **Сохранить**.

Исключения аутентификации будут добавлены.

Настройка формата журнала доступа

Информация о всех запросах веб-ресурсов, которые обрабатывает сервис Squid, сохраняется в файле `access.log`. Этот файл называется *журналом доступа*. Вы можете изменить формат, в котором записи о запросах будут сохраняться в журнале доступа.

► Чтобы настроить формат журнала доступа, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Журнал**.
2. Переведите переключатель в положение **Включено**.
3. Выберите один из следующих форматов журнала доступа:

- **По умолчанию.**

Формат журнала доступа, используемый сервисом Squid по умолчанию. При выборе этого варианта в конфигурационный файл `squid.conf` добавляются следующие строки:

```
logformat kl_format %6tr %>a %Ss/%03>Hs %<st %rm %ru %[un %Sh/%<a %mt  
access_log syslog:local2.info kl_format
```

В журнал доступа сохраняются время и статус запроса, адрес источника соединения,

информация об HTTP-заголовках веб-ресурса.

- **Пользовательский.**

Вы можете изменить состав и формат данных, сохраняемых сервисом Squid в журнал доступа. Это может понадобиться, например, для обработки журнала сторонними программами, требующими определенного формата.

При выборе этого варианта в конфигурационный файл squid.conf добавляются следующие строки:

```
logformat custom_format <значение в поле Форма записи (format specification)>
```

```
access_log syslog:local2.info custom_format
```

4. Если вы выбрали вариант **Пользовательский**, в поле **Форма записи (format specification)** введите код формата.

Вы можете использовать предустановленные форматы **Squid**, **Common**, **Combined**, **Referrer** и **Useragent** с помощью ссылок под полем ввода.

Более подробную информацию о форматах журнала доступа вы можете найти на сайте [www.squid-cache.org http://www.squid-cache.org/Doc/config/logformat/](http://www.squid-cache.org/Doc/config/logformat/).

5. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Формат журнала доступа будут настроен. Информация о запросах веб-ресурсов, обрабатываемых сервисом Squid, будет сохраняться в файле access.log в заданном формате.

Восстановление параметров до значений по умолчанию

► Чтобы восстановить параметры встроенного прокси-сервера до значений по умолчанию, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Общие**.
2. В правом нижнем углу перейдите по ссылке **Изменить все параметры на значения по умолчанию**.
3. В окне подтверждения нажмите на кнопку **Да**.

Все параметры прокси-сервера будут изменены на значения по умолчанию, в том числе параметры аутентификации, журнала доступа и управления SSL-соединениями. Будут удалены все сертификаты для перехвата SSL-соединений, SSL-правила и отпечатки доверенных сертификатов.

Расшифровка TLS/SSL-соединений

Функциональность доступна только в программе, развернутой из ISO-файла. При установке программы из rpm/deb-пакета администратору требуется настроить расшифровку TLS/SSL-соединений средствами прокси-сервера.

Компьютеры пользователей могут устанавливать соединение с веб-ресурсами как в открытом, так и в зашифрованном виде. Kaspersky Web Traffic Security может выполнять проверку обоих видов трафика. Открытые соединения проверяются с помощью стандартных правил обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. [84](#)). Чтобы обрабатывать зашифрованный трафик, требуется настроить расшифровку TLS/SSL-соединений. Если расшифровка не настроена, программа не сможет применить все параметры правил доступа, а также выполнить проверку с помощью модулей Антивирус и Анти-Фишинг в рамках правил защиты.

В документации и веб-интерфейсе программы термин SSL используется как устоявшийся синоним шифрования (SSL-соединения, SSL-правила). Однако для установки зашифрованных соединений рекомендуется использовать протокол TLS версии 1.2, так как протокол SSL является устаревшим и небезопасным.

Расшифровка SSL-соединений состоит из следующих этапов.

1. Ознакомление с особенностями обработки зашифрованных соединений

Для правильного понимания логики работы программы и корректной настройки параметров рекомендуется предварительно ознакомиться с особенностями обработки CONNECT-запросов (см. раздел "Обработка CONNECT-запросов" на стр. [223](#)) и установки TLS-соединений (см. раздел "О TLS-соединениях" на стр. [229](#)).

2. Добавление сертификата для перехвата SSL-соединений (см. раздел "Работа с сертификатами для перехвата SSL-соединений" на стр. [234](#))

После добавления одного или нескольких сертификатов требуется назначить один из них активным (см. раздел "Назначение сертификата активным" на стр. [241](#)). Если ни один сертификат не является активным, включение расшифровки SSL-соединений недоступно.

3. Включение расшифровки SSL-соединений (см. раздел "Включение и отключение расшифровки SSL-соединений" на стр. [244](#))

4. Выбор действия над SSL-соединениями по умолчанию (на стр. [245](#))

Действие по умолчанию будет применяться к SSL-соединениям, которые не удовлетворяют условиям ни одного SSL-правила.

5. Создание и настройка SSL-правил (см. раздел "Работа с SSL-правилами" на стр. [245](#))

С помощью SSL-правил вы можете задать действия программы над SSL-соединениями в зависимости от источника или назначения соединения.

6. Добавление доверенных сертификатов (см. раздел "Работа с доверенными сертификатами" на стр. [251](#))

Прокси-сервер будет присваивать статус *Доверенный* сертификатам безопасности веб-ресурсов, к

которым применяется действие **Bump**.

В этом разделе

Обработка CONNECT-запросов	223
О TLS-соединениях.....	229
Работа с сертификатами для перехвата SSL-соединений.....	234
Включение и отключение расшифровки SSL-соединений.....	244
Выбор действия над SSL-соединениями по умолчанию	245
Работа с SSL-правилами	245
Работа с доверенными сертификатами	251

Обработка CONNECT-запросов

При обработке трафика, передаваемого по протоколу HTTPS, результат применения действий программы **Заблокировать** и **Перенаправить** отличается от применения этих действий к трафику, передаваемому по протоколу HTTP. Пользователю не отображается страница блокировки, и не выполняется перенаправление на заданный URL-адрес. Вместо этого соединение обрывается.

Это связано с тем, что для установки шифрованных соединений по протоколу HTTPS компьютер пользователя запрашивает у прокси-сервера соединение с веб-сервером с помощью HTTP-сообщения, содержащего метод CONNECT (далее также "CONNECT-запрос"). Возможности прокси-серверов по обработке CONNECT-запросов и ответу на них ограничены на уровне HTTP-протокола. Прокси-сервер может либо уведомить пользователя об успешной установке соединения, либо прервать соединение.

Чтобы действия **Заблокировать** и **Перенаправить** применялись корректно, вам требуется включить расшифровку TLS/SSL-соединений (см. раздел "Включение и отключение расшифровки SSL-соединений" на стр. [244](#)), а также добавить метод CONNECT в исключения (см. раздел "Настройка исключений в правилах обработки трафика" на стр. [227](#)) или создать для него правило обхода (см. раздел "Создание правила обхода" на стр. [228](#)). При отсутствии правил обработки трафика, разрешающих CONNECT-запросы, соединение будет прервано.

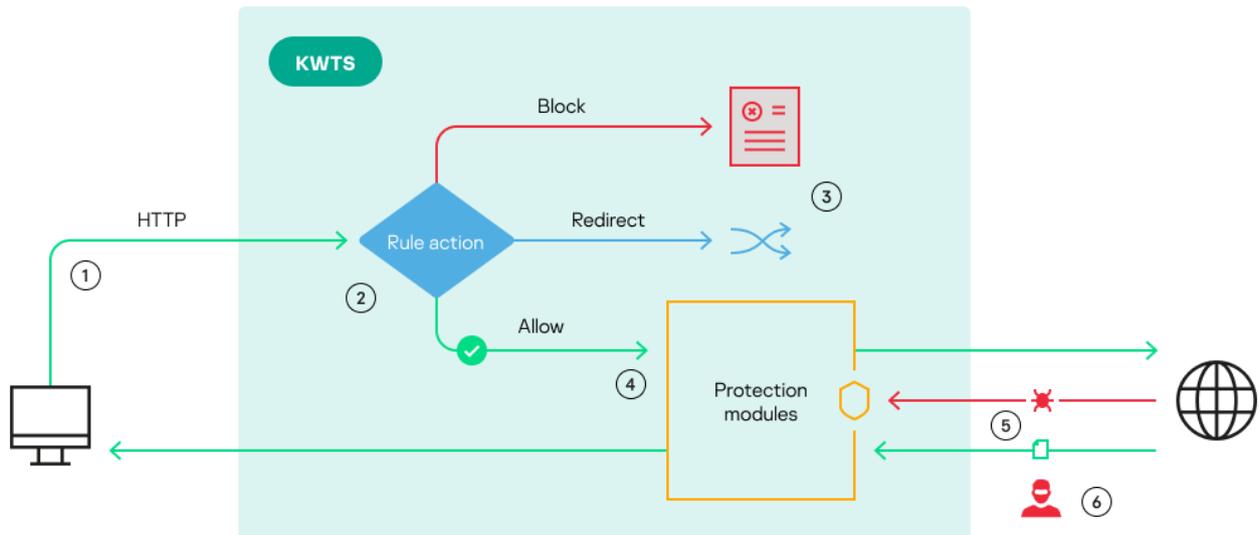
Разрешение CONNECT-запросов может привести к снижению защиты IT-инфраструктуры организации. Рекомендуется добавлять метод CONNECT в исключения только в тех правилах обработки трафика, для которых отображение страницы блокировки и выполнение перенаправления являются критичными.

Далее в этой статье приведены особенности и различия в обработке трафика, передаваемого по протоколу HTTP с помощью стандартных HTTP-сообщений, и трафика, передаваемого по протоколу HTTPS, когда для установки шифрованных соединений используются CONNECT-запросы.

Обработка стандартных HTTP-сообщений

Большинство HTTP-методов (например, GET, POST, DELETE, HEAD, OPTIONS, PATCH, PUT, TRACE) предназначено для обмена HTTP-сообщениями между клиентом, то есть компьютером пользователя, и веб-сервером, на котором хранится запрашиваемый веб-ресурс. Kaspersky Web Traffic Security может

проверять такие HTTP-сообщения и применять к ним все доступные в программе действия. Принципы обработки HTTP-сообщений в программе Kaspersky Web Traffic Security представлены на рисунке ниже.

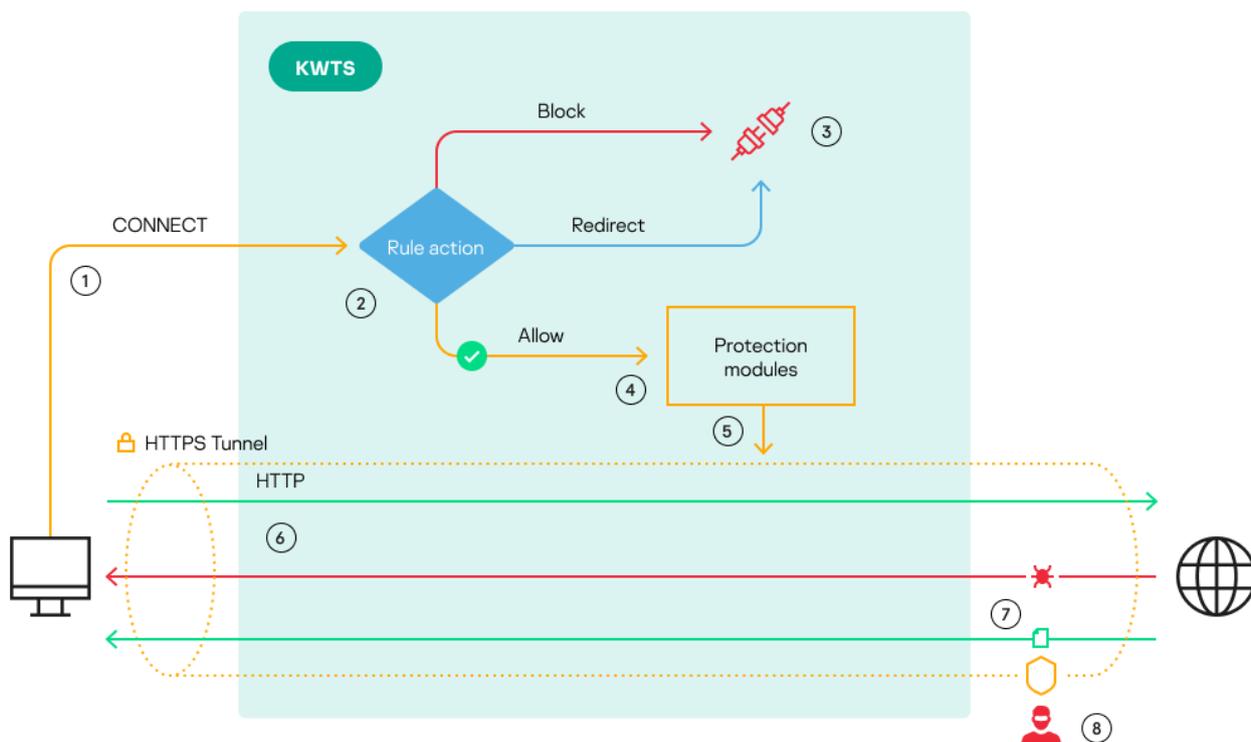


Нумерация на рисунке соответствует следующим этапам обработки стандартных HTTP-сообщений:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на прокси-сервер.
2. Программа проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правила доступа выполняется действие **Заблокировать**, пользователю отображается страница блокировки. Если выполняется действие **Перенаправить**, пользователь перенаправляется на заданный URL-адрес.
4. Если в результате применения правила доступа выполняется действие **Разрешить**, то программа переходит к проверке трафика с помощью правил защиты или политики защиты по умолчанию. При отсутствии обнаруженных угроз запрос пользователя передается на веб-сервер.
5. Полученный ответ от веб-сервера также проверяется модулями защиты на наличие вирусов и других угроз. При обнаружении угроз программа блокирует трафик, а при их отсутствии передает ответ веб-сервера на компьютер пользователя.
6. При попытке несанкционированного доступа злоумышленники могут перехватить данные, так как трафик передается в нешифрованном виде.

Особенности обработки CONNECT-запросов

При попытке получить доступ к веб-ресурсу по протоколу HTTPS компьютер пользователя отправляет на прокси-сервер CONNECT-запрос на соединение с веб-сервером. В результате обмена параметрами шифрования и сертификатами безопасности между компьютером пользователя и веб-сервером устанавливается туннелированное защищенное соединение по протоколу TLS. Внутри этого туннеля клиент и веб-сервер обмениваются HTTP-сообщениями с использованием стандартных HTTP-методов (GET, POST и т.д.). По умолчанию прокси-сервер не может анализировать содержимое зашифрованного соединения и вмешиваться в обмен сообщениями внутри туннеля. Механизм обработки зашифрованных соединений по умолчанию представлен на рисунке ниже.



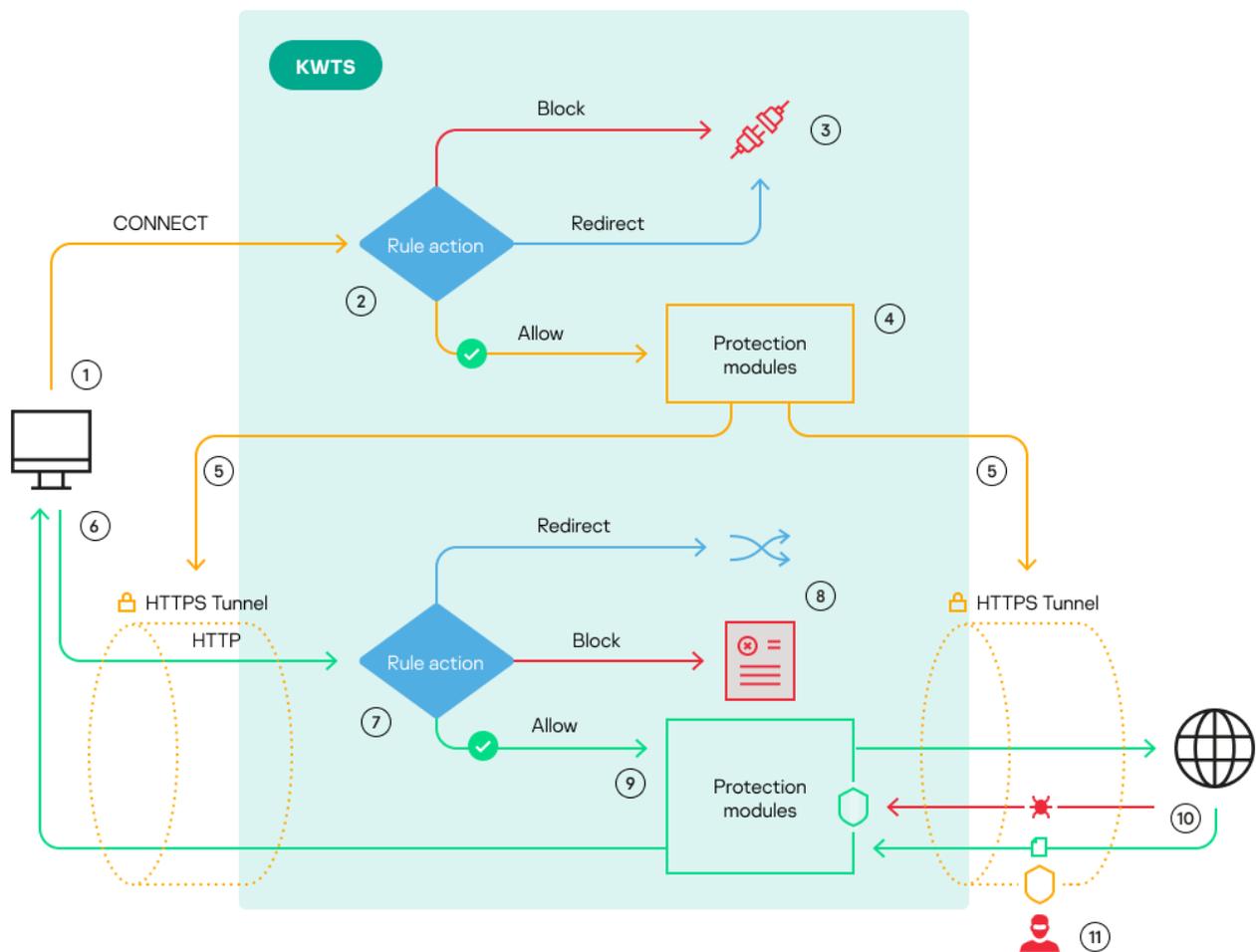
Нумерация на рисунке соответствует следующим этапам обработки зашифрованных соединений по умолчанию:

1. Компьютер пользователя при помощи CONNECT-запроса запрашивает у прокси-сервера организацию зашифрованного канала связи с веб-сервером.
2. Программа проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правил выполняется действие **Заблокировать** или **Перенаправить**, соединение обрывается. Пользователю не отображается страница блокировки, и он не перенаправляется на заданный URL-адрес.
4. Если в результате применения правила доступа выполняется действие **Разрешить**, программа передает CONNECT-запрос для дальнейшей обработки модулями защиты.
5. При успешной проверке CONNECT-запроса модулями защиты прокси-сервер формирует зашифрованный канал связи между компьютером пользователя и веб-сервером.
6. Внутри зашифрованного канала связи компьютер пользователя обменивается с веб-сервером обычными HTTP-сообщениями. При этом прокси-сервер не может получить доступ к этим

сообщениям и передать их на проверку модулям защиты, так как передаваемые данные зашифрованы.

7. Ответ веб-сервера также передается компьютеру пользователя напрямую без проверки модулями защиты. Это снижает уровень защиты ИТ-инфраструктуры организации, так как на компьютер пользователя может поступать трафик, содержащий угрозы.
8. При попытке несанкционированного доступа злоумышленники не могут перехватить данные, так как трафик передается внутри зашифрованного канала.

Чтобы программа могла проверять трафик, передаваемый внутри зашифрованного канала связи, модулями защиты, вам требуется настроить расшифровку TLS/SSL-соединений. Механизм обработки зашифрованных соединений при включенной расшифровке TLS/SSL-соединений представлен на рисунке ниже.



Нумерация на рисунке соответствует следующим этапам обработки зашифрованных соединений при включенной расшифровке TLS/SSL-соединений:

1. Компьютер пользователя при помощи CONNECT-запроса запрашивает у прокси-сервера организацию зашифрованного канала связи с веб-сервером.
2. Программа проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правила доступа выполняется действие **Заблокировать** или **Перенаправить**, соединение обрывается. Пользователю не отображается страница блокировки, и

он не перенаправляется на заданный URL-адрес.

4. Если в результате применения правила доступа выполняется действие **Разрешить**, программа передает CONNECT-запрос для дальнейшей обработки модулями защиты.
5. При успешной проверке CONNECT-запроса модулями защиты между компьютером пользователя и прокси-сервером, а также между прокси-сервером и веб-сервером устанавливаются зашифрованные каналы связи.
6. Внутри зашифрованного канала связи компьютер пользователя обменивается с веб-сервером обычными HTTP-запросами. Программа получает доступ ко всем передаваемым данным и может применять к ним правила защиты.
7. Программа проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
8. Если в результате применения правила доступа выполняется действие **Заблокировать**, пользователю отображается страница блокировки. Если выполняется действие **Перенаправить**, пользователь перенаправляется на заданный URL-адрес.
9. Если в результате применения правила доступа выполняется действие **Разрешить**, то программа переходит к проверке трафика с помощью правил защиты или политики защиты по умолчанию. При отсутствии обнаруженных угроз запрос пользователя передается на веб-сервер.
10. Полученный ответ от веб-сервера также проверяется модулями защиты на наличие вирусов и других угроз. При обнаружении угроз программа блокирует трафик, а при их отсутствии передает ответ веб-сервера на компьютер пользователя по зашифрованному каналу связи.
11. При попытке несанкционированного доступа злоумышленники не могут перехватить данные, так как трафик передается внутри зашифрованного канала связи.

В этом разделе

Настройка исключений в правилах обработки трафика	227
Создание правила обхода	228

Настройка исключений в правилах обработки трафика

Перед созданием исключений для CONNECT-запросов убедитесь, что вы включили расшифровку TLS/SSL-соединений (см. раздел "Включение и отключение расшифровки SSL-соединений" на стр. [244](#)). В противном случае зашифрованные соединения не будут проверены модулями Антивирус и Анти-Фишинг. Это может привести к заражению компьютеров пользователей.

► Чтобы настроить исключения для CONNECT-запросов в правилах обработки трафика, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Правила**.
2. Выберите закладку **Доступ**.
3. Выберите правило, для которого требуется корректно отображать страницу блокировки или выполнять перенаправление пользователя.

Откроется страница **Просмотреть правило**.

4. Нажмите на кнопку **Изменить**.
Откроется страница **Изменить правило**.
5. Выберите закладку **Исключения**.
6. Нажмите на кнопку **+ Добавить исключение**.
7. Если вы хотите добавить исключение только для пользователей с заданными критериями, в блоке параметров **Инициатор** нажмите на кнопку **+ Условия правила** и укажите нужные критерии.
Если критерии не указаны, исключение распространяется на всех пользователей.
8. В блоке параметров **Фильтрация трафика** нажмите на кнопку **+ Условия правила**.
9. В появившемся раскрывающемся списке слева выберите **HTTP-метод**.
10. В раскрывающемся списке справа выберите **CONNECT**.
11. Нажмите на кнопку **Сохранить**.

Исключение будет настроено. Программа не будет проверять HTTP-сообщения, содержащие метод CONNECT.

Создание правила обхода

Перед созданием правила обхода убедитесь, что вы включили расшифровку TLS/SSL-соединений (см. раздел "Включение и отключение расшифровки SSL-соединений" на стр. [244](#)). Если расшифровка TLS/SSL-соединений не настроена, HTTP-сообщения, содержащие метод CONNECT, не будут проверены модулями Антивирус и Анти-Фишинг. Это может привести к заражению компьютеров пользователей.

- Чтобы создать правило обхода для CONNECT-запросов, выполните следующие действия:
1. В веб-интерфейсе программы выберите раздел **Правила**.
 2. Выберите закладку **Обход**.
 3. Нажмите на кнопку **Добавить правило**.
Откроется окно **Добавить правило**.
 4. В раскрывающемся списке **Действие** выберите **Разрешить без проверки**.
 5. Если вы хотите добавить правило только для пользователей с заданными критериями, в блоке параметров **Инициатор** нажмите на кнопку **+ Условия правила** и укажите нужные критерии.
Если критерии не указаны, правило распространяется на всех пользователей.
 6. В блоке параметров **Фильтрация трафика** нажмите на кнопку **+ Условия правила**.
 7. В появившемся раскрывающемся списке слева выберите **HTTP-метод**.
 8. В раскрывающемся списке справа выберите **CONNECT**.
 9. В поле **Название правила** введите название правила.
 10. Если требуется, в поле **Комментарий** укажите любую дополнительную информацию о правиле.
 11. Переведите переключатель **Статус** в положение **Включено**.

12. Нажмите на кнопку **Добавить**.

Правило обхода будет создано и отобразится в таблице правил. Программа будет пропускать без проверки все HTTP-сообщения, содержащие метод CONNECT.

О TLS-соединениях

Когда пользователь хочет подключиться к веб-ресурсу по протоколу HTTPS, требуется установить защищенное шифрованное соединение между его компьютером и веб-сервером, на котором хранится требуемый веб-ресурс. После установки базового TCP/IP-соединения клиент и сервер обмениваются сертификатами безопасности и параметрами шифрования. В результате создается шифрованный канал связи с помощью протокола TLS (Transport Layer Security). Поэтому шифрованные соединения называют также TLS-соединениями. Внутри этого канала данные передаются по протоколу прикладного уровня, например, HTTP.

Если в программе выключена расшифровка TLS/SSL-соединений, то прокси-сервер пересылает сообщения между клиентом и сервером, не вмешиваясь в процесс установки шифрованного соединения. В этом случае модули защиты Kaspersky Web Traffic Security (Антивирус и Анти-Фишинг) не могут проверить данные, передаваемые внутри шифрованного канала связи. Это снижает уровень защиты IT-инфраструктуры организации. Поэтому рекомендуется включить расшифровку TLS/SSL-соединений.

При включении расшифровки TLS/SSL-соединений в параметрах программы прокси-сервер получает возможность вмешиваться в процесс установки соединения. В этом случае программа может применять к трафику действия, заданные в SSL-правилах, или действия по умолчанию, если проверяемый трафик не удовлетворяет условиям ни одного SSL-правила.

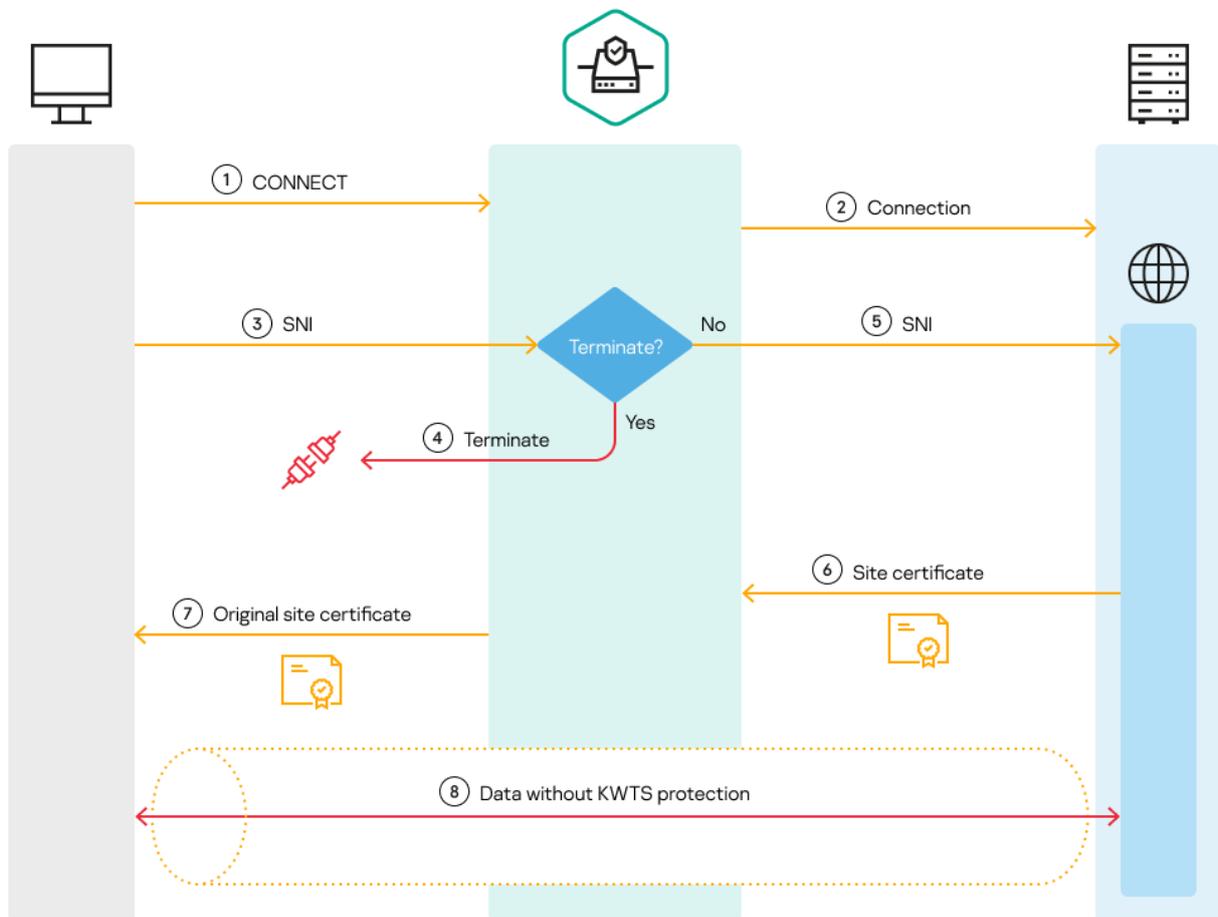
В программе предусмотрены следующие действия для обработки шифрованных соединений:

- **Tunnel.**
- **Tunnel with SNI check.**
- **Bump.**
- **Terminate.**

Для обеспечения максимального уровня защиты рекомендуется выбирать действие **Bump**. Действия **Tunnel** и **Tunnel with SNI check** рекомендуется использовать только для веб-ресурсов или приложений, не поддерживающих работу при расшифровке передаваемого трафика (например, банковские приложения).

Применение действий Tunnel, Tunnel with SNI check или Terminate

Принципы установки шифрованных соединений при применении действий **Tunnel**, **Tunnel with SNI check** или **Terminate** представлены на рисунке ниже.



Установка шифрованного соединения состоит из следующих этапов:

1. Запрос клиента

Клиент отправляет на прокси-сервер CONNECT-запрос на соединение с веб-сервером. Этот запрос содержит полное доменное имя (FQDN) или IP-адрес веб-сервера, на котором размещается запрашиваемый веб-ресурс.

2. Передача запроса серверу

Прокси-сервер формирует и отправляет запрос на соединение с веб-сервером, получает от него ответ и передает этот ответ клиенту.

3. Передача прокси-серверу SNI и других параметров шифрования клиента

Клиент передает прокси-серверу набор поддерживаемых параметров шифрования, а также поле SNI, в рамках которого указано полное доменное имя (далее также "FQDN") нужного веб-ресурса (веб-сайта).

4. Проверка на необходимость прерывания соединения

Если согласно действиям, заданным в SSL-правилах, или действию по умолчанию к запросу применяется действие **Terminate**, то соединение прерывается. Пользователю не отображается страница блокировки.

5. Передача веб-серверу SNI и других параметров шифрования клиента

Если к запросу не было применено действие **Terminate**, прокси-сервер передает веб-серверу поле SNI и другие параметры шифрования от имени клиента.

6. Передача сертификата веб-ресурса прокси-серверу

Веб-сервер возвращает прокси-серверу свой набор поддерживаемых параметров шифрования, а также сертификат веб-ресурса, к которому пользователь запросил доступ, на основе поля SNI.

7. Передача сертификата веб-ресурса клиенту

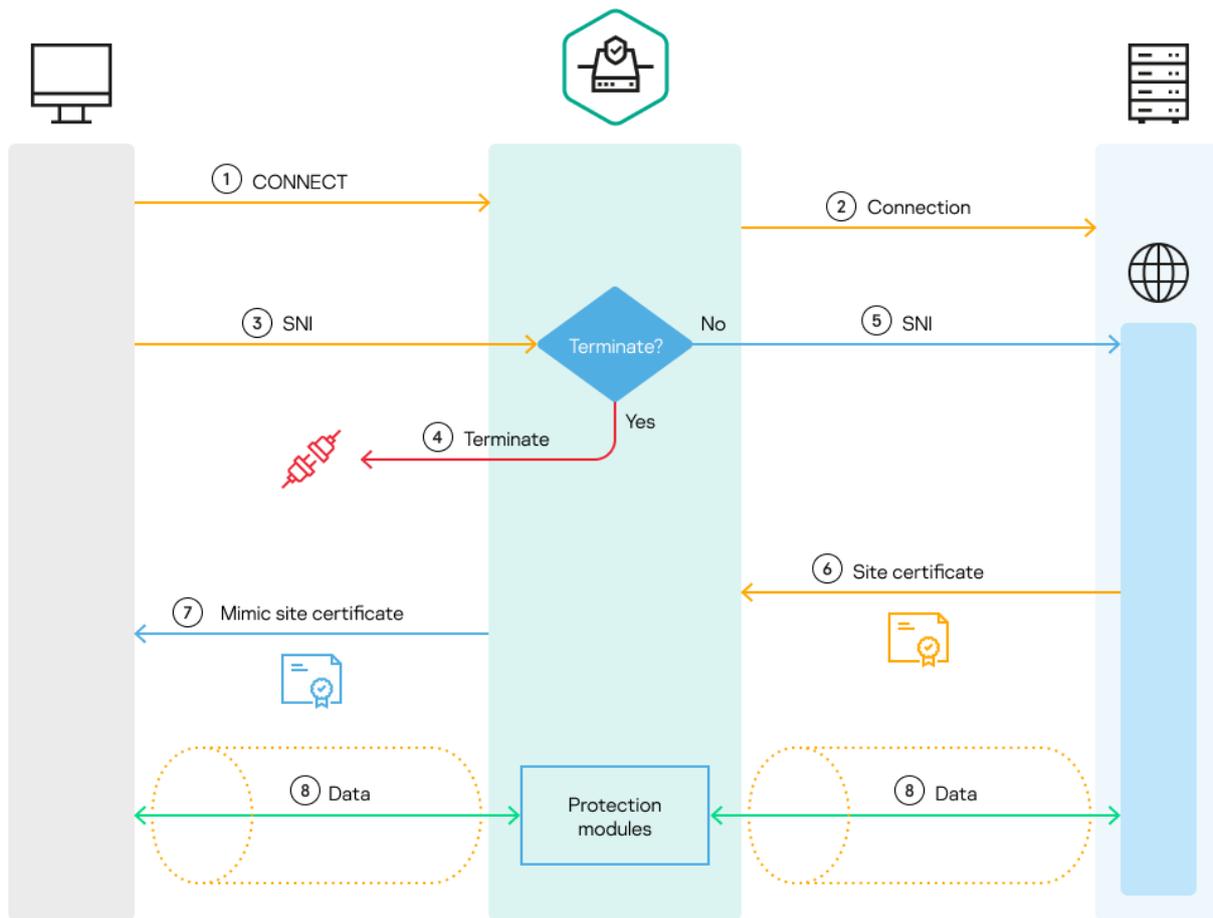
Прокси-сервер передает клиенту сертификат и параметры шифрования, полученные от веб-сервера.

8. Установка защищенного соединения

Клиент и сервер согласуют остальные детали подключения. После этого создается защищенный канал связи, внутри которого клиент и сервер могут обмениваться данными.

Применение действий Terminate и Bump

Принципы обработки шифрованных соединений при применении действий **Terminate** и **Bump** представлены на рисунке ниже. В этом случае шаги 5 и 7 отличаются от базовой схемы установки шифрованных соединений. На шаге 5 прокси-сервер передает поле SNI и другие параметры шифрования не от имени клиента, а от своего имени. Прокси-сервер получает от веб-сервера сертификат запрашиваемого веб-ресурса, формирует на его основе свой (подменный) сертификат и передает этот подменный сертификат клиенту.



Различия в процессе обработки программой шифрованного соединения в зависимости от заданного действия представлен в таблице ниже.

Таблица 20. Обработка шифрованных соединений программой в зависимости от заданного действия

Без участия прокси-сервера	Tunnel	Tunnel with SNI check	Bump	Terminate
----------------------------	--------	-----------------------	------	-----------

Без участия прокси-сервера	Tunnel	Tunnel with SNI check	Bump	Terminate
Запрос клиента.	Запрос клиента. Прокси-сервер разрешает создание защищенного канала на основе IP-адреса или FQDN веб-сервера.	Запрос клиента.	Запрос клиента.	Запрос клиента.
Ответ сервера.	Ответ сервера.	Ответ сервера.	Ответ сервера.	Ответ сервера.
Передача SNI и других параметров шифрования клиента.	Передача SNI и других параметров шифрования клиента.	Передача SNI и других параметров шифрования клиента. Прокси-сервер разрешает создание защищенного канала на основе SNI запрашиваемого веб-ресурса.	Передача SNI и других параметров шифрования клиента. Прокси-сервер отправляет эти данные на веб-сервер, но не от имени клиента, а от своего имени.	Соединение прерывается. Пользователю не отображается страница блокировки.
Передача сертификата запрашиваемого веб-ресурса.	Передача сертификата запрашиваемого веб-ресурса.	Передача сертификата запрашиваемого веб-ресурса.	Передача сертификата запрашиваемого веб-ресурса. Прокси-сервер перехватывает сертификат, присланный веб-сервером, и формирует на его основе свой подменный сертификат.	–

Без участия прокси-сервера	Tunnel	Tunnel with SNI check	Bump	Terminate
Установка защищенного соединения.	Установка защищенного соединения. Программа не может выполнить проверку передаваемых данных модулями Антивирус и Анти-Фишинг.	Установка защищенного соединения. Программа не может выполнить проверку передаваемых данных модулями Антивирус и Анти-Фишинг.	Установка защищенного соединения. Создается два канала: один между клиентом и прокси-сервером, а второй между прокси-сервером и веб-сервером. Программа может анализировать содержимое защищенных каналов и применять правила обработки трафика к передаваемым внутри канала данным.	–

Работа с сертификатами для перехвата SSL-соединений

Для расшифровки SSL-соединений требуется добавить один или несколько сертификатов, а затем назначить один из добавленных сертификатов активным (см. раздел "Назначение сертификата активным" на стр. [241](#)). Остальные сертификаты будут отображаться со статусом *Неактивный*. Вы можете в любой момент назначить активным другой сертификат.

Вы можете использовать сертификаты следующих типов:

- Самоподписанный сертификат (см. раздел "Добавление самоподписанного сертификата" на стр. [235](#)).
- Сертификат на основе CSR (см. раздел "Добавление сертификата на основе CSR" на стр. [236](#)).
- Сертификат в формате PFX (см. раздел "Добавление сертификата в формате PFX" на стр. [238](#)).

Сравнительные характеристики поддерживаемых в программе типов сертификатов приведены в таблице ниже.

Таблица 21. Сравнительные характеристики поддерживаемых типов сертификатов

Характеристика	Самоподписанный	На основе CSR	В формате PFX
----------------	-----------------	---------------	---------------

Характеристика	Самоподписанный	На основе CSR	В формате PFX
Необходимость использовать собственный центр сертификации	Нет	Да	Да
Необходимость распространять сертификат на компьютеры локальной сети организации	Да	Нет	Нет
Хранение закрытого ключа сертификата вне кластера	Нет	Нет	Да
Возможность вручную настроить параметры сертификата	Доступно заполнение только некоторых полей	Доступно заполнение только некоторых полей	Да

В этом разделе

Добавление самоподписанного сертификата	235
Добавление сертификата на основе CSR	236
Добавление сертификата в формате PFX	238
Просмотр информации о сертификате	241
Назначение сертификата активным	241
Скачивание сертификата	242
Удаление сертификата	242
Импорт сертификата на компьютеры пользователей	242

Добавление самоподписанного сертификата

► Чтобы добавить самоподписанный сертификат, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. Нажмите на кнопку **Добавить сертификат**.
Откроется окно **Создать сертификат**.
3. Выберите вариант **Самоподписанный**.
4. В поле **Организация** введите название организации.
5. В поле **Общее имя** введите доменное имя сервера, для которого создается сертификат.

6. Нажмите на кнопку **Добавить**.

Сертификат будет добавлен и отобразится в таблице сертификатов для перехвата SSL-соединений.

Добавление сертификата на основе CSR

Добавление сертификата на основе CSR состоит из следующих этапов.

1. Создание файла запроса в веб-интерфейсе программы (см. раздел "Создание файла запроса" на стр. [236](#))
2. Формирование сертификата на основе файла запроса в центре сертификации (см. раздел "Формирование сертификата в центре сертификации" на стр. [237](#))
3. Загрузка сформированного сертификата в веб-интерфейсе программы (см. раздел "Загрузка сертификата в веб-интерфейсе программы" на стр. [238](#))

В программе доступна загрузка отдельных сертификатов в виде файлов с расширениями .pem, .der, .cer, .crt, а также файлов-контейнеров PKCS#7 с расширением .p7b, содержащих цепочку сертификатов.

В этом разделе

Создание файла запроса.....	236
Формирование сертификата в центре сертификации	237
Загрузка сертификата в веб-интерфейсе программы	238

Создание файла запроса

► *Чтобы создать файл запроса, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. Нажмите на кнопку **Добавить сертификат**.
Откроется окно **Создать сертификат**.
3. Выберите вариант **Файл запроса CSR**.
4. В поле **Организация** введите название организации.
5. В поле **Общее имя** введите полное доменное имя (FQDN) сервера, для которого создается сертификат.
6. Нажмите на кнопку **Добавить**.
Запись о запросе CSR отобразится в таблице сертификатов для перехвата SSL-соединений.
7. Выберите созданную запись о запросе CSR.
Откроется окно **Просмотреть сертификат**.
8. Нажмите на кнопку **Создать файл запроса**.

Файл запроса будет сохранен в папку загрузки браузера. Используйте этот файл запроса для формирования сертификата в центре сертификации (см. раздел "Формирование сертификата в центре

сертификации" на стр. [237](#)).

Формирование сертификата в центре сертификации

Инструкция приведена для центра сертификации Microsoft Enterprise Certification Authority, развернутом на сервере Windows Server 2016.

Рекомендуется использовать браузер Internet Explorer. В других браузерах могут некорректно отображаться некоторые страницы центра сертификации Microsoft Enterprise Certification Authority.

► Чтобы сформировать сертификат на основе CSR, выполните следующие действия:

1. Откройте созданный ранее файл запроса (см. раздел "Создание файла запроса" на стр. [236](#)) в любом текстовом редакторе и скопируйте его содержимое в буфер обмена.
2. Откройте в браузере страницу вашего центра сертификации: `https://<адрес сервера>/certsrv`.
3. Выберите **Request a certificate**.
Откроется страница **Request a Certificate**.
4. Выберите **advanced certificate request**.
Откроется страница **Advanced Certificate Request**.
5. Выберите **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
Откроется страница **Submit a Certificate Request or Renewal Request**.
6. В поле **Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)** вставьте содержимое файла запроса, скопированное на шаге 1.
7. В раскрывающемся списке **Certificate Template** выберите **Subordinate Certification Authority**.
8. Нажмите на кнопку **Submit**.
Откроется страница **Certificate Issued**.
9. Выполните следующие действия:
 - a. Выберите кодировку файла сертификата.
Программа поддерживает работу с сертификатами в кодировке DER и Base64.
 - b. Выберите формат сертификата:
 - Если вы хотите скачать файл конечного сертификата с расширением .cer, не содержащий промежуточных сертификатов, выберите **Download certificate**.
 - Если вы хотите скачать полную цепочку сертификатов в формате PKCS#7-контейнера с расширением .p7b, выберите **Download certificate chain**.

Рекомендуется скачать полную цепочку сертификатов, чтобы избежать проблем с проверкой промежуточных центров сертификации.

Сертификат будет сформирован и сохранен на вашем компьютере в папке загрузки браузера.

Загрузка сертификата в веб-интерфейсе программы

► Чтобы загрузить сертификат на основе CSR в веб-интерфейсе программы, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. В таблице сертификатов для перехвата SSL-соединений выберите запись о сертификате, для которого был сформирован файл запроса.
Откроется окно **Просмотреть сертификат**.
3. Нажмите на кнопку **Загрузить сертификат**.
Откроется окно выбора файлов.
4. Выберите файл сертификата (см. раздел "Формирование сертификата в центре сертификации" на стр. [237](#)), сформированный в центре сертификации, и нажмите на кнопку **Open**.

В окне **Просмотреть сертификат** отобразится отпечаток сертификата и дата его истечения.

Сертификат будет загружен. В таблице сертификатов для перехвата SSL-соединений тип сертификата изменится с **Файл запроса CSR на основе CSR**.

Добавление сертификата в формате PFX

Добавление сертификата в формате PFX состоит из следующих этапов.

1. Формирование сертификата в центре сертификации (на стр. [238](#))
Сертификат с закрытым ключом формируется в формате PKCS#12-контейнера и сохраняется в хранилище сертификатов текущего пользователя.
2. Экспорт сертификата в файл (на стр. [239](#))
После формирования сертификата необходимо экспортировать его вместе с закрытым ключом в файл с расширением .p12 или .pfx.
3. Загрузка сертификата в веб-интерфейсе программы (на стр. [240](#))

В этом разделе

Формирование сертификата в центре сертификации	238
Экспорт сертификата в файл	239
Загрузка сертификата в веб-интерфейсе программы	240

Формирование сертификата в центре сертификации

Инструкция приведена для центра сертификации Microsoft Certification Authority, развернутом на сервере Windows Server 2016.

Рекомендуется использовать браузер Internet Explorer. В других браузерах могут некорректно отображаться некоторые страницы центра сертификации Microsoft Certification Authority.

► Чтобы сформировать PFX-сертификат с закрытым ключом, выполните следующие действия:

1. Откройте в браузере страницу вашего центра сертификации: `https://<адрес сервера>/certsrv`.
2. Выберите **Request a certificate**.
Откроется страница **Request a certificate**.
3. Выберите **advanced certificate request**.
Откроется страница **Advanced Certificate Request**.
4. Выберите **Create and submit a request to this CA**.
Откроется страница **Advanced Certificate Request**.
5. В раскрывающемся списке **Certificate Template** выберите **Subordinate Certification Authority**.
6. В блоке параметров **Identifying Information For Offline Template** заполните информацию о вашей организации.

Поле **Name** является обязательным.

7. В блоке параметров **Key Options** выполните следующие действия:
 - a. Выберите вариант **Create new key set**.
 - b. В поле **Key Size** введите значение 2048.
 - c. Выберите вариант **Automatic key container name**.
 - d. Установите флажок **Mark keys as exportable**.
8. В блоке параметров **Additional Options** убедитесь, что флажок **Save request** снят.
9. Нажмите на кнопку **Submit**.
Откроется страница **Certificate Issued**.
10. Выберите **Install this certificate**.

Сертификат с закрытым ключом будет сформирован и сохранен в хранилище сертификатов вашей учетной записи.

Экспорт сертификата в файл

► Чтобы экспортировать сертификат с закрытым ключом в файл, выполните следующие действия:

1. Откройте консоль управления Microsoft (MMC).
2. Выберите **File** → **Add/Remove Snap-in**.

Откроется окно **Add or Remove Snap-ins**.

3. Выберите оснастку **Certificates** и нажмите кнопку **Add**.

Откроется окно **Certificates Snap-in**.

4. Выберите **My user account** и нажмите **Finish**.
5. В окне **Add/Remove Snap-ins** нажмите **OK**.
6. В дереве консоли выберите **Certificates – Current User** → **Personal** → **Certificates**.
7. В рабочей области выберите сертификат, сформированный ранее (см. раздел "Формирование сертификата в центре сертификации" на стр. [238](#)), и двойным нажатием откройте его свойства.
8. Выберите закладку **Details**.
9. Нажмите кнопку **Copy to File**.

Запустится мастер экспорта сертификата.

10. В окне **Export Private Key** выберите вариант **Yes, export the private key**.
11. В окне **Export File Format** выполните следующие действия:
 - a. Выберите вариант **Personal Information Exchange – PKCS #12 (.PFX)**.
 - b. Установите флажок **Include all certificates in the certification path if possible**.
12. В окне **Security** выполните следующие действия:
 - a. Установите флажок **Password**.
 - b. В поле ввода под флажком задайте пароль для защиты сертификата.
 - c. В поле **Confirm password** повторите пароль.
13. В окне **File to Export** выполните следующие действия:
 - a. Нажмите на кнопку **Browse**.
 - b. Откроется окно **Save as**.
 - c. Выберите путь для сохранения файла сертификата на вашем компьютере.
 - d. Введите имя файла и нажмите на кнопку **Save**.
14. В окне **Completing the Certificate Export Wizard** нажмите на кнопку **Finish**.

Сертификат с закрытым ключом будет экспортирован в файл. Файл будет сохранен на вашем компьютере по указанному пути.

Загрузка сертификата в веб-интерфейсе программы

► *Чтобы загрузить сертификат с закрытым ключом в веб-интерфейсе программы, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. Нажмите на кнопку **Добавить сертификат**.
Откроется окно **Создать сертификат**.
3. Выберите вариант **В формате PFX**.
4. Нажмите на кнопку **Загрузить**.

Откроется окно выбора файла.

5. Выберите файл, в который вы экспортировали сертификат с закрытым ключом (см. раздел "Экспорт сертификата в файл" на стр. [239](#)), и нажмите на кнопку **Открыть**.
6. Имя файла сертификата отобразится в поле ввода слева от кнопки **Загрузить**.
7. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.
8. Нажмите на кнопку **Добавить**.

Сертификат будет добавлен и отобразится в таблице сертификатов для перехвата SSL-соединений.

Просмотр информации о сертификате

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

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. В таблице сертификатов для перехвата SSL-соединений выберите сертификат, информацию о котором вы хотите просмотреть.

Откроется окно **Просмотреть сертификат**.

В окне содержится следующая информация о сертификате:

- **Статус** – статус использования сертификата.
- **Тип** – один из следующих типов сертификата:
 - **Самоподписанный**.
 - **Файл запроса CSR**.
 - **В формате PFX**.
- **Срок действия** – дата и время окончания срока действия сертификата.
- **Отпечаток SHA256** – отпечаток сертификата SHA256.
- **Субъект** – общее имя (CN, Common Name) и название организации владельца сертификата (O, Organization).

Назначение сертификата активным

► *Чтобы назначить сертификат активным, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. В таблице сертификатов для перехвата SSL-соединений выберите сертификат, который вы хотите назначить активным.

Откроется окно **Просмотреть сертификат**.

3. Нажмите на кнопку **Назначить активным**.

Сертификат будет назначен активным. В таблице напротив сертификата отобразится значок .

Скачивание сертификата

► Чтобы скачать сертификат, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. В таблице сертификатов для перехвата SSL-соединений выберите сертификат, который вы хотите скачать.

Откроется окно **Просмотреть сертификат**.

3. Нажмите на одну из следующих кнопок в зависимости от требуемого формата сертификата:
 - **P7B-цепочка** – цепочка сертификатов в формате .p7b.
 - **CRT** – конечный сертификат в формате .crt.

Сертификат или цепочка сертификатов будут сохранены в папку загрузки браузера.

Удаление сертификата

► Чтобы удалить сертификат, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. В таблице сертификатов для перехвата SSL-соединений выберите сертификат, который вы хотите удалить.

Откроется окно **Просмотреть сертификат**.

Удаление активного сертификата при включенном управлении SSL-соединениями недоступно.

3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Сертификат будет удален.

Импорт сертификата на компьютеры пользователей

После добавления сертификата для перехвата SSL-соединений (см. раздел "Работа с сертификатами для перехвата SSL-соединений" на стр. [234](#)) требуется сделать этот сертификат доверенным для браузеров на компьютерах пользователей. Для этого вам нужно импортировать его в системное хранилище доверенных сертификатов операционной системы Windows.

Браузер Mozilla Firefox использует собственное хранилище сертификатов. Подробнее об импорте сертификата в хранилище Mozilla Firefox см. в инструкции ниже.

Вы можете импортировать сертификат одновременно на все компьютеры, входящие в домен, с помощью групповых политик Windows. Подробнее о групповых политиках см. в документации к операционной системе.

Если у вас нет возможности использовать для распространения сертификата групповые политики Windows, вам требуется вручную импортировать сертификат на каждый компьютер локальной сети организации.

► *Чтобы импортировать сертификат в хранилище доверенных сертификатов Windows вручную, выполните следующие действия:*

1. Скопируйте предварительно скачанный сертификат (см. раздел "Скачивание сертификата" на стр. [242](#)) на компьютер пользователя.
2. Двойным щелчком мыши откройте файл сертификата.
3. В открывшемся окне на закладке **General** нажмите на кнопку **Install Certificate**.
Запустится мастер импорта сертификата.
4. В приветственном окне мастера выберите один из следующих вариантов импорта сертификата:
 - **Current User.**
Сертификат будет доступен только при подключении под учетной записью текущего пользователя.
 - **Local Machine.**
Сертификат будет доступен для всех пользователей этого компьютера.

Для выбора этого варианта необходимо обладать правами локального администратора операционной системы.

Откроется окно **Certificate Store**.

5. Выберите вариант **Place all certificates in the following store** и нажмите на кнопку **Browse**.
Откроется окно **Select Certificate Store**.
6. Выберите хранилище **Trusted Root Certification Authorities** и нажмите на кнопку **OK**.
В окне **Certificate Store** отобразится название выбранного хранилища.
7. Нажмите на кнопку **Next**.
8. В завершающем окне мастера нажмите на кнопку **Finish**.
9. В сообщении об успешном импорте сертификата нажмите на кнопку **OK**.
Сертификат будет импортирован в системное хранилище доверенных сертификатов Windows.

► *Чтобы импортировать сертификат в хранилище браузера Mozilla Firefox вручную, выполните следующие действия:*

1. Скопируйте предварительно скачанный сертификат (см. раздел "Скачивание сертификата" на

стр. [242](#)) на компьютер пользователя.

2. В меню браузера Mozilla Firefox выберите пункт **Options**.
3. В открывшемся окне выберите закладку **Privacy & Security**.
Откроется страница **Browser Privacy**.
4. В блоке параметров **Security** в разделе **Certificates** нажмите на кнопку **View Certificates**.
Откроется окно **Certificate Manager**.
5. На закладке **Authorities** нажмите на кнопку **Import**.
Откроется окно выбора файла.
6. Выберите файл сертификата и нажмите на кнопку **Open**.
Откроется окно **Downloading Certificate**.
7. Установите флажок **Trust this CA to identify websites** и нажмите на кнопку **OK**.
Сертификат отобразится в списке сертификатов в окне **Certificate Manager**.
8. Нажмите на кнопку **OK**.
Сертификат будет импортирован в хранилище браузера Mozilla Firefox.

Включение и отключение расшифровки SSL-соединений

Для расшифровки SSL-соединений требуется добавить сертификат (см. раздел "Работа с сертификатами для перехвата SSL-соединений" на стр. [234](#)) и назначить его активным (см. раздел "Назначение сертификата активным" на стр. [241](#)).

► Чтобы включить или отключить расшифровку SSL-соединений, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.
2. Переведите переключатель **Расшифровывать TLS/SSL-соединения** в положение **Включено** или **Выключено**.

Переключатель доступен только при наличии активного сертификата для перехвата SSL-соединений.

3. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Расшифровка SSL-соединений будет включена или отключена.

Выбор действия над SSL-соединениями по умолчанию

Действие по умолчанию применяется, если SSL-соединение, содержащее CONNECT-запрос, не удовлетворяет условиям ни одного SSL-правила (см. раздел "Работа с SSL-правилами" на стр. [245](#)).

► Чтобы выбрать действие над SSL-соединениями по умолчанию, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL**.

2. В раскрывающемся списке **Действие по умолчанию** выберите один из следующих вариантов:

- **Tunnel with SNI check.**

Программа не будет перехватывать CONNECT-запросы, для которых не заданы правила обработки SSL-соединений. Эти запросы не будут учитываться в статистике обработанного трафика в разделе **Мониторинг**. При этом могут не применяться правила защиты, а также следующие условия правил доступа: **MIME-тип HTTP-сообщения**, **MIME-тип части HTTP-сообщения**, **Размер файла**, **HTTP-метод**.

- **Bump.**

Программа будет перехватывать CONNECT-запросы и анализировать содержимое зашифрованных соединений, для которых не заданы правила обработки SSL-соединений. Для сервисов, не поддерживающих перехват CONNECT-запросов, необходимо создать правила обработки SSL-соединений с действием **Tunnel**. При отсутствии таких правил SSL-соединение может быть заблокировано в случае ошибки перехвата.

- **Terminate.**

Программа будет блокировать CONNECT-запросы, для которых не заданы правила обработки SSL-соединений.

3. Нажмите на кнопку **Сохранить**.

Действие над SSL-соединениями по умолчанию будет настроено.

Работа с SSL-правилами

Вы можете настроить обработку зашифрованных соединений с помощью SSL-правил (см. раздел "Создание SSL-правила" на стр. [246](#)).

SSL-правила позволяют выбирать действия программы над SSL-соединениями в зависимости от следующих условий:

- источник соединения (IP-адрес или User Agent);
- назначение соединения (IP-адрес или имя хоста);
- порт назначения соединения.

Вы можете использовать в рамках одного SSL-правила одно условие или несколько условий, объединенных логическими операторами И / ИЛИ.

Все SSL-правила отображаются в таблице **SSL-правила**. Они проверяются в порядке расположения в таблице сверху вниз. Если заданные в правиле условия не выполняются, программа переходит к следующему правилу. Как только заданные в очередном правиле условия выполняются, к SSL-соединению

применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается. Вы можете изменять порядок применения SSL-правил (см. раздел "Изменение порядка применения SSL-правил" на стр. [250](#)), перемещая их в таблице **SSL-правила**.

В этом разделе

Создание SSL-правила	246
Просмотр информации об SSL-правиле	249
Изменение SSL-правила.....	249
Включение и отключение SSL-правила.....	250
Изменение порядка применения SSL-правил.....	250
Удаление SSL-правила.....	250

Создание SSL-правила

► Чтобы создать SSL-правило, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
2. Нажмите на кнопку **Добавить правило**.
Откроется окно **Добавить правило**.
3. В раскрывающемся списке **Действие** выберите действие, которое программа будет выполнять над SSL-соединением:

- **Tunnel.**

Программа не будет перехватывать CONNECT-запросы, которые удовлетворяют заданным условиям. Эти запросы не будут учитываться в статистике обработанного трафика в разделе **Мониторинг**.

При этом могут не применяться правила защиты, а также следующие критерии фильтрации в правилах доступа: **MIME-тип HTTP-сообщения**, **MIME-тип части HTTP-сообщения**, **Размер файла**, **HTTP-метод**.

- **Tunnel with SNI check.**

Программа не будет перехватывать CONNECT-запросы, которые удовлетворяют заданным условиям и для которых была выполнена проверка SNI. Эти запросы не будут учитываться в статистике обработанного трафика в разделе **Мониторинг**.

При этом могут не применяться правила защиты, а также следующие критерии фильтрации в правилах доступа: **MIME-тип HTTP-сообщения**, **MIME-тип части HTTP-сообщения**, **Размер файла**, **HTTP-метод**.

- **Bump.**

Программа будет перехватывать CONNECT-запросы, которые удовлетворяют заданным условиям, и анализировать содержимое зашифрованных соединений.

- **Terminate.**

Программа будет блокировать CONNECT-запросы, которые удовлетворяют заданным условиям.

Для сервисов, не поддерживающих перехват CONNECT-запросов, рекомендуется выбирать действие **Tunnel**. При применении действий **Bump** и **Tunnel with SNI check** SSL-соединение может быть заблокировано в случае ошибки перехвата.

По умолчанию задано действие **Tunnel**.

4. В блоке параметров **Источник** нажмите на кнопку **Добавить**.
5. В появившемся раскрывающемся списке выберите критерий фильтрации для источника соединения:
 - **IP-адрес.**

Если в качестве критерия фильтрации вы выбрали **IP-адрес**, выполните следующие действия:

1. В поле справа от раскрывающегося списка нажмите на область ввода.
Откроется окно **IP-адреса**.

2. Введите один или несколько IP-адресов.

Вы можете указывать IP-адреса в одном из следующих форматов:

- IPv4-адрес (например, 172.16.5.6).
- IPv4-подсеть с маской в формате CIDR notation (например, 192.168.1.0/24).
- IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6-подсеть с маской в формате CIDR notation (например, fc00::/7).

При указании нескольких IP-адресов используйте точку с запятой или новую строку в качестве разделителя.

3. Нажмите на кнопку **Добавить**.

Добавленные IP-адреса отобразятся в таблице под полем ввода. Если введенное значение имеет недопустимый формат, слева от него появится значок . Вы можете изменить этот адрес с помощью кнопки  в правой части строки.

4. Нажмите на кнопку **Сохранить**.

- **User agent.**

Если в качестве критерия фильтрации вы выбрали **User agent**, введите его название в поле справа от раскрывающегося списка.

При указании нескольких значений используйте точку с запятой в качестве разделителя.

1. В блоке параметров **Назначение** нажмите на кнопку **Добавить**.
2. В появившемся раскрывающемся списке выберите критерий фильтрации для назначения соединения:
 - **IP-адрес.**

Если в качестве критерия фильтрации вы выбрали **IP-адрес**, выполните следующие действия:

1. В поле справа от раскрывающегося списка нажмите на область ввода.
Откроется окно **IP-адреса**.
2. Введите один или несколько IP-адресов.
Вы можете указывать IP-адреса в одном из следующих форматов:
 - IPv4-адрес (например, 172.16.5.6).
 - IPv4-подсеть с маской в формате CIDR notation (например, 192.168.1.0/24).
 - IPv6-адрес (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
 - IPv6-подсеть с маской в формате CIDR notation (например, fc00::/7).При указании нескольких IP-адресов используйте точку с запятой или новую строку в качестве разделителя.
3. Нажмите на кнопку **Добавить**.
Добавленные IP-адреса отобразятся в таблице под полем ввода. Если введенное значение имеет недопустимый формат, слева от него появится значок . Вы можете изменить этот адрес с помощью кнопки  в правой части строки.
4. Нажмите на кнопку **Сохранить**.
 - **Имя хоста**.

Если в качестве критерия фильтрации вы выбрали **Имя хоста**, выполните следующие действия:

1. В поле справа от раскрывающегося списка нажмите на область ввода.
Откроется окно **Имена хостов**.
2. Введите одно или несколько имен хостов.
При указании нескольких имен используйте точку с запятой или новую строку в качестве разделителя.

Чтобы включить поддомены, используйте точку в начале значения. В этом случае недопустимо указывать поддомены в качестве отдельных записей, так как такие записи могут привести к ошибкам в работе прокси-сервера. Например, если вы указали `.example.org`, не следует добавлять запись `abc.example.org`.

3. Нажмите на кнопку **Добавить**.
Добавленные имена хостов отобразятся в таблице под полем ввода.
4. Если вы хотите, чтобы в фильтр попадали все поддомены указанного имени, установите флажок **Включить поддомены**.

Если вы ввели имя хоста с точкой в начале значения, флажок **Включить поддомены** будет установлен автоматически.

5. Нажмите на кнопку **Сохранить**.

6. В поле **Порты** введите один или несколько портов назначения.
Правило будет применяться только к соединениям, использующим заданные порты.
 7. В поле **Название** введите название правила.
 8. Если требуется, укажите любую дополнительную информацию о правиле в поле **Комментарий**.
 9. Включите или выключите использование правила с помощью переключателя **Статус**.
 10. Нажмите на кнопку **Добавить**.
- SSL-правило будет создано и отобразится в таблице на закладке **SSL-правила**.

Просмотр информации об SSL-правиле

► *Чтобы просмотреть информацию об SSL-правиле, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
2. В таблице SSL-правил выберите правило, информацию о котором вы хотите просмотреть.
Откроется окно **Просмотреть правило**.

В окне отображается следующая информация:

- **Статус** – статус использования SSL-правила.
- **Действие** – действие, которое программа выполняет над SSL-соединениями, удовлетворяющими заданным критериям фильтрации.
- **Порты** – порт назначения.
- **Название** – название SSL-правила.
- **Комментарий** – дополнительная информация, указанная при создании SSL-правила.

Изменение SSL-правила

► *Чтобы изменить SSL-правило, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
 2. В таблице SSL-правил выберите правило, параметры которого вы хотите изменить.
Откроется окно **Просмотреть правило**.
 3. Нажмите на кнопку **Изменить**.
Откроется окно **Изменить правило**.
 4. Внесите необходимые изменения.
 5. Нажмите на кнопку **Сохранить**.
- SSL-правило будет изменено.

Включение и отключение SSL-правила

► Чтобы включить или отключить SSL-правило, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
 2. В таблице SSL-правил выберите правило, которое вы хотите включить или отключить.
Откроется окно **Просмотреть правило**.
 3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить SSL-правило.
 4. Нажмите на кнопку **Сохранить**.
- SSL-правило будет включено или отключено.

Изменение порядка применения SSL-правил

SSL-правила проверяются в порядке расположения в таблице сверху вниз. Если заданные в правиле условия не выполняются, программа переходит к следующему правилу. Как только заданные в очередном правиле условия выполняются, к SSL-соединению применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается.

Вы можете изменять порядок применения SSL-правил, перемещая записи о правилах в таблице.

► Чтобы изменить порядок применения SSL-правил, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
2. В таблице SSL-правил нажмите на значок  в левой части строки, расположение которой вы хотите изменить, и перетащите строку с записью об SSL-правиле вверх или вниз.
3. Нажмите на кнопку **Сохранить**.

Порядок применения SSL-правил будет изменен.

Удаление SSL-правила

► Чтобы удалить SSL-правило, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **SSL-правила**.
2. В таблице SSL-правил выберите правило, которое вы хотите удалить.
Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

SSL-правило будет удалено.

Работа с доверенными сертификатами

При установке шифрованного соединения по протоколу HTTPS на компьютере пользователя выполняется проверка сертификата безопасности запрашиваемого веб-ресурса. В некоторых случаях браузер может не доверять предоставленному сертификату (например, если он является самоподписанным или содержит ошибки). Тогда пользователю будет отображаться предупреждение о небезопасном соединении.

Если вы уверены в безопасности веб-ресурса и не хотите выполнять проверку сертификата при каждом соединении, вы можете добавить этот сертификат в локальное хранилище доверенных корневых сертификатов на компьютере пользователя. Эту процедуру придется повторить вручную на всех компьютерах, устанавливающих соединение с данным веб-ресурсом.

Чтобы избежать многократного повторения этой операции, вы можете добавить отпечаток сертификата в список доверенных сертификатов Kaspersky Web Traffic Security. Прокси-сервер будет передавать сертификат запрашиваемого веб-ресурса на компьютер пользователя со статусом *Доверенный*. Пользователю не будет выводиться уведомление о небезопасном соединении.

Доверенные сертификаты целесообразно добавлять только для веб-ресурсов, к которым согласно параметрам SSL-правил (см. раздел "Работа с SSL-правилами" на стр. 245) применяется действие **Bump**. При применении других действий прокси-сервер не перехватывает сертификат безопасности и не может присвоить ему статус *Доверенный*.

Список доверенных сертификатов формируется на Управляющем узле, а затем применяется на всех узлах кластера.

В этом разделе

Добавление доверенного сертификата.....	251
Просмотр информации о доверенном сертификате.....	252
Изменение доверенного сертификата	252
Включение и отключение использования доверенного сертификата	253
Удаление доверенного сертификата.....	253

Добавление доверенного сертификата

► *Чтобы добавить доверенный сертификат, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Доверенные сертификаты**.
2. Нажмите на кнопку **Добавить**.
Откроется окно **Добавить доверенный сертификат**.
3. В поле **Отпечаток SHA1** введите отпечаток доверенного сертификата.
4. Если требуется, в поле **Комментарий** введите любую информацию о добавляемом доверенном сертификате.

5. Включите или выключите использование доверенного сертификата с помощью переключателя **Статус**.
6. Нажмите на кнопку **Добавить**.

Доверенный сертификат будет добавлен и отобразится в таблице **Доверенные сертификаты**.

Просмотр информации о доверенном сертификате

► *Чтобы просмотреть информацию о доверенном сертификате, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Доверенные сертификаты**.
2. В таблице доверенных сертификатов выберите сертификат, информацию о котором вы хотите просмотреть.

Откроется окно **Просмотреть доверенный сертификат**.

В окне отображается следующая информация:

- **Статус** – статус использования доверенного сертификата.
- **Отпечаток SHA1** – отпечаток доверенного сертификата.
- **Комментарий** – информация о доверенном сертификате, указанная при его добавлении.

Изменение доверенного сертификата

► *Чтобы изменить доверенный сертификат, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Доверенные сертификаты**.
2. В таблице доверенных сертификатов выберите сертификат, параметры которого вы хотите изменить.

Откроется окно **Просмотреть доверенный сертификат**.

3. Нажмите на кнопку **Изменить**.

Откроется окно **Изменить доверенный сертификат**.

4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Доверенный сертификат будет изменен.

Включение и отключение использования доверенного сертификата

► Чтобы включить или отключить использование доверенного сертификата, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Доверенные сертификаты**.
2. В таблице доверенных сертификатов выберите сертификат, использование которого вы хотите включить или отключить.
Откроется окно **Просмотреть доверенный сертификат**.
3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование доверенного сертификата.
4. Нажмите на кнопку **Сохранить**.

Использование доверенного сертификата будет включено или отключено.

Удаление доверенного сертификата

► Чтобы удалить доверенный сертификат, выполните следующие действия:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Встроенный прокси-сервер** → **Доверенные сертификаты**.
2. В таблице доверенных сертификатов выберите сертификат, который вы хотите удалить.
Откроется окно **Просмотреть доверенный сертификат**.
3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Доверенный сертификат будет удален.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (<https://support.kaspersky.ru/general/certificates>) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (<https://community.kaspersky.com/>).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. [257](#)).

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки	257
Техническая поддержка по телефону	257
Техническая поддержка через Kaspersky CompanyAccount	258
Получение информации для Службы технической поддержки	259

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. [254](#)), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2b>) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2b>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

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

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

Портал Kaspersky CompanyAccount доступен на следующих языках:

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

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

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файлы трассировки*. Файлы трассировки позволяют отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка. Вы можете выбрать, какие события будут записаны в файлы трассировки (ошибки или информационные сообщения). Все файлы трассировки помещаются в архив, который вы можете передать в Службу технической поддержки.

Файлы трассировки могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Необходимо согласовать состав отправляемого архива со Службой безопасности вашей организации. Перед отправкой журнала трассировки удалите из него все данные, которые вы считаете конфиденциальными.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на сервере и другая диагностическая информация.

Отладочная информация о работе программы записывается в соответствии с заданным уровнем трассировки (см. раздел "Изменение уровня трассировки" на стр. [260](#)). Место хранения зависит от комплекта поставки:

- категория Local0 журнала отладочной информации при разворачивании программы из iso-файла;
- папка /var/log/kaspersky/kwts при установке программы из rpm- или deb-пакета.

В этом разделе

Запуск трассировки.....	259
Изменение уровня трассировки.....	260
Просмотр журналов трассировки	260
Сохранение файла трассировки на компьютере	261

Запуск трассировки

► Чтобы запустить трассировку, выполните следующие действия:

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



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

3. Выберите пункт **Запустить трассировку**.

Откроется окно **Выбор узлов для запуска трассировки**.

4. В таблице серверов установите флажки напротив тех серверов, для которых вы хотите сформировать файлы трассировки.
5. Нажмите на кнопку **Запустить**.

Откроется окно **Журналы трассировки для Службы технической поддержки** с результатом запуска трассировки. Созданный журнал трассировки содержит отдельный файл для каждого сервера.

Изменение уровня трассировки

Изменение уровня трассировки сохраняется в конфигурации программы и не влияет на уже созданные файлы трассировки.

► *Чтобы выбрать уровень трассировки, выполните следующие действия:*

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



2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Изменить уровень трассировки**.

Откроется окно **Уровень трассировки**.

4. Выберите один из следующих вариантов:

- **Уровень ошибки.**
- **Уровень отладки.**

Этот уровень трассировки значительно повышает требования к подсистеме хранения данных и снижает производительность программы. Используйте уровень отладки только если Служба технической поддержки "Лаборатории Касперского" просит предоставить файлы трассировки такого типа.

5. Нажмите на кнопку **Сохранить**.

Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Трассировка будет производиться в соответствии с выбранным уровнем трассировки.

Просмотр журналов трассировки

► *Чтобы просмотреть журналы трассировки, выполните следующие действия:*

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



2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Просмотреть журналы трассировки**.

Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.

4. Если вы хотите посмотреть, информация о каких серверах содержится в журнале трассировки, нажмите на кнопку  в выбранной строке.

Сохранение файла трассировки на компьютере

► *Чтобы сохранить файл трассировки на компьютере, выполните следующие действия:*

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

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

3. Выберите пункт **Просмотреть журналы трассировки**.

Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.

4. Нажмите на кнопку  напротив названия журнала трассировки, файлы которого вы хотите загрузить.

5. В строке с нужным файлом нажмите на кнопку **Скачать**.

Файл трассировки будет сохранен на компьютере в папке загрузки браузера.

Приложение 1. 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.

Приложение 2. Нормализация URL-адресов

Kaspersky Web Traffic Security поддерживает импорт URL-адресов, состоящих из четырех частей и представленных в следующем формате:

<протокол>://<домен>:<порт>/<путь>

Указание домена является обязательным. Остальные части URL-адреса могут быть опущены.

Пример:

`https://example.com:8080/path`

Здесь `https` – протокол, `example.com` – домен, `8080` – порт, `path` – путь.

Если в процессе нормализации URL-адреса произошла ошибка и адрес не был принят программой, рекомендуется выполнить следующие действия.

1. Определите, с какой частью URL-адреса возникла проблема. Для этого добавляйте части адреса последовательно по следующему алгоритму:
 - a. <домен>.
 - b. <протокол>://<домен>.
 - c. <протокол>://<домен>:<порт>.
 - d. <протокол>://<домен>:<порт>/<путь>.
2. Проверьте, соответствует ли значение части URL-адреса, с которой возникла проблема, требованиям, приведенным в таблице ниже.

Таблица 22. Требования к URL-адресу для успешного выполнения нормализации

Часть URL-адреса	Требования
Протокол	<ul style="list-style-type: none"> • Должен начинаться с буквы латинского алфавита (ASCII A–Z, a–z). • Может содержать в себе буквы латинского алфавита (ASCII A–Z, a–z), цифры от 0 до 9, а также знаки плюса, минуса и точку.
Домен	<ul style="list-style-type: none"> • Допускается указывать IPv4-, IPv6-адреса (в квадратных скобках), а также FQDN. • Допускается использование следующих символов: <code>. _ ~ ! \$ & ' () * + , =</code>
Порт	Допускается использовать цифровое значение в диапазоне от 1 до 65535.

Часть URL-адреса	Требования
Путь	<ul style="list-style-type: none"> • Допускается использование одного или нескольких сегментов, разделенных символом /. • В каждом сегменте допускается использование латинских букв (ASCII a-z), цифр (0-9), символов в кодировке UTF, %-encoded символов, а также следующих символов: - . _ ~ : @ ! \$ & ' () * , =

1. Если указанный URL-адрес содержит точку с запятой, укажите его без пути. Вы сможете указать путь позже в списке добавленных URL-адресов.
2. Убедитесь, что части указанного URL-адреса не содержат символы : / ? # [] @. Эти символы являются разделителями между частями URL-адреса.

Приложение 3. Категории веб-ресурсов

Категории веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Порнография, эротика.**
- **Нудизм.**
- **Белье.**
- **Секс-образование.**
- **Знакомства для взрослых.**
- **ЛГБТ.**
- **Интим-магазины.**
- **Аборты.**

Алкоголь, табак, наркотические и психотропные вещества

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Наркотики.**
- **Алкоголь.**
- **Табак.**

Культура и общество

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Религии, религиозные объединения.**
- **Власть, политика, закон.**
- **Дом, семья.**
- **Новостные ресурсы.**
- **Вооруженные силы.**
- **Оружие, взрывчатые вещества, пиротехника.**
- **Поиск работы.**
- **Рестораны, еда, кафе.**

- **Астрология, эзотерика.**
- **Финансы, экономика.**
- **Бизнес.**

Программное обеспечение, аудио, видео

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Торренты.**
- **Файловые обменники.**
- **Аудио, видео.**

Информационные технологии

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Средства анонимного доступа.**
- **Поисковые машины, сервисы.**
- **Хостинг.**
- **Реклама, тизерные сети.**
- **Интернет-сервисы.**
- **Компьютерная техника, электроника.**
- **Информационная безопасность.**
- **Спам-сайты.**

Интернет-магазины, банки, платежные системы

Категория включает веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. Вы можете отдельно выбрать следующие подкатегории:

- **Интернет-магазины.**
- **Банки.**
- **Платежные системы.**
- **Криптовалюты и майнинг.**

Ненависть и дискриминация

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Насилие.**
- **Нецензурная лексика.**
- **Экстремизм, расизм.**
- **Самоповреждение, самоубийство.**

Общение в сети

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Веб почта.**
- **Социальные сети.**
- **Чаты, форумы.**
- **Блоги.**
- **Сайты знакомств.**

Образование

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Школы, университеты.**
- **Книги, писатели.**
- **Образовательные порталы, базы знаний.**

Хобби и развлечения

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Компьютерные игры.**
- **Охота, рыбалка.**
- **Путешествия, поездки.**
- **ТВ, радио .**
- **Дикие и домашние животные.**
- **Юмор.**
- **Музыка.**
- **Транспорт.**
- **Искусство.**

Красота, здоровье и спорт

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Спорт, спортивные игры.**
- **Здоровье.**
- **Мода, стиль.**
- **Медицина, фармацевтика.**

Азартные игры, лотереи, тотализаторы

Категория включает веб-ресурсы, предлагающие пользователям финансовое участие в игровой деятельности, даже если это не является обязательным условием использования веб-ресурса, а также информацию, способную вызвать желание участвовать в азартных играх, тотализаторах и лотереях. Вы можете отдельно выбрать следующие подкатегории:

- **Лотереи.**
- **Казино, карточные игры.**
- **Онлайн-тотализаторы.**

Другие

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Детский интернет.**
- **Недвижимость.**
- **Анорексия.**

Заблокировано законодательством Российской Федерации

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Защита детей (139-ФЗ, 436-ФЗ).**
- **Федеральный список экстремистских материалов (114-ФЗ).**
- **Единый реестр Роскомнадзора.**

Запрещено полицией

Категория включает подкатегорию **Запрещено полицией Японии**. В эту подкатегорию входят веб-ресурсы, предоставляемые по соглашению с японской полицией, только для японских клиентов.

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

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

Глоссарий

I

ICAP-сервер

Сервер, реализующий ICAP-протокол. Этот протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером по ICAP-протоколу. Kaspersky Web Traffic Security получает данные с прокси-сервера организации после их обработки на ICAP-сервере.

K

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля Kerberos. Keytab-файлы используются в удаленных системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

M

MIB (Management Information Base)

Виртуальная база данных, используемая для управления объектами, которые передаются по протоколу SNMP.

N

NTLM-аутентификация

Механизм аутентификации, основанный на проверке подлинности запроса сервера и ответа клиента. Для шифрования запроса и ответа используются хеши пароля пользователя, которые передаются по сети. При захвате сетевого трафика злоумышленники могут получить доступ к хешам пароля, что делает этот механизм менее надежным, чем Kerberos-аутентификация.

P

PTR-запись

DNS-запись, связывающая IP-адрес компьютера с его доменным именем.

R

Replay cache

Кеш, используемый в технологии Kerberos для хранения записей о запросах пользователей на аутентификацию. Этот механизм помогает защитить инфраструктуру от атак повторного воспроизведения. Во время таких атак злоумышленники записывают трафик пользователя, чтобы воспроизвести ранее отправленные им сообщения и успешно пройти аутентификацию на прокси-сервере. При использовании replay cache сервер аутентификации обнаруживает дубликат запроса и отправляет в ответ сообщение об ошибке.

S

SELinux (Security-Enhanced Linux)

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

SNI (Server Name Indication)

Расширение протокола TLS, передающее имя веб-сайта, с которым требуется установить соединение. SNI необходим в случаях, когда несколько сервисов, работающих по протоколу HTTPS, расположены на одном физическом сервере и используют один IP-адрес, но при этом у каждого сервиса есть свой сертификат безопасности.

SNMP-агент

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

работе программы.

SNMP-ловушка

Уведомление о событиях работы программы, отправляемое SNMP-агентом.

Squid

Программный пакет, выполняющий функцию кеширующего прокси-сервера для протоколов HTTP(S) и FTP. Сервис Squid использует списки контроля доступа для распределения доступа к ресурсам.

SRV-запись

Стандарт в DNS, определяющий местоположение, то есть имя хоста и номер порта серверов для определенных служб.

SSL Bumping

Режим работы сервиса Squid, используемый для перехвата содержимого зашифрованных HTTPS-сеансов.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

Т

TLS-шифрование

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

Б

Базовая аутентификация

Механизм аутентификации, при котором имя пользователя и пароль передаются для проверки на сервер в незашифрованном виде.

В

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

И

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

Источник обновлений

Ресурс, содержащий обновления антивирусных баз программы Kaspersky Web Traffic Security. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

К

Кластер

Группа серверов с установленной программой Kaspersky Web Traffic Security, объединенных для централизованного управления через веб-интерфейс программы.

О

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Правило доступа

Список разрешений и запретов доступа пользователей к указанным веб-ресурсам и направлению трафика.

Правило защиты

Список проверок трафика на вирусы, фишинг, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. [141](#)), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, проводимых при выполнении заданных условий.

Правило обработки трафика

Набор действий, которые программа выполняет над веб-ресурсом, удовлетворяющим заданным условиям.

Правило обхода

Набор критериев фильтрации трафика, согласно которым пользователям разрешается или запрещается доступ к веб-ресурсам без выполнения проверок по правилам доступа и правилам защиты.

Р

Рабочая область

Набор параметров и прав доступа, применимых к выделенной группе пользователей.

Репутационная фильтрация

Облачная служба, использующая технологии определения репутации сообщений. Информация о появлении новых видов спама в облачной службе появляется раньше, чем в базах модуля Анти-Спам, что дает возможность повысить скорость и точность обнаружения признаков спама в сообщении.

С

Сервис nginx

Программное обеспечение для UNIX-систем, используемое в качестве HTTP-сервера или почтового прокси-сервера.

Серийный номер лицензии

Уникальное сочетание букв и цифр, использующееся для однозначной идентификации приобретателя лицензии на программу.

Служба каталогов

Программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

Схема расположения графиков

Вид окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб некоторых графиков.

Т

Трассировка

Запись отладочной информации о работе программы.

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:

Kaspersky VirusDesk:

Сообщество пользователей "Лаборатории Касперского":

<https://securelist.ru/>

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

<https://community.kaspersky.com>
(<https://community.kaspersky.com/>)

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google Chrome – товарный знак Google, Inc.

Microsoft, Windows, Windows Server, Active Directory, Hyper-V и Internet Explorer – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Oracle – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

Parallels Desktop является зарегистрированным товарным знаком Parallels International GmbH в США и / или других странах.

CentOS – товарный знак компании Red Hat, Inc.

VMware, VMware ESXi и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

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