KASPERSKY lab

Kaspersky Secure Mail Gateway

Подготовительные процедуры и руководство по эксплуатации

643.46856491.00085-02 90 01

Версия программы: 1.1.1.24

Уважаемый пользователь!

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

Дата редакции документа: 08.09.2017

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

Содержание

Об этом руководстве

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Secure Mail Gateway".

Подготовительные процедуры изложены в разделах "Подготовка к созданию виртуальной машины", "Подготовка образов виртуальной машины", "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 и администрирование Kaspersky Security Mail Gateway, а также поддержка организаций, использующих Kaspersky Security Mail Gateway.

В этом разделе

В этом руководстве

В руководство включены следующие разделы:

Источники информации о программе (см. стр. 22)

Этот раздел содержит описание источников информации о программе.

О Kaspersky Secure Mail Gateway

Этот раздел содержит краткий обзор и функциональные возможности решения Kaspersky Secure Mail Gateway. Из раздела вы узнаете о режимах работы Kaspersky Secure Mail Gateway, аппаратных и программных требованиях.

Требования (см. стр. 26)

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

Разделение доступа к функциям программы по пользовательским ролям (см. стр. 30)

Этот раздел содержит описание ролей пользователей программы, а также действия, которые могут выполнять пользователи программы.

Режимы работы Kaspersky Secure Mail Gateway (см. стр. 32)

Этот раздел содержит описание режимов работы программы.

Лицензирование программы (см. стр. 34)

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

Подготовка к созданию виртуальной машины (см. стр. 49)

Этот раздел содержит описание действий, которые нужно выполнить перед созданием виртуальной машины программы.

Подготовка образов виртуальной машины (см. стр. 50)

Этот раздел содержит описание действий, которые нужно выполнить для подготовки образов виртуальной машины программы.

Развертывание образа виртуальной машины программы в гипервизоре VMware ESXi™ (см. стр. 52)

Этот раздел содержит пошаговые инструкции по развертыванию образа виртуальной машины программы в гипервизоре VMware ESXi.

Развертывание образа виртуальной машины программы в гипервизоре Microsoft® Hyper-V® (см. стр. 57)

Этот раздел содержит информацию о развертывании образа виртуальной машины программы в гипервизоре Microsoft Hyper-V.

Подготовка программы к работе (см. стр. 64)

Этот раздел содержит пошаговые инструкции по подготовке к работе и первоначальной настройке Kaspersky Secure Mail Gateway, которую нужно выполнить после развертывания образа виртуальной машины программы.

Запуск виртуальной машины программы (см. стр. 94)

Этот раздел содержит информацию о запуске виртуальной машины Kaspersky Secure Mail Gateway.

Изменение конфигурации виртуальной машины (см. стр. 95)

Этот раздел содержит информацию о том, как изменить конфигурацию виртуальной машины в гипервизоре, который вы используете.

Начало работы в веб-интерфейсе программы (см. стр. 97)

Этот раздел содержит информацию о том, как начать работу в веб-интерфейсе программы.

Интеграция Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации (см. стр. 99)

Этот раздел содержит инструкции по интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации.

Процедура приемки (см. стр. 118)

Этот раздел содержит описание безопасного состояния программы, а также проверки работоспособности модулей Антивирус и Анти-Спам.

Мониторинг Kaspersky Secure Mail Gateway (см. стр. 125)

Этот раздел содержит информацию о мониторинге почтового трафика, последних обнаруженных угроз и ресурсов системы.

Работа с правилами обработки сообщений (см. стр. 129)

Этот раздел содержит информацию о правилах обработки сообщений, настройке их параметров и настройке параметров Kaspersky Secure Mail Gateway для каждого правила обработки сообщений.

Домены и настройка маршрутизации электронной почты (см. стр. 147)

Этот раздел содержит информацию о том, как создавать транспортную таблицу, настраивать маршрутизацию электронной почты, настраивать TLS-безопасность для входящих и исходящих сообщений, добавлять DKIM-подпись к сообщениям электронной почты.

Использование протокола TLS в работе Kaspersky Secure Mail Gateway (см. стр. 165)

Этот раздел содержит информацию об использовании протокола TLS в работе Kaspersky Secure Mail Gateway и о настройке параметров использования протокола.

Хранилище (см. стр. 172)

Этот раздел содержит информацию о хранилище и работе с ним.

Очередь сообщений Kaspersky Secure Mail Gateway (см. стр. 183)

Этот раздел содержит информацию об очередях сообщений Kaspersky Secure Mail Gateway.

Отчеты о работе Kaspersky Secure Mail Gateway (см. стр. 193)

Этот раздел содержит информацию о том, как создавать и просматривать отчеты о работе Kaspersky Secure Mail Gateway.

Общие параметры Kaspersky Secure Mail Gateway (см. стр. 208)

Этот раздел содержит информацию об общих параметрах программы.

Настройка параметров MTA (см. стр. 221)

Этот раздел содержит информацию о настройке основных параметров MTA.

Обновление баз Kaspersky Secure Mail Gateway (см. стр. 230)

Этот раздел содержит информацию об обновлении антивирусных баз, баз модулей Анти-Спам и Анти-Фишинг.

Антивирусная защита сообщений (см. стр. 239)

Этот раздел содержит информацию об антивирусной защите сообщений и настройке ее параметров.

Защита сообщений от спама (см. стр. 258)

Этот раздел содержит информацию о защите сообщений от спама и настройке ее параметров.

Анти-Спам карантин (см. стр. 274)

Этот раздел содержит информацию об Анти-Спам карантине.

Защита KATA и интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform (см. стр. 277)

Этот раздел содержит информацию о защите Kaspersky Anti Targeted Attack Platform и об интеграции Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform.

Черные и белые списки адресов (см. стр. 291)

Этот раздел содержит информацию о черных и белых списках адресов электронной почты, которые можно создавать и редактировать в Kaspersky Secure Mail Gateway.

Соединение с LDAP-сервером (см. стр. 298)

Этот раздел содержит информацию о соединении Kaspersky Secure Mail Gateway с LDAP-сервером и о настройке параметров и фильтров соединения с LDAP-сервером.

Работа с программой по протоколу SNMP (см. стр. 311)

Этот раздел содержит информацию о работе с программой по протоколу SNMP, а также о настройке ловушек событий, возникающих во время работы Kaspersky Secure Mail Gateway.

Информация о системе для Службы технической поддержки (см. стр. 315)

Этот раздел содержит информацию о том, как сформировать архив с информацией о Kaspersky Secure Mail Gateway для отправки в Службу технической поддержки "Лаборатории Касперского".

Журнал аудита Kaspersky Secure Mail Gateway (см. стр. 318)

Этот раздел содержит информацию о работе с журналом аудита Kaspersky Secure Mail Gateway.

Настройка даты и времени в Kaspersky Secure Mail Gateway (см. стр. 326)

Этот раздел содержит информацию о настройке даты и времени в программе.

Хранение данных пользователей (см. стр. 327)

Этот раздел содержит информацию о данных пользователей программы, об использовании этих данных программой, а также о том, какие пользователи программы имеют доступ к этим данным.

Устранение уязвимостей и установка критических обновлений программы (см. стр. 331)

Этот раздел содержит информацию об установке критических обновлений программы для устранения уязвимостей.

Действия после сбоя или неустранимой ошибки в работе программы (см. стр. 332)

Этот раздел содержит информацию о действиях после сбоя или неустранимой ошибки в работе программы.

Обращение в Службу технической поддержки (см. стр. 333)

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

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО "Лаборатория Касперского" (см. стр. 343)

Этот раздел содержит информацию об АО "Лаборатория Касперского".

Информация о стороннем коде (см. стр. 345)

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Соответствие терминов (см. стр. 353)

Этот раздел содержит таблицу соответствия терминов в документе и ФСТЭК.

Приложение (см. стр. 354)

Этот раздел содержит перечень значений параметров программы в сертифицированном режиме.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

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.

В этом разделе

Источники информации для самостоятельного поиска

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Secure Mail Gateway:

- страница Kaspersky Secure Mail Gateway на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Secure Mail Gateway 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. 333).

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

Страница Kaspersky Secure Mail Gateway на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Secure Mail Gateway (http://www.kaspersky.ru/business-security/mail-security-appliance) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Secure Mail Gateway содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Secure Mail Gateway в Базе знаний

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

На странице Kaspersky Secure Mail Gateway в Базе знаний (http://support.kaspersky.ru/ksmg) 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 Secure Mail Gateway, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка Kaspersky Secure Mail Gateway (справка веб-интерфейса)

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

Электронная справка создана для удобства пользователей и не является полноценным эквивалентом настоящего документа.

Документация

В комплект поставки программы включено Руководство пользователя Kaspersky Secure Mail Gateway, с помощью которого вы можете установить программу и произвести настройку параметров программы.

Обсуждение программ "Лаборатории Касперского" на форуме

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

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

О Kaspersky Secure Mail Gateway

Программное изделие "Kaspersky Security Mail Gateway" представляет собой средство антивирусной защиты типов "Б" четвертого класса защиты и предназначено для применения на серверах информационных систем в виртуальных средах.

Основными угрозами, для противостояния которым используется ОО, 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 ОО;
- управление работой ОО;
- управление параметрами ОО;
- управление установкой обновлений (актуализации) БД ПКВ ОО;
- аудит безопасности ОО;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- выполнение проверок сообщений электронной почты.

.

Требования

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

Аппаратные и программные требования

Аппаратные и 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 6.9.

Объем дискового пространства в каталогах / и /root (как правило, это раздел /dev/sda2) – не менее 250 ГБ.

Программные требования для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway

Образ виртуальной машины Kaspersky Secure Mail Gateway может быть развернут на следующих гипервизорах:

- VMware ESXi 5.5 Update 2.
- VMware ESXi 6.0.
- Microsoft Hyper-V Server 2012 R2.

Аппаратные требования для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway

Ресурсы, выделенные для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway, должны удовлетворять следующим требованиям:

- сетевой адаптер E1000;

- объем дискового пространства – не менее 100 ГБ;
- не менее 4 ГБ оперативной памяти;
- 1 четырехъядерный процессор.

Программные требования для работы с Kaspersky Secure Mail Gateway через веб-интерфейс

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

- Mozilla™ Firefox™ версии 39.
- Internet Explorer® версии 11.
- Google Chrome™ версии 43.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).

11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.

12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.

13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.

14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).

15. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, равное 3, 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, отвечающие следующим требованиям:

    - минимальная длина пароля - 8 символов;
    - пароль содержит только символы в кодировке ASCII;
    - пароль содержит минимум один символ верхнего регистра;
    - пароль содержит минимум один символ нижнего регистра;
    - пароль содержит минимум одну цифру.

.

Разделение доступа к функциям программы по пользовательским ролям

В Kaspersky Secure Mail Gateway предусмотрены следующие учетные записи:

- Учетная запись администратора виртуальной машины Kaspersky Secure Mail Gateway (см. раздел "Шаг 11. Установка пароля администратора виртуальной машины" на стр. 86) (далее также "администратор сервера", "администратор виртуальной машины") Administrator для управления сервером.
- Учетная запись администратора веб-интерфейса (см. раздел "Шаг 10. Установка пароля администратора веб-интерфейса" на стр. 85) Administrator для работы в веб-интерфейсе программы.
- Учетная запись HelpDesk (см. раздел "Об учетной записи HelpDesk" на стр. 212) для получения ограниченного доступа к параметрам программы.

Все учетные записи администратора создаются при установке программы. Данные каждой из этих учетных записей хранятся на сервере программы.

Учетная запись администратора сервера служит для управления сервером с виртуальной машиной программы. Под этой учетной записью вы можете выключить или перезагрузить сервер.

Учетная запись администратора сервера имеет доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору необходимо обеспечить безопасность сервера самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на сервере.

Учетная запись администратора веб-интерфейса программы Administrator создается при установке программы и предназначена для сотрудников вашей организации, в чьи

обязанности входит управление Kaspersky Secure Mail Gateway через веб-интерфейс программы.

Учетная запись HelpDesk предназначена для получения ограниченного доступа к параметрам программы. С помощью учетной записи HelpDesk администратор веб-интерфейса программы может предоставить другому пользователю права для выполнения некоторых операций, например, для расследования инцидентов с сообщениями, помещенными в хранилище.

Режимы работы Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway может работать в обычном режиме, в режиме ограниченного трафика или в сертифицированном режиме.

В обычном режиме Kaspersky Secure Mail Gateway разрешен доступ в интернет и соединение со следующими серверами, расположенными за пределами IT-инфраструктуры вашей организации:

- Серверами обновлений баз KSN.
- DNS-серверами.
- Серверами обновлений баз Kaspersky Secure Mail Gateway.

В режиме ограниченного трафика Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации.

В режиме ограниченного трафика параметры компонентов Kaspersky Secure Mail Gateway, требующих доступ в интернет, по умолчанию принимают следующие значения:

- Использование KSN отключено.
- SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений отключены, соединение с DNS-серверами запрещено.
- Функция Enforced Anti-Spam Updates отключена в параметрах модуля Анти-Спам.
- В качестве источника обновлений баз Kaspersky Secure Mail Gateway используется Kaspersky Security Center или локальный источник обновлений баз Kaspersky Secure Mail Gateway.

В сертифицированном режиме Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации.

Вы можете выбрать сертифицированный режим работы Kaspersky Secure Mail Gateway при развертывании образа виртуальной машины Kaspersky Secure Mail Gateway.

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Secure Mail Gateway.
- 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 основе 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 Secure Mail Gateway 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 Secure Mail Gateway). Чтобы продолжить использование Kaspersky Secure Mail Gateway в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

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

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

- тип лицензии.

О ключе

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

Вы можете добавить ключ в программу, применив *файл ключа*.

Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

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

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Ключ для пробной лицензии не может быть добавлен в качестве дополнительного ключа.

> Дополнительный ключ может быть добавлен только при наличии активного ключа.

Для Kaspersky Secure Mail Gateway используются ключи следующих типов:

- *Полнофункциональный ключ*. При добавлении ключа программа работает в режиме полной функциональности, осуществляются проверки на спам, вирусы и другие

программы, представляющие угрозу, проверка подлинности отправителей сообщений и проверка сообщений в Kaspersky Anti Targeted Attack Platform.

- *Ключ для антивирусной защиты*. При добавлении ключа программа производит поиск вирусов и других программ, представляющих угрозу, проверку подлинности отправителей сообщений и проверку сообщений в Kaspersky Anti Targeted Attack Platform. Программа не производит проверку на спам. Статус, присвоенный программой сообщению при проверке, содержит информацию об ограниченной функциональности.

- *Ключ для защиты от спама*. При добавлении ключа программа производит проверку на спам, проверку подлинности отправителей сообщений и проверку сообщений в Kaspersky Anti Targeted Attack Platform. Программа не производит поиск вирусов и других программ, представляющих угрозу. Статус, присвоенный программой сообщению при проверке, содержит информацию об ограниченной функциональности.

Тип дополнительного ключа должен соответствовать типу ранее добавленного активного ключа. Если тип дополнительного ключа не соответствует типу ранее добавленного активного ключа, то после того как дополнительный ключ станет активным, доступная функциональность программы изменится в соответствии с типом дополнительного ключа.

Антивирусные базы и базы Анти-Спама обновляются независимо от типа ключа.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Secure Mail Gateway или после заказа пробной версии Kaspersky Secure Mail Gateway.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться в Службу технической поддержки (http://support.kaspersky.ru).
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://activation.kaspersky.com/ru/) на основе имеющегося кода активации.

О подписке

Подписка на Kaspersky Secure Mail Gateway – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств).

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Secure Mail Gateway после окончания ограниченной подписки ее требуется продлить. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Чтобы использовать Kaspersky Secure Mail Gateway по подписке, требуется применить код активации. После применения кода активации устанавливается активный ключ, определяющий лицензию на использование программы по подписке. При этом дополнительный ключ может быть установлен только с помощью кода активации и не может быть установлен с помощью файла ключа.

> Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Secure Mail Gateway.

О предоставлении данных

Для работы программы используются данные, на отправку и обработку которых требуется согласие администратора Kaspersky Secure Mail Gateway.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в Лицензионном соглашении (например, при установке

программы или при обновлении системы в разделе **Параметры**, подразделе **Обновление системы** главного окна веб-интерфейса программы).

Согласно условиям принятого Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении (см. раздел "О Лицензионном соглашении" на стр. 35) в пункте Предоставление информации. Эта информация требуется для повышения уровня защиты почтового сервера.

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

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

Данные пользователя могут содержаться в следующих компонентах Kaspersky Secure Mail Gateway:

- Очереди сообщений (имена файлов, адреса электронной почты отправителей и получателей сообщений, тексты сообщений).
- Хранилище (имена файлов, адреса электронной почты отправителей и получателей сообщений, тексты сообщений).
- Отчетах о работе программы (имена файлов, адреса электронной почты отправителей и получателей сообщений).
- Журнале аудита (адреса электронной почты отправителей и получателей сообщений, имена файлов вложений, IP-адреса компьютеров отправителей сообщений).
- Файлах трассировки (имена файлов, пути к файлам, имена прокси-серверов, данные учетных записей пользователей, IP-адреса компьютеров, подключающихся к источникам обновлений баз программы, имена и IP-адреса источников обновлений, информация о загружаемых файлах и скорости загрузки).

- Файлах, в которых хранятся параметры соединения с LDAP-сервером и прокси-сервером (данные учетных записей пользователей LDAP-сервера и прокси-сервера).

При подключении к DNS-, SURBL- и DNSBL-серверам, Kaspersky Secure Mail Gateway будет использовать IP-адреса и FQDN-имена доменов, обращающихся к этим серверам.

Дамп формируется при сбоях программы и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные, включая фрагменты содержания писем и анализируемых файлов.

Администратор локальной сети организации несет ответственность за доступ к данной информации.

По умолчанию формирование дампа в Kaspersky Secure Mail Gateway отключено.

Данные очереди сообщений электронной почты, обрабатываемой Kaspersky Secure Mail Gateway в данный момент, а также учетных записей пользователей LDAP-сервера и прокси-сервера хранятся в Kaspersky Secure Mail Gateway в незашифрованном виде.

Администратору Kaspersky Secure Mail Gateway необходимо обеспечить безопасность этих данных самостоятельно.

Администратор Kaspersky Secure Mail Gateway несет ответственность за доступ к данной информации.

Данные о событиях и процессах работы Kaspersky Secure Mail Gateway записываются и хранятся в следующих журналах Kaspersky Secure Mail Gateway:

- журнале аудита;
- журнале трассировки.

Просмотр информации о лицензии и добавленных ключах

► *Чтобы просмотреть информацию о лицензии и добавленных ключах,*

в главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Лицензирование**.

В рабочей области в блоке **Активный ключ** отображается следующая информация о ключах:

- буквенно-цифровая последовательность ключа;
- статус ключа;
- тип лицензии;
- количество пользователей;
- дата активации программы;
- дата окончания срока годности ключа;
- количество дней до окончания срока годности ключа.

Обновление информации о лицензии и добавленных ключах

► *Чтобы обновить информацию о лицензии и добавленных ключах, выполните следующие действия:*

17. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Лицензирование**.

18. Нажмите на кнопку **Обновить** в правом верхнем углу окна.

Информация о лицензии и добавленных ключах обновится.

Добавление файла ключа

► *Чтобы добавить файл ключа, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Лицензирование**.
2. Нажмите на кнопку **Добавить файл ключа**.

   Откроется окно **Добавление ключа**.
3. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, который вы хотите добавить.
5. Нажмите на кнопку **ОК**.

Добавленные ключи могут иметь статус *активный* и *дополнительный.* Первый добавленный ключ автоматически становится активным. Вы можете использовать программу сразу же после добавления активного ключа.

После добавления активного ключа вы можете добавить дополнительный ключ. Дополнительный ключ автоматически начнет использоваться в качестве активного ключа по истечении срока годности активного ключа.

Удаление ключа

► *Чтобы удалить ключ, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Лицензирование**.
2. В рабочей области окна установите флажок рядом с тем ключом, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление данных о лицензии**.

4. Нажмите на кнопку **Да**.

Выбранный ключ будет удален.

Если вы удалили активный ключ, и в Kaspersky Secure Mail Gateway был ранее добавлен дополнительный ключ, то дополнительный ключ автоматически станет активным.

Если вы удалите активный и дополнительный ключи, вы не сможете использовать программу в режиме той функциональности, которую предусматривает ваша лицензия.

Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией

В Kaspersky Secure Mail Gateway предусмотрены различные режимы работы в зависимости от лицензии.

Без лицензии

В этом режиме Kaspersky Secure Mail Gateway работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите активный ключ.

В режиме **Без лицензии** Kaspersky Secure Mail Gateway не выполняет проверку сообщений электронной почты.

Пробная лицензия

В этом режиме Kaspersky Secure Mail Gateway выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа пробной лицензии, Kaspersky Secure Mail Gateway прекращает проверку сообщений электронной почты и обновление баз.

Для возобновления работы Kaspersky Secure Mail Gateway необходимо установить ключ коммерческой лицензии.

Коммерческая лицензия

В этом режиме Kaspersky Secure Mail Gateway выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа коммерческой лицензии Kaspersky Secure Mail Gateway продолжает проверку сообщений электронной почты, но прекращает обновление баз.

Для возобновления обновления баз необходимо установить новый ключ коммерческой лицензии или продлить срок действия ключа коммерческой лицензии.

В Kaspersky Secure Mail Gateway предусмотрены ключи коммерческой лицензии следующих типов:

- *Полнофункциональный ключ*. При добавлении ключа программа работает в режиме полной функциональности, осуществляются проверки на спам, вирусы и другие программы, представляющие угрозу.
- *Ключ для антивирусной защиты*. При добавлении ключа программа производит поиск вирусов и других программ, представляющих угрозу, не производит проверку на спам. Статус, присвоенный программой сообщению при проверке на спам, содержит информацию об ограниченной функциональности.
- *Ключ для защиты от спама*. При добавлении ключа программа производит проверку на спам, не производит поиск вирусов и других программ, представляющих угрозу. Статус, присвоенный программой сообщению при поиске вирусов и других программ, представляющих угрозу, содержит информацию об ограниченной функциональности.

Черный список ключей

В ряде случаев ключ может быть занесен в черный список ключей. Если это произошло, Kaspersky Secure Mail Gateway прекращает проверку сообщений электронной почты, но продолжает попытки обновления баз на случай, если ключ будет исключен из черного списка ключей.

Как только ключ будет исключен из черного списка ключей, Kaspersky Secure Mail Gateway возобновит проверку сообщений электронной почты в соответствии с действующей лицензией.

После отключения проверки сообщений электронной почты в Kaspersky Secure Mail Gateway продолжает работать почтовый агент MTA, соединение с LDAP-сервером, журнал событий, отчеты о работе Kaspersky Secure Mail Gateway, а также остается доступно управление всеми параметрами Kaspersky Secure Mail Gateway, кроме параметров защиты, через веб-интерфейс.

Уведомления о скором истечении срока действия лицензии

После каждого обновления баз программа выполняет проверку срока действия лицензии. Когда до окончания срока действия лицензии остается количество дней, указанное в параметре **Отправлять уведомление за**, программа начинает отправлять уведомления на указанные вами адреса электронной почты администратора Kaspersky Secure Mail Gateway (см. раздел "Настройка адресов электронной почты администратора" на стр. 211).

По умолчанию программа начинает отправлять уведомления об истечении срока действия лицензии за 30 дней до истечения срока действия лицензии.

Уведомления об истечении срока действия лицензии отправляются один раз в сутки.

Уведомления об истечении срока действия лицензии прекращают отправляться в следующих случаях:

- Вы добавили ключ, срок годности которого превышает срок годности активного ключа и значение параметра **Отправлять уведомление за**.
- Срок действия лицензии истек. В этом случае отправляется уведомление о том, что срок действия лицензии истек.

► *Чтобы настроить дату начала отправки уведомлений, изменить заголовок и текст уведомления об истечении срока действия лицензии, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Уведомления**.

2. В блоке **Срок действия лицензии скоро истечет** по любой ссылке откройте окно **Параметры уведомления**.

3. В поле **Тема** введите заголовок уведомления об истечении срока действия лицензии.

4. В поле **Сообщение** введите текст уведомления об истечении срока действия лицензии.

5. В списке **Отправлять уведомление за** укажите, за сколько дней до истечения срока действия лицензии вы хотите начать получать уведомления.

6. Нажмите на кнопку **Сохранить**.

   Окно **Параметры уведомления** закроется.

► *Чтобы включить или отключить отправку уведомлений об истечении срока действия лицензии, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Уведомления**.

2. В блоке **Срок действия лицензии скоро истечет** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Срок действия лицензии скоро истечет**, если вы хотите включить отправку уведомлений об истечении срока действия лицензии.

   - Выключите переключатель рядом с названием блока параметров **Срок действия лицензии скоро истечет**, если вы хотите отключить отправку уведомлений об истечении срока действия лицензии.

Если в программе установлен дополнительный ключ, уведомление не отправляется. После истечения срока годности активного ключа дополнительный ключ автоматически становится активным.

Если срок годности дополнительного ключа истекает раньше, чем программа должна начать отправлять уведомление, первое уведомление будет отправлено в момент замены активного ключа дополнительным.

Подготовка к созданию виртуальной машины

Перед созданием виртуальной машины Kaspersky Secure Mail Gateway вам нужно выполнить следующие действия:

- Убедиться, что ваш сервер удовлетворяет аппаратным и программным требованиям.
- Создать виртуальную машину с установленной операционной системой CentOS 6.9.
- Войти в систему на созданной виртуальной машине под учетной записью root.
- Установить дополнительные пакеты, необходимые для сборки пакета OVA:
  - qemu-img;
  - squashfs-tools;
  - mkisofs;
  - pxz.
- Загрузить пакет VMware-ovftool-4.1.0-2459827-lin.x86_64.bundle с сайта www.vmware.com и выполнить команды:

  ```
  chmod 755 VMware-ovftool-4.1.0-2459827-lin.x86_64.bundle

  ./VMware-ovftool-4.1.0-2459827-lin.x86_64.bundle
  ```

- Установить локальный репозиторий. Для этого выполните следующие действия:
  - Создайте каталог /srv, если его нет в вашей файловой системе.
  - Перейдите в каталог /srv.
  - Распакуйте архив repos.tar.

Подготовка образов виртуальной машины

Программа g. Перед началом установки программы вам необходимо создать образы OVA и ISO с установленной программой.

► *Чтобы создать образы OVA и ISO, выполните следующие действия:*

1. Скопируйте архивы ova.tar и bases.tgz в каталог /root.

   > Для корректного создания образов необходим пустой архив bases.tgz. Актуальные базы вы можете скачать после начала работы программы и установки ключа.

2. Распакуйте архив ova.tar.
3. Перейдите в каталог ova.
4. Скопируйте в каталог kaspersky_rpms следующие версии rmp:
   - klms-appliance-1.1.0-373.i386.rpm;
   - klms-1.1.0-373.i386.rpm;
   - klms_de-1.1.0-379.noarch.rpm;
   - klms_fr-1.1.0-379.noarch.rpm;
   - klms_zh-CN-1.1.0-379.noarch.rpm;
   - klms_zh-TW-1.1.0-379.noarch.rpm;
   - klms_ru-1.1.0-379.noarch.rpm;
   - klnagent-10.1.0-114.i386.rpm;
   - ram-0.4.4-5.noarch.rpm;
   - klmsui-1.1.0-373.appliance.x86_64.rpm.

5. Запустите сборку образов, выполнив команду:

```
./build.sh ova '1.1.0.379' 'x86_64-redhat-linux' '' BUILD=ova,iso
UPDATES=yes \

MD5=yes RAM_FRAMEWORK_VER=0.4.4-5
```

Созданные образы виртуальных машин будут сохранены в /root/ova/build_ova/ksmg-1.0.0-379.x86_64.ova и /root/ova/ksmg-1.1.0-379.x86_64.iso.

Развертывание образа виртуальной машины программы в гипервизоре VMware ESXi

Этот раздел содержит пошаговые инструкции по развертыванию образа виртуальной машины программы в гипервизоре VMware ESXi.

В этом разделе

Подготовка к развертыванию

Перед развертыванием образа виртуальной машины программы убедитесь, что версия VMware ESXi и аппаратные ресурсы, выделенные для виртуальной машины, удовлетворяют программным и аппаратным требованиям.

Шаг 1. Выбор образа виртуальной машины

Образ виртуальной машины программы распространяется в пакете формата OVF.

► *Чтобы развернуть образ виртуальной машины из пакета OVF, выполните следующие действия:*

1. Запустите программу VMware vSphere™ Client.
2. В меню **File** выберите пункт **Deploy OVF Template**.

   Запустится мастер развертывания и откроется окно **Deploy OVF Template**.
3. В окне **Deploy OVF Template** укажите файл с расширением ova, содержащий образ виртуальной машины.
4. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 2. Просмотр сведений об образе виртуальной машины

► *Чтобы просмотреть сведения об образе виртуальной машины программы, выполните следующие действия:*

1. Ознакомьтесь со сведениями об образе виртуальной машины, выбранной на предыдущем шаге.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 3. Просмотр Лицензионного соглашения

Для продолжения развертывания вам нужно принять условия Лицензионного соглашения. Если условия Лицензионного соглашения не приняты, развертывание не выполняется.

► *Чтобы принять условия Лицензионного соглашения, выполните следующие действия:*

1. В окне **Deploy OVF Template** нажмите на кнопку **Accept**.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 4. Назначение имени виртуальной машины

► *Чтобы назначить имя виртуальной машины программы, выполните следующие действия:*

1. Введите имя виртуальной машины в поле **Name** (см. рисунок ниже).

   > Имя должно быть уникальным среди используемых виртуальных машин.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 5. Выбор хранилища данных виртуальной машины

► *Чтобы выбрать хранилище данных (`destination storage`) VMware ESXi-хоста, в котором будут храниться файлы виртуальной машины программы, выполните следующие действия:*

1. Выберите хранилище данных в списке.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 6. Выбор варианта размещения файлов виртуальной машины

► *Чтобы выбрать вариант размещения файлов виртуальной машины программы в хранилище данных VMware ESXi-хоста, выполните следующие действия:*

1. Выберите один из следующих вариантов списка:

   - **Thick Provision Lazy Zeroed**. Для файлов виртуальной машины сразу резервируется указанный объем дискового пространства. Блоки данных внутри выделенного объема замещаются данными виртуальной машины по мере обращения.

   - **Thick Provision Eager Zeroed**. Для файлов виртуальной машины сразу резервируется указанный объем дискового пространства. Блоки данных дискового пространства сразу очищаются.

   - **Thin Provision**. Для файлов виртуальной машины резервируется минимально необходимый объем. При необходимости этот объем увеличивается.

     Рекомендуется использовать один из вариантов Thick Provision.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера развертывания.

Шаг 7. Запуск и завершение развертывания образа виртуальной машины

► *Чтобы запустить развертывание образа виртуальной машины и убедиться, что развертывание завершилось правильно, выполните следующие действия:*

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

2. Установите флажок **Power on after deployment**, если вы хотите, чтобы виртуальная машина автоматически запустилась после развертывания.

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

   Запустится развертывание образа виртуальной машины.

4. Установите флажок **Close this dialog when completed**, если вы хотите, чтобы окно индикации хода развертывания образа виртуальной машины автоматически закрылось после завершения развертывания.

5. После завершения развертывания нажмите на кнопку **Close**.

После развертывания образа виртуальной машины перейдите к первоначальной настройке виртуальной машины.

Развертывание образа виртуальной машины в гипервизоре Microsoft Hyper-V

Этот раздел содержит пошаговые инструкции по развертыванию образа виртуальной машины Kaspersky Secure Mail Gateway в гипервизоре Microsoft Hyper-V.

В этом разделе

Подготовка к развертыванию

Для развертывания в гипервизоре Microsoft Hyper-V используется ISO-образ виртуальной машины программы.

Перед развертыванием образа виртуальной машины программы убедитесь, что версия Microsoft Hyper-V и аппаратные ресурсы, выделенные для виртуальной машины, удовлетворяют аппаратным и программным требованиям.

Шаг 1. Запуск мастера создания виртуальной машины

► *Чтобы развернуть виртуальную машину в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

1. Запустите программу Microsoft Hyper-V Manager.
2. В левой части окна выберите сервер, на котором вы хотите развернуть образ виртуальной машины.
3. В контекстном меню выберите пункт **New** → **Virtual Machine**.

Откроется мастер создания виртуальной машины.

Шаг 2. Выбор имени и расположения виртуальной машины

► *Чтобы выбрать имя и расположение новой виртуальной машины в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

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:

    a. Установите флажок **Store the virtual machine in a different location**.

    b. 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.

Шаг 3. Выбор поколения виртуальной машины

► *Чтобы выбрать поколение виртуальной машины, выполните следующие действия:*

1. Выберите вариант **Generation 1**.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Шаг 4. Выделение памяти для виртуальной машины

► *Чтобы указать объем памяти, который вы хотите выделить для новой виртуальной машины, выполните следующие действия:*

1. В поле **Startup memory** укажите объем выделяемой памяти.

2. Если вы хотите использовать динамическую память, установите флажок **Use Dynamic Memory for this virtual machine**.

3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Шаг 5. Настройка сетевого подключения

► *Чтобы настроить сетевое подключение новой виртуальной машины, выполните следующие действия:*

1. В раскрывающемся списке выберите вариант подключения сетевого адаптера.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Шаг 6. Подключение виртуального жесткого диска

► *Чтобы подключить виртуальный жесткий диск для установки операционной системы, выполните следующие действия:*

1. Выберите один из следующих вариантов:

   - Если вы хотите создать новый виртуальный жесткий диск, выберите вариант **Create a virtual hard disk** и выполните следующие действия:

     1. В поле **Name** введите имя нового виртуального жесткого диска.

     1. В поле **Location** укажите путь к папке, в которой будет расположен виртуальный жесткий диск.

     2. В поле **Size** введите размер виртуального жесткого диска.

   - Если вы хотите подключить существующий виртуальный жесткий диск, выберите вариант **Use an existing virtual hard disk** и в поле **Location** укажите путь до виртуального жесткого диска.

   - Если вы хотите подключить виртуальный жесткий диск позже, выберите вариант **Attach a virtual hard disk later**.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Шаг 7. Выбор способа установки операционной системы

► *Чтобы выбрать способ установки операционной системы виртуальной машины в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

1. Выберите один из следующих вариантов:

   - Если вы хотите установить операционную систему позже, выберите вариант **Install an operating system later**.

   - Если вы хотите установить операционную систему с загрузочного CD- или DVD-диска, выберите вариант **Install an operating system from a bootable CD / DVD-ROM** и выполните следующие действия:

     1. В блоке параметров **Media** выберите вариант **Image file (.iso)**.

     1. Укажите путь к ISO-образу виртуальной машины.

   Другие способы установки Kaspersky Secure Mail Gateway не поддерживаются.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Шаг 8. Завершение создания виртуальной машины

► *Чтобы завершить создание образа виртуальной машины в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

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

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

Мастер завершит свою работу. В правой части окна программы Microsoft Hyper-V Manager появится новая виртуальная машина.

Шаг 9. Запуск виртуальной машины

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

1. В правой части окна щелкните правой клавишей мыши по виртуальной машине, на которую вы хотите установить операционную систему.
2. В контекстном меню выберите команду **Start**.

Виртуальная машина запустится.

Шаг 10. Подключение к виртуальной машине и запуск мастера первоначальной настройки

► *Чтобы подключиться к виртуальной машине и начать первоначальную настройку Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В правой части окна щелкните правой клавишей мыши по виртуальной машине, к которой вы хотите подключиться.
2. В контекстном меню выберите команду **Connect**.

   Откроется консоль управления виртуальной машины. После подключения к виртуальной машине в консоли управления появится надпись `Press any key to continue`.
3. Нажмите на любую клавишу.

   Запустится мастер первоначальной настройки и откроется окно **Welcome to software installation wizard**.
4. Нажмите на кнопку **Ok**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 11. Просмотр Лицензионного соглашения

На этом шаге вам нужно отклонить или принять условия Лицензионного соглашения программы. Для перемещения по тексту используйте клавиши управления курсором.

► *Чтобы отклонить или принять условия Лицензионного соглашения, выполните следующие действия:*

1. Выберите один из следующих вариантов:

   - **I do not accept the agreement**, если вы хотите отклонить условия Лицензионного соглашения.

   - **I accept the agreement**, если вы хотите принять условия Лицензионного соглашения.

2. Нажмите на клавишу **Enter**.

Если вы отклонили условия Лицензионного соглашения, развертывание виртуальной машины программы завершается.

Если вы приняли условия Лицензионного соглашения, вы перейдете к следующему шагу мастера первоначальной настройки.

Шаг 12. Установка программы на виртуальную машину

► *Чтобы запустить установку виртуальной машины программы, выполните следующие действия:*

1. В окне **Select device** выберите диск, на который вы хотите установить виртуальную машину программы.

2. Нажмите на клавишу **Enter**.

Начнется установка виртуальной машины, это может занять несколько минут. По завершении установки в консоли управления появится надпись `Press any key to continue`.

3. Нажмите на любую клавишу.

   Виртуальная машина перезагрузится.

После установки виртуальной машины перейдите к первоначальной настройке виртуальной машины.

Подготовка программы к работе

В этом разделе перечислены действия, которые вам нужно выполнить, чтобы подготовить программу к работе.

Интерфейс Kaspersky Secure Mail Gateway

Работа с Kaspersky Secure Mail Gateway осуществляется через веб-интерфейс.

Главное окно веб-интерфейса содержит следующие элементы:

- дерево консоли управления в левой части главного окна веб-интерфейса программы;
- рабочую область в правой части главного окна веб-интерфейса программы.

Дерево консоли управления Kaspersky Secure Mail Gateway

В дереве консоли управления отображаются разделы Kaspersky Secure Mail Gateway и подразделы функциональных компонентов Kaspersky Secure Mail Gateway.

В дереве консоли управления Kaspersky Secure Mail Gateway отображаются следующие разделы:

- **Мониторинг** – раздел, содержащий данные мониторинга Kaspersky Secure Mail Gateway.
- **Правила** – раздел, содержащий правила обработки сообщений.
- **Домены** – раздел, в котором вы можете добавить, изменить или удалить информацию о доменах и адресах электронной почты, настроить параметры Kaspersky Secure Mail Gateway для этих доменов и адресов электронной почты.
- **Ключи шифрования** – раздел, в котором вы можете добавить, изменить или удалить DKIM- и TLS-ключи шифрования.
- **Хранилище** – раздел, содержащий информацию о хранилище сообщений и фильтр поиска сообщений в хранилище.
- **Очередь сообщений** – раздел, содержащий информацию об очереди сообщений почтового агента MTA и фильтр поиска сообщений в очереди.
- **Отчеты** – раздел, содержащий отчеты о работе почтового сервера.

- **Параметры** – раздел, в котором вы можете настроить параметры Kaspersky Secure Mail Gateway.

- **Быстрая настройка MTA** – мастер настройки основных параметров MTA, с помощью которого вы можете быстро интегрировать Kaspersky Secure Mail Gateway в почтовую инфраструктуру вашей организации при первом запуске веб-интерфейса Kaspersky Secure Mail Gateway, а также переопределить параметры MTA при последующих запусках веб-интерфейса Kaspersky Secure Mail Gateway.

  После того, как вы пройдете все шаги мастера **Быстрая настройка MTA**, Kaspersky Secure Mail Gateway сбросит все значения параметров MTA и заменит их на значения, которые вы ввели в мастере быстрой настройки MTA.

Рабочая область окна веб-интерфейса Kaspersky Secure Mail Gateway

Рабочая область содержит информацию о разделах, которые вы выбираете в консоли управления, а также элементы управления, с помощью которых вы можете изменять параметры программы.

Для разделов, предусматривающих работу с параметрами Kaspersky Secure Mail Gateway, в рабочей области главного окна параметры сгруппированы в **блоки параметров**.

Состояние защиты почтового сервера

В разделе **Мониторинг** главного окна веб-интерфейса Kaspersky Secure Mail Gateway в правой части рабочей области отображается следующая информация о состоянии защиты почтового сервера:

- состояние работы модуля Анти-Спам, актуальность баз модуля Анти-Спам, количество сообщений в Анти-Спам карантине;
- состояние работы модуля Антивирус, актуальность баз модуля Антивирус;
- состояние соединения с сервером KATA, количество сообщений в KATA-карантине (если вы используете программу Kaspersky Anti Targeted Attack Platform);
- состояние подключения к Kaspersky Private Security Network;
- информация о последнем обновлении баз программы;
- состояние подключения к LDAP-серверам;
- срок действия лицензии и предупреждение о скором истечении срока действия лицензии, если он скоро истечет;
- информация о состоянии отправки и приема сообщений почтовым агентом MTA.

По умолчанию модули Анти-Спам и Антивирус включены, контентная фильтрация, проверка подлинности отправителей сообщений и защита KATA отключены.

Об участии в Kaspersky Security Network и использовании Kaspersky Private Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Secure Mail Gateway использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (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 Secure Mail Gateway 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 Secure Mail Gateway, 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 Secure Mail Gateway 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 Secure Mail Gateway, его можно изменить в любой момент.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. Руководство администратора Kaspersky Private Security Network.

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 (http://www.kaspersky.ru/find_partner_office).

Настройка использования Kaspersky Private Security Network

► *Чтобы настроить использование Kaspersky Private Security Network, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. В блоке **Внешние службы** по ссылке **Использование KSN / KPSN** откройте окно **Использование KSN / KPSN**.
3. В списке действий выберите **Использовать KPSN**.
4. В строке **Загрузить конфигурационный файл KPSN** нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
5. Выберите конфигурационный файл KPSN, который вы хотите добавить.

   Конфигурационный файл KPSN должен быть в формате ZIP-архива.
6. Нажмите на кнопку **ОК**.

   Окно выбора файлов закроется.
7. В блоке **Внешние службы** по ссылке **Ждать ответ от KSN** откройте окно **Внешние службы**.
8. В поле **Ждать ответ от KSN** укажите максимальное время ожидания ответа от KSN в секундах. Вы можете указать значение в интервале от 1 до 300 сек.

   Значение по умолчанию: 10 сек.

9. Нажмите на кнопку **Применить**.

Использование Kaspersky Private Security Network будет настроено.

Первоначальная настройка программы

После развертывания образа виртуальной машины программы выполните ее первоначальную настройку.

Первоначальная настройка виртуальной машины представляет собой последовательность шагов. Мастер первоначальной настройки программы запускается автоматически после первого включения виртуальной машины.

Подготовка к первоначальной настройке виртуальной машины в гипервизоре VMware ESXi

► *Чтобы приступить к первоначальной настройке виртуальной машины программы в гипервизоре VMware ESXi, выполните следующие действия:*

1. Запустите программу VMware vSphere Client.
2. Выберите виртуальную машину Kaspersky Secure Mail Gateway в списке виртуальных машин в левой части главного окна программы.
3. Включите виртуальную машину, нажав на кнопку  в панели управления главного окна программы.
4. Откройте консоль VMware vSphere Client, выбрав закладку **Console** в правой части главного окна программы и следуйте шагам мастера первоначальной настройки.

Подготовка к первоначальной настройке виртуальной машины в гипервизоре Microsoft Hyper-V

► *Чтобы приступить к первоначальной настройке виртуальной машины Kaspersky Secure Mail Gateway в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

1. Запустите программу Microsoft Hyper-V Manager.
2. В разделе **Virtual Machines** выберите виртуальную машину, первоначальную настройку которой вы хотите произвести.
3. Включите виртуальную машину, нажав на кнопку  в панели управления главного окна программы.

   Запустится консоль управления виртуальной машиной Kaspersky Secure Mail Gateway.
4. Следуйте шагам мастера первоначальной настройки программы.

Шаг 1. Выбор языка для просмотра Лицензионного соглашения

► *Чтобы установить язык, на котором будут отображаться тексты Лицензионного соглашения программы и Положения о Kaspersky Security Network, выполните следующие действия:*

1. Выберите язык из списка.

   Доступные языки зависят от пакетов локализаций, включенных в вашу поставку Kaspersky Secure Mail Gateway.
2. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге вам нужно отклонить или принять условия Лицензионного соглашения программы. Для перемещения по тексту используйте клавиши управления курсором.

► *Чтобы отклонить или принять условия Лицензионного соглашения, выполните следующие действия:*

1. Выберите один из следующих вариантов:

   - **I do not accept the agreement**, если вы хотите отклонить условия Лицензионного соглашения.

   - **I accept the agreement**, если вы хотите принять условия Лицензионного соглашения.

2. Нажмите на клавишу **Enter**.

Если вы отклонили условия Лицензионного соглашения, первоначальная настройка программы завершается. Мастер первоначальной настройки предложит вам выключить виртуальную машину.

Если вы приняли условия Лицензионного соглашения, мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 3. Выбор режима работы программы

На этом шаге вам нужно выбрать режим работы программы внутри IT-инфраструктуры вашей организации.

Kaspersky Secure Mail Gateway может работать в обычном режиме или в сертифицированном режиме.

В обычном режиме программе разрешен доступ в интернет и соединение со следующими серверами, расположенными за пределами IT-инфраструктуры вашей организации:

- Серверами обновлений баз KSN.

- DNS-серверами.

- Серверами обновлений баз программы (см. раздел "Об источниках обновлений" на стр. 231).

В сертифицированном режиме программе запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации. Кроме того, когда программа работает в сертифицированном режиме, администратор не имеет возможности просматривать журнал событий из меню администратора программы.

В сертифицированном режиме параметры компонентов программы, которые требуют доступ в интернет, по умолчанию принимают следующие значения:

- Использование KSN отключено.
- SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений отключены, соединение с DNS-серверами запрещено.
- Параметр Enforced Anti-Spam Updates (см. раздел "Настройка параметров модуля Анти-Спам" на стр. 261) отключен в параметрах модуля Анти-Спам.
- В качестве источника обновлений баз программы используется Kaspersky Security Center или локальный источник обновлений баз Kaspersky Secure Mail Gateway (см. раздел "Об источниках обновлений" на стр. 231).

► *Чтобы выбрать режим работы программы, выполните следующие действия:*

1. Выберите один из следующих вариантов перевода программы в сертифицированный режим работы:
   - **No**, если вы не хотите переводить программу в сертифицированный режим работы и хотите, чтобы программа работала в обычном режиме.
   - **Yes**, если вы хотите перевести программу в сертифицированный режим работы.
2. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 4. Выбор языка ввода для работы с программой

► *Чтобы настроить язык ввода, используемый при работе с программой, выполните следующие действия:*

1. Выберите язык ввода в списке.

2. Нажмите на кнопку **OK**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 5. Установка часового пояса

► *Чтобы установить часовой пояс для Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. Выберите страну из списка, отображенного на экране консоли.

2. Нажмите на клавишу **Enter**.

   Отобразится список часовых поясов, доступных для выбранной страны.

3. Выберите часовой пояс.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения выбора часового пояса.

5. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 6. Назначение имени хоста (myhostname)

► *Чтобы указать имя хоста программы для использования DNS-серверами (`myhostname`), выполните следующие действия:*

1. В поле **hostname** введите полное доменное имя сервера программы.

Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).

2. Нажмите на кнопку **Ok**.

   После того, как вы назначили имя хоста программы, виртуальная машина попытается получить сетевые параметры автоматически с использованием DHCP-сервера и загрузить базы программы.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 7. Настройка сетевого интерфейса

На этом шаге настройте параметры сетевого интерфейса программы: включите или отключите сетевой интерфейс, назначьте IP-адрес и маску сети.

В этом разделе

Включение и отключение сетевого интерфейса

Для настройки программы необходимо, чтобы хотя бы один сетевой интерфейс был включен. Вам может понадобиться отключить сетевой интерфейс, если вы используете несколько сетевых интерфейсов и хотите временно отключить один из них.

► *Чтобы отключить сетевой интерфейс, выполните следующие действия:*

1. Выберите параметр **Enabled**.

2. Нажмите на клавишу **Enter**.

   Параметр **Enabled** примет значение **no**.

3. Перейдите к назначению IP-адреса и маски сети (см. раздел "Назначение IP-адреса и маски сети с помощью DHCP-сервера" на стр. 76, "Назначение статического IP-адреса и маски сети" на стр. 77), чтобы завершить настройку сетевого интерфейса.

► *Чтобы включить сетевой интерфейс, выполните следующие действия:*

1. Убедитесь, что параметр **Enabled** имеет значение **yes**.

   По умолчанию сетевой интерфейс включен.

2. Перейдите к назначению IP-адреса и маски сети (см. раздел "Назначение IP-адреса и маски сети с помощью DHCP-сервера" на стр. 76, "Назначение статического IP-адреса и маски сети" на стр. 77), чтобы завершить настройку сетевого интерфейса.

Назначение IP-адреса и маски сети с помощью DHCP-сервера

► *Чтобы назначить IP-адрес и маску сети с помощью DHCP-сервера, выполните следующие действия:*

1. Убедитесь, что параметр **Use DHCP** имеет значение **yes**.

   > Вам может понадобиться использовать DHCP-сервер для назначения IP-адреса и маски сети, если вы настраиваете программу в тестовом режиме.

   По умолчанию использование DHCP-сервера для назначения IP-адреса и маски сети включено.

2. Выберите **Continue**.

3. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Назначение статического IP-адреса и маски сети

► *Чтобы назначить статический IP-адрес и маску сети, выполните следующие действия:*

1. Выберите параметр **Use DHCP**.

   Рекомендуется назначить статический IP-адрес и маску сети, если вы настраиваете программу в рабочем режиме.

2. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения назначения статических параметров сетевого интерфейса.

3. Нажмите на кнопку **Yes**.

   Отобразится окно ввода статического IP-адреса и маски сети.

4. В поле **Address** введите IP-адрес, который вы хотите назначить для Kaspersky Secure Mail Gateway.

5. В поле **Netmask** введите маску сети, в которой вы используете программу.

6. Нажмите на кнопку **Ok**.

   Мастер первоначальной настройки программы вернется к окну настройки сетевого интерфейса.

7. Проверьте правильность установленных сетевых параметров.

8. Выберите **Continue**.

9. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 8. Настройка сетевых маршрутов

На этом шаге назначьте адрес шлюза, чтобы настроить сетевой маршрут. Вы также можете добавить, удалить или изменить дополнительные статические маршруты сети на этом шаге.

В этом разделе

Назначение адреса шлюза с помощью DHCP-сервера

► *Чтобы назначить адрес шлюза с помощью DHCP-сервера, выполните следующие действия:*

1. Убедитесь, что в списке **Default route** параметр **Gateway** имеет значение **dhcp**.

   > Вам может понадобиться использовать DHCP-сервер для назначения адреса шлюза, если вы настраиваете программу в тестовом режиме.

   По умолчанию использование DHCP-сервера для назначения адреса шлюза включено.

2. Выберите **Continue**.

3. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Назначение статического адреса шлюза

► *Чтобы назначить статический адрес шлюза, выполните следующие действия:*

1. В списке **Default route** выберите параметр **Gateway**.
2. Нажмите на клавишу **Enter**.
3. Если на предыдущем шаге первоначальной настройки Kaspersky Secure Mail Gateway вы выбрали использование DHCP-сервера для настройки сетевого интерфейса, нажмите на кнопку **Yes** в открывшемся окне подтверждения назначения статического адреса шлюза.

   Отобразится окно ввода статического адреса шлюза.
4. В поле **Gateway** введите адрес шлюза.
5. Нажмите на кнопку **Ok**.

   Мастер первоначальной настройки программы вернется к окну настройки сетевых маршрутов.
6. Проверьте правильность параметров установленного сетевого маршрута.

   > Если вы хотите изменить, удалить или добавить дополнительные статические маршруты, перейдите к настройке дополнительных статических маршрутов сети (см. раздел "Добавление дополнительного статического маршрута" на стр. 80).
7. Выберите **Continue**.
8. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Добавление дополнительного статического маршрута

► *Чтобы добавить дополнительный статический маршрут, выполните следующие действия:*

1. Выберите параметр **Edit static routes**.
2. Нажмите на клавишу **Enter**.

   Отобразится окно выбора действия при настройке дополнительных статических маршрутов.
3. Выберите **New route**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно ввода параметров статического маршрута.
5. В поле **Address** введите IP-адрес статического маршрута.
6. В поле **Netmask** введите маску сети статического маршрута.
7. В поле **Gateway** введите адрес шлюза.
8. Нажмите на кнопку **Ok**.

   Отобразится окно выбора сетевого интерфейса, в котором вы хотите настроить статический маршрут.
9. Выберите сетевой интерфейс.
10. Нажмите на клавишу **Enter**.

    Отобразится окно со списком дополнительных статических маршрутов.
11. Выберите **Go back**.
12. Нажмите на клавишу **Enter**.

    Мастер первоначальной настройки программы вернется к окну настройки сетевых маршрутов.

13. Проверьте правильность параметров установленного сетевого маршрута.

14. Выберите **Continue**.

15. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Изменение дополнительного статического маршрута

► *Чтобы изменить дополнительный статический маршрут, выполните следующие действия:*

1. Выберите параметр **Edit static routes**.

2. Нажмите на клавишу **Enter**.

   Отобразится окно со списком дополнительных статических маршрутов.

3. Выберите дополнительный статический маршрут, который вы хотите изменить.

4. Нажмите на клавишу **Enter**.

5. Отобразится окно ввода параметров статического маршрута.

6. Внесите изменения в поле **Address**, если вы хотите изменить IP-адрес статического маршрута.

7. Внесите изменения в поле **Netmask**, если вы хотите изменить маску сети статического маршрута.

8. Внесите изменения в поле **Gateway**, если вы хотите изменить адрес шлюза.

9. Нажмите на кнопку **Ok**.

   Отобразится окно выбора сетевого интерфейса, в котором вы хотите настроить статический маршрут.

10. Выберите сетевой интерфейс.

11. Нажмите на клавишу **Enter**.

    Отобразится окно со списком дополнительных статических маршрутов.

12. Выберите **Go back**.

13. Нажмите на клавишу **Enter**.

    Мастер первоначальной настройки программы вернется к окну настройки сетевых маршрутов.

14. Проверьте правильность параметров установленного сетевого маршрута.

15. Выберите **Continue**.

16. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Удаление дополнительного статического маршрута

► *Чтобы удалить дополнительный статический маршрут, выполните следующие действия:*

1. Выберите параметр **Edit static routes**.

2. Нажмите на клавишу **Enter**.

   Отобразится окно со списком дополнительных статических маршрутов.

3. Выберите **Delete routes**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно выбора статического маршрута для удаления.

5. Выберите маршрут, который вы хотите удалить.

6. Нажмите на кнопку **Delete**.

Мастер первоначальной настройки программы вернется к окну со списком оставшихся после удаления дополнительных статических маршрутов или, если вы удалили все дополнительные маршруты, отобразит окно выбора действия над маршрутами.

7. Выберите **Go back**.
8. Нажмите на клавишу **Enter**.

   Мастер первоначальной настройки программы вернется к окну настройки сетевых маршрутов.

9. Проверьте правильность параметров установленного сетевого маршрута.
10. Выберите **Continue**.
11. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 9. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы с виртуальной машиной Kaspersky Secure Mail Gateway.

В этом разделе

Назначение DNS-адресов с помощью DHCP-сервера

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. Выберите имя вашего сетевого интерфейса (например, **eth0**) в окне настройки использования DHCP-сервера для назначения DNS-адресов.

   > Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете программу в тестовом режиме.

2. Нажмите на клавишу **Enter**.

   Отобразится окно настройки параметров DNS с помощью DHCP-сервера.

3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.

4. Выберите **Continue**.

5. Нажмите на клавишу **Enter**.

   Отобразится окно с параметрами сети Kaspersky Secure Mail Gateway.

6. Выберите **Continue**.

7. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перезагрузит виртуальную машину с новыми значениями параметров и перейдет к следующему шагу.

Назначение статических DNS-адресов

► *Чтобы назначить статические DNS-адреса, выполните следующие действия:*

1. Выберите **no** в окне настройки использования DHCP-сервера для назначения DNS-адресов.

> Рекомендуется назначить статические DNS-адреса, если вы настраиваете программу в рабочем режиме.

2. Нажмите на клавишу **Enter**.

   Отобразится окно ввода статических DNS-адресов.

3. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Secure Mail Gateway.

4. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.

5. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.

6. Нажмите на кнопку **Ok**.

   Отобразится окно настройки статических параметров DNS.

7. Проверьте правильность установленных параметров DNS.

8. Выберите **Continue**.

9. Нажмите на клавишу **Enter**.

   Отобразится окно с параметрами сети Kaspersky Secure Mail Gateway.

10. Выберите **Continue**.

11. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перезагрузит виртуальную машину с новыми значениями параметров и перейдет к следующему шагу.

Шаг 10. Установка пароля администратора веб-интерфейса

► *Чтобы установить пароль администратора для доступа к веб-интерфейсу (учетная запись* `Administrator`*), выполните следующие действия:*

1. В поле **Test input** введите любые символы и проверьте раскладку клавиатуры.

2. В поле **Password** введите пароль администратора для доступа к веб-интерфейсу Kaspersky Secure Mail Gateway (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 97).

   Пароль должен содержать:

   - минимум восемь символов;
   - только символы в кодировке ASCII;
   - минимум один символ верхнего регистра;
   - минимум один символ нижнего регистра;
   - минимум одну цифру.

3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 11. Установка пароля администратора виртуальной машины

Администратор Kaspersky Secure Mail Gateway обладает правами на управление виртуальной машиной. Администратор может выключить, перезагрузить виртуальную машину, изменить ее сетевые параметры в консоли управления. Для администрирования Kaspersky Secure Mail Gateway используется учетная запись admin и задается отдельный пароль администратора.

► *Чтобы установить пароль администратора для работы с программой в консоли управления (учетная запись `admin`), выполните следующие действия:*

1. В поле **Test input** введите любые символы и проверьте раскладку клавиатуры.
2. В поле **Password** введите пароль администратора для управления параметрами программы.

   Пароль должен содержать:

- минимум восемь символов;
- только символы в кодировке ASCII;
- минимум один символ верхнего регистра;
- минимум один символ нижнего регистра;
- минимум одну цифру.

3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 12. Указание адресов электронной почты администратора почтового сервера

► *Чтобы указать адреса электронной почты администратора почтового сервера Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В поле **admins' emails** введите адреса электронной почты администратора программы. Вы можете ввести несколько адресов через запятую.
2. Нажмите на кнопку **Ok**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 13. Настройка соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center

На этом шаге настройте соединение Kaspersky Secure Mail Gateway с Kaspersky Security Center с помощью мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Программа Kaspersky Security Center предназначена для централизованного решения административных задач управления и мониторинга Kaspersky Secure Mail Gateway.

Kaspersky Security Center выполняет роль *сервера администрирования*.

В состав программы входит а*гент администрирования* (`nagent`).

Kaspersky Security Center позволяет администратору выполнять следующие задачи по управлению программой:

- добавлять активный и дополнительный ключи;
- запускать задачу обновления баз программы;
- отображать информацию о состоянии защиты программы;
- запускать и останавливать программу.

В этом разделе

Включение агента администрирования

Для настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center необходимо, чтобы агент администрирования был включен.

По умолчанию агент администрирования отключен.

► *Чтобы включить агент администрирования, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Enabled**.
2. Убедитесь, что параметр **Enabled** имеет значение **yes**.
3. Если параметр **Enabled** имеет значение **no**, нажмите на клавишу **Enter**.

Продолжайте выполнять действия по настройке соединения в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Ввод адреса сервера администрирования

► *Чтобы ввести адрес сервера администрирования Kaspersky Security Center, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Address**.
2. Нажмите на клавишу **Enter**.

   Откроется окно ввода адреса сервера администрирования.
3. Введите DNS-имя или IP-адрес сервера администрирования Kaspersky Security Center.
4. Нажмите на кнопку **Ok**.

Продолжайте выполнять действия по настройке соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Указание номера порта подключения к серверу администрирования

► *Чтобы указать номер порта подключения к серверу администрирования Kaspersky Security Center, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Port**.
2. Нажмите на клавишу **Enter**.

Откроется окно ввода порта подключения к серверу администрирования.

3. Введите номер порта подключения к серверу администрирования или используйте порт по умолчанию (13000).

4. Нажмите на кнопку **Ok**.

Продолжайте выполнять действия по настройке соединения в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Использование SSL-соединения при передаче данных

Вы можете включить использование SSL-соединения при передаче данных на сервер администрирования Kaspersky Security Center.

По умолчанию использование SSL-соединения при передаче данных на сервер администрирования Kaspersky Security Center включено.

► *Чтобы включить использование SSL-соединения, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Use SSL**.

2. Убедитесь, что параметр **Use SSL** имеет значение **yes**.

3. Если параметр **Use SSL** имеет значение **no**, нажмите на клавишу **Enter**.

Продолжайте выполнять действия по настройке соединения в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Использование шлюза при подключении к серверу администрирования

Вы можете выбрать один из вариантов использования шлюза при подключении Kaspersky Secure Mail Gateway к серверу администрирования Kaspersky Security Center:

- отключить использование шлюза;

- включить использование шлюза;
- включить использование агента администрирования в качестве шлюза.

По умолчанию использование шлюза при подключении к серверу администрирования отключено, соединение с Kaspersky Security Center устанавливается напрямую.

► *Чтобы отключить использование шлюза при подключении программы к серверу администрирования, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Gw mode**.
2. Убедитесь, что параметр **Gw mode** имеет значение **don't use**.
3. Если параметр **Gw mode** имеет любое другое значение, нажимайте на клавишу **Enter** до тех пор, пока параметр **Gw mode** не примет значение **don't use**.

► *Чтобы включить использование шлюза при подключении программы к серверу администрирования, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Gw mode**.
2. Нажимайте на клавишу **Enter** до тех пор, пока параметр **Gw mode** не примет значение **use gateway**.
3. Выберите параметр **Gateway**.
4. Нажмите на клавишу **Enter**.

   Откроется окно ввода адреса шлюза.
5. Введите DNS-имя или IP-адрес шлюза, который вы хотите использовать при подключении к серверу администрирования Kaspersky Security Center.
6. Нажмите на кнопку **Ok**.

► *Чтобы включить использование агента администрирования в качестве шлюза при подключении программы к серверу администрирования, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Gw mode**.

2. Нажимайте на клавишу **Enter** до тех пор, пока параметр **Gw mode** не примет значение **act as gateway**.

Перейдите к проверке соединения программы с Kaspersky Security Center в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center.

Шаг 14. Проверка соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center

► *Чтобы проверить соединение программы с Kaspersky Security Center, выполните следующие действия в окне мастера настройки соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center:*

1. Выберите параметр **Check Status**.

2. Нажмите на клавишу **Enter**.

3. Если вы изменяли значения параметров соединения программы с Kaspersky Security Center при настройке соединения Kaspersky Secure Mail Gateway с Kaspersky Security Center, нажмите на кнопку **Yes** в открывшемся окне подтверждения сохранения изменений.

   Окно подтверждения сохранения изменений параметров соединения с Kaspersky Security Center закроется.

   Параметр **Check Status** примет значение, соответствующее статусу соединения программы с Kaspersky Security Center.

   Например, если соединение программы с Kaspersky Security Center установлено успешно, параметр **Check Status** примет значение **OK**.

4. Выберите **Continue**.

5. Нажмите на клавишу **Enter**.

Мастер первоначальной настройки программы перейдет к следующему шагу.

Шаг 15. Отображение параметров подключения к веб-интерфейсу

Если сетевое соединение настроено успешно, на этом шаге первоначальная настройка Kaspersky Secure Mail Gateway завершается, и отображается окно с параметрами подключения к веб-интерфейсу.

Запомните или запишите IP-адрес, указанный в окне **IP address information**, и нажмите на кнопку **Ok**.

Первоначальная настройка Kaspersky Secure Mail Gateway завершена.

Если в вашей сети не используется DHCP-сервер, Kaspersky Secure Mail Gateway не сможет автоматически получить параметры подключения к веб-интерфейсу программы, и IP-адрес подключения к веб-интерфейсу не отобразится в окне **IP address information**. В этом случае вы можете настроить параметры подключения к веб-интерфейсу программы вручную через меню администратора Kaspersky Secure Mail Gateway.

Запуск виртуальной машины программы

После первоначальной настройки виртуальная машина Kaspersky Secure Mail Gateway запускается автоматически. Для обеспечения взаимодействия с существующей почтовой инфраструктурой требуется дополнительная настройка почтового сервера, предустановленного на виртуальной машине Kaspersky Secure Mail Gateway.

Вы можете получить информацию о процессе работы Kaspersky Secure Mail Gateway, а также настроить правила обработки сообщений и параметры защиты через веб-интерфейс (см. стр. 97).

Вы также можете настроить параметры и управлять работой виртуальной машины из меню администратора в консоли управления программой.

Изменение конфигурации виртуальной машины

Вы можете изменять конфигурацию виртуальных машин в гипервизорах VMware ESXi и Microsoft Hyper-V. Например, вы можете добавлять или удалять виртуальные жесткие диски, добавлять или удалять виртуальные сетевые адаптеры или изменять объем виртуальной оперативной памяти.

В этом разделе

Изменение конфигурации виртуальной машины в гипервизоре VMware ESXi

► *Чтобы изменить конфигурацию виртуальной машины в гипервизоре VMware ESXi, выполните следующие действия:*

1. Запустите программу VMware vSphere Client.
2. В списке виртуальных машин в левой части главного окна программы выберите виртуальную машину, конфигурацию которой вы хотите изменить.
3. Нажатием правой кнопки мыши раскройте меню.
4. Выберите пункт меню **Edit Settings**.

   Откроется окно **Virtual Machine Properties**.

5. Выберите закладку с группой параметров конфигурации виртуальной машины, которые вы хотите изменить.

6. Выберите параметры конфигурации виртуальной машины, которые вы хотите изменить.

7. В правой части окна произведите изменения конфигурации виртуальной машины.

Подробнее об изменении конфигурации виртуальной машины в гипервизоре VMware ESXi см. в документации к гипервизору VMware ESXi.

Изменение конфигурации виртуальной машины в гипервизоре Microsoft Hyper-V

► *Чтобы изменить конфигурацию виртуальной машины в гипервизоре Microsoft Hyper-V, выполните следующие действия:*

1. Запустите программу Microsoft Hyper-V Manager.

2. В разделе **Virtual Machines** выберите виртуальную машину, конфигурацию которой вы хотите изменить.

3. В меню **Actions** в правой части окна выберите пункт **Settings**.

   Откроется окно **Settings**.

4. В левой части окна выберите параметры конфигурации виртуальной машины, которые вы хотите изменить.

5. В правой части окна произведите изменения конфигурации виртуальной машины.

Подробнее об изменении конфигурации виртуальной машины в гипервизоре Microsoft Hyper-V см. в документации к гипервизору Microsoft Hyper-V.

Отключение синхронизации времени виртуальной машины и хоста

Синхронизация времени позволяет обеспечить постоянное соответствие времени гостевой операционной системы и хоста средствами гипервизора. Если синхронизация времени включена, то время гостевой операционной системы всегда синхронизировано с временем хоста.

Если вы хотите использовать протокол сетевого времени (*Network Time Protocol*), рекомендуется отключить синхронизацию времени на уровне гипервизора:

- Для настройки гипервизора ESXi обратитесь к документации VMware ESXi https://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vmtools.install.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html.
- Для настройки гипервизора Hyper-V обратитесь к документации Microsoft https://technet.microsoft.com/en-gb/library/dn798346(v=ws.11).aspx.

Начало работы в веб-интерфейсе программы

После установки и первоначальной настройки программы вы можете начать работу в веб-интерфейсе Kaspersky Secure Mail Gateway.

► *Чтобы начать работу в веб-интерфейсе программы, выполните следующие действия:*

1. В браузере введите IP-адрес веб-интерфейса программы, полученный при установке программы.

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

2. В поле **Имя пользователя** введите `Administrator`.

3. В поле **Пароль** введите пароль, заданный при установке программы.

4. Нажмите на кнопку **Войти**.

Откроется главная страница веб-интерфейса Kaspersky Secure Mail Gateway.

Интеграция Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации

Kaspersky Secure Mail Gateway интегрируется в существующую почтовую инфраструктуру организации и не является самостоятельной почтовой системой. Например, Kaspersky Secure Mail Gateway не доставляет сообщения электронной почты получателям и не управляет учетными записями пользователей.

Вы можете интегрировать Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации одним из следующих способов:

- Напрямую.
- Через пограничный шлюз, на котором включена SMTP-проверка адресов электронной почты получателей сообщений.

  Перед настройкой интеграции Kaspersky Secure Mail Gateway через пограничный шлюз вам нужно указать, включена ли SMTP-проверка адресов электронной почты получателей сообщений на пограничном шлюзе, на который Kaspersky Secure Mail Gateway будет пересылать сообщения с внутренних доменов.
- Через пограничный шлюз, на котором отключена SMTP-проверка адресов электронной почты получателей сообщений.

Вы можете настроить основные параметры интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации с помощью мастера быстрой настройки MTA, а также выполнить действия по интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации вручную в веб-интерфейсе программы.

После того, как вы пройдете все шаги мастера **Быстрая настройка MTA**, Kaspersky Secure Mail Gateway сбросит все значения параметров MTA и заменит их на значения, которые вы ввели в мастере быстрой настройки MTA.

В этом разделе

Интеграция напрямую

Интеграция напрямую – интеграция, при которой Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты напрямую из интернета и перенаправлять их на внутренние почтовые серверы, а также принимать сообщения с внутренних почтовых серверов и перенаправлять их в интернет.

► *Чтобы настроить интеграцию Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации напрямую, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Быстрая настройка MTA**.

2. В блоке **Интеграция Kaspersky Secure Mail Gateway в почтовую инфраструктуру** выберите **Интегрировать напрямую**.

3. По ссылке **Начать интеграцию** перейдите к выполнению шагов мастера.

В этом разделе

Шаг 1. Добавление локальных доменов (relay_domains)

На этом шаге добавьте локальные домены вашей организации, для которых Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты извне. Kaspersky Secure Mail Gateway будет принимать сообщения только для указанных вами доменов. Сообщения, предназначенные для получения другими доменами, будут отклонены.

Если локальные домены не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения для ваших внутренних почтовых серверов.

► *Чтобы добавить локальные домены вашей организации, выполните следующие действия:*

1. По ссылке **Добавить домен** откройте окно **Добавление домена**.
2. В поле **Введите имя домена** введите имя домена, для которого Kaspersky Secure Mail Gateway будет принимать сообщения.

   Вводите имена доменов в формате FQDN.
3. Нажмите на кнопку **ОК**.
4. Окно **Добавление домена** закроется.

Имена доменов вводятся по одному. Повторите действия по добавлению имен доменов в список для всех добавляемых имен доменов.

По ссылке **Сохранить и перейти к настройке маршрутизации электронной почты** перейдите к следующему шагу мастера.

Шаг 2. Настройка маршрутизации электронной почты (transport_map)

На этом шаге настройте маршрутизацию электронной почты.

Kaspersky Secure Mail Gateway по умолчанию использует параметры вашего DNS-сервера для маршрутизации электронной почты. Вы можете настроить маршрутизацию электронной почты вручную. Для этого необходимо создать транспортную таблицу. В нее нужно ввести имена доменов, для которых предназначены сообщения электронной почты, а затем ввести IP-адреса или FQDN-имена доменов, на которые Kaspersky Secure Mail Gateway будет перенаправлять сообщения, предназначенные для этих доменов.

Пример:

Если вы хотите, чтобы сообщения, предназначенные для домена example.com, перенаправлялись на адрес 1.1.1.0:25, вам нужно выполнить следующие действия:

1. Добавить домен example.com в транспортную таблицу.
2. Указать IP-адрес 1.1.1.0 и номер порта 25 для маршрутизации сообщений, предназначенных для домена example.com.

► *Чтобы настроить маршрутизацию электронной почты, выполните следующие действия:*

1. По ссылке **Добавить запись в транспортную таблицу** откройте окно **Маршрутизация электронной почты**.
2. В поле **Введите имя домена** введите имя домена, для которого предназначены сообщения электронной почты.

Вводите имена доменов в формате FQDN.

3. В поле **Введите адрес назначения сообщений (IPv4, доменное имя или FQDN)** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

4. В поле **Укажите номер порта соединения с адресом назначения** выберите номер порта.

   Значение по умолчанию: 25.

5. Выберите один из следующих вариантов:

   - **Не включать поиск MX-записей**.
   - **Включить поиск MX-записей (для доменных имен или FQDN)**.

6. Нажмите на кнопку **ОК**.

7. Окно **Маршрутизация электронной почты** закроется.

> Записи транспортной таблицы добавляются по одной. Повторите действия по добавлению записей в транспортную таблицу для всех добавляемых записей.

По ссылке **Сохранить и перейти к добавлению доверенных сетей и узлов сети** перейдите к следующему шагу мастера.

Шаг 3. Добавление доверенных сетей и узлов сети (mynetworks)

На этом шаге создайте список доверенных сетей и узлов сети, которым разрешено пересылать сообщения электронной почты через Kaspersky Secure Mail Gateway.

Как правило, это внутренние сети и узлы сети вашей организации.

Например, вы можете указать IP-адреса серверов Microsoft Exchange, используемых в вашей организации.

Если доверенные сети не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения с внутренних почтовых серверов и перенаправлять их за пределы сети вашей организации.

► *Чтобы добавить список доверенных сетей и узлов сети, выполните следующие действия:*

1. По ссылке **Добавить доверенную сеть или узел сети** откройте окно **Добавление доверенной сети**.
2. В поле **Введите адрес назначения сообщений (IPv4, доменное имя или FQDN)** введите адрес сети или адрес подсети.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN. .
3. Нажмите на кнопку **ОК**.
4. Окно **Добавление доверенной сети** закроется.

Адреса добавляются по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов.

По ссылке **Сохранить и перейти к завершению интеграции** перейдите к следующему шагу мастера.

См. также

Шаг 4. Завершение интеграции Kaspersky Secure Mail Gateway напрямую

На этом шаге просмотрите введенные вами данные интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации и подтвердите свой выбор.

По окончании интеграции в почтовую инфраструктуру организации автоматически настроены следующие параметры Kaspersky Secure Mail Gateway:

- Включена SPF-проверка подлинности отправителей сообщений.
- Включена SMTP-проверка адресов электронной почты получателей сообщений (на стр. 227).

После того, как вы пройдете все шаги мастера **Быстрая настройка MTA**, Kaspersky Secure Mail Gateway сбросит все значения параметров MTA и заменит их на значения, которые вы ввели в мастере быстрой настройки MTA.

Интеграция через пограничный шлюз (SMTP-проверка адресов получателей включена)

Интеграция через пограничный шлюз, на котором включена SMTP-проверка адресов электронной почты получателей сообщений – интеграция, при которой Kaspersky Secure Mail Gateway принимает сообщения с промежуточного шлюза и пересылает их на внутренние почтовые серверы, а также принимает сообщения с внутренних почтовых серверов и пересылает их на пограничный шлюз. При этом на пограничном шлюзе включена SMTP-проверка адресов электронной почты получателей сообщений.

SMTP-проверка адресов электронной почты получателей сообщений используется почтовыми системами для предотвращения приема сообщений для несуществующих адресов.

► *Чтобы настроить интеграцию Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации* через пограничный шлюз, на котором включена SMTP-проверка адресов электронной почты получателей сообщений*, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Быстрая настройка MTA**.

2. В блоке **Интеграция Kaspersky Secure Mail Gateway в почтовую инфраструктуру** выберите **Интегрировать через пограничный шлюз**.

3. По ссылке **Начать интеграцию** перейдите в раздел **SMTP-проверка адресов получателей сообщений на пограничном шлюзе**.

4. Выберите **На пограничном шлюзе включена SMTP-проверка адресов получателей сообщений**.

5. По ссылке **Перейти к добавлению локальных доменов** перейдите к выполнению шагов мастера.

В этом разделе

Шаг 1. Добавление локальных доменов (relay_domains)

На этом шаге добавьте локальные домены вашей организации, для которых Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты извне. Kaspersky Secure Mail Gateway будет принимать сообщения только для указанных вами доменов. Сообщения, предназначенные для получения другими доменами, будут отклонены.

Если локальные домены не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения для ваших внутренних почтовых серверов.

► *Чтобы добавить локальные домены вашей организации, выполните следующие действия:*

1. По ссылке **Добавить домен** откройте окно **Добавление домена**.
2. В поле **Введите имя домена** введите имя домена, для которого Kaspersky Secure Mail Gateway будет принимать сообщения.

   Вводите имена доменов в формате FQDN.
3. Нажмите на кнопку **ОК**.
4. Окно **Добавление домена** закроется.

Имена доменов вводятся по одному. Повторите действия по добавлению имен доменов в список для всех добавляемых имен доменов.

По ссылке **Сохранить и перейти к настройке маршрутизации электронной почты** перейдите к следующему шагу мастера.

Шаг 2. Настройка маршрутизации электронной почты (transport_map)

На этом шаге настройте маршрутизацию электронной почты.

Kaspersky Secure Mail Gateway по умолчанию использует параметры вашего DNS-сервера для маршрутизации электронной почты. Вы можете настроить маршрутизацию электронной почты вручную. Для этого необходимо создать транспортную таблицу. В нее нужно ввести имена доменов, для которых предназначены сообщения электронной почты, а затем ввести IP-адреса или FQDN-имена доменов, на которые Kaspersky Secure Mail Gateway будет перенаправлять сообщения, предназначенные для этих доменов.

Пример:

Если вы хотите, чтобы сообщения, предназначенные для домена example.com, перенаправлялись на адрес 1.1.1.0:25, вам нужно выполнить следующие действия:

1. Добавить домен example.com в транспортную таблицу.
2. Указать IP-адрес 1.1.1.0 и номер порта 25 для маршрутизации сообщений, предназначенных для домена example.com.

► *Чтобы настроить маршрутизацию электронной почты, выполните следующие действия:*

1. По ссылке **Добавить запись в транспортную таблицу** откройте окно **Маршрутизация электронной почты**.
2. В поле **Введите имя домена** введите имя домена, для которого предназначены сообщения электронной почты.

Вводите имена доменов в формате FQDN.

3. В поле **Введите адрес назначения сообщений (IPv4, доменное имя или FQDN)** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

4. В поле **Укажите номер порта соединения с адресом назначения** выберите номер порта.

   Значение по умолчанию: 25.

5. Выберите один из следующих вариантов:

   - **Не включать поиск MX-записей**.
   - **Включить поиск MX-записей (для доменных имен или FQDN)**.

6. Нажмите на кнопку **ОК**.

   Окно **Маршрутизация электронной почты** закроется.

> Записи транспортной таблицы добавляются по одной. Повторите действия по добавлению записей в транспортную таблицу для всех добавляемых записей.

По ссылке **Сохранить и перейти к вводу адреса пограничного шлюза** перейдите к следующему шагу мастера.

Шаг 3. Ввод адреса пограничного шлюза (relayhost)

На этом шаге введите адрес вашего пограничного шлюза. Kaspersky Secure Mail Gateway будет перенаправлять все сообщения на этот адрес.

Например: 192.0.2.1 или domain.com.

Если вы настроили маршрутизацию электронной почты для отдельных доменов, Kaspersky Secure Mail Gateway будет перенаправлять сообщения электронной почты на адреса, указанные для каждого домена.

► *Чтобы ввести адрес пограничного шлюза, выполните следующие действия:*

1. В поле ввода укажите IP-адрес или доменное имя пограничного шлюза.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

2. Выберите один из следующих вариантов:

   - **Не включать поиск MX-записей**.
   - **Включить поиск MX-записей (для доменных имен или FQDN)**.

По ссылке **Сохранить и перейти к добавлению доверенных сетей и узлов сети** перейдите к следующему шагу мастера.

Шаг 4. Добавление доверенных сетей и узлов сети (mynetworks)

На этом шаге создайте список доверенных сетей и узлов сети, которым разрешено пересылать сообщения электронной почты через Kaspersky Secure Mail Gateway.

Как правило, это внутренние сети и узлы сети вашей организации.

Например, вы можете указать IP-адреса серверов Microsoft Exchange, используемых в вашей организации.

Если доверенные сети не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения с внутренних почтовых серверов и перенаправлять их за пределы сети вашей организации.

► *Чтобы добавить список доверенных сетей и узлов сети, выполните следующие действия:*

1. По ссылке **Добавить доверенную сеть или узел сети** откройте окно **Добавление доверенной сети**.

2. В поле **Добавьте адрес сети или узла сети** введите имя домена, для которого предназначены сообщения электронной почты.

   Вводите имена доменов в формате FQDN.

3. Нажмите на кнопку **ОК**.

4. Окно **Добавление доверенной сети** закроется.

> Адреса добавляются по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов.

По ссылке **Сохранить и перейти к завершению интеграции** перейдите к следующему шагу мастера.

Шаг 5. Завершение интеграции через пограничный шлюз (SMTP-проверка включена)

На этом шаге просмотрите введенные вами данные интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации и подтвердите свой выбор.

По окончании интеграции в почтовую инфраструктуру организации автоматически настроены следующие параметры Kaspersky Secure Mail Gateway:

- Отключена SPF-проверка подлинности отправителей сообщений.

> Не включайте SPF-проверку подлинности отправителей сообщений, поскольку отправителем сообщений выступает пограничный шлюз, с которого Kaspersky Secure Mail Gateway принимает сообщения.

- Отключена DMARC-проверка подлинности доменов, с которых Kaspersky Secure Mail Gateway получает сообщения.

  Не включайте DMARC-проверку подлинности доменов, поскольку Kaspersky Secure Mail Gateway получает сообщения с промежуточного шлюза.

- Включена SMTP-проверка адресов электронной почты получателей сообщений (на стр. 227).

  Не отключайте SMTP-проверку адресов электронной почты получателей сообщений, поскольку SMTP-проверка адресов электронной почты получателей сообщений включена на пограничном шлюзе.

После того, как вы пройдете все шаги мастера **Быстрая настройка MTA**, Kaspersky Secure Mail Gateway сбросит все значения параметров MTA и заменит их на значения, которые вы ввели в мастере быстрой настройки MTA.

Интеграция через пограничный шлюз (SMTP-проверка адресов получателей отключена)

Интеграция через пограничный шлюз, на котором отключена SMTP-проверка адресов электронной почты получателей сообщений – интеграция, при которой Kaspersky Secure Mail Gateway принимает сообщения с пограничного шлюза и пересылает их на внутренние почтовые серверы, а также принимает сообщения с внутренних почтовых серверов и пересылает их на пограничный шлюз. При этом на пограничном шлюзе отключена SMTP-проверка адресов электронной почты получателей сообщений.

SMTP-проверка адресов электронной почты получателей сообщений используется почтовыми системами для предотвращения приема сообщений для несуществующих адресов.

► *Чтобы настроить интеграцию Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации* через пограничный шлюз, на котором отключена

SMTP-проверка адресов электронной почты получателей сообщений, *выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Быстрая настройка MTA**.

2. В блоке **Интеграция Kaspersky Secure Mail Gateway в почтовую инфраструктуру** выберите **Интегрировать через пограничный шлюз**.

3. По ссылке **Начать интеграцию** перейдите в раздел **SMTP-проверка адресов получателей сообщений на пограничном шлюзе**.

4. Выберите **На пограничном шлюзе отключена SMTP-проверка адресов получателей сообщений**.

5. По ссылке **Перейти к настройке маршрутизации электронной почты** перейдите к выполнению шагов мастера.

В этом разделе

Шаг 1. Настройка маршрутизации электронной почты (transport_map)

На этом шаге настройте маршрутизацию электронной почты.

Kaspersky Secure Mail Gateway по умолчанию использует параметры вашего DNS-сервера для маршрутизации электронной почты. Вы можете настроить маршрутизацию электронной почты вручную. Для этого необходимо создать транспортную таблицу. В нее нужно ввести имена доменов, для которых предназначены сообщения электронной почты, а затем ввести

IP-адреса или FQDN-имена доменов, на которые Kaspersky Secure Mail Gateway будет перенаправлять сообщения, предназначенные для этих доменов.

Пример:

Если вы хотите, чтобы сообщения, предназначенные для домена example.com, перенаправлялись на адрес 1.1.1.0:25, вам нужно выполнить следующие действия:

1. Добавить домен example.com в транспортную таблицу.
2. Указать IP-адрес 1.1.1.0 и номер порта 25 для маршрутизации сообщений, предназначенных для домена example.com.

► *Чтобы настроить маршрутизацию электронной почты, выполните следующие действия:*

1. По ссылке **Добавить запись в транспортную таблицу** откройте окно **Маршрутизация электронной почты**.
2. В поле **Введите имя домена** введите имя домена, для которого предназначены сообщения электронной почты.

   Вводите имена доменов в формате FQDN.
3. В поле **Введите адрес назначения сообщений (IPv4, доменное имя или FQDN)** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.
4. В поле **Укажите номер порта соединения с адресом назначения** выберите номер порта.

   Значение по умолчанию: 25.
5. Выберите один из следующих вариантов:

   - **Не включать поиск MX-записей**.

- **Включить поиск MX-записей (для доменных имен или FQDN)**.

6. Нажмите на кнопку **ОК**.

   Окно **Маршрутизация электронной почты** закроется.

> Записи транспортной таблицы добавляются по одной. Повторите действия по добавлению записей в транспортную таблицу для всех добавляемых записей.

По ссылке **Сохранить и перейти к вводу адреса пограничного шлюза** перейдите к следующему шагу мастера.

Шаг 2. Ввод адреса пограничного шлюза (relayhost)

На этом шаге введите адрес вашего пограничного шлюза. Kaspersky Secure Mail Gateway будет перенаправлять все сообщения на этот адрес.

Например: 192.0.2.1 или domain.com.

Если вы настроили маршрутизацию электронной почты для отдельных доменов, Kaspersky Secure Mail Gateway будет перенаправлять сообщения электронной почты на адреса, указанные для каждого домена.

► *Чтобы ввести адрес пограничного шлюза, выполните следующие действия:*

1. В поле ввода укажите IP-адрес или доменное имя пограничного шлюза.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

2. Выберите один из следующих вариантов:

   - **Не включать поиск MX-записей**.
   - **Включить поиск MX-записей (для доменных имен или FQDN)**.

По ссылке **Сохранить и перейти к добавлению доверенных сетей и узлов сети** перейдите к следующему шагу мастера.

Шаг 3. Добавление доверенных сетей и узлов сети (mynetworks)

На этом шаге создайте список доверенных сетей и узлов сети, которым разрешено пересылать сообщения электронной почты через Kaspersky Secure Mail Gateway.

Как правило, это внутренние сети и узлы сети вашей организации.

Например, вы можете указать IP-адреса серверов Microsoft Exchange, используемых в вашей организации.

Если доверенные сети не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения с внутренних почтовых серверов и перенаправлять их за пределы сети вашей организации.

► *Чтобы добавить список доверенных сетей и узлов сети, выполните следующие действия:*

1. По ссылке **Добавить доверенную сеть или узел сети** откройте окно **Добавление доверенной сети**.
2. В поле **Добавьте адрес сети или узла сети** введите имя домена, для которого предназначены сообщения электронной почты.

   Вводите имена доменов в формате FQDN.
3. Нажмите на кнопку **ОК**.

   Окно **Добавление доверенной сети** закроется.

   Адреса добавляются по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов.

По ссылке **Сохранить и перейти к завершению интеграции** перейдите к следующему шагу мастера.

Шаг 4. Завершение интеграции через пограничный шлюз (SMTP-проверка отключена)

На этом шаге просмотрите введенные вами данные интеграции Kaspersky Secure Mail Gateway в почтовую инфраструктуру организации и подтвердите свой выбор.

По окончании интеграции в почтовую инфраструктуру организации автоматически настроены следующие параметры Kaspersky Secure Mail Gateway:

- Отключена SPF-проверка подлинности отправителей сообщений.

  Не включайте SPF-проверку подлинности отправителей сообщений, поскольку отправителем сообщений выступает пограничный шлюз, с которого Kaspersky Secure Mail Gateway принимает сообщения.

- Отключена DMARC-проверка подлинности доменов, с которых Kaspersky Secure Mail Gateway получает сообщения.

  Не включайте DMARC-проверку подлинности доменов, поскольку Kaspersky Secure Mail Gateway получает сообщения с промежуточного шлюза.

- Отключена SMTP-проверка адресов электронной почты получателей сообщений (на стр. 227).

  Не включайте SMTP-проверку адресов электронной почты получателей сообщений, поскольку SMTP-проверка адресов электронной почты получателей сообщений отключена на пограничном шлюзе.

После того, как вы пройдете все шаги мастера **Быстрая настройка MTA**, Kaspersky Secure Mail Gateway сбросит все значения параметров MTA и заменит их на значения, которые вы ввели в мастере быстрой настройки MTA.

Процедура приемки

После установки программы перед ее вводом в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности и приведение конфигурации программы в соответствие с сертифицированной конфигурацией.

Перед запуском программа проверяет контрольные суммы модулей программы. Если при установке какого-либо модуля программы произошла ошибка, программа отображает сообщение об ошибке. Вам необходимо переустановить программу.

В этом разделе

Безопасное состояние программы

Программа находится в безопасном состоянии, если она работает в *сертифицированном режиме.* В сертифицированном режиме Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации. Параметры программы находятся в рамках допустимых значений, приведенных в приложении к данному документу.

Вы можете выбрать сертифицированный режим работы Kaspersky Secure Mail Gateway при развертывании образа виртуальной машины Kaspersky Secure Mail Gateway.

В сертифицированном режиме параметры компонентов программы, которые требуют доступ в интернет, по умолчанию принимают следующие значения:

- Использование KSN отключено.

- SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений отключены, соединение с DNS-серверами запрещено.
- Параметр Enforced Anti-Spam Updates отключен в параметрах модуля Анти-Спам.
- В качестве источника обновлений баз программы используется Kaspersky Security Center или локальный источник обновлений баз Kaspersky Secure Mail Gateway.

Проверка работоспособности. Eicar

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе.
- Программа находится в безопасном состоянии.

Проверка работы программы с использованием тестового файла EICAR

Вы можете проверить, как работает защита интернет-трафика, антивирусная защита файлов и проверка на вирусы с помощью тестового файла EICAR.

Не забудьте возобновить антивирусную защиту интернет-трафика и антивирусную защиту файлов после завершения работы с тестовым файлом EICAR.

► *Чтобы проверить защиту интернет-трафика с использованием тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
2. Сохраните тестовый файл EICAR.

   Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы по запрашиваемому веб-адресу и заблокирует сохранение объекта.
3. Если требуется, используйте виды тестового файла EICAR.

► *Чтобы проверить антивирусную защиту файлов с использованием тестового файла EICAR или его вида, выполните следующие действия:*

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

   Когда защита приостановлена, не рекомендуется подключать устройство к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб этому устройству.

2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

3. Сохраните тестовый файл EICAR.

4. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.

5. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.

6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

7. Запустите сохраненный файл.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.

► *Чтобы проверить, как работает поиск вирусов с использованием тестового файла EICAR или его вида, выполните следующие действия*:

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

   Когда защита приостановлена, не рекомендуется подключать устройство к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб этому устройству.

2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

3. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.

4. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.

5. Запустите проверку сохраненного файла.

   Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.

6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

Проверка антивирусной защиты сообщений с использованием тестового файла EICAR

Вы можете проверить работу антивирусной защиты сообщений с помощью тестового файла EICAR или одного из видов тестового файла EICAR.

► *Чтобы проверить антивирусную защиту сообщений с использованием тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

2. Сохраните тестовый файл EICAR.

3. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Secure Mail Gateway.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

► *Чтобы проверить антивирусную защиту сообщений с использованием одного из видов тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

2. Сохраните тестовый файл EICAR.
3. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.
4. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.
5. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Secure Mail Gateway.

   Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.
6. Запустите сохраненный файл.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.

Проверка работоспособности модуля Анти-Спам

Вы можете проверить работоспособность модуля Анти-Спам с помощью образца спама.

В качестве образца спама используется строка GTUBE (Generic Test for Unsolicited Bulk Email): XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X.

Чтобы проверить работоспособность модуля Анти-Спам, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. Включите переключатель рядом с названием блока параметров **Анти-Спам**, если он выключен.
3. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

4. В списке правил по ссылке с названием правила откройте правило, которое вы хотите использовать для проверки работоспособности модуля Анти-Спам.

5. Включите переключатель рядом с названием блока параметров **Анти-Спам**, если он выключен.

6. Установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**, если он снят.

7. Запустите утилиту SwithMail.

8. Укажите адрес отправителя, назначения, а также адрес программы.

9. Откройте закладку Email Content.

10. В поле Email Subject введите gtube.

11. В поле Email Body введите строку GTUBE.

12. Нажмите на кнопку Test Settings.

    Тестовое спам-сообщение будет отправлено.

13. Перейдите в почтовый ящик пользователя, адрес электронной почты которого вы указали в качестве адреса назначения.

14. Убедитесь, что отправленное вами письмо было доставлено с меткой [Spam].

15. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.

16. Убедитесь, что в списке копий сообщений хранилища появилась запись об отправленном тестовом спам-сообщении.

    Если запись не появилась, проверьте, правильно ли вы настроили фильтрацию сообщений в хранилище.

17. В списке копий сообщений хранилища в нижней части рабочей области в строке с информацией о сообщении, которое вы хотите просмотреть, установите флажок и нажмите на кнопку **Просмотреть**.

Откроется копия сообщения.

18. Убедитесь, что в открывшейся копии сообщения рядом с параметром **Причина помещения в хранилище** появилась запись Anti-Spam.

Мониторинг Kaspersky Secure Mail Gateway

Этот раздел содержит информацию о мониторинге почтового трафика, последних обнаруженных угроз и ресурсов системы.

В этом разделе

Мониторинг почтового трафика

Чтобы оценить состояние почтового трафика Kaspersky Secure Mail Gateway, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Мониторинг**.
2. В рабочей области выберите закладку **Почтовый трафик**.
3. Выберите один из периодов отображения информации о почтовом трафике.

   Вы можете просмотреть информацию о почтовом трафике за следующие периоды: **час**, **день**, **неделя** или **30 дней**.
4. Выберите способ отображения информации на диаграммах.

Вы можете просмотреть диаграммы обнаруженных сообщений **по количеству** или **по размеру**.

5. Отметьте статусы сообщений (например, **Чистых**, **Зараженных**, **Со спамом** или все сообщения), информацию о которых вы хотите просмотреть.

В рабочей области отобразятся диаграммы почтового трафика за выбранный период.

Мониторинг последних обнаруженных угроз

Чтобы просмотреть список последних обнаруженных угроз, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Мониторинг**.

2. В рабочей области выберите закладку **Последние обнаруженные угрозы**.

Отобразится список **Последние обнаруженные зараженные объекты** – 5 последних обнаруженных объектов.

Мониторинг использования ресурсов системы

► *Чтобы оценить состояние использования ресурсов системы, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Мониторинг**.

2. В рабочей области выберите закладку **Ресурсы системы**.

3. Установите флажки рядом с типами данных, которые вы хотите отобразить на диаграмме загрузки системы (например, вы можете выбрать **Процессор**, **ОЗУ**, **Файл подкачки** или все).

4. Установите флажки рядом с типами данных, которые вы хотите отобразить на диаграмме загрузки сетевых интерфейсов (например, вы можете выбрать **Передача**, **Прием** или все).

В рабочей области отобразятся диаграммы **Система** и **Сетевые интерфейсы** с выбранными вами данными.

Мониторинг состояния служб и работы почтового агента MTA

В разделе **Мониторинг** главного окна веб-интерфейса Kaspersky Secure Mail Gateway в правой части рабочей области отображается следующая информация:

- состояние работы модуля Анти-Спам, актуальность баз модуля Анти-Спам, количество сообщений в Анти-Спам карантине;
- состояние работы модуля Антивирус, актуальность баз модуля Антивирус;
- состояние соединения с сервером KATA, количество сообщений в KATA-карантине (если вы используете программу Kaspersky Anti Targeted Attack Platform);
- состояние работы модуля Анти-Фишинг, актуальность баз модуля Анти-Фишинг;
- состояние подключения к Kaspersky Security Network или Kaspersky Private Security Network (если вы используете решение Kaspersky Private Security Network);
- информация о последнем обновлении баз программы;
- состояние подключения к LDAP-серверам;
- срок действия лицензии и предупреждение о скором истечении срока действия лицензии, если он скоро истечет;
- информация о состоянии отправки и приема сообщений почтовым агентом MTA.

По умолчанию модули Анти-Спам, Антивирус и Анти-Фишинг включены, контентная фильтрация, проверка подлинности отправителей сообщений и защита KATA отключены.

См. также

Работа с правилами обработки сообщений

Правило обработки сообщений (далее также "правило") – заданное множество пар адресов отправителей и получателей, сообщения электронной почты которых Kaspersky Secure Mail Gateway обрабатывает в соответствии с одними и теми же значениями параметров. Принадлежность сообщения электронной почты к правилу определяется наличием в этом правиле как адреса отправителя, так и адреса получателя.

По умолчанию в программе предусмотрены следующие предустановленные правила обработки сообщений:

- **WhiteList** – обработка сообщений из глобального белого списка адресов.
- **BlackList** – обработка сообщений из глобального черного списка адресов.
- **Default** – обработка сообщений по предустановленным "Лабораторией Касперского" параметрам.

Обрабатывая сообщение электронной почты, Kaspersky Secure Mail Gateway просматривает комбинацию адресов *отправитель-получатель* каждого правила, начиная с правила с наивысшим приоритетом (1). Если совпадение не найдено, Kaspersky Secure Mail Gateway проверяет комбинацию адресов правила со следующим приоритетом (2). Как только комбинация адресов отправитель-получатель найдена в каком-либо правиле, к сообщению применяются параметры обработки, заданные в этом правиле.

Если ни одно правило не содержит комбинацию адресов отправитель-получатель, сообщение обрабатывается в соответствии с параметрами, заданными для предустановленного правила **Default**.

Для каждого правила вы можете задать собственные параметры обработки сообщений электронной почты.

В этом разделе

Создание правила обработки сообщений

► *Чтобы создать правило обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В верхней части рабочей области нажмите на кнопку **Создать**.

   Откроется новое правило обработки сообщений.
3. Выберите блок **Общие параметры правила**.
4. В поле **Название правила (обязательно)** введите название нового правила.

   Название правила должно быть уникальным в списке правил Kaspersky Secure Mail Gateway.
5. В поле **Описание правила** введите описание правила.
6. В блоке параметров **Режим работы правила** выберите один из следующих вариантов обработки сообщений:

   - **Использовать параметры модулей проверки**, если вы хотите, чтобы при обработке сообщений в соответствии с этим правилом программа использовала

параметры модулей Антивирус, Анти-Спам, Анти-Фишинг и параметры контентной фильтрации, заданные для этого правила.

В нижней части рабочей области отобразятся (если они были скрыты) следующие блоки параметров, в которых вы можете настроить параметры Kaspersky Secure Mail Gateway для правила:

- **Анти-Спам** (см. раздел "**Включение и отключение проверки сообщений на спам для правила**" на стр. 260).
- **Антивирус** (см. раздел "**Включение и отключение антивирусной проверки для правила**" на стр. 246).
- **Защита KATA** (см. раздел "**Включение и отключение защиты KATA для правила**" на стр. 287).
- **Анти-Фишинг**.
- **Контентная фильтрация**.
- **Уведомления**.
- **Примечание к сообщению**.
- **Предупреждение о небезопасном сообщении**.
- **Проверка подлинности отправителей сообщений**.

- **Отклонять без проверки**, если вы хотите, чтобы при обработке сообщений в соответствии с этим правилом программа отклоняла сообщения, не проверяя их.

- **Удалять без уведомления отправителя**, если вы хотите, чтобы при обработке сообщений в соответствии с этим правилом программа удаляла сообщения без уведомления отправителя.

- **Пропускать без проверки**, если вы хотите, чтобы при обработке сообщений в соответствии с этим правилом программа доставляла сообщения получателям, не проверяя их.

  В нижней части рабочей области отобразится блок **Примечание к сообщению**, в котором вы можете настроить примечания к сообщениям, обрабатываемым в соответствии с этим правилом.

7. В нижней части рабочей области нажмите на кнопку **Создать**.

Правило будет создано и добавлено в список правил в разделе **Правила**.

Для того чтобы правило использовалось в работе Kaspersky Secure Mail Gateway, требуется настроить список отправителей сообщений (см. раздел "Добавление адресов электронной почты" на стр. 134) и список получателей сообщений для этого правила.

Вы также можете создать правило, скопировав существующее правило и изменив его параметры (см. раздел "Создание копии правила обработки сообщений" на стр. 132).

По умолчанию правилу присваивается наименьший приоритет из всех ранее созданных правил. Вы можете изменить приоритет правила.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146). По умолчанию новое правило отключено и не используется в работе программы.

Создание копии правила обработки сообщений

► *Чтобы создать копию правила обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. Установите флажок в строке с названием правила, которое вы хотите скопировать.

3. В верхней части рабочей области нажмите на кнопку **Копировать**.

4. В блоке **Общие параметры правила** в поле **Название правила (обязательно)** измените название правила.

   Название правила должно быть уникальным с списке правил Kaspersky Secure Mail Gateway.

5. В нижней части рабочей области нажмите на кнопку **Создать**.

Копия правила будет создана и добавлена в список правил в разделе **Правила**.

Вы можете изменить описание, параметры правила и параметры Kaspersky Secure Mail Gateway для этого правила (см. раздел "Создание правила обработки сообщений" на стр. 130).

По умолчанию правилу присваивается наименьший приоритет из всех ранее созданных правил. Вы можете изменить приоритет правила.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146). По умолчанию новое правило отключено и не используется в работе программы.

Настройка списков отправителей и получателей сообщений для правила

Для того чтобы правило использовалось в работе Kaspersky Secure Mail Gateway, вам необходимо настроить списки отправителей и получателей сообщений для этого правила.

Вы можете выполнять следующие действия по настройке списков отправителей и получателей сообщений:

- Создавать списки отправителей и получателей сообщений. Вы можете добавлять в списки IP-адреса отправителей сообщений, адреса электронной почты и учетные записи LDAP отправителей и получателей сообщений.
- Копировать адреса из списков отправителей и получателей сообщений в буфер обмена и вставлять адреса из буфера обмена в списки отправителей и получателей сообщений.
- Удалять адреса из списков отправителей и получателей сообщений. Вы можете удалять из списков отдельные адреса, очищать списки отправителей и получателей, а также удалять учетные записи LDAP (см. раздел "Добавление учетных записей LDAP в списки отправителей и получателей сообщений" на стр. 137) из списков **Список**

LDAP-записей отправителей и **Список LDAP-записей получателей** на промежуточном этапе настройки списков отправителей и получателей сообщений.

В этом разделе

Добавление адресов электронной почты

► *Чтобы добавить адреса электронной почты в списки отправителей и получателей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, в который вы хотите добавить адреса электронной почты:
   - **Отправители**, если вы хотите добавить адреса электронной почты в список отправителей сообщений.
   - **Получатели**, если вы хотите добавить адреса электронной почты в список получателей сообщений.

5. Под названием списка нажмите на кнопку со значком типа адреса отправителя или получателя и в контекстном меню кнопки выберите **Адреса электронной почты**.

6. В поле справа от значка **Адреса электронной почты** введите адрес электронной почты.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

   Регулярные выражения нечувствительны к регистру.

7. Нажмите на кнопку **Добавить** справа от поля ввода.

   Добавленный адрес электронной почты отобразится в выбранном вами списке со значком **Адреса электронной почты**.

8. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под выбранным вами списком.

9. После того, как вы добавили в список все адреса электронной почты, в нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Добавление IP-адресов

Вы можете добавить IP-адреса только в список отправителей сообщений. Добавление IP-адресов в список получателей сообщений не предусмотрено.

► *Чтобы добавить IP-адреса в список отправителей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.

3. Выберите блок **Общие параметры правила**.

4. В блоке **Отправители** нажмите на кнопку со значком типа адреса отправителя и в контекстном меню кнопки выберите **IP-адреса**.

5. В поле справа от значка **IP-адреса** введите IP-адрес отправителя сообщений.

   IP-адреса вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых IP-адресов.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1), IPv4-адрес подсети с маской (например, 192.0.0.0/16), IPv6-адрес (например, 2607:f0d0:1002:51::4) или IPv6-адрес подсети с маской (например, fc00::/7).

6. Нажмите на кнопку **Добавить** справа от поля ввода.

   Добавленный IP-адрес отобразится в списке отправителей сообщений со значком **IP-адреса**.

7. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком отправителей сообщений.

8. После того, как вы добавили в список все IP-адреса, в нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Добавление учетных записей LDAP в списки отправителей и получателей сообщений

► *Чтобы добавить учетные записи LDAP в списки отправителей и получателей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.

3. Выберите блок **Общие параметры правила**.

4. Выберите список, в который вы хотите добавить учетные записи LDAP:

   - **Отправители**, если вы хотите добавить учетные записи LDAP в список отправителей сообщений.

   - **Получатели**, если вы хотите добавить учетные записи LDAP в список получателей сообщений.

5. Под названием списка нажмите на кнопку со значком типа адреса отправителя или получателя и в контекстном меню кнопки выберите **LDAP-записи**.

6. Справа от поля ввода нажмите на кнопку **Найти**.

   Откроется окно в зависимости от списка, в который вы добавляете учетные записи LDAP:

   - **Настройка списка отправителей для правила**, если вы добавляете учетные записи LDAP в список отправителей сообщений.

   - **Настройка списка получателей для правила**, если вы добавляете учетные записи LDAP в список получателей сообщений.

7. В открывшемся окне в поле **LDAP-запись отправителя** или **LDAP-запись получателя** введите строку поиска учетных записей во внешней службе каталогов.

8. Нажмите на кнопку **Найти** справа от поля ввода.

   В поле под кнопкой **Найти** отобразится список найденных учетных записей.

9. Выберите учетные записи LDAP, которые вы хотите добавить в список отправителей или получателей сообщений.

   Вы можете выбрать несколько учетных записей LDAP.

10. Нажмите на кнопку **Добавить в список** под списком.

    Выбранные вами учетные записи отобразятся в списке:

    - **Список LDAP-записей отправителей**, если вы добавляете учетные записи LDAP в список отправителей сообщений.
    - **Список LDAP-записей получателей**, если вы добавляете учетные записи LDAP в список получателей сообщений.

11. Нажмите на кнопку **ОК** в нижней части окна:

    - **Настройка списка отправителей для правила**, если вы добавляете учетные записи LDAP в список отправителей сообщений.
    - **Настройка списка получателей для правила**, если вы добавляете учетные записи LDAP в список получателей сообщений.

    Окно, в котором вы добавляли учетные записи LDAP, закроется.

    Добавленные вами учетные записи LDAP отобразятся в списке адресов со значком **LDAP-записи**.

12. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком адресов.

13. В нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Удаление учетных записей LDAP из списков отправителей и получателей сообщений

Вы можете удалять учетные записи LDAP из списков отправителей и получателей сообщений (см. раздел "Удаление адресов" на стр. 143).

► *Чтобы удалить учетные записи LDAP из списков отправителей и получателей сообщений,выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, в котором вы хотите выполнить действия с учетными записями LDAP:
   - **Отправители**, если вы хотите выполнить действия с учетными записями LDAP отправителей сообщений.
   - **Получатели**, если вы хотите выполнить действия с учетными записями LDAP получателей сообщений.
5. Под названием списка нажмите на кнопку со значком типа адреса отправителя или получателя и в контекстном меню кнопки выберите **LDAP-записи**.
6. Справа от поля ввода нажмите на кнопку **Найти**.

Откроется окно в зависимости от списка, в котором вы выполняете действия с учетными записями LDAP:

- **Настройка списка отправителей для правила**, если вы выполняете действия с учетными записями LDAP в списке отправителей сообщений.
- **Настройка списка получателей для правила**, если вы выполняете действия с учетными записями LDAP в списке получателей сообщений.

7. В нижней части окна выберите учетные записи LDAP, которые вы хотите удалить из списка:

   - **Список LDAP-записей отправителей**, если вы удаляете учетные записи LDAP из списка отправителей сообщений.
   - **Список LDAP-записей получателей**, если вы удаляете учетные записи LDAP из списка получателей сообщений.

   Вы можете выбрать несколько учетных записей LDAP.

8. Нажмите на кнопку **Удалить из списка** под списком.

   Выбранные учетные записи будут удалены из выбранного вами списка.

9. Нажмите на кнопку **ОК** в нижней части окна:

   - **Настройка списка отправителей для правила**, если вы удаляете учетные записи LDAP из списка отправителей сообщений.
   - **Настройка списка получателей для правила**, если вы удаляете учетные записи LDAP из списка получателей сообщений.

   Окно, в котором вы удаляли учетные записи LDAP, закроется.

   Удаленные учетные записи LDAP будут также удалены из списка адресов отправителей или получателей сообщений выбранного вами правила.

10. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком адресов.

11. В нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списка отправителей или получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Копирование и вставка адресов

► *Чтобы скопировать адреса из списка отправителей или получателей сообщений в правиле обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей или получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, из которого вы хотите скопировать адреса в буфер обмена:
   - **Отправители**, если вы хотите скопировать адреса из списка отправителей сообщений.
   - **Получатели**, если вы хотите скопировать адреса из списка получателей сообщений.
5. По ссылке **Копировать** под выбранным списком откройте окно **Экспорт записей в буфер обмена**.
6. В списке **Выберите тип** выберите тип адресов, которые вы хотите скопировать:
   - **Адреса электронной почты**, если вы хотите скопировать адреса электронной почты.
   - **IP-адреса**, если вы хотите скопировать IP-адреса (только из списка отправителей сообщений).

- **LDAP-записи**, если вы хотите скопировать учетные записи LDAP.

В поле под списком типов адресов отобразится список адресов выбранного вами типа.

7. Выделите адреса, которые вы хотите скопировать.
8. Скопируйте адреса в буфер обмена.
9. В нижней части окна **Экспорт записей в буфер обмена** нажмите на кнопку **Отмена**.

   Окно **Экспорт записей в буфер обмена** закроется.

► *Чтобы вставить адреса из буфера обмена в списки отправителей или получателей сообщений в правиле обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, в который вы хотите вставить адреса из буфера обмена:
   - **Отправители**, если вы хотите вставить адреса из буфера обмена в список отправителей сообщений.
   - **Получатели**, если вы хотите вставить адреса из буфера обмена в список получателей сообщений.
5. По ссылке **Вставить** под выбранным списком откройте окно **Импорт записей из буфера обмена**.
6. В списке **Выберите тип** выберите тип адресов, которые вы хотите вставить из буфера обмена:
   - **Адреса электронной почты**, если вы хотите вставить адреса электронной почты.
   - **IP-адреса**, если вы хотите вставить IP-адреса (только в список отправителей сообщений).

- **LDAP-записи**, если вы хотите вставить учетные записи LDAP.

7. В поле под списком типов адресов вставьте адреса из буфера обмена.
8. В нижней части окна **Экспорт записей в буфер обмена** нажмите на кнопку **Вставить**.

   Окно **Импорт записей из буфера обмена** закроется.

   Добавленные вами адреса отобразятся в списке отправителей или получателей сообщений со значками, соответствующими типам адресов.
9. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком отправителей или получателей сообщений.
10. В нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Удаление адресов

Вы можете удалять отдельные адреса из списков отправителей и получателей, а также очищать списки отправителей и получателей в правиле обработки сообщений.

► *Чтобы удалить адреса из списка отправителей или получателей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, из которого вы хотите удалить адреса:

- **Отправители**, если вы хотите удалить адреса из списка отправителей сообщений.
- **Получатели**, если вы хотите удалить адреса из списка получателей сообщений.

5. В списке выберите адрес, который вы хотите удалить.
6. Нажмите на значок удаления справа от адреса, который вы хотите удалить.

   Адрес будет удален из списка отправителей или получателей сообщений.
7. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком отправителей или получателей сообщений.
8. В нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

► *Чтобы очистить список отправителей или получателей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, в котором вы хотите выполнить действия со списками отправителей и получателей сообщений.
3. Выберите блок **Общие параметры правила**.
4. Выберите список, из которого вы хотите удалить все адреса:
   - **Отправители**, если вы хотите очистить список отправителей сообщений.
   - **Получатели**, если вы хотите очистить список получателей сообщений.
5. По ссылке под выбранным списком откройте окно подтверждения действия:
   - **Очистить список отправителей**, если вы хотите очистить список отправителей сообщений.
   - **Очистить список получателей**, если вы хотите очистить список получателей сообщений.

6. Нажмите на кнопку **Да**.

   Окно подтверждения действия закроется.

   Все адреса будут удалены из списка отправителей или получателей сообщений.

7. Если вы хотите отменить последнее действие, перейдите по ссылке **Отменить последнее действие** под списком отправителей или получателей сообщений.

8. В нижней части рабочей области нажмите на кнопку **Применить**.

Изменения списков отправителей и получателей сообщений сохранятся в правиле обработки сообщений, которое вы настраиваете.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Удаление правил обработки сообщений

► *Чтобы удалить правила обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. Установите флажок в строках с названиями одного или нескольких правил, которые вы хотите удалить.

3. В верхней части рабочей области нажмите на кнопку **Удалить**.

Выбранные вами правила обработки сообщений будут удалены.

Включение и отключение правила обработки сообщений

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. Выполните одно из следующих действий:

   - Включите переключатель в строке с названием того правила, которое вы хотите включить.

   - Выключите переключатель в строке с названием того правила, которое вы хотите отключить.

Домены и настройка маршрутизации электронной почты

Этот раздел содержит информацию о том, как добавлять домены и адреса электронной почты в транспортную таблицу, настраивать маршрутизацию электронной почты для этих доменов, удалять домены из списка, настраивать режимы TLS-безопасности для входящих и исходящих сообщений электронной почты и добавлять DKIM-подпись к сообщениям.

Kaspersky Secure Mail Gateway по умолчанию использует параметры вашего DNS-сервера для маршрутизации электронной почты. Вы можете настроить маршрутизацию электронной почты вручную. Для этого необходимо создать транспортную таблицу. В нее нужно ввести имена доменов, для которых предназначены сообщения электронной почты, а затем ввести IP-адреса или FQDN-имена доменов, на которые Kaspersky Secure Mail Gateway будет перенаправлять сообщения, предназначенные для этих доменов.

Пример:

Если вы хотите, чтобы сообщения, предназначенные для домена example.com, перенаправлялись на адрес 1.1.1.0:25, вам нужно выполнить следующие действия:

1. Добавить домен example.com в транспортную таблицу.
2. Указать IP-адрес 1.1.1.0 и номер порта 25 для маршрутизации сообщений, предназначенных для домена example.com.

В этом разделе также описана настройка маршрутизации электронной почты для локальных доменов (relay_domains).

Локальные домены (relay_domains) – домены вашей организации, для которых Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты извне. Kaspersky Secure Mail Gateway будет принимать сообщения только для указанных вами доменов. Сообщения, предназначенные для получения другими доменами, будут отклонены.

Если локальные домены не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения для ваших внутренних почтовых серверов.

В этом разделе

Добавление записи в транспортную таблицу и настройка маршрутизации электронной почты (transport_map)

► *Чтобы добавить запись в транспортную таблицу и настроить маршрутизацию электронной почты, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания записи.

3. В блоке параметров **Тип записи** выберите один из следующих типов записи:

   - **Домен**, если вы хотите добавить домен в транспортную таблицу.

   - **Поддомены домена**, если вы хотите добавить поддомены домена в транспортную таблицу.

   - **Адрес эл. почты**, если вы хотите добавить адрес электронной почты в транспортную таблицу.

4. В поле **Домен / Адрес эл. почты** введите имя домена, имена поддоменов в формате FQDN или адрес электронной почты.

5. Установите флажок рядом с названием параметра **Локальный домен**, если вы хотите добавить локальный домен (см. раздел "Добавление локального домена (relay_domain)" на стр. 151).

6. В блоке параметров **Маршрутизация электронной почты** включите переключатель рядом с названием параметра **Настроить маршрутизацию электронной почты**.

7. В блоке параметров **Протокол** выберите один из протоколов передачи электронной почты:

   - **SMTP**, если вы хотите настроить передачу электронной почты по протоколу SMTP.

- **LMTP**, если вы хотите настроить передачу электронной почты по протоколу LMTP.

8. В поле **Адрес назначения и номер порта** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), маску подсети в нотации CIDR (например, fc00::/7), доменное имя или FQDN.

9. В блоке **Поиск MX-записей** включите или отключите поиск MX-записей. Выберите один из следующих вариантов:

   - **Выкл**, если вы хотите отключить поиск MX-записей.
   - **Вкл**, если вы хотите включить поиск MX-записей.

10. Если вы добавляете домен или поддомены домена, в блоке параметров **Режим TLS-шифрования для всех исходящих сообщений почтового сервера** выберите один из следующих вариантов:

    - **Использовать режим TLS-шифрования, установленный для всех исходящих сообщений почтового сервера**, если для этого домена вы хотите использовать режим TLS-шифрования соединения, установленный для всех исходящих сообщений почтового сервера.
    - **Изменить режим TLS-шифрования сообщений для этого домена**, если вы хотите настроить другой режим TLS-шифрования соединения для этого домена.

11. Если вы выбрали изменение режима TLS-шифрования для этого домена, в списке **Изменить режим TLS-шифрования сообщений для этого домена** выберите тот режим TLS-шифрования соединения, который вы хотите установить.

12. Если вы хотите настроить добавление DKIM-подписи к сообщениям с адресов этого домена, в блоке параметров **DKIM-подпись к сообщениям с адресов домена** выполните следующие действия:

    a. Нажмите на кнопку **Добавить**.

    Откроется окно **Создание DKIM-подписи для домена**.

    b. В поле **Селектор** введите имя, по которому вы сможете найти DKIM-подпись.

c. В списке **Имя ключа** выберите DKIM-ключ, на основе которого будет добавлена DKIM-подпись к сообщениям.

d. Нажмите на кнопку **ОК**.

Окно **Создание DKIM-подписи для домена** закроется.

13. Нажмите на кнопку **Добавить** в нижней части окна.

Добавленная запись отобразится в транспортной таблице.

Добавление локального домена (relay_domain)

► *Чтобы добавить локальный домен вашей организации, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания записи.

3. В блоке параметров **Тип записи** выберите тип записи **Домен**.

4. В поле **Домен / Адрес эл. почты** введите имя домена, для которого Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты извне.

   Вводите имя домена в формате FQDN.

5. Установите флажок рядом с названием параметра **Локальный домен**.

   Kaspersky Secure Mail Gateway будет принимать сообщения только для указанных вами доменов. Сообщения, предназначенные для получения другими доменами, будут отклонены.

6. В блоке параметров **Маршрутизация электронной почты** включите переключатель рядом с названием параметра **Настроить маршрутизацию электронной почты**.

7. В блоке параметров **Протокол** выберите один из протоколов передачи электронной почты:

   - **SMTP**, если вы хотите настроить передачу электронной почты по протоколу SMTP.

   - **LMTP**, если вы хотите настроить передачу электронной почты по протоколу LMTP.

8. В поле **Адрес назначения и номер порта** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), маску подсети в нотации CIDR (например, fc00::/7), доменное имя или FQDN.

9. В блоке **Поиск MX-записей** включите или отключите поиск MX-записей. Выберите один из следующих вариантов:

   - **Выкл**, если вы хотите отключить поиск MX-записей.

   - **Вкл**, если вы хотите включить поиск MX-записей.

10. В блоке параметров **Режим TLS-шифрования для всех исходящих сообщений почтового сервера** выберите один из следующих вариантов:

    - **Использовать режим TLS-шифрования, установленный для всех исходящих сообщений почтового сервера**, если для этого домена вы хотите использовать режим TLS-шифрования соединения, установленный для всех исходящих сообщений почтового сервера.

    - **Изменить режим TLS-шифрования сообщений для этого домена**, если вы хотите настроить другой режим TLS-шифрования соединения для этого домена.

11. Если вы выбрали настройку другого режима TLS-шифрования соединения для этого домена, в списке **Изменить режим TLS-шифрования сообщений для этого домена** выберите режим TLS-шифрования соединения, который вы хотите установить.

12. Если вы хотите настроить добавление DKIM-подписи к сообщениям с адресов этого домена, в блоке параметров **DKIM-подпись к сообщениям с адресов домена** выполните следующие действия:

    a. Нажмите на кнопку **Добавить**.

    Откроется окно **Создание DKIM-подписи для домена**.

    b. В поле **Селектор** введите имя, по которому вы сможете найти DKIM-подпись.

    c. В списке **Имя ключа** выберите DKIM-ключ, на основе которого будет добавлена DKIM-подпись к сообщениям.

    d. Нажмите на кнопку **ОК**.

    Окно **Создание DKIM-подписи для домена** закроется.

13. Нажмите на кнопку **Добавить** в нижней части окна.

Домен, для которого Kaspersky Secure Mail Gateway будет принимать сообщения, отобразится в списке доменов.

Удаление записи из транспортной таблицы

► *Чтобы удалить запись из транспортной таблицы, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. В списке доменов установите флажок рядом с каждой записью, которую вы хотите удалить из транспортной таблицы.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия **Удаление**.

4. Нажмите на кнопку **Да**.

Запись будет удалена из транспортной таблицы.

Изменение маршрутизации электронной почты для домена (transport_map)

► *Чтобы изменить маршрутизацию электронной почты для домена, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. В транспортной таблице по ссылке с именем домена раскройте параметры маршрутизации электронной почты для этого домена.

3. В блоке параметров **Протокол** выберите один из протоколов передачи электронной почты:

   - **SMTP**, если вы хотите настроить передачу электронной почты по протоколу SMTP.

   - **LMTP**, если вы хотите настроить передачу электронной почты по протоколу LMTP.

4. В поле **Адрес назначения и номер порта** введите IP-адрес или доменное имя сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), маску подсети в нотации CIDR (например, fc00::/7), доменное имя или FQDN.

5. В блоке **Поиск MX-записей** включите или отключите поиск MX-записей. Выберите один из следующих вариантов:

   - **Выкл**, если вы хотите отключить поиск MX-записей.

   - **Вкл**, если вы хотите включить поиск MX-записей.

6. В поле **Адрес назначения и номер порта** введите IP-адрес сервера, на который вы хотите настроить маршрутизацию электронной почты.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

7. Нажмите на кнопку **ОК** в нижней части окна.

Маршрутизация электронной почты будет изменена для домена.

Об использовании протокола TLS в работе Kaspersky Secure Mail Gateway

Протокол TLS (*Transport Layer Security* – безопасность транспортного уровня, далее также "TLS") – это протокол шифрования соединения между двумя серверами, обеспечивающий защищенную передачу данных между узлами сети Интернет.

Сеанс с использованием протокола TLS (далее также TLS-сеанс) – это последовательность следующих событий:

1. Сервер, с которого отправляются сообщения электронной почты (*Клиент*), устанавливает соединение с сервером, на который отправляются сообщения электронной почты (*Сервер*).
2. Серверы начинают взаимодействие по протоколу SMTP.
3. Клиент с помощью команды `STARTTLS` предлагает Серверу использовать TLS в рамках SMTP-взаимодействия.
4. Если Сервер может использовать TLS, он отвечает командой `Ready to start TLS` и отправляет Клиенту сертификат Сервера.
5. Клиент принимает сертификат и, если на нем настроены необходимые значения параметров, проверяет подлинность сертификата Сервера.
6. Клиент и Сервер включают режим шифрования данных.
7. Серверы выполняют обмен данными.
8. Сеанс заканчивается.

Вы можете настроить режим TLS-безопасности для ситуаций, когда Kaspersky Secure Mail Gateway принимает сообщения от другого сервера (действует как Сервер (см. раздел "Настройка TLS-безопасности для входящих сообщений электронной почты" на стр. 156)) или

пересылает сообщения на другой сервер (действует как Клиент (см. раздел "Настройка TLS-безопасности для исходящих сообщений электронной почты" на стр. 158)), а также настроить параметры TLS для отдельных доменов и групп доменов (см. раздел "Домены и настройка маршрутизации электронной почты" на стр. 147), использующих один и тот же IP-адрес.

Настройка TLS-безопасности для входящих сообщений электронной почты

► *Чтобы настроить режим TLS-безопасности для ситуации, когда Kaspersky Secure Mail Gateway принимает сообщения от другого сервера (выступает в роли Сервера), выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. По любой ссылке откройте окно **Параметры TLS**.

3. В блоке параметров **Режим TLS-безопасности сервера** выберите один из следующих режимов использования TLS-шифрования соединения между Kaspersky Secure Mail Gateway и сервером, отправляющим сообщения электронной почты:

   - **Не использовать TLS-шифрование**, если вы не хотите использовать TLS-шифрование соединения с сервером, отправляющим сообщения электронной почты.

     В этом случае Kaspersky Secure Mail Gateway принимает все сообщения в незашифрованном виде.

   - **Предлагать TLS-шифрование**, если вы хотите, чтобы Kaspersky Secure Mail Gateway предлагал серверу, отправляющему сообщения электронной почты, использовать TLS-шифрование соединения.

     В этом случае Kaspersky Secure Mail Gateway с помощью команды `STARTTLS` предлагает серверу, отправляющему сообщения электронной почты, использовать TLS-шифрование, но принимает сообщения независимо от ответа сервера.

- **Требовать TLS-шифрование**, если вы хотите, чтобы Kaspersky Secure Mail Gateway требовал от сервера, отправляющего сообщения электронной почты, использовать TLS-шифрование соединения.

  В этом случае сервер, отправляющий сообщения электронной почты (Клиент), с помощью команды `STARTTLS` предлагает Kaspersky Secure Mail Gateway использовать TLS-шифрование. Kaspersky Secure Mail Gateway отвечает командой `Ready to start TLS` и отправляет Клиенту сертификат Сервера, а также требует, чтобы Клиент проверял подлинность сертификата Сервера. После того, как Клиент проверил подлинность сертификата Сервера, устанавливается зашифрованное TLS-соединение.

4. В блоке параметров **Предоставление TLS-сертификата сервера** выберите TLS-сертификат сервера, который Kaspersky Secure Mail Gateway будет отправлять Клиенту на проверку подлинности в начале каждого TLS-сеанса.

   Вы можете создать или импортировать TLS-сертификат в разделе **Ключи шифрования**, подразделе **TLS** главного окна веб-интерфейса Kaspersky Secure Mail Gateway.

5. В блоке параметров **Запрос клиентского TLS-сертификата** выберите один из следующих вариантов:

   - **Не запрашивать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway не запрашивал TLS-сертификат клиента.

   - **Запрашивать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway запрашивал TLS-сертификат клиента, но мог пересылать сообщения независимо от результата проверки сертификата.

   - **Требовать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway требовал TLS-сертификат клиента и не пересылал сообщения, если обнаруживает неверное имя или недостоверность клиентского TLS-сертификата.

Устанавливайте режим **Запрашивать** или **Требовать** только если вы уверены, что клиенты, которых поддерживает ваш почтовый сервер, могут предоставить верифицируемый TLS-сертификат.

6. Нажмите на кнопку **ОК**.

Настройка TLS-безопасности для исходящих сообщений электронной почты

► *Чтобы настроить режим TLS-безопасности для ситуации, когда Kaspersky Secure Mail Gateway перенаправляет сообщения на другой сервер (выступает в роли Клиента), выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. По любой ссылке откройте окно **Параметры TLS**.

3. В блоке параметров **Режим TLS-безопасности клиента** выберите один из следующих режимов TLS-шифрования соединения между Kaspersky Secure Mail Gateway и сервером, принимающим сообщения электронной почты:

   - **Не использовать TLS-шифрование**, если вы не хотите использовать TLS-шифрование соединения с сервером, принимающим сообщения электронной почты.

     В этом случае Kaspersky Secure Mail Gateway перенаправляет все сообщения в незашифрованном виде.

   - **Проверять возможность TLS-шифрования**, если вы хотите, чтобы Kaspersky Secure Mail Gateway пытался установить TLS-сессию с принимающим почтовым сервером и, если принимающий сервер не поддерживает TLS, перенаправлял сообщения в незашифрованном виде.

- **Требовать TLS-шифрование и не проверять сертификат**, если вы хотите, чтобы Kaspersky Secure Mail Gateway перенаправлял сообщения только в случае, если принимающий почтовый сервер поддерживает TLS, но независимо от достоверности его TLS-сертификата.

- **Требовать TLS-шифрование и проверять сертификат**, если вы хотите, чтобы Kaspersky Secure Mail Gateway перенаправлял сообщения только в случае, если принимающий почтовый сервер поддерживает TLS, его TLS-сертификат достоверен и имя сертификата соответствует доменному имени сервера.

  Kaspersky Secure Mail Gateway не перенаправляет сообщения при нарушении этих условий.

4. Нажмите на кнопку **ОК**.

О DKIM-подписи к исходящим сообщениям

DKIM-подпись к исходящим сообщениям – это цифровая подпись, которая добавляется к сообщениям, отправляемым с адресов электронной почты определенного домена для идентификации пользователей по имени домена организации.

Технология DomainKeys Identified Mail (DKIM) объединяет несколько существующих методов антифишинга и антиспама с целью повышения качества классификации и идентификации легитимной электронной почты. Вместо традиционного IP-адреса для определения отправителя сообщения технология DKIM добавляет в него цифровую подпись, связанную с именем домена организации.

Включение и отключение добавления DKIM-подписи к исходящим сообщениям

► *Чтобы включить или отключить добавление DKIM-подписи к исходящим сообщениям, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. В верхней части рабочей области по ссылке **DKIM-подпись** откройте окно **Параметры DKIM**.

3. В раскрывающемся списке **DKIM-подпись** выберите один из следующих вариантов:

   - **Вкл**, если вы хотите включить добавление DKIM-подписи к исходящим сообщениям.

   - **Выкл**, если вы хотите отключить добавление DKIM-подписи к исходящим сообщениям.

4. Нажмите на кнопку **ОК**.

Окно **Параметры DKIM** закроется.

Подготовка к добавлению DKIM-подписи к исходящим сообщениям

Вы можете настроить добавление DKIM-подписи к сообщениям в веб-интерфейсе Kaspersky Secure Mail Gateway.

Настройка добавления DKIM-подписи к сообщениям состоит из следующих этапов:

1. Включение добавления DKIM-подписи к исходящим сообщениям.

2. Создание или импорт DKIM-ключа.

3. Добавление DKIM-подписи к сообщениям, отправляемым с адресов электронной почты определенного домена.

Для того чтобы удаленный почтовый сервер мог проверить DKIM-подпись, добавляемую к исходящим сообщениям, вам нужно получить DNS-запись открытого DKIM-ключа в веб-интерфейсе Kaspersky Secure Mail Gateway и добавить ее в параметры вашего DNS-сервера.

► *Чтобы получить DNS-запись открытого DKIM-ключа, выполните следующие действия в веб-интерфейсе Kaspersky Secure Mail Gateway:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.

2. Если в рабочей области отобразилось значение параметра **Выкл**, выполните следующие действия:

   a. По ссылке **DKIM-подпись** откройте окно **Параметры DKIM**.

   b. В раскрывающемся списке **DKIM-подпись** выберите **Вкл**.

   c. Нажмите на кнопку **ОК**.

   Окно **Параметры DKIM** закроется.

3. В списке доменов по ссылке с именем домена, для адресов которого вы хотите настроить добавление DKIM-подписи к исходящим сообщениям, откройте окно изменения записи.

4. В блоке параметров **DKIM-подпись к сообщениям с адресов домена** нажмите на кнопку **Добавить**.

   Откроется окно **Создание DKIM-подписи для домена**.

5. В поле **Селектор** введите имя, по которому вы сможете найти DKIM-подпись.

6. В списке **Имя ключа** выберите DKIM-ключ, на основе которого будет добавлена DKIM-подпись к сообщениям.

7. Нажмите на кнопку **ОК**.

   Окно **Создание DKIM-подписи для домена** закроется.

В блоке параметров **DKIM-подпись к сообщениям с адресов домена** в поле **DNS запись** отобразится DNS-запись открытого DKIM-ключа для определенного домена.

► *Чтобы добавить открытый DKIM-ключ в параметры вашего DNS-сервера, выполните следующие действия:*

1. Авторизуйтесь на вашем DNS-сервере под учетной записью администратора.

2. Найдите страницу, содержащую информацию об обновлении DNS-записей того домена, для адресов которого вы хотите настроить добавление DKIM-подписи к исходящим сообщениям.

   Например, страница может носить название "Управление DNS", "Управление сервером имен" или "Дополнительные настройки".

3. Найдите записи формата TXT того домена, для адресов которого вы хотите настроить добавление DKIM-подписи к исходящим сообщениям.

4. В списке записей формата TXT добавьте DNS-запись открытого DKIM-ключа для определенного домена следующего содержания:

   ```
   <селектор>._domainkey.<имя домена, для которого вы хотите добавить открытый DKIM-ключ>. IN TXT ( "v=<версия DKIM>; k=rsa; s=email" "p=<DNS-запись открытого DKIM-ключа>")
   ```

Пример DNS-записи открытого DKIM-ключа:

```
mail._domainkey.example.com IN TXT ( "v=DKIM1; k=rsa;
s=email" "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtyb09IeTJtIxTE
ohP/wa8eZOuiFJxL3pjk+1R81ajQyTb4J8Dj23RbjOKCZGFdyJfj7MUUL9MpvAo6OL9Krf
aF8ehR7MbHhaix1qPDfSP5a97vl9/6KR2TKJfi+0dQ/pMLJMbnXfdWeoDoDBUK0++B8HHC
nSpLTxsH/YDOtjKaHFxbU6DMEICTiVBWR+yeWopdWi9kPNT5SJ5H")
```

> Подробнее о назначении параметров DNS-записи открытого DKIM-ключа см. в документе RFC 5617.

5. Сохраните изменения.

> Синтаксис примера DNS-записи приведен для добавления в параметры DNS-сервера BIND. Синтаксис DNS-записи, добавляемой в параметры других DNS-серверов, может незначительно отличаться от приведенного примера.

Добавление DKIM-подписи к сообщениям с адресов определенного домена

Перед добавлением DKIM-подписи к сообщениям с адресов определенного домена необходимо создать или импортировать DKIM-ключ.

► *Чтобы добавить DKIM-подпись к сообщениям, отправляемым с адресов электронной почты определенного домена, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Домены**.
2. Если в рабочей области отобразилось значение параметра **Выкл**, выполните следующие действия:
   a. По ссылке **DKIM-подпись** откройте окно **Параметры DKIM**.
   b. В раскрывающемся списке **DKIM-подпись** выберите **Вкл**.
   c. Нажмите на кнопку **ОК**.

   Окно **Параметры DKIM** закроется.
3. В списке доменов выберите домен, для которого вы хотите добавить DKIM-подпись к исходящим сообщениям.
4. В блоке параметров **DKIM-подпись к сообщениям с адресов домена** нажмите на кнопку **Добавить**.
5. Откроется окно **Создание DKIM-подписи для домена**.
6. В поле **Селектор** введите имя, по которому вы сможете найти DKIM-подпись.
7. В списке **Имя ключа** выберите DKIM-ключ, на основе которого будет добавлена DKIM-подпись к сообщениям.

8. Нажмите на кнопку **ОК**.

Окно **Создание DKIM-подписи для домена** закроется.

После того как вы настроили добавление DKIM-подписи к сообщениям в веб-интерфейсе Kaspersky Secure Mail Gateway и для того, чтобы удаленный почтовый сервер мог проверить эту DKIM-подпись, вам нужно добавить открытый DKIM-ключ в параметры вашего DNS-сервера (см. раздел "Подготовка к добавлению DKIM-подписи к исходящим сообщениям" на стр. 160).

Использование протокола TLS в работе Kaspersky Secure Mail Gateway

Этот раздел содержит информацию об использовании протокола TLS в работе Kaspersky Secure Mail Gateway и о настройке параметров использования протокола.

В этом разделе

Создание TLS-сертификата

► *Чтобы создать TLS-сертификат, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Ключи шифрования**, подраздел **TLS**.

2. В верхней части рабочей области нажмите на кнопку **Создать**.

3. В поле **Имя TLS-сертификата** введите имя TLS-сертификата для отправки SMTP-клиенту на проверку подлинности в начале каждого TLS-сеанса.

   TLS-сертификат сервера предоставляется, если Kaspersky Secure Mail Gateway выполняет роль почтового сервера (принимает сообщения).

Имя TLS-сертификата не может быть пустым.

4. В поле **Штат (Область)** введите штат или область, в которой находится ваша организация.

5. В поле **Город** введите город, в котором находится ваша организация.

6. В поле **Код страны** введите двухбуквенный код страны, в которой находится ваша организация.

   Например, вы можете ввести RU для России или US для США.

7. В поле **Название организации** введите название вашей организации.

8. В поле **Название подразделения организации** введите название подразделения организации, для которого вы создаете TLS-сертификат.

9. В поле **Адрес электронной почты** введите адрес электронной почты администратора Kaspersky Secure Mail Gateway.

10. Нажмите на кнопку **ОК**.

Созданный вами TLS-сертификат отобразится в списке TLS-сертификатов в рабочей области главного окна веб-интерфейса программы.

Удаление TLS-сертификата

► *Чтобы удалить TLS-сертификат, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Ключи шифрования**, подраздел **TLS**.

2. В списке TLS-сертификатов установите флажок рядом с именем одного или нескольких сертификатов, которые вы хотите удалить.

3. В верхней части рабочей области нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия **Удаление выбранных элементов**.

4. Нажмите на кнопку **Да**.

Окно **Удаление выбранных элементов** закроется.

TLS-сертификат будет удален.

Подготовка самоподписанного TLS-сертификата к импорту

Самоподписанный TLS-сертификат, предназначенный для импорта в Kaspersky Secure Mail Gateway, должен удовлетворять следующим требованиям:

- Файл сертификата должен иметь уникальное имя в списке сертификатов, используемых в Kaspersky Secure Mail Gateway.
- Файл сертификата и файл закрытого ключа должны иметь формат PEM.
- Длина ключа должна быть 1024 бит или более.

В качестве примера приведена инструкция по подготовке к импорту самоподписанного TLS-сертификата сервера server_cert.pem, закрытый ключ которого находится в файле key.pem.

► *Чтобы подготовить самоподписанный TLS-сертификат к импорту в Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В файле закрытого ключа удалите пароль доступа к сертификату, если он использовался. Для этого выполните команду:

   ```
   # openssl rsa -in <имя файла закрытого ключа>.pem -out <имя файла закрытого ключа после удаления пароля>.pem
   ```

   Например, вы можете выполнить следующую команду:

   ```
   # openssl rsa -in key.pem -out key-nopass.pem
   ```

2. Объедините закрытый ключ и сертификат сервера в один файл. Для этого выполните команду:

```
% cat <имя файла закрытого ключа после удаления пароля>.pem <имя сертификата сервера>.pem <имя сертификата сервера после объединения файлов>.pem
```

Например, вы можете выполнить следующую команду:

```
% cat key-nopass.pem server_cert.pem > cert.pem
```

Самоподписанный TLS-сертификат (например, cert.pem) готов к импорту в Kaspersky Secure Mail Gateway.

Подготовка TLS-сертификата, подписанного центром сертификации, к импорту

TLS-сертификат, подписанный центром сертификации (сертификат CA), предназначенный для импорта в Kaspersky Secure Mail Gateway, должен удовлетворять следующим требованиям:

- Файл сертификата должен иметь уникальное имя в списке сертификатов, используемых в Kaspersky Secure Mail Gateway.
- Файлы сертификата сервера, промежуточного и корневого сертификатов CA и файл закрытого ключа должны иметь формат PEM.
- Длина ключа должна быть 1024 бит или более.
- Необходимо иметь полную *цепочку сертификатов* – путь от сертификата сервера к корневому сертификату CA.

  При получении сертификата CA может потребоваться использовать промежуточный сертификат в дополнение к сертификату сервера.
- Порядок указания сертификатов в цепочке сертификатов должен быть следующим: сначала сертификат самого сервера, затем промежуточные сертификаты CA.
- В цепочке сертификатов не должны быть пропущены промежуточные сертификаты.

- В цепочке сертификатов не должно быть сертификатов, не относящихся к текущей сертификации.

В качестве примера приведена инструкция по подготовке к импорту TLS-сертификата сервера, подписанного центром сертификации server_cert.pem, закрытый ключ которого находится в файле key.pem. Имя промежуточного сертификата сервера intermediate CA, имя корневого сертификата root CA.

► *Чтобы подготовить TLS-сертификат, подписанный центром сертификации, к импорту в Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В файле TLS-сертификата удалите пароль доступа к сертификату, если он использовался. Для этого выполните команду:

   ```
   # openssl rsa -in <имя файла закрытого ключа>.pem -out <имя файла закрытого ключа после удаления пароля>.pem
   ```

   Например, вы можете выполнить следующую команду:

   ```
   # openssl rsa -in key.pem -out key-nopass.pem
   ```

2. Выполните одно из следующих действий:

   - Если вы не уверены, что клиенты, которым сервер будет предоставлять этот сертификат, имеют собственные копии корневого и промежуточного сертификатов CA, объедините закрытый ключ, сертификат сервера, промежуточный сертификат и корневой сертификат CA в один файл. Для этого выполните команду:

     ```
     % cat <имя файла закрытого ключа после удаления пароля>.pem <имя сертификата сервера>.pem <имя промежуточного сертификата CA>.pem <имя корневого сертификата CA>.pem <имя TLS-сертификата после объединения файлов>.pem
     ```

     Например, вы можете выполнить следующую команду:

     ```
     % cat key-nopass.pem server_cert.pem intermediate_CA.pem root_CA.pem > cert.pem
     ```

   - Если вы уверены, что клиенты, которым сервер будет предоставлять этот сертификат, имеют собственные копии корневого и промежуточного сертификатов

CA, объедините закрытый ключ и сертификат сервера в один файл. Для этого выполните команду:

```
% cat <имя файла закрытого ключа после удаления пароля>.pem <имя сертификата сервера>.pem <имя сертификата сервера после объединения файлов>.pem
```

Например, вы можете выполнить следующую команду:

```
% cat key-nopass.pem server_cert.pem > cert.pem
```

TLS-сертификат, подписанный центром сертификации (например, cert.pem), готов к импорту в Kaspersky Secure Mail Gateway.

Импорт TLS-сертификата из файла

Перед тем как импортировать TLS-сертификаты в веб-интерфейсе Kaspersky Secure Mail Gateway, вам нужно подготовить их к импорту.

Вы можете подготовить к импорту сертификаты следующих типов:

- самоподписанный TLS-сертификат (см. раздел "Подготовка самоподписанного TLS-сертификата к импорту" на стр. 167);
- TLS-сертификат, подписанный центром сертификации (далее также сертификат CA) (см. раздел "Подготовка TLS-сертификата, подписанного центром сертификации, к импорту" на стр. 168).

Самоподписанные сертификаты обычно используются для тестирования и отладки SSL- и TLS-шифрования соединений. На публичных серверах рекомендуется использовать сертификаты, подписанные центрами сертификации (сертификаты CA).

► *Чтобы импортировать TLS-сертификат из файла, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Ключи шифрования**, подраздел **TLS**.
2. В верхней части рабочей области нажмите на кнопку **Импортировать**.

3. В поле **Имя TLS-сертификата** введите имя, которое вы хотите присвоить импортируемому TLS-сертификату.

4. Нажмите на кнопку **Просмотр** справа от поля **Выберите файл TLS-сертификата**.

   Откроется окно выбора файлов браузера, который вы используете.

5. Выберите файл TLS-сертификата, который вы хотите импортировать, и нажмите на кнопку **Открыть** вашего браузера.

   > Файл сертификата (см. раздел "Подготовка самоподписанного TLS-сертификата к импорту" на стр. 167, "Подготовка TLS-сертификата, подписанного центром сертификации, к импорту" на стр. 168) должен содержать TLS-сертификат и закрытый TLS-ключ с расширением pem. Закрытый ключ не должен быть зашифрован или защищен паролем.

   Окно выбора файлов закроется.

6. Нажмите на кнопку **ОК**.

TLS-сертификат отобразится в списке TLS-сертификатов в рабочей области главного окна веб-интерфейса программы.

Хранилище

Хранилище предназначено для копий сообщений, которые Kaspersky Secure Mail Gateway сохраняет во время обработки. Копии сообщений хранятся в хранилище в недоступном для чтения виде и поэтому не угрожают безопасности вашего компьютера.

Kaspersky Secure Mail Gateway помещает в хранилище копии сообщений:

- которым модуль Антивирус присвоил один из статусов проверки (см. раздел "О статусах антивирусной проверки сообщений" на стр. 245) и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями при антивирусной проверке" на стр. 249);
- которым модуль Анти-Спам присвоил один из статусов проверки (см. раздел "О статусах проверки сообщений на спам" на стр. 259) и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями при проверке на спам" на стр. 268);
- которым модуль Анти-Фишинг присвоил один из статусов проверки и перед выполнением над ними действий;
- которым по результатам контентной фильтрации присвоен один из статусов проверки и перед выполнением над ними действий;
- которым по результатам проверки в KATA присвоен один из статусов проверки и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями по результатам проверки KATA" на стр. 288);
- которым по результатам проверки подлинности отправителей сообщений присвоен один из статусов проверки и перед выполнением над ними действий;
- адреса отправителей которых обнаружены в персональном черном списке адресов (см. раздел "Настройка параметров персонального черного списка адресов" на стр. 293) и перед выполнением над ними действий.

Копии сообщений помещаются в хранилище вместе с вложениями.

По умолчанию максимальный объем хранилища составляет 7,32 ГБ. Как только объем хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из хранилища самые старые копии сообщений. Когда объем хранилища снова становится меньше порогового значения, программа прекращает удалять копии сообщений из хранилища.

В этом разделе

Настройка параметров хранилища

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.
2. По любой ссылке откройте окно **Параметры хранилища**.
3. В поле **Максимальный размер хранилища** укажите максимальный объем, который хранилище может занимать на жестком диске.

   Рекомендуется указать значение не менее 100 МБ.
4. В поле **Порог свободного места для отправки оповещения** укажите порог свободного места в хранилище, по достижении которого программа отправляет уведомление администратору Kaspersky Secure Mail Gateway.

5. В списке **Разрешить доставку зараженных сообщений** выберите один из следующих вариантов:

   - **Да**, если вы хотите разрешить доставку (см. раздел "Доставка сообщения из хранилища получателям" на стр. 178) зараженных сообщений из хранилища получателям.

   - **Нет**, если вы хотите запретить доставку (см. раздел "Доставка сообщения из хранилища получателям" на стр. 178) зараженных сообщений из хранилища получателям.

   > Этот параметр применяется для учетной записи HelpDesk (см. раздел "Настройка параметров учетной записи HelpDesk" на стр. 212). Пользователь под учетной записью Administrator может доставлять сообщения из хранилища (см. раздел "Доставка сообщения из хранилища получателям" на стр. 178) получателям независимо от значения параметра **Разрешить доставку зараженных сообщений**.

6. В списке **Действия над сообщениями, если хранилище недоступно** выберите один из следующих вариантов:

   - **Продолжать обработку**, если вы хотите, чтобы обработка сообщений продолжалась независимо от возможности доступа к хранилищу.

   - **Сообщать о временной ошибке сервера**, если вы хотите, чтобы отправлялось уведомление о том, что хранилище временно недоступно.

   - **Отклонять сообщения**, если вы хотите, чтобы сообщения отклонялись, когда хранилище недоступно.

7. В поле **Тема уведомления о доставке сообщения во вложении** введите тему уведомления. Например, Message delivery from Backup.

8. В поле **Тело уведомления о доставке сообщения во вложении** введите текст уведомления. Например, вы можете ввести предупреждение о том, что сообщение, доставленное из хранилища, может быть небезопасно и содержать вирусы.

9. Нажмите на кнопку **ОК**.

Окно **Параметры хранилища** закроется.

Поиск копий сообщений в хранилище

► *Чтобы найти копии сообщений в хранилище, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.
2. В рабочей области под кнопками **Доставить**, **Просмотреть**, **Удалить** и **Сохранить** по любой ссылке откройте окно **Поисковый фильтр**.
3. В поле **От кого** введите текст поиска адресов электронной почты отправителей сообщений.

   Вы можете ввести адрес электронной почты (например, example-email@example.com), имя домена (например, example.com) или несколько символов из адреса электронной почты (например, exa).

4. В поле **Кому** введите текст поиска адресов электронной почты получателей сообщений.
5. В поле **Тема** введите текст поиска заголовков сообщений.
6. В поле **ID сообщения** введите текст поиска идентификатора сообщения на почтовом сервере.
7. В списке **ID правила** выберите идентификатор правила, по которому обрабатывались сообщения.
8. В списке **ID** выберите идентификатор сообщения в хранилище.
9. В списке **Интервал** выберите интервал, прошедший с момента обработки сообщений и помещения их копий в хранилище.

   Вы можете выбрать один из следующих интервалов:

   - **Час**.

- **Сутки**.
- **Неделя**.
- **2 недели**.
- **Месяц**.
- **3 месяца**.
- **Год**.
- **Пользовательский**.

10. Если вы выбрали интервал **Пользовательский**, выполните следующие действия:

    a. В полях **начало** укажите дату и время начала интервала поиска.

    b. В полях **конец** укажите дату и время конца интервала поиска.

11. В блоке параметров **Тип проверки** установите флажки рядом с названиями модулей Kaspersky Secure Mail Gateway, по результатам проверки которыми сообщения были помещены в хранилище.

    Вы можете выбрать один или несколько модулей проверки:

    - **Анти-Спам**.
    - **Антивирус**.
    - **Контентная фильтрация**.
    - **Анти-Фишинг**.
    - **Персональный черный список адресов**.
    - **Проверка подлинности**.
    - **Защита KATA**.

12. В блоке параметров **Размер сообщения (КБ)** укажите ограничение поиска по размеру сообщений в килобайтах.

Вы можете установить одно из следующих ограничений:

- **Меньше или равно** определенного размера сообщения в килобайтах.
- **Больше или равно** определенного размера сообщения в килобайтах.

13. Нажмите на кнопку **ОК**.

Копии сообщений, удовлетворяющие параметрам поиска, отобразятся в списке копий сообщений в разделе **Хранилище**.

Просмотр информации о сообщении в хранилище

► *Чтобы просмотреть информацию о сообщении в хранилище, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.
2. В списке копий сообщений хранилища в нижней части рабочей области выполните одно из следующих действий:
   - В строке с информацией о сообщении, которое вы хотите просмотреть, перейдите по любой из ссылок **От кого**, **Кому** или **Тема**.
   - В строке с информацией о сообщении, которое вы хотите просмотреть, установите флажок и нажмите на кнопку **Просмотреть**.

   Откроется копия сообщения, содержащая следующую информацию о сообщении:
   - **ID**.
   - **Тема**.
   - **Сообщение обработано по правилу**.
   - **ID правила**.
   - **От кого**.

- **Кому**.
- **Копия**.
- **Скрытая копия**.
- **Результат проверки** с перечислением модулей проверки **Анти-Спам**, **Антивирус**, **Контентная фильтрация**, **Анти-Фишинг**, **Проверка подлинности** и **Защита KATA**.
- **Причина помещения в хранилище**.
- **Действие**.
- **Время помещения в хранилище**.
- **ID сообщения на почтовом сервере**.
- **Размер сообщения**.
- **Время отправления**.
- **Время получения**.
- **Вложения**.
- **Вирус**.
- **Дата выпуска антивирусных баз**.
- **Дата выпуска баз Анти-Спама**.

3. Если вы хотите вернуться к списку копий сообщений хранилища, нажмите на кнопку **К списку сообщений** в верхней части рабочей области.

Доставка сообщения из хранилища получателям

Если вы считаете сообщение в хранилище безопасным, вы можете доставить его из хранилища получателям.

Вы можете доставить сообщение из хранилища после предварительного просмотра (см. раздел "Просмотр информации о сообщении в хранилище" на стр. 177) или отметив сообщения, которые вы хотите доставить, в списке копий сообщений хранилища (одно или несколько сообщений).

Доставка зараженных сообщений может угрожать безопасности компьютеров получателей.

Перед тем как доставить зараженное сообщение получателю, убедитесь, что доставка зараженных сообщений разрешена в параметрах хранилища (см. раздел "Настройка параметров хранилища" на стр. 173) (для персональных учетных записей и учетной записи HelpDesk).

► *Чтобы доставить сообщение из хранилища получателям, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.

2. В списке копий сообщений хранилища в нижней части рабочей области установите флажки в строках с информацией о сообщениях, которые вы хотите доставить.

3. Нажмите на кнопку **Доставить** в верхней части рабочей области.

   Откроется окно **Доставить сообщение**.

4. Установите флажок рядом с названием параметра **Доставить сообщение в виде вложения**, если вы хотите доставить сообщение в виде вложения.

5. Установите флажок рядом с названием параметра **На адреса электронной почты получателей из заголовка сообщения**, если вы хотите доставить сообщение на адреса электронной почты получателей, которым это сообщение было отправлено.

6. Установите флажок рядом с названием параметра **На дополнительные адреса электронной почты**, если вы хотите доставить сообщение на дополнительные адреса электронной почты.

7. Если вы выбрали доставку сообщения на дополнительные адреса электронной почты, в поле под названием параметра **На дополнительные адреса электронной почты** введите адреса электронной почты, на которые вы хотите доставить сообщение.

8. Нажмите на кнопку **ОК**.

   Окно **Доставить сообщение** закроется.

   Сообщение будет помещено в очередь на доставку.

9. Если вы хотите вернуться к списку копий сообщений хранилища, нажмите на кнопку **К списку сообщений** в верхней части рабочей области.

   В списке копий сообщений хранилища отобразится надпись **Сообщение помещено в очередь на доставку**.

10. Если вы хотите скрыть надпись **Сообщение помещено в очередь на доставку**, перейдите по ссылке **Скрыть** в правой части строки с надписью.

Сохранение сообщения из хранилища в файле

Если вы считаете сообщение в хранилище безопасным, вы можете сохранить его в файле на жестком диске.

Вы можете сохранить сообщение из хранилища после предварительного просмотра (см. раздел "Просмотр информации о сообщении в хранилище" на стр. 177) или отметив сообщение, которое вы хотите сохранить, в списке копий сообщений хранилища.

Сохранение зараженных сообщений на жестком диске может угрожать безопасности вашего компьютера.

► *Чтобы сохранить сообщение из хранилища в файле, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.

2. В списке копий сообщений хранилища в нижней части рабочей области установите флажок в строке с информацией о сообщении, которое вы хотите сохранить.

3. Нажмите на кнопку **Сохранить** в верхней части рабочей области.

   Сообщение будет сохранено на жестком диске вашего компьютера в той директории, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с Kaspersky Secure Mail Gateway.

   Например, если вы используете операционную систему Microsoft Windows®, и в параметрах вашего браузера в качестве директории загрузки файлов из интернета указана папка Downloads, сообщение будет сохранено в папку Downloads на жестком диске вашего компьютера.

4. Если вы хотите вернуться к списку копий сообщений хранилища, нажмите на кнопку **К списку сообщений** в верхней части рабочей области.

Удаление копии сообщения из хранилища

Вы можете удалить копию сообщения из хранилища после предварительного просмотра (см. раздел "Просмотр информации о сообщении в хранилище" на стр. 177) или отмечая сообщения, которые вы хотите удалить, в списке копий сообщений хранилища (одно или несколько сообщений).

► *Чтобы удалить одно или несколько сообщений из хранилища, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Хранилище**.

2. В списке копий сообщений хранилища в нижней части рабочей области установите флажки в строках с информацией о сообщениях, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить** в верхней части рабочей области.

4. Откроется окно **Удаление сообщений**.

5. Нажмите на кнопку **Удалить** в окне **Удаление сообщений**.

   Копия сообщения будет удалена из хранилища.

6. Если вы хотите вернуться к списку копий сообщений хранилища, нажмите на кнопку **К списку сообщений** в верхней части рабочей области.

   В списке копий сообщений хранилища отобразится надпись **Отмеченное сообщение удалено**.

7. Если вы хотите скрыть надпись **Отмеченное сообщение удалено**, перейдите по ссылке **Скрыть** в правой части строки с надписью.

Очередь сообщений Kaspersky Secure Mail Gateway

Этот раздел содержит информацию о работе с очередями сообщений Kaspersky Secure Mail Gateway, а также о том, как отсортировать, отфильтровать, принудительно отправить сообщения из очереди сообщений, KATA-карантина и Анти-Спам карантина или выполнить поиск сообщений в очереди.

В этом разделе

Включение и отключение отправки и приема сообщений

► *Чтобы включить или отключить отправку или прием сообщений почтовым агентом Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.

2. В верхней части рабочей области выполните следующие действия:

   - Включите переключатель рядом с названием параметра **Отправка сообщений**, если вы хотите разрешить отправку сообщений почтовым агентом Kaspersky Secure Mail Gateway.

   - Выключите переключатель рядом с названием параметра **Отправка сообщений**, если вы хотите запретить отправку сообщений почтовым агентом Kaspersky Secure Mail Gateway.

     Если в расширенных параметрах MTA (см. раздел "Настройка расширенных параметров MTA" на стр. 223) установлен параметр `Отклонять сообщения на адреса, не прошедшие проверку (reject_unverified_recipient)`, прием сообщений также будет отключен.

   - Включите переключатель рядом с названием параметра **Прием сообщений**, если вы хотите разрешить прием сообщений почтовым агентом Kaspersky Secure Mail Gateway.

   - Выключите переключатель рядом с названием параметра **Прием сообщений**, если вы хотите запретить прием сообщений почтовым агентом Kaspersky Secure Mail Gateway.

Внимание! Эти параметры определяют отправку и прием сообщений почтовым агентом Kaspersky Secure Mail Gateway.

Просмотр информации об очереди сообщений, KATA-карантине и Анти-Спам карантине

► *Чтобы просмотреть информацию об очереди сообщений, KATA-карантине и Анти-Спам карантине,*

в главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.

Отобразится следующая информация:

- **KATA-карантин, размер**. Размер KATA-карантина и процент использования KATA-карантина по сравнению с максимальным размером, заданным в параметрах защиты KATA (см. раздел "Защита KATA и интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform" на стр. 277).
- **KATA-карантин, сообщений**. Количество сообщений в KATA-карантине в настоящий момент.
- **Проверено в KATA, сообщений**. Количество сообщений, проверенных в KATA за последний час.
- **Истекло время ожидания KATA, сообщений**. Количество сообщений, время ожидания проверки в KATA которых истекло за последний час. Максимальное время ожидания проверки в KATA устанавливается в параметрах защиты KATA (см. раздел "Защита KATA и интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform" на стр. 277).
- **Анти-Спам карантин, размер**. Размер Анти-Спам карантина и процент использования Анти-Спам карантина по сравнению с максимальным размером, заданным в параметрах Анти-Спам карантина (см. раздел "Анти-Спам карантин" на стр. 274).
- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине в настоящий момент.
- **Очередь MTA, сообщений**. Общее количество сообщений очереди в настоящий момент.

Сортировка сообщений в очереди

► Чтобы отсортировать *сообщения в очереди*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.

   Откроется таблица сообщений в очереди.

2. Нажмите на кнопку  слева от названия той графы таблицы, по которой вы хотите отсортировать сообщения. Вы можете отсортировать сообщения по одному из следующих показателей:

   - **ID сообщения в очереди** – ID сообщений в очереди.
   - **От** – адрес отправителя сообщений.
   - **Кому** – адрес получателя сообщений.
   - **Размер** – размер сообщений.
   - **Получено** – время поступления сообщений в очередь.
   - **Ошибка** – ошибка проверки сообщений.

► *Чтобы изменить порядок сортировки сообщений в очереди,*

нажмите на кнопку  или  слева от названия той графы таблицы, порядок сортировки сообщений которой вы хотите изменить.

Фильтрация и поиск сообщений по названию очереди

► Чтобы отфильтровать или найти сообщения по *названию очереди*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.

2. По ссылке **Очередь** раскройте список названий очередей.
3. Установите флажки рядом с названиями тех очередей, в которых вы хотите найти сообщения. Вы можете выбрать одну или несколько из следующих очередей:
   - **Deferred**.
   - **Active**.
   - **Inbound (Очереди Maildrop и Incoming)**.
   - **Hold**.
   - **Анти-Спам карантин**.
   - **KATA-карантин**.
4. Нажмите на кнопку **Применить**.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Secure Mail Gateway отобразится список сообщений очереди, сформированный по условиям фильтра.

Если фильтр поиска сообщений не задан, в списке содержатся все сообщения очереди.

Фильтрация и поиск сообщений по ID сообщения в очереди

► Чтобы отфильтровать или найти сообщения по *ID сообщения в очереди*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.
2. По ссылке **ID сообщения в очереди** откройте окно настройки фильтрации сообщений.
3. В поле **ID** введите несколько символов или все символы ID сообщения в очереди.
4. Нажмите на кнопку **Применить**.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Secure Mail Gateway отобразится список сообщений очереди, сформированный по условиям фильтра.

Если фильтр поиска сообщений не задан, в списке содержатся все сообщения очереди.

Фильтрация и поиск сообщений по адресу отправителя сообщений

► Чтобы отфильтровать или найти сообщения *по адресу отправителя сообщений*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.
2. По ссылке **От** откройте окно настройки фильтрации сообщений.
3. В поле **От** введите несколько символов или все символы адреса отправителя сообщений.
4. Нажмите на кнопку **Применить**.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Secure Mail Gateway отобразится список сообщений очереди, сформированный по условиям фильтра.

Если фильтр поиска сообщений не задан, в списке содержатся все сообщения очереди.

Фильтрация и поиск сообщений по адресу получателя сообщений

► Чтобы отфильтровать или найти сообщения *по адресу получателя сообщений*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.
2. По ссылке **Кому** откройте окно настройки фильтрации сообщений.
3. В поле **Кому** введите несколько символов или все символы адреса получателя сообщений.
4. Нажмите на кнопку **Применить**.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Secure Mail Gateway отобразится список сообщений очереди, сформированный по условиям фильтра.

Если фильтр поиска сообщений не задан, в списке содержатся все сообщения очереди.

Фильтрация и поиск сообщений по времени поступления сообщений в очередь

► Чтобы отфильтровать или найти сообщения *по времени поступления сообщений в очередь*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.
2. По ссылке **Получено** раскройте список интервалов для поиска сообщений.
3. Выберите один из следующих интервалов:

- **Прошедший час**.
- **Прошедший день**.
- **Прошедшая неделя**.
- **Пользовательский**.

4. Если вы выбрали пользовательский интервал для поиска сообщений, выполните следующие действия:

    a. В открывшемся календаре укажите даты начала и конца периода поступления сообщений в очередь.

    b. Нажмите на кнопку **Применить**.

    Календарь закроется.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Secure Mail Gateway отобразится список сообщений очереди, сформированный по условиям фильтра.

Если фильтр поиска сообщений не задан, в списке содержатся все сообщения очереди.

Принудительная отправка и удаление сообщений из очереди

Чтобы принудительно отправить или удалить сообщения из очереди, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Очередь сообщений**.
2. В рабочей области просмотрите список сообщений в очереди.
3. Слева от названия типа очереди установите флажки рядом с сообщениями, которые вы хотите обработать.

4. В панели инструментов в верхней части рабочей области нажмите на одну из следующих кнопок:

   - **Отправить**, если вы хотите принудительно отправить отмеченные сообщения.
   - **Отправить все**, если вы хотите принудительно отправить все сообщения.

Частые попытки вне очереди отправить недоставленные сообщения ухудшают скорость отправки остальных сообщений.

   - **Удалить**, если вы хотите удалить отмеченные сообщения.
   - **Удалить все**, если вы хотите удалить все сообщения.

Операция удаления всех сообщений из очереди необратимо удалит все данные из очереди, включая поступившие, но еще не обработанные.

При принудительной отправке сообщений из очереди **KATA-карантин** сообщения в любом случае будут проверены в Kaspersky Anti Targeted Attack Platform, но Kaspersky Secure Mail Gateway не будет ждать результата проверки этих сообщений. Эти сообщения не будут отображаться в очереди на проверку.

См. также

Отчеты о работе Kaspersky Secure Mail Gateway

Этот раздел содержит информацию об отчетах, о том, как создавать и просматривать отчеты о работе почтового сервера.

Вы можете настроить формирование следующих типов отчетов о работе почтового сервера:

- **Ежедневные**.
- **Еженедельные**.
- **Ежемесячные**.
- **Пользовательские**.

В этом разделе

Содержание отчетов о работе Kaspersky Secure Mail Gateway

Вы можете получить информацию о результатах работы Kaspersky Secure Mail Gateway за определенный период из отчетов о работе Kaspersky Secure Mail Gateway.

Отчеты содержат следующую информацию о работе Kaspersky Secure Mail Gateway:

1. Суммарный отчет по обнаружениям. Отчет о результатах работы модулей Kaspersky Secure Mail Gateway отображает количество и объем сообщений, подсчитанных по следующим показателям:
    - Обнаружено в KATA.
    - Обнаружено модулем Антивирус.
    - Обнаружено модулем Анти-Фишинг.
    - Обнаружено модулем Анти-Спам.
    - Нарушений подлинности отправителей.
    - Обработано модулем контентной фильтрации.
    - Чистых.
    - Непроверенных.
    - Всего сообщений.
2. Суммарный отчет по действиям Kaspersky Secure Mail Gateway над сообщениями. Отображает количество и объем сообщений, подсчитанных по следующим показателям:
    - Доставлено сообщений, в том числе:
        - Чистых.
        - Вылеченных.

- С удаленными вложениями.
- Пропущенных.
- Непроверенных.

- Не доставлено сообщений, в том числе:
  - Удаленных.
  - Отклоненных.
  - Отложенных.

- Всего сообщений.

3. Отчет по обнаружениям модуля Антивирус. Отображает количество сообщений, проверенных и не проверенных модулем Антивирус за определенный период и содержит статистику обнаружения сообщений следующих типов:

   - Чистые.
   - Зараженные.
   - Зашифрованные.
   - Ошибки проверки.
   - Непроверенные сообщения по одной или нескольким из следующих причин:
     - Исключены из проверки по правилам обработки глобального черного или белого списков.
     - Исключены из проверки по правилам обработки персональных черных или белых списков.
     - Отключена антивирусная проверка для всех сообщений.
     - Отключена антивирусная проверка для правила, по которому обрабатывалось сообщение.
     - Отсутствуют антивирусные базы.
     - Возникли проблемы с лицензией.

4. Отчет по обнаружениям модуля Анти-Спам. Отображает количество сообщений, проверенных и не проверенных модулем Анти-Спам за определенный период, и содержит статистику обнаружения сообщений следующих типов:

   - Не спам.
   - Спам.
   - Предполагаемый спам.
   - Сообщение от неблагонадежного отправителя.
   - Массовая рассылка.
   - Ошибки проверки.

   Кроме того, отображается количество сообщений в Анти-Спам карантине и количество непроверенных сообщений.

5. Отчет по обнаружениям модуля Анти-Фишинг. Отображает количество сообщений, проверенных и не проверенных модулем Анти-Фишинг за определенный период, и содержит статистику обнаружения сообщений следующих типов:

   - Не фишинг.
   - Фишинг.
   - Вредоносный URL.
   - Ошибки проверки.

   Кроме того, отображается количество непроверенных сообщений.

6. Отчет о результатах контентной фильтрации сообщений. Отображает количество сообщений, обработанных по правилам контентной фильтрации за определенный период, подсчитанных по следующим показателям:

   - Сообщения без нарушений.
   - Сообщения, превышающие допустимый размер.
   - Сообщения, содержащие запрещенное имя вложения.

- Сообщения, содержащие запрещенный тип вложения.

Кроме того, отображается количество непроверенных сообщений.

7. Отчет о примененных правилах обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 129).

8. Отчет о десяти основных источниках спама. Перечисляет адреса источников и количество срабатываний модуля Анти-Спам.

9. Отчет о десяти адресах электронной почты, на которые было отправлено наибольшее количество сообщений, содержащих спам. Перечисляет адреса электронной почты получателей сообщений и количество срабатываний модуля Анти-Спам.

10. Отчет о десяти основных источниках вредоносных объектов по заключению модуля Антивирус. Перечисляет адреса источников и количество срабатываний модуля Антивирус.

11. Отчет о десяти адресах электронной почты, на которые было отправлено наибольшее количество вредоносных объектов по заключению модуля Антивирус. Перечисляет адреса получателей и количество срабатываний модуля Антивирус.

12. Отчет о десяти основных вредоносных объектах по заключению модуля Антивирус. Перечисляет имена объектов и количество срабатываний модуля Антивирус.

Просмотр отчетов о работе Kaspersky Secure Mail Gateway

► Чтобы просмотреть отчеты о работе *Kaspersky Secure Mail Gateway*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты** и подраздел в зависимости от типа отчетов, которые вы хотите просмотреть:

   - **Все отчеты**, если вы хотите просмотреть все отчеты.

   - **Ежедневные**, если вы хотите просмотреть ежедневные отчеты.

- **Еженедельные**, если вы хотите просмотреть еженедельные отчеты.
- **Ежемесячные**, если вы хотите просмотреть ежемесячные отчеты.
- **Пользовательские**, если вы хотите просмотреть пользовательские отчеты.

Откроется страница со списком отчетов выбранного вами типа.

2. В строке с информацией об отчете, который вы хотите просмотреть, перейдите по ссылке **PDF**.

Отчет загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с Kaspersky Secure Mail Gateway.

Например, если вы используете операционную систему Microsoft Windows, и в параметрах вашего браузера в качестве директории загрузки файлов из интернета указана папка Downloads, сообщение будет сохранено в папку Downloads на жестком диске вашего компьютера.

Удаление отчетов о работе Kaspersky Secure Mail Gateway

► Чтобы удалить один или несколько отчетов о работе *Kaspersky Secure Mail Gateway*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты** и подраздел в зависимости от типа отчетов, которые вы хотите удалить:
   - **Все отчеты**, если вы хотите удалить отчеты из списка всех отчетов.
   - **Ежедневные**, если вы хотите удалить отчеты из списка ежедневных отчетов.
   - **Еженедельные**, если вы хотите удалить отчеты из списка еженедельных отчетов.
   - **Ежемесячные**, если вы хотите удалить отчеты из списка ежемесячных отчетов.

- **Пользовательские**, если вы хотите удалить отчеты из списка пользовательских отчетов.

Откроется страница со списком отчетов выбранного вами типа.

2. Установите флажки в строках с информацией об отчетах, которые вы хотите удалить.
3. В верхней части рабочей области нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия **Удаление отчетов**.
4. Нажмите на кнопку **Удалить**.

   Окно **Удаление отчетов** закроется.

Выбранные вами отчеты будут удалены.

Включение и отключение формирования ежедневных отчетов

► *Чтобы включить или отключить формирование ежедневных отчетов о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Ежедневные**.
2. В блоке **Формирование ежедневного отчета** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока **Формирование ежедневного отчета**, если вы хотите включить формирование ежедневных отчетов о работе Kaspersky Secure Mail Gateway.
   - Выключите переключатель рядом с названием блока **Формирование ежедневного отчета**, если вы хотите отключить формирование ежедневных отчетов о работе Kaspersky Secure Mail Gateway.

Настройка параметров ежедневного отчета

► *Чтобы настроить параметры ежедневного отчета о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Ежедневные**.

2. В блоке **Формирование ежедневного отчета** по любой ссылке откройте окно **Параметры ежедневного отчета**.

3. В поле **Время формирования отчета** укажите время, в которое будет формироваться ежедневный отчет.

   Укажите время от 00:00 до 23:59.

4. В списке **Язык отчета** выберите язык, на котором будет формироваться ежедневный отчет.

5. В списке **Формат дат в отчете** выберите формат дат для отображения в ежедневном отчете.

6. Если вы хотите, чтобы Kaspersky Secure Mail Gateway отправлял ежедневный отчет на адреса электронной почты, установите флажок рядом с названием параметра **Отправить отчет** и выполните следующие действия:

   a. Установите флажок рядом с названием параметра **Отправить отчет администратору**, если вы хотите, чтобы Kaspersky Secure Mail Gateway отправлял ежедневный отчет на адреса электронной почты администратора Kaspersky Secure Mail Gateway.

   b. В поле **Отправить отчет на следующие адреса электронной почты** введите адрес электронной почты, на который вы хотите настроить отправку ежедневного отчета.

Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

Регулярные выражения нечувствительны к регистру.

c. Нажмите на кнопку  справа от поля ввода.

Добавленный адрес электронной почты отобразится в списке под полем ввода.

7. Нажмите на кнопку **ОК**.

Окно **Параметры ежедневного отчета** закроется.

В блоке **Формирование ежедневного отчета** отобразятся настроенные вами параметры ежедневного отчета о работе Kaspersky Secure Mail Gateway.

Сформированные отчеты о работе Kaspersky Secure Mail Gateway будут отображаться в списке под блоком **Формирование ежедневного отчета**.

Включение и отключение формирования еженедельных отчетов

► *Чтобы включить или отключить формирование еженедельных отчетов о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Еженедельные**.

2. В блоке **Формирование еженедельного отчета** выполните одно из следующих действий:

- Включите переключатель рядом с названием блока **Формирование еженедельного отчета**, если вы хотите включить формирование еженедельных отчетов о работе Kaspersky Secure Mail Gateway.

- Выключите переключатель рядом с названием блока **Формирование еженедельного отчета**, если вы хотите отключить формирование еженедельных отчетов о работе Kaspersky Secure Mail Gateway.

Настройка параметров еженедельного отчета

► *Чтобы настроить параметры еженедельного отчета о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Еженедельные**.

2. В блоке **Формирование еженедельного отчета** по любой ссылке откройте окно **Параметры еженедельного отчета**.

3. В полях **День недели и время формирования отчета** выберите день недели и укажите время, в которое будет формироваться еженедельный отчет.

   Укажите время от 00:00 до 23:59.

4. В списке **Язык отчета** выберите язык, на котором будет формироваться еженедельный отчет.

5. В списке **Формат дат в отчете** выберите формат дат для отображения в еженедельном отчете.

6. Если вы хотите, чтобы Kaspersky Secure Mail Gateway отправлял еженедельный отчет на адреса электронной почты, установите флажок рядом с названием параметра **Отправить отчет** и выполните следующие действия:

   a. Установите флажок рядом с названием параметра **Отправить отчет администратору**, если вы хотите, чтобы Kaspersky Secure Mail Gateway

отправлял еженедельный отчет на адреса электронной почты администратора Kaspersky Secure Mail Gateway.

b. В поле **Отправить отчет на следующие адреса электронной почты** введите адрес электронной почты, на который вы хотите настроить отправку еженедельного отчета.

> Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

> Регулярные выражения нечувствительны к регистру.

c. Нажмите на кнопку  справа от поля ввода.

Добавленный адрес электронной почты отобразится в списке под полем ввода.

7. Нажмите на кнопку **ОК**.

Окно **Параметры еженедельного отчета** закроется.

В блоке **Формирование еженедельного отчета** отобразятся настроенные вами параметры еженедельного отчета о работе Kaspersky Secure Mail Gateway.

Сформированные отчеты о работе Kaspersky Secure Mail Gateway будут отображаться в списке под блоком **Формирование еженедельного отчета**.

Включение и отключение формирования ежемесячных отчетов

► *Чтобы включить или отключить формирование ежемесячных отчетов о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Ежемесячные**.

2. В блоке **Формирование ежемесячного отчета** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока **Формирование ежемесячного отчета**, если вы хотите включить формирование ежемесячных отчетов о работе Kaspersky Secure Mail Gateway.

   - Выключите переключатель рядом с названием блока **Формирование ежемесячного отчета**, если вы хотите отключить формирование ежемесячных отчетов о работе Kaspersky Secure Mail Gateway.

Настройка параметров ежемесячного отчета

► *Чтобы настроить параметры ежемесячного отчета о работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Ежемесячные**.

2. В блоке **Формирование ежемесячного отчета** по любой ссылке откройте окно **Параметры ежемесячного отчета**.

3. В полях **День месяца и время формирования отчета** укажите день месяца и время, в которое будет формироваться ежемесячный отчет.

   Укажите время от 00:00 до 23:59.

4. В списке **Язык отчета** выберите язык, на котором будет формироваться ежемесячный отчет.

5. В списке **Формат дат в отчете** выберите формат дат для отображения в ежемесячном отчете.

6. Если вы хотите, чтобы Kaspersky Secure Mail Gateway отправлял ежемесячный отчет на адреса электронной почты, установите флажок рядом с названием параметра **Отправить отчет** и выполните следующие действия:

    a. Установите флажок рядом с названием параметра **Отправить отчет администратору**, если вы хотите, чтобы Kaspersky Secure Mail Gateway отправлял ежемесячный отчет на адреса электронной почты администратора Kaspersky Secure Mail Gateway.

    b. В поле **Отправить отчет на следующие адреса электронной почты** введите адрес электронной почты, на который вы хотите настроить отправку ежемесячного отчета.

    > Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

    Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

    > Регулярные выражения нечувствительны к регистру.

    c. Нажмите на кнопку  справа от поля ввода.

    Добавленный адрес электронной почты отобразится в списке под полем ввода.

7. Нажмите на кнопку **ОК**.

    Окно **Параметры ежемесячного отчета** закроется.

В блоке **Формирование ежемесячного отчета** отобразятся настроенные вами параметры ежемесячного отчета о работе Kaspersky Secure Mail Gateway.

Сформированные отчеты о работе Kaspersky Secure Mail Gateway будут отображаться в списке под блоком **Формирование ежемесячного отчета**.

Формирование пользовательского отчета

► *Чтобы сформировать пользовательский отчет, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Отчеты**, подраздел **Пользовательские**.

2. В верхней части рабочей области нажмите на кнопку **Создать**.

   Откроется окно **Параметры пользовательского отчета**.

3. В списке **Отчетный период** выберите период, за который вы хотите сформировать пользовательский отчет и выполните следующие действия в зависимости от выбранного варианта:

   - Если вы выбрали формирование отчета за определенный день, в поле **Сутки** укажите дату, за которую вы хотите сформировать отчет.

   - Если вы выбрали формирование отчета за определенный месяц, в списке **Месяц** выберите месяц, за который вы хотите сформировать отчет.

   - Если вы выбрали формирование отчета за определенный год, в списке **Год** выберите год, за который вы хотите сформировать отчет.

   - Если вы выбрали формирование отчета за определенный диапазон дат, в полях **Диапазон дат** укажите даты начала и конца периода, за который вы хотите сформировать отчет.

4. В списке **Язык отчета** выберите язык, на котором сформируется пользовательский отчет.

5. В списке **Формат дат в отчете** выберите формат дат для отображения в пользовательском отчете.

6. Если вы хотите, чтобы Kaspersky Secure Mail Gateway отправил пользовательский отчет на адреса электронной почты, выполните следующие действия:

    a. Установите флажок рядом с названием параметра **Отправить отчет администратору**, если вы хотите, чтобы Kaspersky Secure Mail Gateway отправил пользовательский отчет на адреса электронной почты администратора Kaspersky Secure Mail Gateway.

    b. В поле **Отправить отчет на следующие адреса электронной почты** введите адрес электронной почты, на который вы хотите настроить отправку пользовательского отчета.

    > Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

    Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

    > Регулярные выражения нечувствительны к регистру.

    c. Нажмите на кнопку  справа от поля ввода.

    Добавленный адрес электронной почты отобразится в списке под полем ввода.

7. Нажмите на кнопку **ОК**.

    Окно **Параметры пользовательского отчета** закроется.

Сформированные отчеты о работе Kaspersky Secure Mail Gateway отобразятся в списке в рабочей области главного окна веб-интерфейса программы.

Общие параметры Kaspersky Secure Mail Gateway

Этот раздел содержит информацию о настройке общих параметров Kaspersky Secure Mail Gateway.

В этом разделе

Настройка параметров соединения с прокси-сервером

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Использовать прокси-сервер** по любой ссылке откройте окно **Параметры соединения**.

3. В блоке параметров **Параметры прокси-сервера** в раскрывающемся списке **Использовать прокси-сервер** выберите один из следующих вариантов:

   - **Да**, если вы хотите включить использование прокси-сервера в работе Kaspersky Secure Mail Gateway.

   - **Нет**, если вы хотите отключить использование прокси-сервера в работе Kaspersky Secure Mail Gateway.

4. В поле **Адрес** введите адрес прокси-сервера.

5. В поле **Порт** укажите номер порта прокси-сервера.

6. В блоке параметров **Параметры аутентификации** в раскрывающемся списке **Аутентификация** выберите один из следующих вариантов:

   - **Не требуется**, если вы не хотите использовать аутентификацию при подключении к прокси-серверу.

   - **Простая**, если вы хотите использовать аутентификацию при подключении к прокси-серверу.

7. Если для параметра **Аутентификация** вы выбрали вариант **Простая**, в полях **Имя пользователя** и **Пароль** введите имя пользователя и пароль подключения к прокси-серверу.

8. В блоке параметров **Параметры соединения с прокси-сервером** в раскрывающемся списке **Не использовать для локальных адресов** выберите одно из следующих значений:

   - **Да**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.
   - **Нет**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.

9. Нажмите на кнопку **ОК**.

► *Чтобы включить или отключить использование прокси-сервера, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В рабочей области выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер в работе Kaspersky Secure Mail Gateway.
   - Выключите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы не хотите использовать прокси-сервер в работе Kaspersky Secure Mail Gateway.

Вы можете включить использование прокси-сервера только после того, как настроите параметры соединения с прокси-сервером.

Настройка адресов электронной почты администратора

► *Чтобы настроить адреса электронной почты администратора для отправки уведомлений, отчетов и других сообщений Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Адреса электронной почты** по ссылке **Адреса администратора** откройте окно **Адреса администратора**.

3. В поле **Адреса электронной почты, на которые Kaspersky Secure Mail Gateway отправляет уведомления, отчеты и сообщения с адреса программы** введите адрес электронной почты администратора.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

   Регулярные выражения нечувствительны к регистру.

4. Нажмите на кнопку **Добавить** справа от поля ввода.

   В окне под кнопкой добавления записей сформируется список адресов электронной почты администратора.

5. Нажмите на кнопку **ОК**.

6. Окно **Адреса администратора** закроется.

Адреса электронной почты отобразятся справа от ссылки **Адреса администратора** в рабочей области главного окна веб-интерфейса программы.

Настройка параметров учетной записи HelpDesk

Этот раздел содержит информацию об учетной записи HelpDesk и о настройке ее параметров.

В этом разделе

Об учетной записи HelpDesk

Учетная запись HelpDesk предназначена для получения ограниченного доступа к параметрам программы. С помощью учетной записи HelpDesk администратор Kaspersky Secure Mail Gateway может предоставить другому пользователю права для выполнения некоторых операций, например, для расследования инцидентов с сообщениями, помещенными в хранилище.

Для получения доступа к веб-интерфейсу Kaspersky Secure Mail Gateway под учетной записью HelpDesk, учетная запись HelpDesk должна быть активирована (см. раздел "Активация и деактивация учетной записи HelpDesk" на стр. 213), а также для этой учетной записи должны быть заданы имя пользователя и пароль (см. раздел "Изменение имени пользователя и пароля учетной записи HelpDesk" на стр. 214).

Пользователю HelpDesk доступны следующие операции в веб-интерфейсе Kaspersky Secure Mail Gateway:

- Просмотр информации о сообщении в хранилище.
- Доставка сообщения из хранилища получателю.

  Значение этого параметра задается в параметрах хранилища (см. раздел "Настройка параметров хранилища" на стр. 173).
- Изменение пользовательских черных и белых списков.
- Операции с отчетами:
  - просмотр готовых отчетов;
  - сохранение готового отчета на жесткий диск;
  - разовое создание отчета с пользовательскими параметрами;
  - регулярное создание ежедневных, еженедельных и ежемесячных отчетов;
  - удаление выбранных отчетов из списка готовых отчетов;
  - изменение параметров формирования отчетов за прошедшие периоды по расписанию.

Активация и деактивация учетной записи HelpDesk

► *Чтобы активировать или деактивировать учетную запись HelpDesk, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Активировать учетную запись HelpDesk** выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Активировать учетную запись HelpDesk**, если вы хотите активировать учетную запись HelpDesk.

- Выключите переключатель рядом с названием блока параметров **Активировать учетную запись HelpDesk**, если вы хотите деактивировать учетную запись HelpDesk.

Изменение имени пользователя и пароля учетной записи HelpDesk

► *Чтобы изменить имя пользователя или пароль учетной записи HelpDesk, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Активировать учетную запись HelpDesk** по любой ссылке откройте окно **Параметры учетной записи HelpDesk**.

3. В блоке **Имя пользователя и пароль учетной записи HelpDesk** выполните следующие действия:

   - Если вы хотите изменить имя пользователя учетной записи HelpDesk, введите новое имя пользователя в поле **Имя пользователя**.

   - Если вы хотите изменить пароль учетной записи HelpDesk, укажите новый пароль в поле **Пароль** и введите его повторно в поле **Подтверждение пароля**.

4. Нажмите на кнопку **ОК**.

   Окно **Параметры учетной записи HelpDesk** закроется.

Предоставление учетной записи HelpDesk доступа к черным и белым спискам пользователя

► *Чтобы предоставить учетной записи HelpDesk доступ к черным и белым спискам пользователя, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Активировать учетную запись HelpDesk** по любой ссылке откройте окно **Параметры учетной записи HelpDesk**.

3. В блоке **Права для учетной записи HelpDesk** в раскрывающемся списке **Разрешить доступ к пользовательским спискам** выберите вариант **Да**.

4. Нажмите на кнопку **ОК**.

   Окно **Параметры учетной записи HelpDesk** закроется.

Предоставление учетной записи HelpDesk доступа к отчетам

► *Чтобы предоставить учетной записи HelpDesk доступ к отчетам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Активировать учетную запись HelpDesk** по любой ссылке откройте окно **Параметры учетной записи HelpDesk**.

3. В блоке **Права для учетной записи HelpDesk** в раскрывающемся списке **Разрешить доступ к отчетам** выберите вариант **Да**.

4. Нажмите на кнопку **ОК**.

   Окно **Параметры учетной записи HelpDesk** закроется.

Изменение пароля учетной записи Administrator

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

1. В левом нижнем углу главного окна веб-интерфейса программы по ссылке **Administrator** откройте окно **Измените пароль**.

2. В поле **Старый пароль** введите текущий пароль учетной записи Administrator.
3. В поле **Новый пароль** ведите новый пароль учетной записи Administrator.
4. В поле **Подтвердите новый пароль** введите новый пароль учетной записи Administrator повторно.
5. Нажмите на кнопку **Изменить пароль**.

Настройка параметров журнала событий и журнала аудита

Вы можете выбрать категорию журнала событий, а также указать уровень ведения журнала событий.

По умолчанию события записываются в журнал категории *Mail* и имеют уровень событий *Info*.

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Параметры журнала событий** по любой ссылке откройте окно **Параметры журнала событий**.
3. В списке **Категория журнала** выберите категорию журнала событий.
4. В списке **Уровень события** выберите уровень журнала событий.
5. В списке **Максимум записей в журнале аудита** выберите максимальное количество записей в журнале аудита.

> Ограничение на количество записей в журнале аудита по умолчанию – 100000 записей. По достижении этого ограничения происходит ротация журнала аудита: Kaspersky Secure Mail Gateway перезаписывает самые старые записи журнала новыми данными.

6. Нажмите на кнопку **ОК**.

Настройка параметров производительности программы

► *Чтобы настроить параметры производительности программы, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Параметры производительности** по ссылке **Количество потоков проверки** откройте окно **Параметры производительности**.
3. В списке **Количество потоков проверки** выберите количество потоков сообщений, которые Kaspersky Secure Mail Gateway может проверять одновременно.
4. Нажмите на кнопку **ОК**.

Настройка вида проверенных сообщений

► *Чтобы настроить вид проверенных сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Параметры сообщений** по ссылке **Добавлять заголовки сообщений** откройте окно **Параметры сообщений**.
3. В списке **Добавлять заголовки сообщений** выберите один из следующих вариантов:
   - **Да**, если вы хотите добавлять заголовки к проверенным сообщениям.
   - **Нет**, если вы не хотите добавлять заголовки к проверенным сообщениям.
4. Нажмите на кнопку **ОК**.

Настройка шаблона сообщений при удалении вложения

► *Чтобы настроить шаблон сообщений при удалении вложения, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **Шаблоны** по ссылке **При удалении вложения** откройте окно **Шаблоны**.

3. В поле **При удалении вложения помещать в тело сообщения следующий текст** введите текст, который вы хотите добавлять к сообщениям, из которых Kaspersky Secure Mail Gateway удаляет вложения.

4. Нажмите на кнопку **ОК**.

Экспорт параметров программы

► *Чтобы экспортировать параметры программы, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **Импорт и экспорт параметров программы** по ссылке **Экспортировать параметры** откройте окно **Экспорт параметров программы**.

3. Нажмите на кнопку **ОК**.

Файл формата KZ загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы Kaspersky Secure Mail Gateway. В файле содержатся все текущие параметры программы, в том числе правила обработки сообщений со всеми получателями и отправителями.

Импорт параметров программы

► *Чтобы импортировать параметры программы, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **Импорт и экспорт параметров программы** по ссылке **Импортировать параметры** откройте окно **Импортировать параметры программы**.

3. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.

4. Выберите файл формата KZ с параметрами программы, который вы хотите загрузить.

5. Выберите один из следующих вариантов импорта параметров программы:

   - **Все параметры**, если вы хотите импортировать все параметры программы.

   - **Выбранные параметры**, если вы хотите выбрать, какие параметры программы импортировать.

6. Если вы импортируете **Выбранные параметры**, установите флажки рядом с теми параметрами программы, которые вы хотите импортировать.

7. Нажмите на кнопку **Далее**.

8. Если импорт параметров программы прошел успешно, нажмите на кнопку **Перезапустить программу**.

Программа будет перезапущена. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Перезапуск программы

► *Чтобы перезапустить программу, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **Импорт и экспорт параметров программы** по ссылке **Перезапустить программу** откройте окно **Подтверждение перезапуска программы**.

3. Нажмите на кнопку **ОК**.

Программа будет перезапущена. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Настройка параметра интеграции с Kaspersky Security Center

После установки Kaspersky Secure Mail Gateway передает информацию о себе в Kaspersky Security Center. На основании этой информации Kaspersky Security Center объединяет все виртуальные машины Kaspersky Secure Mail Gateway в кластер. Кластеру присваивается имя. Вы можете настроить этот параметр интеграции с Kaspersky Security Center.

► *Чтобы настроить параметр интеграции с Kaspersky Security Center, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **Интеграция с Kaspersky Security Center** по ссылке **Идентификатор кластера** откройте окно **Интеграция с Kaspersky Security Center**.

3. В поле **Определите идентификатор кластера Kaspersky Security Center** введите идентификатор кластера Kaspersky Security Center. Например, введите Kaspersky Secure Mail Gateway.

4. Нажмите на кнопку **ОК**.

Настройка параметров MTA

Kaspersky Secure Mail Gateway интегрируется в существующую почтовую инфраструктуру организации и не является самостоятельной почтовой системой. Например, Kaspersky Secure Mail Gateway не доставляет сообщения электронной почты получателям и не управляет учетными записями пользователей.

Вы можете настроить основные параметры MTA с помощью мастера быстрой настройки MTA или вручную в веб-интерфейсе программы.

Этот раздел содержит информацию о настройке параметров MTA вручную.

В этом разделе

Настройка основных параметров MTA

Чтобы настроить основные параметры MTA, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **MTA**.
2. Раскройте блок **Основные параметры**, если он не раскрыт.
3. По любой ссылке в блоке **Основные параметры** откройте окно **Основные параметры MTA**.

4. Если вы хотите изменить доменное имя Kaspersky Secure Mail Gateway (mydomain), в поле **Доменное имя** введите новое доменное имя сервера программы.

5. Если вы хотите изменить полное доменное имя Kaspersky Secure Mail Gateway (myhostname), в поле **Имя хоста** введите новое полное доменное имя сервера программы.

6. В поле **Максимальный размер сообщений** укажите максимальный размер принимаемого или пересылаемого через Kaspersky Secure Mail Gateway сообщения электронной почты, включая SMTP-заголовки. Укажите максимальный размер в байтах.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 20971520 байт.

7. Создайте список доверенных сетей и узлов сети, которым разрешено пересылать сообщения электронной почты через Kaspersky Secure Mail Gateway (mynetworks). Как правило, это внутренние сети и узлы сети вашей организации. Например, вы можете указать IP-адреса серверов Microsoft Exchange, используемых в вашей организации.

   > Если доверенные сети не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения с внутренних почтовых серверов и перенаправлять их за пределы сети вашей организации.

   Выполните следующие действия для каждого адреса, который вы хотите добавить:

   a. В поле **Доверенные сети** введите IP-адрес сети или адрес подсети.

      Вводите IP-адреса в формате IPv4 или адреса подсети в нотации CIDR.

   b. Нажмите на кнопку **Добавить**.

      Добавленный вами IP-адрес сети или адрес подсети отобразится в списке доверенных сетей и узлов сети.

   > Адреса вводятся по одному. Повторите действия по добавлению IP-адресов или адресов подсети в список для всех добавляемых доверенных сетей и узлов сети.

8. В поле **Адрес назначения сообщений** введите адрес вашего пограничного шлюза (relayhost). Kaspersky Secure Mail Gateway будет перенаправлять все сообщения на этот адрес.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1 или 192.0.0.0/16), доменное имя или FQDN.

   Если вы настроили маршрутизацию электронной почты для отдельных доменов (см. раздел "Домены и настройка маршрутизации электронной почты" на стр. 147), Kaspersky Secure Mail Gateway будет перенаправлять сообщения электронной почты на адреса, указанные для каждого домена.

9. В списке **Поиск MX-записей** выберите одно из следующих значений:

   - **Вкл**, если вы хотите включить поиск MX-записей для доменных имен или FQDN.
   - **Выкл**, если вы хотите отключить поиск MX-записей.

10. Нажмите на кнопку **ОК**.

Окно **Основные параметры MTA** закроется.

Настройка расширенных параметров MTA

Чтобы настроить расширенные параметры MTA, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **MTA**.
2. Раскройте блок **Расширенные параметры**.
3. По любой ссылке в верхней части списка параметров откройте окно **Расширенные параметры MTA**.
4. В поле **Текст приветствия SMTP-сервера** введите текст, сопровождающий код 220 в SMTP-приветствии.

5. В поле **Максимум попыток соединения** задайте максимальное количество попыток соединения одного удаленного SMTP-клиента с сервисом SMTP-сервера в минуту.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 0 (не ограничено).

6. В поле **Максимум одновременных соединений** задайте максимальное количество одновременных попыток соединения одного удаленного SMTP-клиента с SMTP-сервером.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 50.

7. В поле **Максимум запросов на доставку сообщений** задайте максимальное количество запросов от одного удаленного SMTP-клиента к SMTP-серверу на доставку сообщений в минуту, независимо от того, принимает почтовый сервер эти сообщения или нет.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 0 (не ограничено).

8. В поле **Максимальная длительность SMTP-сессии** задайте максимальное время, в течение которого должен быть получен запрос от удаленного SMTP-клиента и отправлен ответ SMTP-сервера.

   Значение по умолчанию: 30 сек.

9. В поле **Интервал между соединениями с адресом назначения** задайте интервал между попытками диспетчера очереди почтового агента установить соединение с адресом назначения сообщений, если адрес назначения недоступен.

   Значение по умолчанию: 60 сек.

10. В поле **Минимальный интервал доставки из очереди Deferred** задайте минимальный интервал между попытками доставить сообщение, отложенное в очередь Deferred.

    Значение по умолчанию: 300 сек.

11. В поле **Максимальный интервал доставки из очереди Deferred** задайте максимальный интервал между попытками отправить сообщение, отложенное в очередь Deferred.

    Значение по умолчанию: 4000 сек.

12. В поле **Максимальное хранение сообщения в очереди** задайте ограничение времени хранения в очереди сообщения с постоянным статусом ошибки, по прошествии которого сообщение считается недоставленным.

    Значение по умолчанию: 3 дня.

13. В поле **Интервал обработки очереди Deferred** задайте периодичность сканирования очереди Deferred диспетчером.

    Значение по умолчанию: 1000 сек.

14. В поле **Максимальное хранение сообщений о недоставке** задайте ограничение времени хранения в очереди служебного сообщения с постоянным статусом ошибки, по прошествии которого сообщение считается недоставленным.

    Значение по умолчанию: 3 дня.

15. В поле **Адрес для скрытой копии всех сообщений** укажите необязательный адрес электронной почты для получения "blind carbon copy" всех сообщений, принятых почтовым агентом MTA.

16. В списке **Проверять формат адресов по RFC 821** настройте включение и отключение проверки адресов электронной почты в командах `SMTP MAIL FROM` и `RCPT TO` на то, что адреса заключены в угловые скобки, и что эти адреса не содержат RFC 822-комментариев и фраз. Такая проверка предотвращает получение сообщений от недоброкачественного программного обеспечения.

    Чтобы настроить проверку адресов, в списке **Проверять формат адресов по RFC 821** выберите одно из следующих значений:

    - **Да**, если вы хотите включить проверку.
    - **Нет**, если вы хотите отключить проверку.

Значение по умолчанию: **Да**.

17. Настройте параметр **Отключить проверку адресатов SMTP VRFY**, предусматривающий включение и отключение команды `SMTP VRFY`. Команда `SMTP VRFY` предотвращает сбор адресов электронной почты некоторыми службами.

    Чтобы включить или отключить команду `SMTP VRFY`, в списке **Отключить проверку адресатов SMTP VRFY** выберите одно из следующих значений:

    - **Да**, если вы хотите включить команду.
    - **Нет**, если вы хотите отключить команду.

    Значение по умолчанию: **Да**.

18. В поле **Список неанонсируемых SMTP-сервером команд EHLO** установите флажки рядом с теми не чувствительными к регистру командами `EHLO` (например, `pipelining`, `starttls`, `auth`), которые ваш SMTP-сервер не будет анонсировать в ответе на `EHLO`-запрос от внешнего SMTP-клиента.

    Значения по умолчанию: `silent-discard`, `dsn`, `etrn`.

19. Нажмите на кнопку **ОК**.

    Окно **Расширенные параметры MTA** закроется.

SMTP-проверка адресов электронной почты получателей сообщений

Этот раздел содержит информацию об SMTP-проверке подлинности получателей сообщений и о настройке ее параметров.

В этом разделе

Об SMTP-проверке адресов электронной почты получателей сообщений

SMTP-проверка адресов электронной почты получателей сообщений – проверка существования адресов электронной почты получателей сообщений.

Когда Kaspersky Secure Mail Gateway принимает сообщения для защищенных доменов и направляет их на почтовый сервер back-end, необходимо предотвратить прием Kaspersky Secure Mail Gateway сообщений для несуществующих адресов электронной почты. Это необходимо сделать по двум причинам:

- Прием сообщений для отправки на несуществующие адреса электронной почты нагружает процессор, поскольку почта обрабатывается без необходимости.
- Попытки доставить сообщения на несуществующие адреса электронной почты могут привести к тому, что Kaspersky Secure Mail Gateway или сервер back-end будут создавать уведомления о невозможности доставки сообщений, и из-за таких уведомлений Kaspersky Secure Mail Gateway или ваш почтовый сервер back-end будут добавлены в черный список.

Проверка получателей сообщений не выполняется, если Kaspersky Secure Mail Gateway принимает сообщения с адресов доверенных узлов сети (см. раздел "Настройка основных параметров MTA" на стр. 221).

Включение и отключение SMTP-проверки адресов получателей сообщений

► *Чтобы включить или отключить SMTP-проверки адресов получателей сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **MTA**.

2. Раскройте блок **Расширенные параметры**.

3. По ссылке **Отклонять сообщения на неизвестные домены** или **Отклонять сообщения на адреса, не прошедшие проверку** откройте окно **Расширенные параметры MTA**.

   В списке **Отклонять сообщения на неизвестные домены** выберите одно из следующих значений:

   - **Да**, если вы хотите, чтобы Kaspersky Secure Mail Gateway отклонял запрос доставки сообщения, если в имени домена `RCPT TO` отсутствуют MX-записи DNS-сервера и DNS-адрес или MX-запись искажены (например, приведен адрес MX-хоста нулевой длины).

   - **Нет**, если вы не хотите, чтобы Kaspersky Secure Mail Gateway отклонял запрос доставки сообщения, если в имени домена `RCPT TO` отсутствуют MX-записи DNS-сервера и DNS-адрес или MX-запись искажены (например, приведен адрес MX-хоста нулевой длины).

   Значение по умолчанию: **Да**.

4. Справа от названия параметра **Отклонять сообщения на адреса, не прошедшие проверку** выберите один из следующих вариантов:

- **Нет**, если вы не хотите отклонять сообщения на адреса, не прошедшие проверку.
- **Отклонять, если адрес недоступен**, если вы хотите отклонять запрос доставки сообщения, если адрес `RCPT TO` недоступен.
- **Отклонять, если адреса нет в списке допустимых**, если вы хотите отклонять запрос доставки сообщения, если адреса `RCPT TO` нет в списке допустимых адресов для его класса домена.

5. Нажмите на кнопку **ОК**.

Окно **Расширенные параметры MTA** закроется.

SMTP-проверки адресов получателей сообщений не выполняются, если Kaspersky Secure Mail Gateway принимает сообщения с адресов доверенных узлов сети (см. раздел "Настройка основных параметров MTA" на стр. 221).

Интенсивный почтовый трафик может увеличить нагрузку на почтовый сервер из-за отправки уведомлений о невозможности доставки сообщений.

Обновление баз Kaspersky Secure Mail Gateway

Этот раздел содержит информацию об обновлении антивирусных баз, баз модулей Анти-Спам и Анти-Фишинг.

В этом разделе

Об обновлении баз

Базы модулей Антивирус, Анти-Спам 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 почтового сервера к минимуму, рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически по расписанию или устанавливать пакеты обновлений вручную, загружая их с веб-сайта "Лаборатории Касперского".

Во время установки Kaspersky Secure Mail Gateway получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". Если вы настроили автоматическое обновление баз, Kaspersky Secure Mail Gateway выполняет его по расписанию (с периодичностью один раз в пять минут).

Kaspersky Secure Mail Gateway периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского". По умолчанию если антивирусные базы Kaspersky Secure Mail Gateway не обновляются в течение суток или базы модуля Анти-Спам не обновляются в течение часа с момента, когда "Лаборатория Касперского" опубликовала последние пакеты обновлений, Kaspersky Secure Mail Gateway записывает в журнал событий событие *Базы устарели*. Если антивирусные базы не обновляются в течение недели, или базы модуля Анти-Спам не обновляются в течение суток, Kaspersky Secure Mail Gateway записывает событие *Базы сильно устарели*. Вы можете настроить уведомления администратора об этих событиях.

Об источниках обновлений

Источник обновлений – это ресурс, содержащий обновления баз Kaspersky Secure Mail Gateway.

Основным источником обновлений служат серверы 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 подключения к прокси-серверу (см. раздел "Настройка параметров соединения с прокси-сервером для обновления баз" на стр. 236).

Чтобы уменьшить интернет-трафик, вы можете настроить обновление баз Kaspersky Secure Mail Gateway из *пользовательского источника обновлений (см. раздел "Выбор источника*

обновлений баз" на стр. 232*).* Пользовательским источником обновлений могут служить указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

Если Kaspersky Secure Mail Gateway находится под управлением Kaspersky Security Center, в качестве источника обновлений вы можете выбрать Kaspersky Security Center.

Выбор источника обновлений баз

► *Чтобы выбрать источник обновлений баз, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В блоке **Параметры обновления баз программы** по ссылке **Источник обновлений** откройте окно **Параметры обновления баз программы**.

3. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:

   - **Серверы "Лаборатории Касперского"**.
   - **Kaspersky Security Center**.
   - Пользовательский источник обновлений.

4. Если вы выбрали пользовательский источник обновлений, в поле под **Kaspersky Security Center** укажите веб-адрес пакета обновлений на вашем FTP- или HTTP-сервере или укажите полный путь к директории с пакетом обновлений.

   Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории Касперского"**, если вы хотите получать пакет обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен.

5. Нажмите на кнопку **ОК**.

Настройка расписания и параметров обновления баз

► *Чтобы настроить расписание и параметры обновления баз, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В блоке **Параметры обновления баз программы** по ссылке **Расписание** или **Источник обновлений** откройте окно **Параметры обновления баз программы**.

3. В блоке параметров **Расписание** в раскрывающемся списке выберите один из следующих вариантов:

   - **Вручную** (см. раздел "**Запуск обновления баз вручную**" на стр. 236).
   - **Один раз**.
   - **Еженедельно**.
   - **Каждый месяц**.
   - **Запускать каждые**.

4. В блоке параметров **Расписание** в полях справа от раскрывающегося списка укажите периодичность запуска обновления баз. В зависимости от выбранного расписания вы можете указать следующие значения:

   - Для запуска обновления баз **Один раз** в соответствующих полях укажите дату, в которую должно быть запущено обновление баз, и время запуска обновления баз в указанный день.
   - Для запуска обновления баз **Еженедельно** в соответствующих полях укажите день недели, в который должно быть запущено обновление баз, и время запуска обновления баз в указанный день недели.

     Например, если установлены значения **Понедельник** и **15:00**, обновление баз запускается каждый понедельник в 15 часов.

- Для запуска обновления баз **Каждый месяц** в соответствующих полях укажите день месяца, в который должно быть запущено обновление баз, и время запуска обновления баз в указанный день месяца.

  Например, если установлены значения **20** и **15:00**, обновление баз запускается каждый месяц двадцатого числа в 15 часов.

- Для запуска обновления баз **Запускать каждые** в соответствующих полях укажите периодичность запуска обновления баз в минутах, часах или сутках:

  - Для периодичности запуска обновления баз в минутах выберите значение **мин** в списке в правой части окна, укажите периодичность в минутах, а в поле **начиная с** укажите время первого запуска обновления баз.

    Например, если для периодичности установлено значение **30**, выбрана периодичность **мин**, а в поле **начиная с** указано значение **15:00**, то обновление баз запускается каждые полчаса, начиная с 15 часов.

  - Для периодичности запуска обновления баз в часах выберите значение **ч** в списке в правой части окна, укажите периодичность в часах, а в поле **начиная с** укажите дату и время первого запуска обновления баз.

    Например, если для периодичности установлено значение **3**, выбрана периодичность **ч**, а в поле **начиная с** указаны значения **25.05.2017** и **15:00**, то обновление баз запускается каждые три часа, начиная с 15 часов 25 мая 2017 года.

  - Для периодичности запуска обновления баз в сутках выберите значение **сут** в списке в правой части окна, укажите периодичность в сутках, а в поле **начиная с** укажите время запуска обновления баз.

    Например, если для периодичности установлено значение **2**, выбрана периодичность **сут**, а в поле **начиная с** указано значение **15:00**, то обновление баз запускается один раз в два дня (через день) в 15 часов.

5. В блоке параметров **Параметры обновления** в поле **Случайное отклонение** укажите отклонение от заданного расписанием времени в минутах, в течение которого обновление баз будет запущено на компьютерах, чтобы при запуске обновления баз обращение компьютеров к источнику обновлений происходило не одновременно. Эта возможность предусмотрена для того, чтобы разрешить проблему

одновременного обращения большого числа компьютеров к источнику обновлений при запуске обновления баз.

6. В блоке параметров **Параметры обновления** в поле **Выполнять не более** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.

7. В блоке параметров **Параметры обновления** в списке **Запускать пропущенные задачи** выберите порядок запуска задачи, если в заданное расписанием время обновление не выполнялось, например, по следующим причинам:

   - компьютер был выключен;
   - программа не была запущена.

   Если включен запуск пропущенных задач, при очередном запуске программы на этом компьютере предпринимается попытка запуска задачи обновления баз. Для обновления баз **Вручную** и **Один раз** задача обновления баз запускается сразу после появления компьютера в локальной сети.

   Если запуск пропущенных задач не включен, задачи обновления баз на компьютерах запускаются только по расписанию, а обновление баз **Вручную** и **Один раз** запускается только на компьютерах, подключенных к локальной сети.

8. Нажмите на кнопку **ОК**.

Установка стандартных значений параметров обновления баз

► *Чтобы установить стандартные значения параметров обновления баз и стандартное расписание обновления баз, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В блоке **Параметры обновления баз программы** по ссылке **Расписание** откройте окно **Параметры обновления баз программы**.

3. В нижней части окна **Параметры обновления баз программы** перейдите по ссылке **Установить значения по умолчанию**.

4. Нажмите на кнопку **ОК**.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В рабочей области в блоке **Параметры обновления баз программы** запустите обновление баз по ссылке **Запустить обновление**.

   Ссылка **Запустить обновление** сменится надписью **Выполняется обновление**, и отобразится ход обновления баз.

Настройка параметров соединения с прокси-сервером для обновления баз

► *Чтобы настроить параметры соединения с прокси-сервером для обновления баз, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В блоке **Использовать прокси-сервер** по любой ссылке откройте окно **Параметры соединения**.

3. В блоке параметров **Параметры прокси-сервера** в раскрывающемся списке **Использовать прокси-сервер** выберите один из следующих вариантов:

   - **Да**, если вы хотите включить использование прокси-сервера в работе Kaspersky Secure Mail Gateway.

   - **Нет**, если вы хотите отключить использование прокси-сервера в работе Kaspersky Secure Mail Gateway.

4. В поле **Адрес** введите адрес прокси-сервера.

5. В поле **Порт** укажите номер порта прокси-сервера.

6. В блоке параметров **Параметры аутентификации** в раскрывающемся списке **Аутентификация** выберите один из следующих вариантов:

   - **Не требуется**, если вы не хотите использовать аутентификацию при подключении к прокси-серверу.

   - **Простая**, если вы хотите использовать аутентификацию при подключении к прокси-серверу.

7. Если для параметра **Аутентификация** вы выбрали вариант **Простая**, в полях **Имя пользователя** и **Пароль** введите имя пользователя и пароль подключения к прокси-серверу.

8. В блоке параметров **Параметры соединения с прокси-сервером** в раскрывающемся списке **Не использовать для локальных адресов** выберите одно из следующих значений:

   - **Да**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.

   - **Нет**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.

9. Нажмите на кнопку **ОК**.

► *Чтобы включить или отключить использование прокси-сервера, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

2. В рабочей области выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер в работе Kaspersky Secure Mail Gateway.

- Выключите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы не хотите использовать прокси-сервер в работе Kaspersky Secure Mail Gateway.

Вы можете включить использование прокси-сервера только после того, как настроите параметры соединения с прокси-сервером.

Антивирусная защита сообщений

Kaspersky Secure Mail Gateway выполняет антивирусную защиту сообщений: проверяет сообщения электронной почты на вирусы и другие программы, представляющие угрозу, а также лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

Проверку сообщений на вирусы и другие программы, представляющие угрозу, выполняет модуль Антивирус. Модуль Антивирус проверяет тело сообщения и присоединенные к нему файлы любых форматов (вложения) с помощью антивирусных баз. Модуль Антивирус также позволяет обнаруживать и блокировать почтовые вложения, предназначенные для ограниченного числа получателей и представляющие собой компоненты целевых атак на уязвимости в программном обеспечении.

В дополнение к антивирусной проверке сообщений, вы можете включить обнаружение (см. раздел "Настройка параметров модуля Антивирус" на стр. 247) некоторых легальных программ (см. раздел "О защите компьютеров от некоторых легальных программ" на стр. 240) модулем Антивирус.

По результатам антивирусной проверки модуль Антивирус присваивает сообщению один из статусов антивирусной проверки (см. раздел "О статусах антивирусной проверки сообщений" на стр. 245) и добавляет метку, содержащую статус, в начало темы сообщения (поле Тема).

В зависимости от полученного сообщением статуса программа выполняет над сообщением действие, заданное в параметрах правила, по которому обрабатывается сообщение. Вы можете выбирать действия (см. раздел "Настройка действий над сообщениями при антивирусной проверке" на стр. 249), которые программа выполняет над сообщениями с определенным статусом, и настраивать метки (см. раздел "Настройка меток к теме сообщений по результатам антивирусной проверки" на стр. 253) к сообщениям по результатам антивирусной проверки. Перед обработкой программа сохраняет копию сообщения в хранилище.

Вы можете указать максимальный размер проверяемых вложений и определить объекты, не подлежащие антивирусной проверке (см. раздел "Настройка ограничений и исключений из антивирусной проверки сообщений" на стр. 255). Из проверки могут исключаться вложения определенных форматов или вложения с определенными именами.

По умолчанию модуль Антивирус включен. Если требуется, вы можете отключить модуль Антивирус (см. раздел "Включение и отключение антивирусной защиты сообщений" на стр. 245) или отключить антивирусную проверку сообщений для любого правила (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 246).

В этом разделе

О защите компьютеров от некоторых легальных программ

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

Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки

файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Подобные программы описаны в таблице ниже.

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

Тип	Название	Описание
RemoteAdmin	Программы удаленного администрирования	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.

Тип	Название	Описание
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

О статусах антивирусной проверки сообщений

По результатам антивирусной проверки модуль Антивирус присваивает сообщению один из следующих статусов антивирусной проверки:

- *Clean (Чистое сообщение)* – объект не заражен.
- *Infected (Зараженное сообщение)* – объект заражен, не может быть вылечен или лечение объекта не проводилось.
- *Disinfected (Вылеченное сообщение)* – объект вылечен.
- *Encrypted (Зашифрованное сообщение)* – объект проверить невозможно из-за того, что он зашифрован.
- *Error (Ошибка проверки сообщения)* – при проверке объекта произошла ошибка.
- *Attachments with macros (Вложения с макросами)* – сообщение содержит макрос во вложении.

Включение и отключение антивирусной защиты сообщений

► *Чтобы включить или отключить антивирусную защиту сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. В блоке **Антивирус** выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Антивирус**, если вы хотите включить антивирусную защиту сообщений.
   - Выключите переключатель рядом с названием блока параметров **Антивирус**, если вы хотите отключить антивирусную защиту сообщений.

Включение и отключение антивирусной проверки для правила

Вы можете включить или отключить антивирусную проверку сообщений для одного или нескольких правил. По умолчанию антивирусная проверка сообщений включена.

Перед тем как включить или отключить антивирусную проверку сообщений для правила, убедитесь, что модуль Антивирус Kaspersky Secure Mail Gateway включен.

► *Чтобы включить или отключить антивирусную проверку сообщений для правила, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите включить или отключить антивирусную проверку сообщений.
3. Выберите блок **Антивирус**.
4. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Антивирус**, если вы хотите включить антивирусную проверку сообщений для правила.
   - Выключите переключатель рядом с названием блока параметров **Антивирус**, если вы хотите отключить антивирусную проверку сообщений для правила.
5. В нижней части рабочей области нажмите на кнопку **Применить**.

Настройка параметров модуля Антивирус

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Антивирус** по любой ссылке откройте окно **Параметры модуля Антивирус**.

3. В блоке параметров **Защита и эвристический анализ** в раскрывающемся списке **Использовать KSN** выберите один из следующих вариантов:

   - **Да**, если вы хотите использовать службу KSN.

   - **Нет**, если вы не хотите использовать службу KSN.

4. В блоке параметров **Защита и эвристический анализ** в раскрывающемся списке **Использовать эвристический анализ** выберите один из следующих вариантов:

   - **Да**, если вы хотите использовать эвристический анализ.

   - **Нет**, если вы не хотите использовать эвристический анализ.

5. Если вы включили использование эвристического анализа, в блоке параметров **Защита и эвристический анализ** в списке **Уровень эвристического анализа** выберите уровень эвристического анализа.

6. В блоке параметров **Защита и эвристический анализ** в раскрывающемся списке **Я считаю некоторые легальные программы, которые могут быть использованы злоумышленниками, опасными для компьютерной сети организации** выберите один из следующих вариантов:

   - **Да**, если вы считаете, что такие программы при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации.

   - **Нет**, если вы не считаете, что такие программы при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации.

К таким легальным программам (см. раздел "О защите компьютеров от некоторых легальных программ" на стр. 240) относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями. Сообщения, в которых обнаружены эти программы, будут обработаны согласно правилам для зараженных объектов.

7. Если в списке **Я считаю некоторые легальные программы, которые могут быть использованы злоумышленниками, опасными для компьютерной сети организации** вы выбрали **Да**, в блоке параметров **Защита и эвристический анализ** в раскрывающемся списке **Включить обнаружение некоторых легальных программ** выберите один из следующих вариантов:

   - **Да**, если вы хотите включить обнаружение таких программ Kaspersky Secure Mail Gateway.
   - **Нет**, если вы хотите отключить обнаружение таких программ Kaspersky Secure Mail Gateway.

8. В блоке параметров **Производительность** в поле **Максимальная продолжительность проверки** укажите максимальное время антивирусной проверки сообщений в секундах.

   Если антивирусная проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

   - Прерывает проверку сообщения.
   - Выполняет действие над сообщением, которое вы настроили (см. раздел "Настройка действий над сообщениями при антивирусной проверке" на стр. 249).
   - Присваивает сообщению статус *Error.*
   - Добавляет запись следующего содержания в журнал событий /var/log/maillog:

     ```
     <дата и время проверки> <имя хоста Kaspersky Secure Mail Gateway>: not clean: message-id=<ID сообщения>: relay-ip=<IP-адрес компьютера получателя сообщения>: action="Skipped": rules=<ID правила>:
     ```

```
size=<размер сообщения>: mail-from=<адрес электронной почты отправителя сообщения>: rcpt-to=<адрес электронной почты отправителя сообщения>: kt-status="NotScanned, disabled by settings", av-status="Error", ap-status="Clean", as-status="Clean", ma-status="NotScanned, disabled by settings", cf-status="NotScanned, disabled by settings">
```

9. В блоке параметров **Производительность** в поле **Уровень вложенности** укажите максимальный уровень вложенности сообщений, проверяемых модулем Антивирус.

10. Нажмите на кнопку **Применить**.

Установка стандартных значений параметров модуля Антивирус

► *Чтобы установить стандартные значения параметров модуля Антивирус, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Антивирус** по любой ссылке откройте окно **Параметры модуля Антивирус**.

3. В нижней части окна **Параметры модуля Антивирус** перейдите по ссылке **Установить значения по умолчанию**.

4. Нажмите на кнопку **Применить**.

Настройка действий над сообщениями при антивирусной проверке

► *Чтобы настроить действия Kaspersky Secure Mail Gateway над сообщениями при антивирусной проверке, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить действия над сообщениями при антивирусной проверке.

3. Выберите блок **Антивирус**.

4. Включите переключатель рядом с названием блока параметров **Антивирус**, если он выключен.

5. В раскрывающемся списке **Если обнаружен зараженный объект** выберите одно из следующих действий над зараженными сообщениями, представляющими угрозу локальной сети вашей организации:

   - **Лечить**.
   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Лечить**.

6. Если для параметра **Если обнаружен зараженный объект** вы выбрали действие **Лечить**, в раскрывающемся списке **Если вылечить не удалось** в правой части рабочей области выберите одно из следующих действий над зараженными сообщениями, вылечить которые не удалось:

   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Удалить вложение**.

7. Если вы выбрали одно из действий **Лечить**, **Удалить вложение** или **Удалить сообщение**, вы можете настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой. Для этого установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

По умолчанию перед выполнением действий **Лечить**, **Удалить вложение** и **Удалить сообщение** программа помещает копию сообщений в хранилище.

8. В раскрывающемся списке **Если обнаружены ошибки проверки** выберите одно из следующих действий над сообщениями, при проверке которых обнаружены ошибки:

   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Пропустить**.

9. Если вы выбрали одно из действий **Удалить вложение** или **Удалить сообщение**, вы можете настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой. Для этого установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

   По умолчанию перед выполнением действий **Удалить вложение** и **Удалить сообщение** программа помещает копию сообщений в хранилище.

10. В раскрывающемся списке **Если обнаружен зашифрованный объект** выберите одно из следующих действий над сообщениями, содержащими зашифрованные объекты:

    - **Удалить вложение**.
    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Пропустить**.

11. Если вы выбрали одно из действий **Удалить вложение** или **Удалить сообщение**, вы можете настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой. Для этого установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

По умолчанию перед выполнением действий **Удалить вложение** и **Удалить сообщение** программа помещает копию сообщений в хранилище.

12. Установите флажок **Обрабатывать вложения с макросами** если вы хотите, чтобы программа обрабатывала вложения с макросами.

13. В раскрывающемся списке **Если обнаружен макрос** выберите одно из следующих действий над сообщениями, содержащими макросы во вложении:

    - **Удалить вложение**.
    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Удалить вложение**.

14. Если вы выбрали одно из действий **Удалить вложение** или **Удалить сообщение**, вы можете настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой. Для этого установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

    По умолчанию перед выполнением действий **Удалить вложение** и **Удалить сообщение** программа помещает копию сообщений в хранилище

15. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 246), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Настройка меток к теме сообщений по результатам антивирусной проверки

► *Чтобы настроить метки, добавляемые Kaspersky Secure Mail Gateway к теме сообщений по результатам антивирусной проверки, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам антивирусной проверки.

3. Выберите блок **Антивирус**.

4. Включите переключатель рядом с названием блока параметров **Антивирус**, если он выключен.

5. Добавьте метку в поле Тема для зараженных сообщений. Для этого выполните следующие действия:

    a. В блоке параметров **Если обнаружен зараженный объект** по ссылке справа от названия параметра **Добавлять к теме зараженного сообщения текст** откройте окно **Метка для сообщений с вредоносными объектами**.

    b. В поле под названием окна введите текст, который вы хотите добавить в начало темы зараженных сообщений. Например, вы можете добавить метку **Infected**.

    c. Нажмите на кнопку **ОК**.

    Окно **Метка для сообщений с вредоносными объектами** закроется.

6. Добавьте метку в поле Тема для вылеченных сообщений. Для этого выполните следующие действия:

    a. В блоке параметров **Если обнаружен зараженный объект** по ссылке справа от названия параметра **Добавлять к теме вылеченного сообщения текст** откройте окно **Метка для сообщений с вылеченными объектами**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы вылеченных сообщений. Например, вы можете добавить метку **Cured**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для сообщений с вылеченными объектами** закроется.

7. Добавьте метку в поле Тема для сообщений с объектами, при проверке которых обнаружены ошибки. Для этого выполните следующие действия:

a. В блоке параметров **Если обнаружены ошибки проверки** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для сообщений с объектами, вызвавшими ошибки проверки**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, при проверке которых обнаружены ошибки. Например, вы можете добавить метку **Error**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для сообщений с объектами, вызвавшими ошибки проверки** закроется.

8. Добавьте метку в поле Тема для сообщений, содержащих зашифрованные объекты. Для этого выполните следующие действия:

a. В блоке параметров **Если обнаружен зашифрованный объект** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для сообщений с зашифрованными объектами**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений с зашифрованными объектами. Например, вы можете добавить метку **Encrypted**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для сообщений с зашифрованными объектами** закроется.

9. Добавьте метку в поле Тема для сообщений, содержащих макросы во вложении. Для этого выполните следующие действия:

a. В блоке параметров **Если обнаружен макрос** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения сообщений, содержащих макросы во вложении**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, содержащих макросы во вложении. Например, вы можете добавить метку **Attachments with Macros**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для обозначения сообщений, содержащих макросы во вложении** закроется.

10. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 246), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Настройка ограничений и исключений из антивирусной проверки сообщений

► *Чтобы настроить ограничения и исключения из антивирусной проверки сообщений для правила, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить ограничения и исключения из антивирусной проверки сообщений.

3. Выберите блок **Антивирус**.

4. Включите переключатель рядом с названием блока параметров **Антивирус**, если он выключен.

5. Если вы хотите исключить из антивирусной проверки архивы, в блоке параметров **Исключения из проверки** установите флажок **Не проверять архивы**.

6. Если вы хотите исключить из антивирусной проверки вложенные в сообщение объекты определенного размера, в блоке параметров **Исключения из проверки** выполните следующие действия:

    a. По ссылке справа от названия параметра **Не проверять объекты размером более:** откройте окно **Ограничение по размеру сообщений**.

    b. В поле под названием окна введите максимальный размер проверяемых объектов в диапазоне от 0 КБ до 1048576 КБ (1 ГБ).

    Если установлено значение 0 КБ, ограничения размера объектов отсутствуют.

    c. Нажмите на кнопку **ОК**.

    Окно **Ограничение по размеру сообщений** закроется.

7. Если вы хотите исключить из антивирусной проверки вложенные в сообщение объекты с определенными именами, в блоке параметров **Исключения из проверки** выполните следующие действия:

    a. По ссылке справа от названия параметра **Не проверять вложения по маскам имен** откройте окно **Ограничение по маскам имен**.

    b. В поле под названием окна введите маски имен вложенных объектов, которые вы хотите исключить из антивирусной проверки.

    Маски могут содержать любые символы. Разделяйте маски знаком ";".

    c. Нажмите на кнопку **ОК**.

    Окно **Ограничение по маскам имен** закроется.

8. Если вы хотите исключить из антивирусной проверки вложенные в сообщение объекты определенного формата, в блоке параметров **Исключения из проверки** выполните следующие действия:

    a. По ссылке справа от названия параметра **Не проверять вложения по типам файлов** откройте окно **Ограничение по типам файлов**.

b. Установите флажки рядом с теми форматами вложенных объектов, которые вы хотите исключить из антивирусной проверки.

c. Нажмите на кнопку **Закрыть**.

Окно **Ограничение по типам файлов** закроется.

9. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 246), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Защита сообщений от спама

Kaspersky Secure Mail Gateway фильтрует сообщения, проходящие через почтовый сервер, от нежелательной почты (спама).

Проверку сообщений на спам выполняет модуль Анти-Спам. Модуль Анти-Спам проверяет каждое сообщение на присутствие в нем признаков спама. Для этого модуль Анти-Спам, во-первых, проверяет атрибуты сообщения, такие, как: адреса отправителя и получателя, размер сообщения, заголовки (включая заголовки От и Кому). Во-вторых, модуль Анти-Спам анализирует содержание сообщения (включая заголовок Тема) и вложенных файлов. По умолчанию модуль Анти-Спам включен. Если требуется, вы можете отключить модуль Анти-Спам (см. раздел "Включение и отключение защиты сообщений от спама" на стр. 260) или отключить проверку сообщений на спам для любого правила (см. раздел "Включение и отключение проверки сообщений на спам для правила" на стр. 260). Также вы можете ограничить размер сообщений, для которых будет выполняться проверка на спам.

Программа присваивает сообщению, в котором обнаружен спам или вероятный спам, определенный статус (см. раздел "О статусах проверки сообщений на спам" на стр. 259) в соответствии со спам-рейтингом, полученным в результате проверки сообщения модулем Анти-Спам. *Спам-рейтинг сообщения* – это целое число от 0 до 100, которое складывается из баллов, начисленных сообщению программой за каждое срабатывание модуля Анти-Спам. Программа присваивает сообщению спам-рейтинг в том числе на основании ответов DNSBL- и SURBL-серверов, результата SPF- , DKIM- и DMARC-проверок подлинности отправителя сообщения, а также результата репутационной фильтрации сообщений.

Репутационная фильтрация – это 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.

В зависимости от полученного сообщением статуса программа выполняет над сообщением действие, заданное в параметрах правила, по которому обрабатывается сообщение. Вы можете выбирать действия (см. раздел "Настройка действий над сообщениями при проверке на спам" на стр. 268), которые программа выполняет над сообщениями с определенным статусом, и настраивать метки (см. раздел "Настройка меток к теме сообщений по

результатам проверки на спам" на стр. 271) к сообщениям по результатам проверки на спам. По умолчанию программа выполняет над сообщениями действие **Skip (Пропустить)**.

В этом разделе

О статусах проверки сообщений на спам

По результатам проверки на спам модуль Анти-Спам присваивает сообщению один из следующих статусов проверки на спам:

- *Clean (Не спам)* – сообщение не содержит спам.
- *Spam (Спам)* – программа однозначно расценивает сообщение как спам.
- *Probable spam (Предполагаемый спам)* – возможно, сообщение является спамом.
- *Blacklisted (Сообщение от неблагонадежного отправителя)* – адрес электронной почты отправителя входит в глобальный или персональный черный список адресов

(см. раздел "Черные и белые списки адресов" на стр. 291), или IP-адрес или DNS-имя хоста входят в черный список DNSBL (см. раздел "Настройка пользовательского списка DNSBL модуля Анти-Спам" на стр. 263).

- *Massmail (Массовая рассылка)* – сообщение относится к массовой рассылке.
- *Error (Ошибка проверки)* – проверка сообщения завершена с ошибкой.

Включение и отключение защиты сообщений от спама

► *Чтобы включить или отключить защиту сообщений от спама, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. В блоке **Анти-Спам** выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Анти-Спам**, если вы хотите включить защиту сообщений от спама.
   - Выключите переключатель рядом с названием блока параметров **Анти-Спам**, если вы хотите отключить защиту сообщений от спама.

Включение и отключение проверки сообщений на спам для правила

Вы можете включить или отключить проверку сообщений на спам для одного или нескольких правил. По умолчанию проверка сообщений на спам включена.

Перед тем как включить или отключить проверку сообщений на спам для правила, убедитесь, что модуль Анти-Спам Kaspersky Secure Mail Gateway включен.

► *Чтобы включить или отключить проверку сообщений на спам для правила, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите включить или отключить проверку сообщений на спам.

3. Выберите блок **Анти-Спам**.

4. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Анти-Спам**, если вы хотите включить проверку сообщений на спам для правила.

   - Выключите переключатель рядом с названием блока параметров **Анти-Спам**, если вы хотите отключить проверку сообщений на спам для правила.

5. В нижней части рабочей области нажмите на кнопку **Применить**.

Настройка параметров модуля Анти-Спам

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по любой из ссылок **Использовать KSN**, **Использовать службу Enforced Anti-Spam Updates**, **Использовать репутационную фильтрацию** или **Максимальное время проверки** откройте окно **Параметры модуля Анти-Спам**.

3. В блоке параметров **Внешние службы** в раскрывающемся списке **Использовать KSN** выберите один из следующих вариантов:

   - **Да**, если вы хотите использовать службу KSN.

   - **Нет**, если вы не хотите использовать службу KSN.

4. В блоке параметров **Внешние службы** в раскрывающемся списке **Использовать службу Enforced Anti-Spam Updates** выберите один из следующих вариантов:

   - **Да**, если вы хотите использовать функцию принудительного обновления баз модуля Анти-Спам.
   - **Нет**, если вы не хотите использовать функцию принудительного обновления баз модуля Анти-Спам.

5. В блоке параметров **Внешние службы** в раскрывающемся списке **Использовать репутационную фильтрацию** выберите один из следующих вариантов:

   - **Да**, если вы хотите использовать репутационную фильтрацию.
   - **Нет**, если вы не хотите использовать репутационную фильтрацию.

6. В блоке параметров **Производительность** в поле **Максимальное время проверки** укажите максимальное время проверки сообщений на спам в секундах.

   Если проверка сообщения на спам не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

   - Прерывает проверку сообщения (действие **Пропустить**).
   - Присваивает сообщению статус *Error.*
   - Доставляет сообщение получателю.
   - Добавляет запись следующего содержания в журнал событий /var/log/maillog:

     ```
     <дата и время проверки> <имя хоста Kaspersky Secure Mail Gateway>: not clean: message-id=<ID сообщения>: relay-ip=<IP-адрес компьютера получателя сообщения>: action="Skipped": rules=<ID правила>: size=<размер сообщения>: mail-from=<адрес электронной почты отправителя сообщения>: rcpt-to=<адрес электронной почты отправителя сообщения>: kt-status="NotScanned, disabled by settings", av-status="Clean", ap-status="Clean", as-status="Error", ma-status="NotScanned, disabled by settings", cf-status="NotScanned, disabled by settings">
     ```

7. Нажмите на кнопку **Применить**.

Установка стандартных значений параметров модуля Анти-Спам

► *Чтобы установить стандартные значения параметров модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по любой из ссылок **Использовать KSN**, **Использовать службу Enforced Anti-Spam Updates**, **Использовать репутационную фильтрацию** или **Максимальное время проверки** откройте окно **Параметры модуля Анти-Спам**.

3. В нижней части окна **Параметры модуля Анти-Спам** перейдите по ссылке **Установить значения по умолчанию**.

4. Нажмите на кнопку **Применить**.

Настройка пользовательского списка DNSBL модуля Анти-Спам

Вы можете создать *пользовательский список DNSBL-серверов* для повышения уровня обнаружения спама. На DNSBL-серверах хранятся списки IP-адресов, которые были ранее замечены в рассылке спама и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам (см. раздел "О статусах проверки сообщений на спам" на стр. 259).

► *Чтобы создать пользовательский список DNSBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по ссылке **Пользовательский список DNSBL** откройте окно **Пользовательский список DNSBL**.

3. В поле под названием окна **Пользовательский список DNSBL** введите DNS-имена или IP-адреса DNSBL-серверов.

   Вы можете ввести только символы a–z, A–Z, 0–9, "-" и ".", символ "-" не должен быть последним. Например, вы можете добавить в список DNS-имя dns-bl.example.com или IP-адрес 10.0.0.1.

   Вводите каждое DNS-имя или IP-адрес с новой строки.

4. Нажмите на кнопку **Применить**.

► *Чтобы просмотреть пользовательский список DNSBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по ссылке **Пользовательский список DNSBL** откройте окно **Пользовательский список DNSBL**.

3. Нажмите на кнопку **Применить** или **Отмена** по завершении работы со списком.

   Окно **Пользовательский список DNSBL** закроется.

► *Чтобы удалить записи из пользовательского списка DNSBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по ссылке **Пользовательский список DNSBL** откройте окно **Пользовательский список DNSBL**.

3. В поле под названием окна выделите одну или несколько записей, которые вы хотите удалить.

4. Нажмите на клавишу **DELETE**.

5. Нажмите на кнопку **Применить**.

Настройка пользовательского списка SURBL модуля Анти-Спам

Вы можете создать *пользовательский список SURBL-серверов* для повышения уровня обнаружения спама. На SURBL-серверах хранятся списки веб-адресов, которые были ранее замечены в теме или в теле сообщений, расцененных как спам и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам (см. раздел "О статусах проверки сообщений на спам" на стр. 259).

► *Чтобы создать пользовательский список SURBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по ссылке **Пользовательский список SURBL** откройте окно **Пользовательский список SURBL**.

3. В поле под названием окна **Пользовательский список DNSBL** введите DNS-имена или IP-адреса SURBL-серверов.

   Вы можете ввести только символы a–z, A–Z, 0–9, "-" и ".", символ "-" не должен быть последним. Например, вы можете добавить в список DNS-имя dns-bl.example.com или IP-адрес 10.0.0.1.

   Вводите каждое DNS-имя или IP-адрес с новой строки.

4. Нажмите на кнопку **Применить**.

► *Чтобы просмотреть пользовательский список SURBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам** по ссылке **Пользовательский список SURBL** откройте окно **Пользовательский список SURBL**.

3. Нажмите на кнопку **Применить** или **Отмена** по завершении работы со списком.

Окно **Пользовательский список SURBL** закроется.

► *Чтобы удалить записи из пользовательского списка SURBL модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. В блоке **Анти-Спам** по ссылке **Пользовательский список SURBL** откройте окно **Пользовательский список SURBL**.
3. В поле под названием окна выделите одну или несколько записей, которые вы хотите удалить.
4. Нажмите на клавишу **DELETE**.
5. Нажмите на кнопку **Применить**.

Настройка параметров модуля Анти-Спам для правила

Вы можете настроить параметры модуля Анти-Спам для одного или нескольких правил.

► *Чтобы настроить параметры модуля Анти-Спам для правила, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить параметры модуля Анти-Спам.
3. Выберите блок **Анти-Спам**.
4. Включите переключатель рядом с названием блока параметров **Анти-Спам**, если он выключен.
5. В блоке параметров **Общие параметры** установите флажки рядом с названиями общих параметров, которые вы хотите включить:

a. **Использовать технологии обработки графических изображений**, если вы хотите использовать технологию GSG, позволяющую идентифицировать изображения, содержащие текст, чтобы затем определить, является ли текст спамом. Текст распознается вне зависимости от того, был ли он модифицирован, повернут на изображении, «зашумлен» или подвергнут любой другой обработке, скрывающей назначение отправленного изображения.

b. **Проверять вложения в формате RTF**, если вы хотите, чтобы модуль Анти-Спам проверял вложенные в сообщения объекты в формате RTF.

6. В блоке параметров **Проверка с использованием внешних служб** установите флажки рядом с названиями параметров использования внешних служб, которые вы хотите включить:

   a. **Использовать пользовательский список DNSBL** (см. раздел "**Настройка пользовательского списка DNSBL модуля Анти-Спам**" на стр. 263), если вы хотите, чтобы модуль Анти-Спам проверял наличие адресов отправителей на DNSBL-серверах, указанных в пользовательском списке DNSBL.

   Вы можете просмотреть пользовательский список DNSBL по ссылке **пользовательский** в названии параметра **Использовать пользовательский список DNSBL**.

   b. **Использовать пользовательский список SURBL** (см. раздел "**Настройка пользовательского списка SURBL модуля Анти-Спам**" на стр. 265), если вы хотите, чтобы модуль Анти-Спам проверял наличие веб-адресов из темы и тела сообщений на SURBL-серверах, указанных в пользовательском списке SURBL.

   Вы можете просмотреть пользовательский список SURBL по ссылке **пользовательский** в названии параметра **Использовать пользовательский список SURBL**.

7. В блоке параметров **Увеличивать спам-рейтинг, если** установите флажки рядом с названиями языков и шрифтов, использование которых в сообщении может увеличивать спам-рейтинг сообщения:

   a. **Сообщение написано на китайском языке**, если вы хотите, чтобы модуль Анти-Спам увеличивал спам-рейтинг сообщений, написанных на китайском языке.

b. **Сообщение написано на японском языке**, если вы хотите, чтобы модуль Анти-Спам увеличивал спам-рейтинг сообщений, написанных на японском языке.

c. **Сообщение написано на корейском языке**, если вы хотите, чтобы модуль Анти-Спам увеличивал спам-рейтинг сообщений, написанных на корейском языке.

d. **Сообщение написано на тайском языке**, если вы хотите, чтобы модуль Анти-Спам увеличивал спам-рейтинг сообщений, написанных на тайском языке.

e. **Сообщение написано с использованием кириллицы**, если вы хотите, чтобы модуль Анти-Спам увеличивал спам-рейтинг сообщений, написанных с использованием кириллицы.

8. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что проверка сообщений на спам для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Настройка действий над сообщениями при проверке на спам

► *Чтобы настроить действия Kaspersky Secure Mail Gateway над сообщениями при проверке на спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить действия над сообщениями при проверке на спам.

3. Выберите блок **Анти-Спам**.

4. Включите переключатель рядом с названием блока параметров **Анти-Спам**, если он выключен.

5. В раскрывающемся списке **Если обнаружен спам** выберите одно из следующих действий над сообщениями, содержащими спам:

   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

6. Если вы хотите настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой, установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

   По умолчанию перед выполнением действия **Удалить сообщение** программа помещает копию сообщений в хранилище.

7. В раскрывающемся списке **Если обнаружен предполагаемый спам** выберите одно из следующих действий над сообщениями, содержащими предполагаемый спам:

   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

8. Если вы хотите настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой, установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

   По умолчанию перед выполнением действия **Удалить сообщение** программа помещает копию сообщений в хранилище.

9. В раскрывающемся списке **Если адрес отправителя сообщения находится в черном списке DNSBL** выберите одно из следующих действий над сообщениями, отправитель которых обнаружен в списке DNSBL (см. раздел "Настройка пользовательского списка DNSBL модуля Анти-Спам" на стр. 263) и которому присвоен

статус (см. раздел "О статусах проверки сообщений на спам" на стр. 259) *Blacklisted (неблагонадежный)*:

- **Удалить сообщение**.
- **Отклонить**.
- **Пропустить**.

10. Если вы хотите настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой, установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

    По умолчанию перед выполнением действия **Удалить сообщение** программа помещает копию сообщений в хранилище.

11. В раскрывающемся списке **Если обнаружена массовая рассылка** выберите одно из следующих действий над сообщениями, в которых обнаружена массовая рассылка:

    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

12. Если вы хотите настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой, установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**.

    По умолчанию перед выполнением действия **Удалить сообщение** программа помещает копию сообщений в хранилище.

13. В нижней части рабочей области нажмите на кнопку **Применить**.

По умолчанию для всех сообщений выбрано действие **Пропустить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что проверка сообщений на спам для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Настройка меток к теме сообщений по результатам проверки на спам

► *Чтобы настроить метки, добавляемые Kaspersky Secure Mail Gateway к теме сообщений по результатам проверки на спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам проверки на спам.

3. Выберите блок **Анти-Спам**.

4. Включите переключатель рядом с названием блока параметров **Анти-Спам**, если он выключен.

5. Добавьте метку в поле Тема для сообщений, содержащих спам. Для этого выполните следующие действия:

    a. В блоке параметров **Если обнаружен спам** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения спама**.

    b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, содержащих спам. Например, вы можете добавить метку **Spam**.

    c. Нажмите на кнопку **ОК**.

    Окно **Метка для обозначения спама** закроется.

6. Добавьте метку в поле Тема для сообщений, которые предположительно содержат спам. Для этого выполните следующие действия:

a. В блоке параметров **Если обнаружен предполагаемый спам** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения предполагаемого спама**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, предположительно содержащих спам. Например, вы можете добавить метку **Probable spam**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для обозначения предполагаемого спама** закроется.

7. Добавьте метку в поле Тема для сообщений, отправитель которых обнаружен в списке DNSBL (см. раздел "Настройка пользовательского списка DNSBL модуля Анти-Спам" на стр. 263) и которому присвоен статус (см. раздел "О статусах проверки сообщений на спам" на стр. 259) *Blacklisted (неблагонадежный)*. Для этого выполните следующие действия:

   a. В блоке параметров **Если адрес отправителя сообщения находится в черном списке DNSBL** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения сообщений из черного списка DNSBL**.

   b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений от неблагонадежных отправителей. Например, вы можете добавить метку **Blacklisted**.

   c. Нажмите на кнопку **ОК**.

   Окно **Метка для обозначения сообщений из черного списка DNSBL** закроется.

8. Добавьте метку в поле Тема для сообщений, в которых обнаружена массовая рассылка. Для этого выполните следующие действия:

   a. В блоке параметров **Если обнаружена массовая рассылка** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения массовой рассылки**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, в которых обнаружена массовая рассылка. Например, вы можете добавить метку **MASSMAIL**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для обозначения массовой рассылки** закроется.

9. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что проверка сообщений на спам для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Анти-Спам карантин

Сообщения электронной почты, результат проверки которых модулем Анти-Спам еще не окончателен, временно помещаются в Анти-Спам карантин. Вы можете настроить параметры Анти-Спам карантина.

В этом разделе

Включение и отключение использования Анти-Спам карантина

► *Чтобы включить или отключить использования Анти-Спам карантина, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам карантин** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Анти-Спам карантин**, если вы хотите включить использование Анти-Спам карантина.

   - Выключите переключатель рядом с названием блока параметров **Анти-Спам карантин**, если вы хотите отключить использование Анти-Спам карантина.

Настройка параметров Анти-Спам карантина

Сообщения электронной почты, результат проверки которых модулем Анти-Спам еще не окончателен, временно помещаются в Анти-Спам карантин. Вы можете настроить параметры Анти-Спам карантина.

► *Чтобы настроить параметры Анти-Спам карантина, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам карантин** по любой из ссылок **Максимальное время нахождения сообщения в карантине**, **Максимальный размер Анти-Спам карантина** или **Максимальное количество сообщений в Анти-Спам карантине** откройте окно **Параметры модуля Анти-Спам карантин**.

3. В поле **Максимальное время нахождения сообщения в карантине** укажите максимальное время нахождения сообщения в Анти-Спам карантине, по истечении которого сообщение будет доставлено получателю.

4. В поле **Максимальный размер Анти-Спам карантина** укажите максимальный размер Анти-Спам карантина. При превышении этого размера карантина сообщения не будут помещаться в карантин.

5. В поле **Максимальное количество сообщений в Анти-Спам карантине** укажите максимальное количество сообщений в Анти-Спам карантине. При превышении этого количества сообщения не будут помещаться в карантин.

6. Нажмите на кнопку **Применить**.

Установка стандартных значений параметров Анти-Спам карантина

► *Чтобы установить стандартные значения параметров модуля Анти-Спам, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Анти-Спам карантин** по любой из ссылок **Максимальное время нахождения сообщения в карантине**, **Максимальный размер Анти-Спам карантина** или **Максимальное количество сообщений в Анти-Спам карантине** откройте окно **Параметры модуля Анти-Спам карантин**.

3. В нижней части окна **Параметры модуля Анти-Спам карантин** перейдите по ссылке **Установить значения по умолчанию**.

4. Нажмите на кнопку **Применить**.

Защита KATA и интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform

Вы можете настроить интеграцию Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform (KATA) – решение (далее также "программа"), 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 (далее также "APT").

В результате интеграции Kaspersky Secure Mail Gateway сможет отправлять сообщения электронной почты на проверку Kaspersky Anti Targeted Attack Platform и получать результат проверки. KATA проверяет сообщения на наличие признаков целевых атак и вторжений в IT-инфраструктуру организации.

По результатам проверки KATA Kaspersky Secure Mail Gateway может блокировать отдельные сообщения.

В этом разделе

Ввод параметров интеграции на стороне Kaspersky Secure Mail Gateway

► *Чтобы ввести параметры интеграции Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Secure Mail Gateway в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. Выберите блок **Защита KATA**.

3. Включите переключатель рядом с названием блока параметров **Защита KATA**.

4. В блоке **Защита KATA** по любой ссылке откройте окно **Защита KATA**.

5. В поле **KATA Central Node IPv4-адрес** введите IP-адрес сервера Kaspersky Anti Targeted Attack Platform с компонентом Central Node.

6. В поле **KATA Central Node порт** введите порт подключения к серверу Kaspersky Anti Targeted Attack Platform с компонентом Central Node.

7. В поле **Максимальное время ожидания ответа от KATA** введите максимальное время ожидания результата проверки сообщения программой Kaspersky Anti Targeted Attack Platform.

8. В поле **Максимальный размер KATA-карантина** введите максимальный размер карантина Kaspersky Anti Targeted Attack Platform. При превышении этого размера карантина сообщения не будут помещаться в карантин.

9. В поле **Максимальное количество сообщений в KATA-карантине** введите максимальное количество сообщений в карантине Kaspersky Anti Targeted Attack Platform. При превышении этого количества сообщения не будут помещаться в карантин.

10. Если вы хотите установить значения параметров **KATA Central Node порт**, **Максимальное время ожидания ответа от KATA**, **Максимальный размер KATA-карантина** и **Максимальное количество сообщений в KATA-карантине** по

умолчанию, перейдите по ссылке **Установить значения по умолчанию** в нижней части окна **Защита KATA**.

11. Нажмите на кнопку **Применить**.

    Окно **Защита KATA** закроется.

Kaspersky Secure Mail Gateway попытается установить соединение с сервером Kaspersky Anti Targeted Attack Platform с компонентом Central Node.

Перейдите к подтверждению интеграции Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Anti Targeted Attack Platform.

Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform

► *Чтобы подтвердить интеграцию Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. Войдите в консоль управления сервера Kaspersky Anti Targeted Attack Platform с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора сервера Kaspersky Anti Targeted Attack Platform с компонентом Central Node и пароль администратора.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите пункт **Program settings**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно **Select action**.
5. Выберите действие **Configure KSMG Sensor connections**.
6. Нажмите на клавишу **ENTER**.

   Отобразится окно **Configure KSMG Sensor connections**.
7. Выберите строку с IP-адресом сервера Kaspersky Secure Mail Gateway. Строка неподтвержденного соединения отмечена "звездочкой".
8. Нажмите на клавишу **ENTER**.

   Отобразится окно с отпечатками открытых сертификатов соединения Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform.
9. Убедитесь, что сертификат Kaspersky Secure Mail Gateway соответствует отпечатку сертификата в веб-интерфейсе Kaspersky Secure Mail Gateway.
10. Выберите **Accept KSMG Sensor**.

11. Нажмите на клавишу **ENTER**.

    Вы вернетесь в окно **Configure KSMG Sensor connections**. Строка с IP-адресом сервера Kaspersky Secure Mail Gateway не будет отмечена "звездочкой".

Интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Anti Targeted Attack Platform будет подтверждена.

Проверка соединения Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform

► *Чтобы проверить соединение Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Secure Mail Gateway в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. Выберите блок **Защита KATA**.

3. Включите переключатель рядом с названием блока параметров **Защита KATA**.

4. В блоке **Защита KATA** по ссылке **Состояние соединения с KATA** откройте окно **Состояние соединения с KATA**.

   Рядом с названием параметра **KATA Central Node IPv4-адрес** отобразится IP-адрес сервера Kaspersky Anti Targeted Attack Platform с компонентом Central Node.

   Рядом с названием параметра **Статус подключения** отобразится статус соединения Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform.

   Рядом с названием параметра **Отпечаток открытого ключа KSMG** отобразится отпечаток сертификата Kaspersky Secure Mail Gateway.

   Рядом с названием параметра **Отпечаток открытого ключа KATA** отобразится отпечаток сертификата Kaspersky Anti Targeted Attack Platform.

Если в окне **Состояние соединения с KATA** отобразились отпечатки сертификатов обоих серверов и статус соединения Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform **Connected**, интеграция Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform настроена верно и соединение между серверами установлено.

Настройка отправки сообщений Kaspersky Secure Mail Gateway на проверку Kaspersky Anti Targeted Attack Platform

► *Чтобы настроить отправку сообщений электронной почты Kaspersky Secure Mail Gateway на проверку Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить отправку сообщений электронной почты Kaspersky Secure Mail Gateway на проверку Kaspersky Anti Targeted Attack Platform.

3. Выберите блок **Защита KATA**.

4. Включите переключатель рядом с названием блока параметров **Защита KATA**, если он выключен.

5. В раскрывающемся списке **Если KATA обнаружила событие** выберите одно из следующих действий над сообщениями, в которых KATA обнаружила события:

   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

6. Добавьте метку в поле Тема для сообщений, в которых KATA обнаружила события. Для этого выполните следующие действия:

   a. В блоке параметров **Защита KATA** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для сообщений, в которых KATA обнаружила событие**.

b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, в которых KATA обнаружила события. Например, вы можете добавить метку **KATA detect**.

c. Нажмите на кнопку **ОК**.

Окно **Метка для сообщений, в которых KATA обнаружила событие** закроется.

7. Установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище,** если вы хотите настроить автоматическое сохранение копий сообщений в хранилище перед их обработкой.

8. В нижней части рабочей области нажмите на кнопку **Применить**.

Вы настроили отправку сообщений электронной почты Kaspersky Secure Mail Gateway на проверку Kaspersky Anti Targeted Attack Platform для выбранного правила.

Включение и отключение защиты KATA

► *Чтобы включить или отключить защиту KATA, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Secure Mail Gateway в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Защита KATA** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Защита KATA**, если вы хотите включить защиту Kaspersky Anti Targeted Attack Platform.

   - Выключите переключатель рядом с названием блока параметров **Защита KATA**, если вы хотите отключить защиту Kaspersky Anti Targeted Attack Platform.

Настройка параметров защиты KATA

► *Чтобы настроить параметры защиты KATA и интеграции Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Secure Mail Gateway в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.
2. Выберите блок **Защита KATA**.
3. Включите переключатель рядом с названием блока параметров **Защита KATA**.
4. В блоке **Защита KATA** по любой ссылке откройте окно **Защита KATA**.
5. В поле **Максимальное время ожидания ответа от KATA** введите максимальное время ожидания результата проверки сообщения программой Kaspersky Anti Targeted Attack Platform.
6. В поле **Максимальный размер KATA-карантина** введите максимальный размер карантина Kaspersky Anti Targeted Attack Platform. При превышении этого размера карантина копии сообщений не будут помещаться в карантин.
7. В поле **Максимальное количество сообщений в KATA-карантине** введите максимальное количество сообщений в карантине Kaspersky Anti Targeted Attack Platform. При превышении этого количества копии сообщений не будут помещаться в карантин.
8. Нажмите на кнопку **Применить**.

Установка стандартных значений параметров защиты KATA

► *Чтобы установить стандартные значения параметров защиты KATA, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке **Защита KATA** по любой ссылке откройте окно **Защита KATA**.

3. В нижней части окна **Защита KATA** перейдите по ссылке **Установить значения по умолчанию**.

4. Нажмите на кнопку **Применить**.

Включение и отключение защиты KATA для правила

Вы можете включить или отключить защиту KATA для одного или нескольких правил. По умолчанию защита KATA включена.

Перед тем как включить или отключить защиту KATA для правила, убедитесь, что защита KATA включена в параметрах программы (см. раздел "Включение и отключение защиты KATA" на стр. 285).

► *Чтобы включить или отключить защиту KATA для правила, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите включить или отключить защиту KATA.

3. Выберите блок **Защита KATA**.

4. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Защита KATA**, если вы хотите включить защиту KATA для правила.

   - Выключите переключатель рядом с названием блока параметров **Защита KATA**, если вы хотите отключить защиту KATA для правила.

5. В нижней части рабочей области нажмите на кнопку **Применить**.

Настройка действий над сообщениями по результатам проверки KATA

► *Чтобы настроить действия Kaspersky Secure Mail Gateway над сообщениями по результатам проверки KATA, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить действия над сообщениями по результатам проверки KATA.
3. Выберите блок **Защита KATA**.
4. Включите переключатель рядом с названием блока параметров **Защита KATA**, если он выключен.
5. В раскрывающемся списке **Если KATA обнаружила событие** выберите одно из следующих действий над сообщениями, в которых KATA обнаружила события:
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Удалить сообщение**.
6. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что защита KATA для правила включена (см. раздел "Включение и отключение защиты KATA для правила" на стр. 287), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Настройка меток к теме сообщений по результатам проверки KATA

► *Чтобы настроить метки, добавляемые Kaspersky Secure Mail Gateway к теме сообщений по результатам проверки KATA, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.

2. В списке правил по ссылке с названием правила откройте правило, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам проверки KATA.

3. Выберите блок **Защита KATA**.

4. Включите переключатель рядом с названием блока параметров **Защита KATA**, если он выключен.

5. Добавьте метку в поле Тема для сообщений, в которых KATA обнаружила событие. Для этого выполните следующие действия:

    a. В блоке параметров **Защита KATA** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для сообщений, в которых KATA обнаружила событие**.

    b. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщений, в которых KATA обнаружила событие. Например, вы можете добавить метку **KATA detect**.

    c. Нажмите на кнопку **ОК**.

    Окно **Метка для сообщений, в которых KATA обнаружила событие** закроется.

6. В нижней части рабочей области нажмите на кнопку **Применить**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что защита KATA для правила включена (см. раздел "Включение и отключение защиты KATA для правила" на стр. 287), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 146).

Черные и белые списки адресов

Этот раздел содержит информацию о черных и белых списках адресов электронной почты, которые можно создавать и редактировать в Kaspersky Secure Mail Gateway.

В этом разделе

О черных и белых списках адресов

Черные и белые списки адресов предоставляют возможность более точно настроить реакцию почтовой системы на сообщения, не являющиеся спамом официально (например, новостные рассылки).

Существует два вида черных и белых списков адресов:

- *Персональные*. Содержат адреса отправителей сообщений для одного получателя. Персональный белый список адресов пропускает сообщения без проверки на спам. При этом выполняется проверка на фишинг, вирусы и другие программы, представляющие угрозу, а также выполняется контентная фильтрация.

- *Глобальные*. Содержат адреса отправителей и получателей сообщений. Вы можете задать такие списки в предустановленных правилах обработки сообщений WhiteList и BlackList (см. раздел "Работа с правилами обработки сообщений" на стр. 129). Вы также можете создать правила с указанием адресов отправителей и получателей,

сообщения от которых нужно отклонять без проверки, удалять без уведомления отправителя, пропускать без проверки.

Обработка сообщения, адреса отправителя и получателей которого состоят в глобальном черном или белом списке адресов, выполняется следующим образом:

- Если адреса отправителя и получателей сообщения состоят в глобальном черном списке адресов, программа отклоняет это сообщение или удаляет его без уведомления отправителя.
- Если адреса отправителя и получателей сообщения состоят в глобальном белом списке адресов, программа пропускает сообщение без проверки.
- Если адреса отправителя и получателей сообщения состоят одновременно в глобальном белом и черном списке адресов, программа обрабатывает сообщение по правилу с большим приоритетом.

Сообщение обрабатывается по правилу персонального белого или персонального черного списка адресов, если оно не попадает под действие глобального черного или белого списков адресов.

Принцип обработки сообщения, адрес отправителя которого состоит в персональном черном или белом списке адресов, следующий:

- Если адрес отправителя сообщения состоит в персональном черном списке адресов и один из адресов получателей сообщения принадлежит владельцу персонального черного списка адресов, сообщение не доставляется получателю – владельцу персонального черного списка. В зависимости от указанного действия над сообщениями, попадающими в персональный черный список, программа удаляет или отклоняет сообщение. Также программа может поместить сообщение в хранилище.
- Если адрес отправителя содержится в персональном белом списке адресов, сообщение будет доставлено получателю в зависимости от результатов антивирусной проверки, проверки на фишинг, контентной фильтрации, проверки подлинности отправителя сообщения и проверки сообщения в KATA.
- Если адрес отправителя содержится одновременно в черном и белом персональных списках адресов, сообщение обрабатывается в соответствии с персональным белым списком адресов.

Настройка параметров персонального черного списка адресов

Чтобы настроить параметры персонального черного списка адресов электронной почты, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Защита**.

2. В блоке параметров **Параметры персонального черного списка** по любой ссылке откройте окно **Параметры черного списка**.

3. В списке **Если адрес электронной почты отправителя в черном списке адресов** выберите одно из следующих действий над сообщениями:

   - **Удалить сообщение**, если вы хотите удалять сообщения, адрес отправителя которых находится в персональном черном списке.

   - **Отклонить**, если вы хотите отклонять сообщения, адрес отправителя которых находится в персональном черном списке.

4. В списке **Помещать сообщение в хранилище** выберите одно из следующих значений:

   - **Да**, если вы хотите помещать сообщения, адрес отправителя которых находится в персональном черном списке, в хранилище.

   - **Нет**, если вы не хотите помещать сообщения, адрес отправителя которых находится в персональном черном списке, в хранилище.

5. Нажмите на кнопку **Применить**.

Просмотр персональных черных и белых списков адресов

Для работы с персональными черным и белыми списками адресов из веб-интерфейса Kaspersky Secure Mail Gateway необходимо подключится к LDAP-серверу (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 299).

Чтобы просмотреть персональные черные и белые списки адресов электронной почты, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В блоке параметров **Персональные черные и белые списки адресов** по ссылке **Доступ к черным и белым спискам** откройте окно **Персональные черные и белые списки адресов**.

3. В поле **Поиск по имени пользователя или названию группы в службе каталогов LDAP** введите строку поиска персональных черных и белых списков адресов по имени пользователя или названию группы в службе каталогов LDAP.

4. Нажмите на кнопку **Найти** справа от поля ввода.

   Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.

5. Нажмите на LDAP-запись пользователя, персональный черный и белый списки адресов которого вы хотите просмотреть.

6. По завершении работы с персональными списками пользователя нажмите на кнопку **Закрыть**.

Окно **Персональные черные и белые списки адресов** закроется.

Добавление адресов в персональные черные и белые списки адресов

Для получения доступа к персональным черным и белым спискам адресов из веб-интерфейса Kaspersky Secure Mail Gateway необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 300).

Для работы с персональными черным и белыми списками адресов из веб-интерфейса Kaspersky Secure Mail Gateway необходимо подключится к LDAP-серверу (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 299).

Чтобы добавить адреса в персональные черные и белые списки адресов электронной почты, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.
2. В блоке параметров **Персональные черные и белые списки адресов** по ссылке **Доступ к черным и белым спискам** откройте окно **Персональные черные и белые списки адресов**.
3. В поле **Поиск по имени пользователя или названию группы в службе каталогов LDAP** введите строку поиска персональных черных и белых списков адресов по имени пользователя или названию группы в службе каталогов LDAP.
4. Нажмите на кнопку **Найти** справа от поля ввода.

   Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.
5. Нажмите на LDAP-запись пользователя, в персональный черный и белый списки адресов которого вы хотите добавить адреса.

   В нижней части окна отобразятся персональный черный и белый списки адресов.

6. В поле ввода адресов того списка адресов, в который вы хотите добавить адреса электронной почты, введите адрес электронной почты, который вы хотите добавить.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

   Регулярные выражения нечувствительны к регистру.

7. Нажмите на кнопку  справа от поля ввода.

   Добавленный адрес электронной почты отобразится в выбранном вами списке.

8. По завершении работы с персональными списками пользователя нажмите на кнопку **Применить**.

Окно **Персональные черные и белые списки адресов** закроется.

Удаление адресов из персональных черных и белых списков адресов

Для получения доступа к персональным черным и белым спискам адресов из веб-интерфейса Kaspersky Secure Mail Gateway необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 300) и подключиться к нему (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 299).

Чтобы удалить адреса из персональных черных и белых списков адресов электронной почты, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В блоке параметров **Персональные черные и белые списки адресов** по ссылке **Доступ к черным и белым спискам** откройте окно **Персональные черные и белые списки адресов**.

3. В поле **Поиск по имени пользователя или названию группы в службе каталогов LDAP** введите строку поиска персональных черных и белых списков адресов по имени пользователя или названию группы в службе каталогов LDAP.

4. Нажмите на кнопку **Найти** справа от поля ввода.

   Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.

5. Нажмите на LDAP-запись пользователя, из персонального черного и белого списков адресов которого вы хотите удалить адреса.

   В нижней части окна отобразятся персональный черный и белый списки адресов.

6. В списке адресов, из которого вы хотите удалить адрес, выделите адрес электронной почты, который вы хотите удалить.

   Адреса электронной почты удаляются по одному. Повторите действия по удалению адресов из списка для всех удаляемых адресов электронной почты.

7. Нажмите на кнопку **Удалить** справа от списка адресов.

   Адрес электронной почты будет удален из выбранного вами списка.

8. По завершении работы с персональными списками пользователя нажмите на кнопку **Применить**.

Окно **Персональные черные и белые списки адресов** закроется.

Соединение с LDAP-сервером

Этот раздел содержит информацию о соединении Kaspersky Secure Mail Gateway с LDAP-сервером и о настройке параметров и фильтров соединения с LDAP-сервером.

В этом разделе

О соединении с LDAP-сервером

Kaspersky Secure Mail Gateway позволяет подключаться к серверам внешних служб каталогов, используемых в вашей организации, по протоколу LDAP.

Служба каталогов – программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

LDAP (Lightweight Directory Access Protocol) – облегченный клиент-серверный протокол доступа к службам каталогов.

Соединение с внешней службой каталогов по протоколу LDAP предоставляет администратору Kaspersky Secure Mail Gateway возможность выполнять следующие задачи:

- Добавлять отправителей или получателей (см. раздел "Добавление учетных записей LDAP в списки отправителей и получателей сообщений" на стр. 137) из внешней службы каталогов в правила обработки сообщений.
- Создавать, изменять и просматривать персональные черные и белые списки адресов (см. раздел "Просмотр персональных черных и белых списков адресов" на стр. 294) пользователей локальной сети организации.
- Просматривать копии сообщений пользователей локальной сети организации в хранилище (см. раздел "Просмотр информации о сообщении в хранилище" на стр. 177).

Подключение и отключение от LDAP-сервера

► *Чтобы подключиться к LDAP-серверу или отключиться от LDAP-сервера, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. По ссылке **Соединение с LDAP-сервером** откройте окно **Соединение с LDAP-сервером**.

3. Выберите один из следующих вариантов подключения к LDAP-серверу:

   - **Не используется**, если вы не хотите использовать LDAP-сервер в работе Kaspersky Secure Mail Gateway.

   - **Active Directory или generic LDAP**, если вы хотите подключиться к LDAP-серверу Microsoft Active Directory или любой другой LDAP-совместимой службы каталогов (например, Red Hat® Directory Server).

4. Если вы хотите ограничить время ожидания ответа сервера, установите флажок рядом с названием параметра **Ограничить время ожидания ответа сервера**.

5. Если вы установили флажок рядом с названием параметра **Ограничить время ожидания ответа сервера**, в поле **Время ожидания ответа сервера в секундах** укажите максимальное время, в течение которого должен быть получен ответ от LDAP-сервера в секундах.

   Значение по умолчанию: 20 сек.

6. Нажмите на кнопку **Применить**.

Окно **Соединение с LDAP-сервером** закроется.

Добавление соединения с LDAP-сервером

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

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. Если в рабочей области отобразилось значение параметра **Соединение с LDAP-сервером Не используется**, выполните следующие действия:

a. По ссылке **Соединение с LDAP-сервером** откройте окно **Соединение с LDAP-сервером**.

b. В списке **LDAP-сервер** выберите **Active Directory или generic LDAP**.

c. Если вы хотите ограничить время ожидания ответа сервера, установите флажок рядом с названием параметра **Ограничить время ожидания ответа сервера**.

d. Если вы установили флажок рядом с названием параметра **Ограничить время ожидания ответа сервера**, в поле **Время ожидания ответа сервера в секундах** укажите максимальное время, в течение которого должен быть получен ответ от LDAP-сервера в секундах.

Значение по умолчанию: 20 сек.

e. Нажмите на кнопку **Применить**.

Окно **Соединение с LDAP-сервером** закроется.

3. В рабочей области нажмите на кнопку **Добавить**.

Откроется окно **Мастер подключения к LDAP-серверу**.

4. На закладке **Параметры соединения** в блоке параметров **Параметры LDAP-сервера** в раскрывающемся списке **LDAP-сервер** выберите одну из следующих внешних служб каталогов:

- **generic LDAP**, если вы хотите добавить соединение с сервером LDAP-совместимой службы каталогов (например, Red Hat Directory Server).
- **Active Directory**, если вы хотите добавить соединение с сервером Microsoft Active Directory.

5. В блоке параметров **Параметры LDAP-сервера** в поле **Адрес сервера** введите IP-адрес в формате IPv4 или FQDN-имя LDAP-сервера, к которому вы хотите подключиться.

6. В блоке параметров **Параметры LDAP-сервера** в списке **Порт подключения** укажите порт подключения к LDAP-серверу.

LDAP-сервер, как правило, принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для подключения к LDAP-серверу по протоколу SSL обычно используется порт 636.

7. В блоке параметров **Параметры LDAP-сервера** в списке **Тип подключения** выберите один из вариантов использования шифрования данных при подключении к LDAP-серверу:

   - **SSL**, если вы хотите использовать SSL.
   - **TLS**, если вы хотите использовать TLS.
   - **Без шифрования**, если вы не хотите использовать технологии шифрования данных при подключении к LDAP-серверу.

8. В блоке параметров **Параметры аутентификации** в поле **Имя пользователя LDAP-сервера** введите имя пользователя LDAP-сервера, у которого есть права на чтение записей каталога (BindDN). Введите имя пользователя в одном из следующих форматов:

   - `cn=<имя пользователя>, ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>`, если вы хотите добавить соединение с сервером LDAP-совместимой службы каталогов (например, Red Hat Directory Server).

     Например, вы можете ввести имя пользователя `cn=LdapServerUser, dc=example, dc=com`, где `LdapServerUser` – имя пользователя LDAP-сервера, `example` – доменное имя каталога, к которому относится учетная запись пользователя, `com` – имя родительского домена, в котором находится каталог.

   - `cn=<имя пользователя>, ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>` или `<имя пользователя>@<имя домена>.<имя родительского домена>`, если вы хотите добавить соединение с сервером Microsoft Active Directory.

Например, вы можете ввести имя пользователя `LdapServerUser@example.com`, где `LdapServerUser` – имя пользователя LDAP-сервера, `example.com` – доменное имя каталога, к которому относится учетная запись пользователя.

9. В блоке параметров **Параметры аутентификации** в поле **Пароль пользователя LDAP-сервера** введите пароль доступа к LDAP-серверу пользователя, указанного в поле **Имя пользователя LDAP-сервера**.

10. В блоке **Параметры поиска** в поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Secure Mail Gateway осуществляет поиск записей.

    Вводите базу поиска в формате `ou=<название подразделения>` (если требуется), `dc=<имя домена>`, `dc=<имя родительского домена>`.

    Например, вы можете ввести базу поиска `ou=people, dc=example, dc=com`, где `people` – уровень в схеме каталога, начиная с которого Kaspersky Secure Mail Gateway 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 Secure Mail Gateway осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

11. Нажмите на кнопку **Проверить**.

    Kaspersky Secure Mail Gateway проверит подключение к LDAP-серверу с указанными вами значениями параметров соединения и аутентификации.

12. Нажмите на кнопку **Далее**.

    Откроется закладка **Фильтры**.

13. В блоке параметров **Настройте LDAP-фильтры** в поле **Авторизация пользователя** задайте фильтр авторизации пользователя (например, для получения доступа пользователя к своим сообщениям в хранилище).

14. Если вы хотите установить стандартные значения фильтра авторизации пользователя, перейдите по ссылке **Установить значения по умолчанию** под полем **Авторизация пользователя**.

15. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск пользователя или группы** задайте фильтр поиска пользователей или группы пользователей.

16. Если вы хотите установить стандартные значения фильтра поиска пользователей или группы пользователей, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск пользователя или группы**.

17. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск DN пользователей и групп по адресу эл. почты** задайте фильтр поиска DN пользователей и групп, в которые они входят, по адресу электронной почты.

18. Если вы хотите установить стандартные значения фильтра поиска DN пользователей и групп, в которые они входят, по адресу электронной почты, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск DN пользователей и групп по адресу эл. почты**.

19. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск групп по DN пользователей** задайте фильтр поиска групп, членом которых является пользователь, по DN пользователя. Этот фильтр используется в случае, если не удалось определить группу пользователей с помощью фильтра, заданного в поле **Поиск DN пользователей и групп по адресу эл. почты**.

20. Если вы хотите установить стандартные значения фильтра поиска групп, членом которых является пользователь, по DN пользователя, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск групп по DN пользователей**.

21. Установите флажок **Использовать рекурсивный поиск**, если вы хотите включить поиск LDAP-записей во вложенных группах.

22. Нажмите на кнопку **Завершить**.

    Окно **Мастер подключения к LDAP-серверу** закроется.

Добавленное вами соединение с внешней службой каталогов отобразится в рабочей области раздела **LDAP** главного окна веб-интерфейса программы.

Удаление соединения с LDAP-сервером

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

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В нижней части рабочей области установите флажок рядом с адресом того LDAP-сервера, который вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия **Удаление**.

4. Нажмите на кнопку **Да**.

   Окно **Удаление** закроется.

Соединение с LDAP-сервером будет удалено.

Включение и отключение соединения с LDAP-сервером

Вы можете включить для использования или отключить соединение с одним или несколькими LDAP-серверами.

► *Чтобы включить или отключить использование соединения с LDAP-сервером, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В нижней части рабочей области выполните одно из следующих действий:

   - Включите переключатель рядом с адресом того LDAP-сервера, соединение с которым вы хотите включить.

- Выключите переключатель рядом с адресом того LDAP-сервера, соединение с которым вы хотите отключить.

Настройка параметров соединения с LDAP-сервером

► *Чтобы настроить параметры соединения с LDAP-сервером, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В нижней части рабочей области выберите LDAP-сервер, параметры соединения с которым вы хотите настроить.

3. В блоке параметров **Параметры соединения с LDAP-сервером** выбранного сервера по любой ссылке откройте окно **Параметры соединения с LDAP-сервером**.

4. В блоке параметров **Параметры LDAP-сервера** в списке **LDAP-сервер** выберите одну из следующих внешних служб каталогов:

   - **generic LDAP**, если вы хотите добавить соединение с сервером LDAP-совместимой службы каталогов (например, Red Hat Directory Server).

   - **Active Directory**, если вы хотите добавить соединение с сервером Microsoft Active Directory.

5. В блоке параметров **Параметры LDAP-сервера** в поле **Адрес сервера** введите IP-адрес в формате IPv4 или FQDN-имя LDAP-сервера, к которому вы хотите подключиться.

6. В блоке параметров **Параметры LDAP-сервера** в списке **Порт подключения** укажите порт подключения к LDAP-серверу.

   LDAP-сервер, как правило, принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для подключения к LDAP-серверу по протоколу SSL обычно используется порт 636.

7. В блоке параметров **Параметры LDAP-сервера** в списке **Тип подключения** выберите один из вариантов использования шифрования данных при подключении к LDAP-серверу:

   - **SSL**, если вы хотите использовать SSL.
   - **TLS**, если вы хотите использовать TLS.
   - **Без шифрования**, если вы не хотите использовать технологии шифрования данных при подключении к LDAP-серверу.

8. В блоке параметров **Параметры аутентификации** в поле **Имя пользователя LDAP-сервера** введите имя пользователя LDAP-сервера, у которого есть права на чтение записей каталога (BindDN). Введите имя пользователя в одном из следующих форматов:

   - `cn=<имя пользователя>, ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>`, если вы хотите добавить соединение с сервером LDAP-совместимой службы каталогов (например, Red Hat Directory Server).

     Например, вы можете ввести имя пользователя `cn=LdapServerUser, dc=example, dc=com`, где `LdapServerUser` – имя пользователя LDAP-сервера, `example` – доменное имя каталога, к которому относится учетная запись пользователя, `com` – имя родительского домена, в котором находится каталог.

   - `cn=<имя пользователя>, ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>` или `<имя пользователя>@<имя домена> <имя родительского домена>`, если вы хотите добавить соединение с сервером Microsoft Active Directory.

     Например, вы можете ввести имя пользователя `LdapServerUser@example.com`, где `LdapServerUser` – имя пользователя LDAP-сервера, `example.com` – доменное имя каталога, к которому относится учетная запись пользователя.

9. В блоке параметров **Параметры аутентификации** в поле **Пароль пользователя LDAP-сервера** введите пароль доступа к LDAP-серверу пользователя, указанного в поле **Имя пользователя LDAP-сервера**.

10. В блоке **Параметры поиска** в поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Secure Mail Gateway осуществляет поиск записей.

    Вводите базу поиска в формате `ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>`.

    Например, вы можете ввести базу поиска `ou=people, dc=example, dc=com`, где `people` – уровень в схеме каталога, начиная с которого Kaspersky Secure Mail Gateway 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 Secure Mail Gateway осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

11. Нажмите на кнопку **Проверить**.

    Kaspersky Secure Mail Gateway проверит подключение к LDAP-серверу с указанными вами значениями параметров соединения и аутентификации.

12. Нажмите на кнопку **Применить**.

    Окно **Параметры соединения с LDAP-сервером** закроется.

Настройка фильтров соединения с LDAP-сервером

► *Чтобы настроить фильтры соединения с LDAP-серверами, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **LDAP**.

2. В нижней части рабочей области выберите LDAP-сервер, фильтры соединения с которым вы хотите настроить.

3. В блоке параметров **Параметры LDAP-фильтров** выбранного сервера по любой ссылке откройте окно **Параметры LDAP-фильтров**.

4. В блоке параметров **Настройте LDAP-фильтры** в поле **Авторизация пользователя** задайте фильтр авторизации пользователя (например, для получения доступа пользователя к своим сообщениям в хранилище).

5. Если вы хотите установить стандартные значения фильтра авторизации пользователя, перейдите по ссылке **Установить значения по умолчанию** под полем **Авторизация пользователя**.

6. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск пользователя или группы** задайте фильтр поиска пользователей или группы пользователей.

7. Если вы хотите установить стандартные значения фильтра поиска пользователей или группы пользователей, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск пользователя или группы**.

8. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск DN пользователей и групп по адресу эл. почты** задайте фильтр поиска DN пользователей и групп, в которые они входят, по адресу электронной почты.

9. Если вы хотите установить стандартные значения фильтра поиска DN пользователей и групп, в которые они входят, по адресу электронной почты, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск DN пользователей и групп по адресу эл. почты**.

10. В блоке параметров **Настройте LDAP-фильтры** в поле **Поиск групп по DN пользователей** задайте фильтр поиска групп, членом которых является пользователь, по DN пользователя. Этот фильтр используется в случае, если не удалось определить группу пользователей с помощью фильтра, заданного в поле **Поиск DN пользователей и групп по адресу эл. почты**.

11. Если вы хотите установить стандартные значения фильтра поиска групп, членом которых является пользователь, по DN пользователя, перейдите по ссылке **Установить значения по умолчанию** под полем **Поиск групп по DN пользователей**.

12. Установите флажок **Использовать рекурсивный поиск**, если вы хотите включить поиск LDAP-записей во вложенных группах.

13. Нажмите на кнопку **ОК**.

Окно **Параметры LDAP-фильтров** закроется.

Работа с программой по протоколу SNMP

Этот раздел содержит информацию о работе с программой по протоколу SNMP, а также о настройке ловушек событий, возникающих во время работы Kaspersky Secure Mail Gateway.

В этом разделе

О получении информации о работе программы по протоколу SNMP

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

В Kaspersky Secure Mail Gateway протокол SNMP используется следующим образом:

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

По протоколу SNMP вы можете получить доступ к следующей информации о Kaspersky Secure Mail Gateway:

- общим сведениям;
- статистике работы Kaspersky Secure Mail Gateway с момента установки программы;
- данным о событиях, возникающих в ходе работы Kaspersky Secure Mail Gateway.

Например, Kaspersky Secure Mail Gateway отправляет SNMP-ловушки в следующих случаях:

- Лицензия обновлена.

  SNMP-ловушка содержит номер лицензии, тип лицензии, доступную функциональность, дату окончания срока действия лицензии.

- Льготный период действия лицензии.

  SNMP-ловушка содержит номер лицензии и количество дней до истечения льготного периода.

  SNMP-ловушка отправляется в начале действия льготного периода, далее один раз в сутки и при перезагрузке Kaspersky Secure Mail Gateway.

Доступ предоставляется только на чтение информации.

Включение и отключение использования SNMP в Kaspersky Secure Mail Gateway

► *Чтобы включить или отключить использование SNMP в работе Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **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.

Настройка параметров подключения к SNMP-серверу

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

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **SNMP**.

2. По ссылке **Адрес и порт подключения к SNMP-серверу** или **Ждать ответ от SNMP-сервера** откройте окно **Параметры подключения к SNMP-серверу**.

3. В поле **Адрес и порт подключения к SNMP-серверу** введите адрес и порт подключения к SNMP-серверу.

   Например, вы можете ввести tcp:localhost:705.

4. В поле **Ждать ответ от SNMP-сервера** 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 сек.

5. Нажмите на кнопку **ОК**.

Включение и отключение отправки SNMP-ловушек

► *Чтобы включить или отключить отправку SNMP-ловушек событий, возникающих в ходе работы Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **SNMP**.

2. Включите переключатель рядом с названием блока **Использовать SNMP**, если он выключен.

3. В блоке **Использовать SNMP** выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Отправлять SNMP-ловушки**, если вы хотите включить отправку SNMP-ловушек.

   - Выключите переключатель рядом с названием блока параметров **Отправлять SNMP-ловушки**, если вы хотите отключить отправку SNMP-ловушек.

Информация о системе для Службы технической поддержки

Вы можете сформировать архив с информацией о системе (работе Kaspersky Secure Mail Gateway) для отправки в Службу технической поддержки "Лаборатории Касперского". Архив может содержать данные о вашей организации, которые вы считаете конфиденциальными. Администратору Kaspersky Secure Mail Gateway необходимо согласовать состав отправляемого архива со Службой безопасности вашей организации.

Перед отправкой архива удалите из него все данные, которые вы считаете конфиденциальными.

В этом разделе

Создание архива с информацией о системе

► *Чтобы создать архив с информацией о системе, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Информация о системе**.

   Откроется окно **Информация о системе для Службы технической поддержки**.

3. Нажмите на кнопку **Создать**.

   Откроется окно **Создать архив с информацией о системе**.

Через несколько секунд архив с информацией о работе Kaspersky Secure Mail Gateway отобразится в списке архивов в окне **Информация о системе для Службы технической поддержки**.

Загрузка архива с информацией о системе на жесткий диск

► *Чтобы загрузить архив с информацией о системе на жесткий диск, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Информация о системе**.

   Откроется окно **Информация о системе для Службы технической поддержки**. Отобразится список архивов с информацией и системе. Если в списке нет архивов с информацией о системе, вы можете создать архив (см. раздел "Создание архива с информацией о системе" на стр. 315).

3. По ссылке с именем архива запустите процесс загрузки архива на жесткий диск.

Архив формата TGZ загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с Kaspersky Secure Mail Gateway.

Удаление архива с информацией о системе

► *Чтобы удалить один или несколько архивов с информацией о системе, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Информация о системе**.

   Откроется окно **Информация о системе для Службы технической поддержки**. Отобразится список архивов с информацией и системе.

3. Установите флажки слева от имени каждого из архивов, который вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

5. Если вы хотите полностью очистить список архивов с информацией о системе, нажмите на кнопку **Удалить все**.

Архивы с информацией о системе будут удалены.

Журнал аудита Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway регистрирует события, связанные с проверкой сообщений электронной почты, в журнале аудита.

Этот раздел содержит информацию о работе с журналом аудита Kaspersky Secure Mail Gateway, а также о том, как отсортировать, отфильтровать события в журнале аудита или выполнить поиск событий по некоторым графам таблицы по указанным вами показателям.

В этом разделе

Просмотр журнала аудита и событий в журнале аудита

► *Чтобы просмотреть журнал аудита Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.
2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.

В таблице отображаются первые 500 событий журнала аудита. Для просмотра большего количества событий используйте фильтрацию и поиск событий в журнале аудита.

► *Чтобы просмотреть событие в журнале аудита Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.
2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.
3. По ссылке с информацией о событии, которое вы хотите просмотреть, откройте окно с информацией об этом событии.
4. Если вы хотите вернуться к таблице событий, нажмите на кнопку **К журналу аудита**.

Сортировка событий в журнале аудита

► Чтобы отсортировать *события в журнале аудита*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.

3. Нажмите на кнопку  слева от названия той графы таблицы, по которой вы хотите отсортировать события. Вы можете отсортировать события по одному из следующих показателей:

   - **Время события** – дата и время, в которое произошло событие.
   - **Тип события** – тип события Kaspersky Secure Mail Gateway. Например, **Проверка сообщений**.
   - **ID субъекта** – идентификатор субъекта. Например, доменное имя сервера Kaspersky Secure Mail Gateway.
   - **Результат** – результат события Kaspersky Secure Mail Gateway. Например, **Успешно** или **Сбой**.
   - **Описание** – описание события и его результата. Например, результат проверки сообщения модулями программы или сообщение о том, что не удалось обновить базы программы.

► *Чтобы изменить порядок сортировки сообщений в очереди,*

нажмите на кнопку  или  слева от названия той графы таблицы, порядок сортировки событий которой вы хотите изменить.

Фильтрация и поиск событий по дате и времени

► Чтобы отфильтровать или найти события по *дате и времени*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.
2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.
3. По ссылке **Время события** раскройте список интервалов для поиска событий.
4. Выберите один из следующих интервалов:
   - **Прошедший час**.
   - **Прошедший день**.
   - **Прошедшая неделя**.
   - **Пользовательский**.
5. Если вы выбрали пользовательский интервал для поиска событий, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий в журнале аудита.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В рабочей области окна **Журнал аудита** отобразится таблица событий в журнале аудита, сформированная по условиям фильтра.

Если фильтр поиска сообщений не задан, в таблице отображаются первые 500 событий журнала аудита.

Фильтрация и поиск событий по типу события

► Чтобы отфильтровать или найти события по *типу события*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.
2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.
3. По ссылке **Тип события** откройте окно настройки фильтрации событий.
4. В поле **Тип события** введите несколько символов или все символы типа событий. Например, вы можете ввести **Проверка сообщений**.
5. Нажмите на кнопку **Применить**.

В рабочей области окна **Журнал аудита** отобразится таблица событий журнала аудита, сформированная по условиям фильтра.

Если фильтр поиска сообщений не задан, в таблице отображаются первые 500 событий журнала аудита.

Фильтрация и поиск событий по идентификатору субъекта

► Чтобы отфильтровать или найти события *по идентификатору субъекта*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.
2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.
3. По ссылке **ID субъекта** откройте окно настройки фильтрации событий.
4. В поле **ID субъекта** введите несколько символов или все символы идентификатора субъекта. Например, вы можете ввести доменное имя сервера Kaspersky Secure Mail Gateway.
5. Нажмите на кнопку **Применить**.

В рабочей области окна **Журнал аудита** отобразится таблица событий журнала аудита, сформированная по условиям фильтра.

Если фильтр поиска сообщений не задан, в таблице отображаются первые 500 событий журнала аудита.

Фильтрация и поиск событий по результату события

► Чтобы отфильтровать или найти события *по результат события*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.

3. По ссылке **Результат** раскройте список результатов события.

4. Выберите один из следующих результатов события:

   - **Успешно**.
   - **Сбой**.

5. Нажмите на кнопку **Применить**.

В рабочей области окна **Журнал аудита** отобразится таблица событий журнала аудита, сформированная по условиям фильтра.

Если фильтр поиска сообщений не задан, в таблице отображаются первые 500 событий журнала аудита.

Фильтрация и поиск событий по описанию события

► Чтобы отфильтровать или найти события по *описанию события*, выполните следующие действия:

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Журнал событий**.

2. В правом нижнем углу окна перейдите по ссылке **Журнал аудита**.

   Откроется окно **Журнал аудита** с таблицей событий в журнале аудита Kaspersky Secure Mail Gateway.

3. По ссылке **Описание** откройте окно настройки фильтрации событий.

4. В поле **Описание** введите несколько символов описания события.

5. Нажмите на кнопку **Применить**.

В рабочей области окна **Журнал аудита** отобразится таблица событий журнала аудита, сформированная по условиям фильтра.

Если фильтр поиска сообщений не задан, в таблице отображаются первые 500 событий журнала аудита.

Настройка даты и времени в Kaspersky Secure Mail Gateway

► *Чтобы установить дату и время в Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Дата и время**.

2. В блоке **Установка даты и времени** нажмите на значок редактирования.

3. Выберите один из следующих вариантов:

   - Если вы хотите синхронизировать время программы с хостом, выберите вариант **Синхронизировать с хостом VMware**.

   - Если вы хотите синхронизировать время с NTP-сервером, выберите вариант **Синхронизировать с NTP-сервером** и в поле **Адрес NTP-сервера** укажите адрес NTP-сервера.

     При выборе этого варианта рекомендуется отключить синхронизацию времени (см. раздел "Отключение синхронизации времени виртуальной машины и хоста" на стр. 97) виртуальной машины и хоста средствами гипервизора.

   - Если вы хотите установить дату и время вручную, выберите вариант **Установить дату и время вручную** и в полях ввода ниже введите необходимые значения даты и времени.

4. Нажмите на кнопку **ОК**.

► *Чтобы установить часовой пояс, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Дата и время**.

2. В блоке **Установка часового пояса** нажмите на значок редактирования.

3. В раскрывающемся списке **Страна** выберите нужную страну.

4. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.

5. Нажмите на кнопку **ОК**.

Хранение данных пользователей

Администратору Kaspersky Secure Mail Gateway требуется обеспечить безопасность данных, используемых программой, самостоятельно. Администратор Kaspersky Secure Mail Gateway несет ответственность за доступ к этим данным.

Kaspersky Secure Mail Gateway использует в процессе работы некоторые данные пользователей. В таблице ниже приведена информация о данных пользователей, их использовании программой, а также о том, какие пользователи программы имеют доступ к этим данным.

Таблица 2. Использование данных пользователей

Данные пользователей	Место использования	Пользователи, имеющие доступ
Статистика о сообщениях электронной почты: • Адреса отправителя и получателей. • Имена зараженных вложений.	Отчеты.	Пользователь под учетной записью HelpDesk.
Информация из сообщений электронной почты: • IP-адрес отправителя. • Адреса отправителя и получателей. • Тема сообщения. • Тело сообщения. • Служебный заголовок сообщения. • Вложения.	• Отчеты. • Хранилище. • Журналы и файлы трассировки программы. • Kaspersky Anti Targeted Attack Platform (при интеграции KSMG с KATA). Данные передаются в зашифрованном виде. • Очередь сообщений MTA. • Анти-Спам карантин. • KATA карантин. • Файлы дампов. • Оперативная память.	• Администратор для работы с программой в консоли и в режиме Technical Support Mode. • Администратор веб-интерфейса программы. • Администратор программы Kaspersky Anti Targeted Attack Platform.
Имя пользователя, пароль и IP-адрес, используемые для входа в веб-интерфейс программы.	• Журналы и файлы трассировки программы. • Файлы дампов. • Оперативная память.	• Администратор для работы с программой в консоли и в режиме Technical Support Mode. • Администратор веб-интерфейса программы.

Данные пользователей	Место использования	Пользователи, имеющие доступ
Учетные данные пользователей LDAP или Active Directory.	• Журналы и файлы трассировки программы. • Файлы дампов. • LDAP-кеш. • Оперативная память.	• Администратор для работы с программой в консоли и в режиме Technical Support Mode. • Администратор веб-интерфейса программы.
Конфигурация программы: • Черные и белые списки адресов. • Учетные записи администратора программы и пользователя HelpDesk. • Учетные записи для подключения к LDAP-серверу и прокси-серверу.	• Конфигурационные файлы программы. • Оперативная память. • Файлы дампов.	• Администратор для работы с программой в консоли и в режиме Technical Support Mode. • Администратор веб-интерфейса программы.
Данные об обновлениях: • IP-адреса, используемые компьютером при подключении к источнику обновлений. • IP-адреса источников обновлений. • Информация о загружаемом файле и скорости загрузки.	Журналы и файлы трассировки программы.	• Администратор для работы с программой в консоли и в режиме Technical Support Mode. • Администратор веб-интерфейса программы.

Устранение уязвимостей и установка критических обновлений программы

"Лаборатория Касперского" может выпускать срочные пакеты обновлений программного обеспечения, устраняющие уязвимости и ошибки. Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского".

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления программных модулей необходимо получать путем обращения в техническую поддержку АО "Лаборатория Касперского" по телефонам: +7 (495) 663-81-47, 8-800-700-88-11 или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (http://forum.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Для предотвращения потери данных в случае возникновения сбоя или ошибки в работе программы рекомендуется периодически сохранять значения параметров, копию хранилища, информацию о системе, а также журнал аудита.

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 "Обращение в Службу технической поддержки" на стр. 333).

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. 22), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

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

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

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

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2c) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2c).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Техническая поддержка через Kaspersky CompanyAccount

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

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

Портал Kaspersky CompanyAccount доступен на следующих языках:

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

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

Глоссарий

A

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

D

DKIM-проверка подлинности отправителей сообщений

Проверка цифровой подписи к сообщениям.

DMARC-проверка подлинности отправителей сообщений

Проверка, определяющая политику и действия над сообщениями по результатам SPF- и DKIM-проверок подлинности отправителей сообщений.

DNSBL

DNS blacklist или DNS blocklist. Пользовательский список DNSBL-серверов, используемый для повышения уровня обнаружения спама. На DNSBL-серверах хранятся списки IP-адресов, которые были ранее замечены в рассылке спама и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам.

K

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* (далее также "*APT*").

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.

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

S

SNMP-агент

Программный модуль сетевого управления Kaspersky Secure Mail Gateway, отслеживает информацию о работе Kaspersky Secure Mail Gateway.

SNMP-ловушка

Уведомление о событиях работы программы, отправляемое SNMP-агентом.

SPF-проверка подлинности отправителей сообщений

Сопоставление IP-адресов отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

SURBL

Spam URI Realtime Blocklists. Пользовательский список SURBL-серверов, используемый для повышения уровня обнаружения спама. На SURBL-серверах хранятся списки веб-адресов, которые были ранее замечены в теме или в теле сообщений, расцененных как спам и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам.

A

Антивирус

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения вирусов в сообщениях электронной почты и вложениях в сообщения электронной почты.

Анти-Спам

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения сообщений, которые классифицируются как спам.

Анти-Фишинг

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения сообщений, которые классифицируются как фишинг.

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

В

Виртуальная машина

Полностью изолированная программная система, которая, исполняя машинно-независимый или машинный код процессора, способна имитировать операционную систему, приложения или устройства (например, компьютер).

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

К

Контентная фильтрация

Фильтрация сообщений электронной почты по размеру сообщения, маскам имен вложенных файлов и форматам вложенных файлов. По результатам контентной фильтрации можно ограничить пересылку сообщений почтовым сервером.

П

Почтовое уведомление

Сообщение электронной почты с описанием события программы или события проверки сообщений, которое Kaspersky Secure Mail Gateway отправляет на заданные адреса электронной почты.

Р

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

Служба каталогов

Программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

У

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии.

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Х

Хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов. Резервные копии создаются перед лечением или удалением зараженных объектов.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной

организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

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

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 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":	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	http://forum.kaspersky.com

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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

Google Chrome – товарный знак Google, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Active Directory, Hyper-V, Microsoft, Internet Explorer и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

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

VMware, VMware ESXi и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Предметный указатель

A

D

L

S

T

A

B

Д

Ж

И

Л

М

О

П

Р

С

Соответствие терминов

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

Таблица 3. Таблица соответствия терминов в документации и ФСТЭК

Термин в документации	Термин в требованиях ФСТЭК
Программа	Продукт, объект оценки, программное изделие
Вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
Антивирусные базы	Базы данных признаков компьютерных вирусов (БД ПКВ)
Антивирусная проверка	Поиск КВ
Администратор веб-интерфейса	Администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

Приложение. 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 4. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Параметры / Защита	Внешние службы	Использование KSN / KPSN	• Не использовать KSN / KPSN • Использовать KPSN
		Включить SPF-проверку подлинности отправителей	Нет
		Включить DKIM-проверку подлинности отправителей	

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
		Включить DMARC-проверку подлинности отправителей	
	Антивирус	Антивирус	Вкл.
		Использовать KSN	Нет
		Использовать эвристический анализ	Вкл.
	Анти-Спам	Анти-Спам	Вкл.
		Использовать KSN	Нет
		Использовать репутационную фильтрацию	
	Анти-Спам карантин	Анти-Спам карантин	Вкл.
	Анти-Фишинг	Анти-Фишинг	Выкл.
	Контентная фильтрация	Контентная фильтрация	
	Защита KATA	Защита KATA	**Вкл.**, если вы используете интеграцию с Kaspersky Anti Targeted Attack Platform

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Правила / Изменить правило для правила **Default**	**Общие параметры правила**	**Режим работы правила**	**Использовать параметры модулей проверки**
	Анти-Спам	**Проверка на спам**	**Вкл.**
	Антивирус	**Антивирусная проверка**	**Вкл.**
		Вредоносные объекты	**Лечить**
		Ошибки проверки объектов	**Пропустить**
		Зашифрованные объекты	
		Обрабатывать вложения с макросами	**Выкл.**
		Макрос во вложении	**Удалить вложение**
	Защита KATA	**Защита KATA**	**Вкл.**, если вы используете интеграцию с Kaspersky Anti Targeted Attack Platform
	Анти-Фишинг	**Проверка на фишинг**	**Выкл.**
	Контентная фильтрация	**Проверка сообщений**	**Выкл.**

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
	Уведомления	Все параметры блока параметров	Не отправлять
	Проверка подлинности отправителей сообщений	Проверка подлинности отправителей сообщений	Выкл.