KASPERSKY lab

Kaspersky Security 8 для Linux Mail Server

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 8.0.2.16

Уважаемый пользователь!

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

Дата редакции документа: 16.11.2017

Обозначение документа: 643.46856491.00061-04 90 01

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

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации (далее также «руководство») программного изделия «Kaspersky Security 8 для Linux Mail Server» (далее также «Kaspersky Security», «программа»).

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки". 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.

Также из этого документа вы можете узнать об источниках информации о программе и способах получения технической поддержки.

Документ адресован специалистам, которые осуществляют установку и администрирование Kaspersky Security, а также специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security.

В этом разделе

В этом документе

В руководство включены следующие разделы:

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

О программе (см. стр. 25)

Этот раздел содержит краткий обзор и функциональные возможности решения Kaspersky Security 8 для Linux Mail Server. Из раздела вы узнаете о режимах работы Kaspersky Security 8 для Linux Mail Server.

Требования (см. стр. 37)

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

Интерфейс Kaspersky Security 8 для Linux Mail Server (см. стр. 42)

Этот раздел содержит описание интерфейса программы.

Лицензирование программы (см. стр. 44)

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

Состояние защиты почтового сервера

Этот раздел содержит информацию о том, как проверить уровень защиты почтового сервера и наличие проблем в защите.

Обеспечение безопасности данных в разных режимах работы программы (см. стр. 60)

Этот раздел содержит информацию об обеспечении безопасности данных в разных режимах работы программы.

Подготовка к установке программы (см. стр. 62)

Этот раздел содержит информацию о подготовке к установке программы.

Установка программы (см. стр. 64)

Этот раздел содержит информацию об установке программы.

Обновление предыдущей версии программы (см. стр. 73)

Этот раздел содержит информацию об обновлении предыдущей версии программы.

Подготовка Kaspersky Security 8 для Linux Mail Server к работе (см. стр. 81)

Этот раздел содержит информацию о подготовке Kaspersky Security 8 для Linux Mail Server к работе.

Подготовка сетевой инфраструктуры вашей организации к работе Kaspersky Security 8 для Linux Mail Server (см. стр. 108)

Этот раздел содержит информацию о сетевой инфраструктуры вашей организации к работе Kaspersky Security 8 для Linux Mail Server.

Запуск и остановка программы (см. стр. 110)

Этот раздел содержит информацию о запуске и остановке программы.

Подготовка веб-интерфейса Kaspersky Security 8 для Linux Mail Server к работе (см. стр. 111)

Этот раздел содержит информацию о подготовке веб-интерфейса Kaspersky Security 8 для Linux Mail Server к работе.

Начало работы в веб-интерфейсе программы (см. стр. 125)

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

Интеграция Kaspersky Security 8 для Linux Mail Server с почтовыми серверами и интерфейсом Amavis вручную (см. стр. 126)

Этот раздел содержит информацию об интеграции Kaspersky Security 8 для Linux Mail Server с почтовыми серверами и интерфейсом Amavis вручную.

Мониторинг Kaspersky Security 8 для Linux Mail Server (см. стр. 156)

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

Работа с правилами обработки сообщений (см. стр. 158)

Этот раздел содержит информацию о правилах обработки сообщений, настройке их параметров и настройке параметров Kaspersky Security 8 для Linux Mail Server для каждого правила обработки сообщений.

Хранилище (см. стр. 177)

Этот раздел содержит информацию о хранилище и работе с ним.

Очередь сообщений Kaspersky Security 8 для Linux Mail Server (см. стр. 188)

Этот раздел содержит информацию об очередях сообщений Kaspersky Security 8 для Linux Mail Server.

Отчеты о работе Kaspersky Security 8 для Linux Mail Server (см. стр. 195)

Этот раздел содержит информацию о том, как создавать и просматривать отчеты о работе Kaspersky Security 8 для Linux Mail Server.

Общие параметры Kaspersky Security 8 для Linux Mail Server (см. стр. 335)

Этот раздел содержит информацию об общих параметрах программы.

Обновление баз Kaspersky Security 8 для Linux Mail Server (см. стр. 202)

Этот раздел содержит информацию об обновлении антивирусных баз.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network (см. стр. 210)

Этот раздел содержит информацию об участии в Kaspersky Security Network и использовании Kaspersky Private Security Network.

Проверка подлинности отправителей сообщений (см. стр. 213)

Этот раздел содержит информацию о технологиях проверки подлинности отправителей сообщений, используемых в Kaspersky Security 8 для Linux Mail Server, и настройке параметров проверки подлинности отправителей сообщений.

Антивирусная защита сообщений (см. стр. 234)

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

Защита KATA и интеграция Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform (см. стр. 253)

Этот раздел содержит информацию о защите Kaspersky Anti Targeted Attack Platform и об интеграции Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform.

Черные и белые списки адресов (см. стр. 268)

Этот раздел содержит информацию о черных и белых списках адресов электронной почты, которые можно создавать и редактировать в Kaspersky Security 8 для Linux Mail Server.

Соединение с LDAP-сервером (см. стр. 275)

Этот раздел содержит информацию о соединении Kaspersky Security 8 для Linux Mail Server с LDAP-сервером и о настройке параметров и фильтров соединения с LDAP-сервером.

Работа с программой по протоколу SNMP (см. стр. 288)

Этот раздел содержит информацию о работе с программой по протоколу SNMP, а также о настройке ловушек событий, возникающих во время работы Kaspersky Security 8 для Linux Mail Server.

Почтовые уведомления Kaspersky Security 8 для Linux Mail Server (см. стр. 292)

Этот раздел содержит информацию о почтовых уведомлениях Kaspersky Security 8 для Linux Mail Server и настройке их параметров.

Ограничение трафика Kaspersky Security 8 для Linux Mail Server (см. стр. 34)

Этот раздел содержит информацию об ограничении трафика Kaspersky Security 8 для Linux Mail Server.

Примечания и предупреждения Kaspersky Security 8 для Linux Mail Server (см. стр. 308)

Этот раздел содержит информацию о примечаниях и предупреждениях Kaspersky Security 8 для Linux Mail Server и настройке их параметров.

Журнал аудита Kaspersky Security 8 для Linux Mail Server (см. стр. 316)

Этот раздел содержит информацию о работе с журналом аудита Kaspersky Security 8 для Linux Mail Server.

Информация о системе для Службы технической поддержки (см. стр. 323)

Этот раздел содержит информацию о том, как сформировать архив с информацией о Kaspersky Security 8 для Linux Mail Server для отправки в Службу технической поддержки "Лаборатории Касперского".

Журнал трассировки (см. стр. 350)

Этот раздел содержит информацию о журнале трассировки.

Управление программой через Kaspersky Security Center (см. стр. 356)

Этот раздел содержит информацию об управлении программой через Kaspersky Security Center.

Публикация событий программы в SIEM-систему (см. стр. 367)

Этот раздел содержит информацию о публикации событий программы в SIEM-систему.

Действия после сбоя или неустранимой ошибки в работе программы (см. стр. 394)

Этот раздел содержит информацию о действиях, которые необходимо выполнить после возникновения сбоя или неустранимой ошибки в работе программы.

Обращение в Службу технической поддержки (см. стр. 396)

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

Приложения (см. стр. 400)

Этот раздел содержит приложения к документу.

Глоссарий

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

АО "Лаборатория Касперского" (см. стр. 417)

Этот раздел содержит информацию об АО "Лаборатория Касперского".

Информация о стороннем коде (см. стр. 419)

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. 427)

Этот раздел содержит таблицу соответствия терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

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.

Приведенные ниже источники информации о программе созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

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

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

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 396).

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

Страница Kaspersky Security 8 для Linux Mail Server на веб-сайте "Лаборатории Касперского"

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

Страница Kaspersky Security 8 для Linux Mail Server содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Security 8 для Linux Mail Server в Базе знаний

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

На странице Kaspersky Security в Базе знаний (http://support.kaspersky.ru/klms8) 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 Security 8 для Linux Mail Server, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка Kaspersky Security 8 для Linux Mail Server (справка веб-интерфейса)

С помощью веб-интерфейса вы можете управлять Kaspersky Security 8 для Linux Mail Server через браузер. Справка содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя через веб-интерфейс Kaspersky Security 8 для Linux Mail Server (далее также "веб-интерфейс").

Форум

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

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

О программе

Программное изделие " Kaspersky Security 8 для Linux Mail Server " (далее также "Kaspersky Security", "программа") представляет собой средство антивирусной защиты типа "Б" второго класса защиты и предназначено для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Security, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация.

В этом разделе приводится информация о режимах работы Kaspersky Security 8 для Linux Mail Server.

В этом разделе

О действиях программы над объектами

В зависимости от статуса, присвоенного сообщению по результатам антивирусной проверки, проверки на спам и контентной фильтрации, программа Kaspersky Security 8 для Linux Mail Server выполняет действия над сообщениями и входящими в их состав объектами. Результат проверки программа записывает в журнал событий.

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

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

- `Skip` – доставить сообщение получателю, не изменяя его.
- `Reject` – не доставлять сообщение получателю. Если выбрано это действие, почтовый сервер – отправитель сообщения получит в качестве кода возврата сообщение об ошибке при отправке сообщения. Получателю сообщение доставлено не будет.

- `DeleteMessage` – удалить сообщение. Если выбрано это действие, почтовый сервер-отправитель сообщения получит уведомление о доставке сообщения, однако получателю сообщение доставлено не будет.

- `DeleteAttachment` – удалить вложение (применяется только по результатам антивирусной проверки).

- `Cure` – лечить зараженный объект (применяется только по результатам антивирусной проверки). Если выбрано это действие, программа пытается вылечить зараженный объект. Если лечение невозможно, к объекту применяется действие `Reject`, `DeleteMessage` или `DeleteAttachment`, заданное в параметрах правила. Если администратор не задал действие в параметрах правила, программа выполняет действие `DeleteAttachment`.

О задачах программы

Задачи Kaspersky Security 8 для Linux Mail Server реализуют часть функциональности программы. Например, задача обновления антивирусных баз UpdaterAVS (далее также "задачи обновления антивирусных баз") и задача обновления баз Анти-Спама UpdaterASP (далее также "задача обновления баз Анти-Спама") выполняют загрузку и установку обновлений антивирусных баз и баз Анти-Спама; задачи создания отчетов по расписанию DailyReport, WeeklyReport и MonthlyReport формируют отчеты о работе программы за день, за неделю и за месяц; задача уведомлений Notifier формирует уведомления о событиях, возникающих во время работы программы.

В состав Kaspersky Security 8 для Linux Mail Server входят следующие задачи:

- Auth (ID=1).

- Backup (ID=2).

- ScanLogic (ID=3).

- Facade (ID=4).

- AvServer (ID=5).

- AspServer (ID=6).

- EventManager (ID=7).
- Licenser (ID=8).
- Notifier (ID=9).
- Statistics (ID=10).
- Updater (ID=11).
- AspMoebius (ID=13).
- AspQuarantine (ID=14).
- SmtpSender (ID=15).
- Snmp (ID=16).
- DailyReport (ID=17).
- WeeklyReport (ID=18).
- MonthlyReport (ID=19).
- EventLogger (ID=20).
- ScanServer (ID=21).
- KLRDS (ID=22).
- Ksn (ID=23).

Большинство задач являются системными и не предназначены для настройки администратором.

Задачи Kaspersky Security 8 для Linux Mail Server могут находиться в одном из следующих статусов выполнения:

- *Started* – выполняется.
- *Starting* – запускается.
- *Stopped* – остановлена.

- *Failed* – завершена с ошибкой.

Об учетных записях пользователей программы

В Kaspersky Security 8 для Linux Mail Server предусмотрены следующие учетные записи:

- Учетная запись администратора веб-интерфейса (см. раздел "Шаг 9. Назначение пароля доступа к веб-интерфейсу программы" на стр. 86) Administrator для работы в веб-интерфейсе программы.
- Учетная запись HelpDesk (см. раздел "Об учетной записи HelpDesk" на стр. 340) для получения ограниченного доступа к параметрам программы.
- Учетная запись пользователя программы.

Учетная запись администратора веб-интерфейса программы Administrator создается при подготовке программы к работе и предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Security 8 для Linux Mail Server 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.

Учетные записи пользователей программы предназначены для сотрудников вашей организации, пользующихся адресами электронной почты вашей организации.

Пользователю программы доступны следующие операции в веб-интерфейсе Kaspersky Security 8 для Linux Mail Server:

- Изменение пользовательских черных и белых списков адресов (см. раздел "О черных и белых списках адресов" на стр. 268).
- Поиск копий сообщений в хранилище (на стр. 180).

- Просмотр информации о сообщениях в хранилище (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 182).
- Доставка сообщения из хранилища получателю (см. раздел "Доставка сообщения из Хранилища получателям" на стр. 184).

  Значение этого параметра задается в параметрах хранилища (см. раздел "Настройка параметров Хранилища" на стр. 178).

Основные компоненты программы

В состав Kaspersky Security 8 для Linux Mail Server входят следующие компоненты:

- *Фильтр* – компонент, получающий и передающий сообщения электронной почты от почтового сервера программе и обратно. В состав Kaspersky Security 8 для Linux Mail Server входят несколько фильтров, использующихся в зависимости от почтового сервера и типа его интеграции с Kaspersky Security 8 для Linux Mail Server:
  - Milter.
  - Smtp-proxy.
  - Dlfunc.
  - Qmail-queue binary.
- Klms-watchdog – основной компонент обработки сообщений электронной почты. Состоит из следующих модулей:
  - Scan Logic – модуль управления проверкой сообщений (далее также – "модуль Scan Logic"), включает в себя MIME-разборщик и контент-фильтр.
  - AV-engine – модуль антивирусной проверки (далее "модуль Антивирус").
  - AS-engine – модуль проверки сообщений на спам (далее "модуль Анти-Спам").
  - Updater – модуль обновления антивирусных баз, а также баз Анти-Спама.

- Backup – модуль резервного хранилища, обеспечивает возможность восстановления сообщений в неизменном виде.
- Auth – модуль, обеспечивающий взаимодействие программы с системами учета пользователей.
- Statistics – модуль статистики, обеспечивает получение статистической информации о работе программы.
- Settings-manager – модуль хранения параметров задач и параметров правил обработки сообщений в базе данных, осуществляет экспорт и импорт этих параметров и оповещает другие модули об их изменении.
- Facade – модуль, обеспечивающий взаимодействие программы с утилитами и системами администрирования.
- Licenser – модуль работы с ключами.
- Notifier – модуль уведомлений, обеспечивает формирование сообщений с важными для администратора уведомлениями.
- Event_manager – модуль, обеспечивающий доставку оповещений о событиях другим модулями программы.
- Smtp_sender – модуль отправки уведомлений.
- Task manager – модуль, управляющий порядком запуска и остановки остальных модулей.

- Klms-postgres – база данных, в которой хранятся параметры программы, статистика, накапливаемая для отчетов, и метаинформация об объектах резервного хранилища. Метаинформация об объектах резервного хранилища может храниться во внешней по отношению к программе базе.

Алгоритм обработки сообщений электронной почты

Программа обрабатывает сообщения электронной почты по следующему алгоритму:

1. Модуль управления проверкой сообщений Scan Logic определяет, каким правилам обработки сообщений принадлежит сообщение на основании комбинации адресов "отправитель-получатель", и выбирает правило с наивысшим приоритетом. Если не обнаружено ни одного правила, содержащего эту комбинацию адресов, программа обрабатывает сообщение в соответствии с параметрами, заданными для предустановленного правила Default.

2. Если сообщение адресовано нескольким получателям, адреса которых принадлежат разным правилам, перед дальнейшей обработкой программа создает несколько виртуальных копий сообщений в соответствии с количеством правил. Для каждой копии программа применяет то правило обработки сообщений, к которому отнесен адрес получателя.

3. Дальнейшие действия программы зависят от параметров выбранного правила обработки сообщений.

    - Если в параметрах правила задана проверка сообщений на спам, модуль Scan Logic передает сообщение электронной почты на проверку модулю Анти-Спам.

      Модуль Анти-Спам проверяет сообщение и присваивает ему один из статусов проверки на спам. Информация о присвоенном статусе содержится в специальном информационном X-заголовке X-KLMS-AntiSpam-Status (см. раздел "Об информационных X-заголовках" на стр. 35), который модуль Scan Logic добавляет к сообщению после обработки. Кроме того, по результатам проверки модуль Scan Logic добавляет метку, содержащую статус, в начало темы сообщения.

    - Если в параметрах правила задана проверка сообщений на наличие фишинга, модуль Scan Logic передает сообщение электронной почты на проверку модулю Анти-Фишинг.

Модуль Анти-Фишинг проверяет сообщение и присваивает ему один из статусов проверки на спам. Информация о присвоенном статусе содержится в специальном информационном X-заголовке X-KLMS-AntiPhishing (см. раздел "Об информационных X-заголовках" на стр. 35), который модуль Scan Logic добавляет к сообщению после обработки. Кроме того, по результатам проверки модуль Scan Logic добавляет метку, содержащую статус, в начало темы сообщения.

- Если в параметрах правила задана контентная фильтрация сообщений, модуль Scan Logic осуществляет контентную фильтрацию по размеру сообщения, а также по имени и формату вложения.

  По результатам контентной фильтрации модуль Scan Logic присваивает сообщению один из статусов контентной фильтрации сообщений.

- Если в параметрах правила задана антивирусная проверка сообщений, модуль Scan Logic передает сообщение электронной почты на проверку модулю Антивирус.

  Встроенный в модуль Антивирус анализатор формата сообщений электронной почты (MIME, RFC2822, UUE) производит разбор проверяемого сообщения на объекты: тело сообщения, вложения и другие. Каждый из полученных объектов отправляется на проверку Антивирусом.

  Антивирус проверяет сообщение сначала как единый объект, а затем по частям и присваивает сообщению один из статусов антивирусной проверки. По результатам проверки модуль Scan Logic добавляет метку, содержащую статус, в начало темы сообщения.

4. В зависимости от полученного статуса программа выполняет над сообщениями действия, заданные в параметрах правила, по которому программа должна обрабатывать сообщение.

Ограничение трафика Kaspersky Security 8 для Linux Mail Server

► *Чтобы перевести Kaspersky Security 8 для Linux Mail Server в режим* ограниченного трафика*, 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. Выберите **Не использовать KSN / KPSN**.

4. Нажмите на кнопку **Применить**.

   Окно **Использование KSN / KPSN** закроется.

5. В блоке **Внешние службы** по ссылке **Разрешить подключение к DNS-серверу** откройте окно **Внешние службы**.

6. В списке справа от названия параметра **Разрешить подключение к DNS-серверу** выберите **Нет**.

7. Нажмите на кнопку **Применить**.

   Окно **Внешние службы** закроется.

8. 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**.

9. В блоке параметров **Внешние службы** в раскрывающемся списке **Использовать службу Enforced Anti-Spam Updates** выберите **Нет**.

10. Нажмите на кнопку **Применить**.

    Окно **Параметры модуля Анти-Спам** закроется.

11. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

12. В блоке **Параметры обновления баз программы** по ссылке **Источник обновлений** откройте окно **Параметры обновления баз программы**.

13. В блоке параметров **Источник обновлений** выберите **Kaspersky Security Center**.

14. Снимите флажок **При недоступности использовать серверы "Лаборатории Касперского"**.

15. Нажмите на кнопку **ОК**.

    Окно **Параметры обновления баз программы** закроется.

Kaspersky Security 8 для Linux Mail Server начнет работать в режиме ограниченного трафика.

Об информационных X-заголовках

По результатам проверки сообщения модуль управления проверкой сообщений Scan Logic добавляет к заголовку сообщения специальные информационные X-заголовки, например:

- X-KLMS-Rule-ID: 1 – список идентификаторов правил обработки сообщений.
- X-KLMS-Message-Action: attachment removed, AntiVirus – действие программы над сообщением.
- X-KLMS-AntiVirus: Kaspersky Security 8.0 for Linux Mail Server, version 8.0.1.517, bases: 2013/11/19 06:41:00 – информация о дате выпуска антивирусных баз.
- X-KLMS-AntiSpam-Method: none – сработавший метод распознавания спама.
- X-KLMS-AntiSpam-Rate: 0 – рейтинг, присвоенный сообщению модулем Анти-Спам.
- X-KLMS-AntiSpam-Status: not_detected – статус, присвоенный сообщению модулем Анти-Спам по результатам проверки на спам.

- X-KLMS-AntiSpam-Envelope-From: someemail@example.com – отправитель сообщения.
- X-KLMS-AntiPhishing: Clean, 2013/11/13 18:22:56 – общий заголовок для сообщений, обработанных модулем Анти-Фишинг.

Поддержка интернационализованных адресов электронной почты

Интернационализованный адрес электронной почты – это адрес, который содержит символы национальных (нелатинских) алфавитов, например:

- кириллица (домен .рф);
- китайский традиционный (домен .中國);
- китайский упрощенный (домен .中国).

Программа обрабатывает сообщения с интернационализованными адресами электронной почты согласно тем же правилам, которые применяются ко всем остальным сообщениям. Кроме того, интернационализованные адреса могут быть использованы для отправки уведомлений и отчетов.

Проверка совпадения как локальной, так и доменной части интернационализованных адресов с адресами и регулярными выражениями, указанными в правилах обработки, производится без учета регистра.

При перемещении сообщения с интернационализованным адресом в очередь сообщений или в хранилище программа сохраняет значения заголовков От и Кому в следующих форматах:

- Оригинальный.

  Интернационализованный адрес сохраняется без изменений.

- Нормализованный.

  Перед сохранением адреса выполняются следующие преобразования:

- преобразование доменной части адреса из Punycode в Unicode;
- приведение адреса к каноническому виду, в котором регистр символов не учитывается (Unicode Case Folding);
- приведение символов с одинаковым начертанием к одинаковому бинарному представлению (Unicode Normalization).

Значения заголовков Тема и ID сохраняются только в нормализованном формате.

При вычислении статистики в отчете программа использует нормализованную форму адресов отправителя и получателей сообщения. При этом интернационализованные адреса, записанные символами разного регистра и / или с использованием Punycode, учитываются как один и тот же адрес.

Требования

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

В этом разделе

Аппаратные и программные требования

Kaspersky Security 8 для Linux Mail Server имеет следующие аппаратные и программные требования:

- Минимальные аппаратные требования:
  - процессор Intel® Xeon® 3040 или Intel Core™ 2 Duo 1,86 ГГц;

- 2 ГБ оперативной памяти;
- раздел подкачки объемом 4 ГБ;
- 4 ГБ на жестком диске для установки программы и хранения временных файлов и файлов журналов.

- Программные требования:
  - Одна из следующих 64-битных операционных систем:
    - Red Hat Enterprise Linux® 7.3 Server.
    - SUSE Linux Enterprise Server 12 SP2.
    - CentOS-6.9.
    - CentOS-7.3.
    - Ubuntu Server 14.04.2 LTS.
    - Ubuntu Server 16.04 LTS.
    - Debian GNU / Linux 8.8, 9.0.
    - FreeBSD™ 11;
    - Astra Linux SE 1.5 — только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды;
    - ALT Linux 7.0.5.
  - Наличие следующих пакетов 32-битных библиотек для 64-битных операционных систем:
    - ia32-libs для Debian и Ubuntu;
    - libgcc.i686, glibc.i686 для Red Hat Enterprise Linux и CentOS;
    - libgcc-32bit, glibc-32bit для SUSE;
    - lib32 для FreeBSD 64bit;
    - compat9x для FreeBSD 10;

- i586-glibc-utils-2.17-alt5.M70C.11, i586-libgcc1-4.7.2-alt7.M70C.5, i586-glibc-pthread-2.17-alt5.M70C.11, i586-glibc-core-2.17-alt5.M70C.11 для ALT Linux 7.0.5.

- Для работы Kaspersky Security 8 для Linux Mail Server требуется язык программирования Perl 5 версии 5.8.5.

Kaspersky Security 8 для Linux Mail Server поддерживает интеграцию со следующими почтовыми серверами:

- Exim-4.86.
- Postfix-2.6.
- Sendmail-8.14.
- Qmail-1.06.

Для работы веб-интерфейса Kaspersky Security 8 для Linux Mail Server на компьютере должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ 53.
- Microsoft Internet Explorer® 11.
- Google Chrome™ 58.

Для работы веб-интерфейса Kaspersky Security 8 для Linux Mail Server на компьютере с установленным веб-интерфейсом должен быть установлен веб-сервер Apache 2.4.

Указания по эксплуатации и требования к среде

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

2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".

3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.

4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).

5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.

6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.

7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.

8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.

9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.

10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).

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

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

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

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

15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.

16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Интерфейс Kaspersky Security 8 для Linux Mail Server

Работа с Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server

В дереве консоли управления отображаются разделы Kaspersky Security 8 для Linux Mail Server и подразделы функциональных компонентов Kaspersky Security 8 для Linux Mail Server.

В дереве консоли управления Kaspersky Security 8 для Linux Mail Server отображаются следующие разделы:

- **Мониторинг** – раздел, содержащий данные мониторинга Kaspersky Security 8 для Linux Mail Server.
- **Правила** – раздел, содержащий правила обработки сообщений.
- **Хранилище** – раздел, содержащий информацию о хранилище сообщений и фильтр поиска сообщений в хранилище.
- **Очередь сообщений** – раздел, содержащий информацию о работе с очередями сообщений в KATA-карантине и Анти-Спам карантине, а также о том, как отсортировать, отфильтровать, принудительно отправить сообщения или выполнить поиск сообщений в очереди.
- **Отчеты** – раздел, содержащий отчеты о работе почтового сервера.
- **Параметры** – раздел, в котором вы можете настроить параметры Kaspersky Security 8 для Linux Mail Server.

Рабочая область окна веб-интерфейса Kaspersky Security 8 для Linux Mail Server

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 Security 8 для Linux Mail Server, в рабочей области главного окна параметры сгруппированы в **блоки параметров**.

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 Security 8 для Linux Mail Server.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

Предусмотрены следующие типы лицензий:

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

Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server). Чтобы продолжить использование Kaspersky Security 8 для Linux Mail Server 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.

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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server или после заказа пробной версии Kaspersky Security 8 для Linux Mail Server.

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

О предоставлении данных

Для работы программы используются данные, на отправку и обработку которых требуется согласие администратора Kaspersky Security 8 для Linux Mail Server.

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. 45) 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 Security 8 для Linux Mail Server:

- 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 событий программы (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 Security 8 для Linux Mail Server будет использовать IP-адреса и FQDN-имена доменов, обращающихся к этим серверам.

Работа с программой из консоли управления Kaspersky Security 8 для Linux Mail Server сервера, на котором установлен Kaspersky Security 8 для Linux Mail Server, под учетной записью суперпользователя позволяет управлять параметрами дампа. Дамп формируется при сбоях программы и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные, включая фрагменты содержания писем и анализируемых файлов.

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

По умолчанию формирование дампа в Kaspersky Security 8 для Linux Mail Server отключено.

Данные очереди сообщений электронной почты, обрабатываемой Kaspersky Security 8 для Linux Mail Server в данный момент, а также учетных записей пользователей LDAP-сервера и прокси-сервера хранятся в Kaspersky Security 8 для Linux Mail Server в незашифрованном виде.

Доступ к этим данным может быть осуществлен из консоли управления сервера, на котором установлен Kaspersky Security 8 для Linux Mail Server, под учетной записью суперпользователя.

Администратору Kaspersky Security 8 для Linux Mail Server необходимо обеспечить безопасность этих данных самостоятельно.

Администратор Kaspersky Security 8 для Linux Mail Server несет ответственность за доступ к данной информации.

Данные о событиях и процессах работы Kaspersky Security 8 для Linux Mail Server записываются и хранятся в следующих журналах Kaspersky Security 8 для Linux Mail Server:

- журнале событий;
- 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:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Лицензирование**.
2. 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server в соответствии с лицензией

В Kaspersky Security 8 для Linux Mail Server предусмотрены различные режимы работы в зависимости от лицензии.

Без лицензии

В этом режиме Kaspersky Security 8 для Linux Mail Server работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите активный ключ.

В режиме **Без лицензии** Kaspersky Security 8 для Linux Mail Server не выполняет проверку сообщений электронной почты.

Пробная лицензия

В этом режиме Kaspersky Security 8 для Linux Mail Server выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа пробной лицензии, Kaspersky Security 8 для Linux Mail Server прекращает проверку сообщений электронной почты и обновление баз.

Для возобновления работы Kaspersky Security 8 для Linux Mail Server необходимо установить ключ коммерческой лицензии.

Коммерческая лицензия

В этом режиме Kaspersky Security 8 для Linux Mail Server выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа коммерческой лицензии Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server возобновит проверку сообщений электронной почты в соответствии с действующей лицензией.

После отключения проверки сообщений электронной почты в Kaspersky Security 8 для Linux Mail Server продолжает работать почтовый агент MTA, соединение с LDAP-сервером, журнал событий, отчеты о работе Kaspersky Security 8 для Linux Mail Server, а также остается доступно управление всеми параметрами Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server (см. раздел "Настройка адресов электронной почты администратора" на стр. 338).

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.

Состояние защиты почтового сервера

В разделе **Мониторинг** главного окна веб-интерфейса Kaspersky Security 8 для Linux Mail Server 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.

Обеспечение безопасности данных в разных режимах работы программы

Рекомендуемая конфигурация Kaspersky Security 8 для Linux Mail Server – конфигурация, при которой все компоненты решения (Kaspersky Security 8 для Linux Mail Server, веб-интерфейс, база PostgreSQL и хранилище) находятся на одном сервере с почтовым агентом MTA. Данные между почтовым агентом MTA и Kaspersky Security 8 для Linux Mail Server передаются в открытом незашифрованном виде.

Если хотя бы один из компонентов Kaspersky Security 8 для Linux Mail Server находится на сервере, отдельном от Kaspersky Security 8 для Linux Mail Server, администратору сети вашей организации необходимо предпринять дополнительные действия по обеспечению безопасности ваших данных, к которым относятся сообщения электронной почты. Например, вы можете физически изолировать сетевое соединение между сервером с MTA и сервером с Kaspersky Security 8 для Linux Mail Server.

Если на сервере, отдельном от MTA и остальных компонентов Kaspersky Security 8 для Linux Mail Server, находится хранилище, по сетевому соединению могут передаваться сообщения электронной почты. Администратору сети вашей организации необходимо обеспечить безопасность соединения между сервером с Kaspersky Security 8 для Linux Mail Server и сервером, на котором находится хранилище. Вы можете обеспечить безопасность соединения одним из следующих способов:

- Физически изолировать сетевое соединение.
- В правилах маршрутизатора ограничить доступ к локальной сети с Kaspersky Security 8 для Linux Mail Server и хранилищем.
- Использовать сетевую файловую систему с шифрованием передаваемых данных. Например, вы можете использовать файловые системы NFS 4 или SMB FS.

Если на сервере, отдельном от MTA и остальных компонентов Kaspersky Security 8 для Linux Mail Server, находится база PostgreSQL, администратору сети вашей организации необходимо обеспечить безопасность соединения между сервером с Kaspersky Security 8

для Linux Mail Server и сервером, на котором находится база PostgreSQL. Вы можете обеспечить безопасность соединения одним из следующих способов:

- Физически изолировать сетевое соединение.
- Настроить SSL-шифрование соединения между сервером с Kaspersky Security 8 для Linux Mail Server и сервером, на котором находится база PostgreSQL.

Подготовка к установке программы

Перед установкой пакета Kaspersky Security 8 для Linux Mail Server вам нужно выполнить следующие действия:

- убедиться, что ваш компьютер удовлетворяет требованиям, приведенным в разделе "Аппаратные и программные требования", а для операционной системы и программных средств, необходимых для установки, установлены самые последние пакеты обновлений, выпущенные производителями;
- загрузить пакет установки Kaspersky Security 8 для Linux Mail Server формата TXZ, DEB или RPM на ваш компьютер;
- установить пакет glibc (для 64-битных операционных систем требуется 32-битная версия glibc).

Перед установкой Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы Debian или Ubuntu, требуется выполнить следующую команду: `# locale-gen en_US.UTF-8`.

Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server требуется, только если вы хотите управлять программой через браузер.

Перед установкой пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server вам нужно выполнить следующее:

- убедиться, что ваш компьютер удовлетворяет аппаратным и программным требованиям;
- загрузить пакет установки веб-интерфейса Kaspersky Security 8 для Linux Mail Server формата DEB или RPM на ваш компьютер (установка пакета веб-интерфейса требуется только если вы хотите управлять программой через браузер);
- установить следующие модули Apache: mod_ssl, mod_include, mod_dir и mod_expires (если они не установлены) и включить их с помощью команды: `# a2enmod` (если они не включены):

```
# a2enmod ssl

# a2enmod include

# a2enmod dir

# a2enmod expires
```

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

Например, если необходимо установить в Debian GNU / Linux 6.0 пакет русской локализации `klms-l10n-ru_<номер_версии>_i386.deb`, то перед установкой пакета убедитесь, что в системе присутствует поддержка русского языка.

► *Чтобы просмотреть список поддерживаемых языков, выполните следующую команду:*

```
# locale -a
```

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

► *Чтобы установить русский язык, выполните следующую команду:*

```
# dpkg-reconfigure locales
```

Теперь вы можете перейти к установке пакета `klms-l10n-ru_<номер_версии>_i386.deb`

Аналогичные действия необходимо производить для любой локализации.

Установка программы

Установка программы включает несколько этапов:

1. Установка пакета Kaspersky Security 8 для Linux Mail Server (на стр. 65).

   Запускать процесс установки пакета Kaspersky Security 8 для Linux Mail Server требуется с правами учетной записи `root`.

2. Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server на одном компьютере с Kaspersky Security 8 для Linux Mail Server" на стр. 67).

   Установка этого пакета требуется, если вы хотите управлять программой через браузер. Пакет веб-интерфейса Kaspersky Security 8 для Linux Mail Server может быть установлен на одном компьютере с пакетом Kaspersky Security 8 для Linux Mail Server или на отдельном компьютере.

В этом разделе

Установка пакета Kaspersky Security 8 для Linux Mail Server

Kaspersky Security 8 для Linux Mail Server распространяется в пакетах форматов TXZ, DEB и RPM.

- *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата RPM, выполните следующую команду:*

  ```
  # rpm -i klms-<номер_версии>.i386.rpm
  ```

- *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

  ```
  # dpkg --force-architecture -i klms_<номер_версии>_i386.deb
  ```

- *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата TXZ на 64-битную операционную систему FreeBSD 11, выполните следующую команду:*

  ```
  # pkg add -f klms-<номер_версии>.txz
  ```

После выполнения команды программа устанавливается автоматически.

После установки пакета программы установите пакет локализации Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка пакета локализации Kaspersky Security 8 для Linux Mail Server" на стр. 65).

Установка пакета локализации Kaspersky Security 8 для Linux Mail Server

Установка пакета английской локализации не требуется.

Установка пакета локализации Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы Linux

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

```
# rpm -i klms_xx-<номер_версии>.noarch.rpm
```

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

► *Чтобы установить пакет локализации из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

```
# dpkg -i klms-110n-xx_<номер_версии>_all.deb
```

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

Установка пакета локализации Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы FreeBSD

► *Чтобы установить пакет локализации формата TXZ на 64-битную операционную систему FreeBSD 11, выполните следующую команду:*

```
# pkg add -f klms_xx-<номер_версии>.txz
```

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

Установка пакета локализации Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы ALT Linux 7.0.5

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

```
# rpm -i klms_xx-<номер_версии>.noarch.rpm
```

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

По умолчанию пакет устанавливает конфигурационный файл в директорию /etc/httpd/conf.d/klmsui_ru.config. Необходимо вручную переписать конфигурационный файл в директорию /etc/httpd2/conf, после чего перезапустить Apache.

Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server на одном компьютере с Kaspersky Security 8 для Linux Mail Server

Веб-интерфейс Kaspersky Security 8 для Linux Mail Server может быть установлен из пакетов формата DEB, RPM или TXZ на одном компьютере с Kaspersky Security 8 для Linux Mail Server.

- *Чтобы установить веб-интерфейс из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:*

  ```
  # rpm -i klmsui-<номер_версии>.x86_64.rpm
  ```

- *Чтобы установить веб-интерфейс из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

  ```
  # dpkg -i klmsui_<номер_версии>_amd64.deb
  ```

- *Чтобы установить веб-интерфейс из пакета формата TXZ на операционную систему FreeBSD 11, выполните следующую команду:*

  ```
  # pkg add -f klmsui-<номер_версии>.txz
  ```

- *Чтобы установить веб-интерфейс из пакета формата RPM на 64-битную операционную систему ALT Linux 7.0.5, выполните следующие предварительные процедуры:*

  1. Чтобы установочный скрипт нашел требуемый бинарный файл /usr/sbin/apachectl, необходимо создать символическую ссылку на файл /usr/sbin/httpd2, т.е. /usr/sbin/apachectl → /usr/sbin/httpd2.

  2. Создать символическую ссылку:

     ```
     conf.d -> /etc/httpd2/conf
     ```

  3. Запустить установочный скрипт, выполнив следующую команду:

     ```
     /opt/kaspersky/klmsui/bin/klmsui-setup.pl
     ```

4. Открыть любым текстовым редактором файл /etc/httpd2/conf/httpd2.conf и в конце добавить строку:

   ```
   Include /etc/httpd2/conf/klmsui.conf
   ```

Все необходимые модули должны быть установлены в Apache, после чего Apache следует перегрузить.

Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server на отдельном компьютере

Веб-интерфейс Kaspersky Security 8 для Linux Mail Server может быть установлен на отдельном компьютере. Настройку взаимодействия Kaspersky Security 8 для Linux Mail Server с веб-интерфейсом необходимо выполнять в следующем порядке:

1. Установить пакет веб-интерфейса Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server" на стр. 69).

2. Настроить модуль взаимодействия программы с утилитами и системами администрирования Facade (см. раздел "Настройка модуля взаимодействия программы с утилитами и системами администрирования Facade" на стр. 69).

3. Настроить подключение веб-интерфейса Kaspersky Security 8 для Linux Mail Server к веб-серверу Apache (см. раздел "Настройка подключения веб-интерфейса Kaspersky Security к веб-серверу Apache" на стр. 71).

В этом разделе

Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server

Веб-интерфейс Kaspersky Security 8 для Linux Mail Server может быть установлен из пакетов формата DEB, RPM или TXZ.

► *Чтобы установить веб-интерфейс из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:*

```
# rpm -i klmsui-<номер_версии>.x86_64.rpm
```

► *Чтобы установить веб-интерфейс из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

```
# dpkg -i klmsui_<номер_версии>_amd64.deb
```

► *Чтобы установить веб-интерфейс из пакета формата TXZ на операционную систему FreeBSD 11, выполните следующую команду:*

```
# pkg add -f klmsui-<номер_версии>.txz
```

Настройка модуля взаимодействия программы с утилитами и системами администрирования Facade

► Чтобы настроить модуль взаимодействия программы с утилитами и системами администрирования Facade, выполните следующие действия:

1. Экспортируйте параметры задачи `Facade` в XML-файл с помощью команды:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <идентификатор задачи Facade> -f <имя файла параметров>
```

или

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings Facade -n -f <имя файла параметров>
```

2. Откройте XML-файл параметров задачи на изменение.
3. В секции `<port> </port>` установите необходимый порт для взаимодействия веб-интерфейса Kaspersky Security 8 для Linux Mail Server.
4. В секции `<interfaceAddress> </interfaceAddress>` укажите IP-адрес компьютера, на котором установлен веб-интерфейс Kaspersky Security 8 для Linux Mail Server.
5. Сохраните внесенные изменения.
6. Импортируйте параметры задачи `Facade` из XML-файла с помощью команды:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <идентификатор задачи Facade> -f <имя файла параметров>
```

или

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings Facade -n -f <имя файла параметров>
```

Настройка подключения веб-интерфейса Kaspersky Security к веб-серверу Apache

► Чтобы настроить подключение *веб-интерфейса Kaspersky Security 8 для Linux Mail Server* к веб-серверу Apache на компьютере, работающем под управлением операционной системы Linux, выполните следующие действия:

1. Откройте файл с параметрами веб-интерфейса Kaspersky Security 8 для Linux Mail Server `/etc/apache2/conf.d/klmsui.conf`

2. В строке

   ```
   FastCgiExternalServer \

   /opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711
   ```

   укажите IP-адрес почтового сервера и порт модуля Facade.

► Чтобы настроить подключение *веб-интерфейса Kaspersky Security 8 для Linux Mail Server* к веб-серверу Apache на компьютере, работающем под управлением операционной системы Debian, выполните следующие действия:

1. Откройте файл с параметрами веб-интерфейса Kaspersky Security 8 для Linux Mail Server `/etc/httpd/conf.d/klmsui.conf`

2. В строке

   ```
   FastCgiExternalServer \

   /opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711
   ```

   укажите IP-адрес почтового сервера и порт модуля Facade.

► Чтобы настроить подключение *веб-интерфейса Kaspersky Security 8 для Linux Mail Server* к веб-серверу Apache на компьютере, работающем под управлением операционной системы FreeBSD, выполните следующие действия:

1. Откройте файл с параметрами веб-интерфейса Kaspersky Security 8 для Linux Mail Server `/usr/local/etc/apache24/Includes/klmsui.conf`

2. В строке

   ```
   FastCgiExternalServer \
   ```

```
/opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711
```

укажите IP-адрес почтового сервера и порт модуля Facade.

Обновление предыдущей версии программы

Для выполнения обновления необходимо принять новое Лицензионное соглашение. При этом лицензия, используемая в предыдущей версии программы, сохраняется и автоматически применяется после обновления.

Обновление Kaspersky Security 8 для Linux Mail Server с предыдущей версии до новой версии включает несколько этапов:

1. Установка пакета Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка Kaspersky Security 8 для Linux Mail Server поверх предыдущей версии" на стр. 74) поверх пакета с предыдущей версией программы.

2. Обновление параметров Kaspersky Security 8 для Linux Mail Server с помощью скрипта обновления параметров программы.

3. Установка пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка веб-интерфейса Kaspersky Security 8 для Linux Mail Server поверх предыдущей версии" на стр. 76) поверх пакета с предыдущей версией веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

   Пункты 1 и 3 можно выполнить одновременно, если Kaspersky Security 8 для Linux Mail Server и веб-интерфейс программы установлены на одном почтовом сервере.

4. Обновление параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server (на стр. 79) с помощью скрипта обновления параметров веб-интерфейса программы.

5. Установка пакетов локализации Kaspersky Security 8 для Linux Mail Server (см. раздел "Подготовка к установке программы" на стр. 62).

Если для предыдущей версии программы были установлены пакеты локализации Kaspersky Security 8 для Linux Mail Server, перед обновлением необходимо удалить пакеты локализации предыдущей версии программы, выполнив одну из следующих команд:

`# rpm -e <packagename>` для пакета локализации формата RPM;

`# dpkg -r <packagename>` для пакета локализации формата DEB;

`# pkg delete <packagename>` для пакета локализации операционной системы FreeBSD.

В этом разделе

Установка Kaspersky Security 8 для Linux Mail Server поверх предыдущей версии

В этом разделе описан порядок установки пакета Kaspersky Security 8 для Linux Mail Server поверх пакета с предыдущей версией программы на компьютерах, работающих под управлением операционных систем Linux и FreeBSD.

Установка Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы Linux

► *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:*

```
# rpm -U klms-<номер_версии>.i386.rpm
```

► *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

```
# dpkg --force-architecture -i klms_<номер_версии>_i386.deb
```

После выполнения команды программа будет установлена автоматически.

Установка Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы FreeBSD

Перед установкой Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы FreeBSD, требуется удалить предыдущую версию программы.

► *Чтобы удалить предыдущую версию Kaspersky Security 8 для Linux Mail Server, выполните следующую команду:*

```
# pkg delete klms
```

Не запускайте скрипт `klms-cleanup` после удаления предыдущей версии Kaspersky Security 8 для Linux Mail Server, так как это приведет к потере установленных значений параметров программы.

► *Чтобы установить Kaspersky Security 8 для Linux Mail Server из пакета формата TXZ на 64-битную операционную систему FreeBSD 11, выполните следующую команду:*

```
# pkg add -f klms-<номер_версии>.txz
```

После выполнения команды программа будет установлена автоматически.

После установки пакета программы установите пакет локализации Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка пакета локализации Kaspersky Security 8 для Linux Mail Server" на стр. 65).

После завершения установки Kaspersky Security 8 для Linux Mail Server требуется запустить скрипт обновления параметров Kaspersky Security 8 для Linux Mail Server.

Установка веб-интерфейса Kaspersky Security 8 для Linux Mail Server поверх предыдущей версии

Установка веб-интерфейса Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы Linux

► *Чтобы установить веб-интерфейс Kaspersky Security 8 для Linux Mail Server из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:*

```
# rpm -U klmsui-<номер_версии>.x86_64.rpm
```

► *Чтобы установить веб-интерфейс Kaspersky Security 8 для Linux Mail Server из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

```
# dpkg -i klmsui_<номер_версии>_amd64.deb
```

После выполнения команды веб-интерфейс программы будет установлен автоматически.

Установка веб-интерфейса Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы FreeBSD

Перед установкой веб-интерфейса Kaspersky Security 8 для Linux Mail Server на компьютер, работающий под управлением операционной системы FreeBSD, требуется удалить веб-интерфейс предыдущей версии программы.

► *Чтобы удалить веб-интерфейс предыдущей версии Kaspersky Security 8 для Linux Mail Server, выполните следующую команду:*

```
# pkg delete klmsui
```

► *Чтобы установить веб-интерфейс Kaspersky Security 8 для Linux Mail Server на операционную систему FreeBSD 11, выполните следующую команду:*

```
# pkg add -f klmsui-<номер_версии>.txz
```

После выполнения команды веб-интерфейс программы будет установлен автоматически.

После завершения установки веб-интерфейса Kaspersky Security 8 для Linux Mail Server требуется запустить скрипт обновления параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server (см. раздел "Обновление параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server" на стр. 79).

Обновление параметров Kaspersky Security 8 для Linux Mail Server

После установки Kaspersky Security 8 для Linux Mail Server требуется запустить скрипт обновления параметров Kaspersky Security 8 для Linux Mail Server. Скрипт обновления параметров Kaspersky Security 8 для Linux Mail Server входит в пакет установки Kaspersky Security 8 для Linux Mail Server.

На компьютерах под управлением операционной системы Linux после обновления предыдущей версии Kaspersky Security 8 для Linux Mail Server до новой версии установленные параметры программы и параметры интеграции программы с почтовым сервером, а также с LDAP-сервером сохраняются. Использование DNSBL- и SURBL-серверов, поставляемых "Лабораторией Касперского", не поддерживается в новой версии программы.

На компьютерах под управлением операционной системы FreeBSD после обновления предыдущей версии Kaspersky Security 8 для Linux Mail Server до новой версии параметры программы и параметры интеграции программы с LDAP-сервером сохраняются. Интеграцию программы с почтовым сервером необходимо выполнить заново вручную или в автоматическом режиме.

Некоторые данные программы удаляются в процессе обновления. Список удаляемых данных и рекомендации по их сохранению см. в таблице ниже.

Таблица 2. Данные, удаляемые при обновлении программы, и рекомендации по их сохранению

Данные	Рекомендации
Отчеты	Создать отчеты и сохранить их за пределами программы
Объекты, помещенные на Анти-Спам карантин	Доставить сообщения, помещенные на Анти-Спам карантин, получателям
Базы Антивируса, Анти-Спама и Анти-Фишинга	Выполнить обновление баз после обновления программы (запускается автоматически при наличии действующей лицензии)
Параметры KSN	Повторно принять или отклонить участие в Kaspersky Security Network (KSN)
Конфигурационные файлы программы	На компьютерах под управлением операционной системы FreeBSD необходимо задать параметры программы заново (не рекомендуется переносить конфигурационные файлы предыдущих версий)

► *Чтобы запустить скрипт обновления параметров Kaspersky Security 8 для Linux Mail Server, выполните следующую команду:*

- для Linux:

  ```
  # /opt/kaspersky/klms/bin/klms-upgrade.pl
  ```

- для FreeBSD:

  ```
  # /usr/local/bin/klms-upgrade.pl
  ```

  Скрипт по шагам запрашивает значения параметров Kaspersky Security 8 для Linux Mail Server.

При обновлении параметров предыдущей версии Kaspersky Security 8 для Linux Mail Server до новой версии вы можете использовать обновление параметров в автоматическом режиме с помощью файла с автоответами.

После обновления для следующих параметров устанавливаются значения по умолчанию:

- **Защита от Юникод-спуфинга**.
- **Защита KATA**.
- **Разрешить доступ к отчетам** (для учетной записи HelpDesk).
- **Отправка уведомлений о персональном хранилище**.
- **Обрабатывать вложения с макросами**.
- **Предварительно поместить копию в хранилище**.
- **Тема и тело уведомления о доставке сообщения во вложении** (для отправки писем из хранилища).
- **Добавлять к теме сообщения текст** (при срабатывании правил Контентной фильтрации).
- **Проверять форматы и имена файлов внутри архивов**.
- **Проверять составные объекты**.

Обновление параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server

После установки веб-интерфейса Kaspersky Security 8 для Linux Mail Server требуется запустить скрипт обновления параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server. Скрипт обновления параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server входит в пакет установки веб-интерфейса программы.

► *Чтобы запустить скрипт обновления параметров веб-интерфейса Kaspersky Security 8 для Linux Mail Server, выполните следующую команду:*

- для Linux:

```
# /opt/kaspersky/klmsui/bin/klmsui-upgrade.pl
```

- для FreeBSD:

```
# /usr/local/bin/klmsui-upgrade.pl
```

При обновлении веб-интерфейса предыдущей версии Kaspersky Security 8 для Linux Mail Server до новой версии вы можете использовать обновление параметров в автоматическом режиме с помощью файла с автоответами.

Подготовка Kaspersky Security 8 для Linux Mail Server к работе

После установки Kaspersky Security 8 для Linux Mail Server требуется выполнить первоначальную настройку программы.

Первоначальная настройка Kaspersky Security 8 для Linux Mail Server представляет собой последовательность шагов, которая реализована в виде скрипта. Скрипт первоначальной настройки Kaspersky Security 8 для Linux Mail Server входит в пакет установки Kaspersky Security 8 для Linux Mail Server.

Первоначальную настройку Kaspersky Security 8 для Linux Mail Server можно выполнить вручную или в автоматическом режиме, используя файл с сохраненными ответами.

В этом разделе

Запуск первоначальной настройки Kaspersky Security 8 для Linux Mail Server вручную

► *Чтобы запустить первоначальную настройку Kaspersky Security 8 для Linux Mail Server вручную, выполните следующую команду:*

- для Linux:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-setup.pl
```

- для FreeBSD:

```
# /usr/local/bin/klms-setup.pl
```

Далее скрипт первоначальной настройки по шагам запрашивает информацию для конфигурирования Kaspersky Security 8 для Linux Mail Server.

Шаг 1. Выбор языка просмотра Лицензионного соглашения и Положения о Kaspersky Security Network

На этом шаге вы можете выбрать язык, на котором будут отображаться тексты Лицензионного соглашения и Положения о Kaspersky Security Network. Для этого введите номер нужного языка из предложенного списка.

Выбор языка доступен, если в операционной системе установлены дополнительные пакеты локализации. Если дополнительные пакеты локализации не установлены, тексты Лицензионного соглашения и Положения о Kaspersky Security Network отображаются на английском языке.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге требуется принять или отклонить условия Лицензионного соглашения.

► *Чтобы просмотреть Лицензионное соглашение, выполните следующие действия:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст Лицензионного соглашения. Для перемещения по тексту используйте клавиши управления курсором или клавишу **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**.

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

3. Выполните одно из следующих действий:

   - Если вы хотите принять условия Лицензионного соглашения, введите `yes` (или `y`).

- Если вы хотите отклонить условия Лицензионного соглашения, введите `no` (или `n`).

4. Нажмите на клавишу **ENTER**.

Если вы отклонили условия Лицензионного соглашения, первоначальная настройка завершается.

Вы также можете просмотреть текст Лицензионного сообщения в файле. Файл с текстом Лицензионного соглашения расположен по следующему пути:

- для программы, установленной на компьютере, работающем под управлением операционной системы Linux: /opt/kaspersky/klms/share/doc/LICENSE, для веб-интерфейса программы: /opt/kaspersky/klmsui/share/doc/LICENSE;
- для программы, установленной на компьютере, работающем под управлением операционной системы FreeBSD: /usr/local/share/doc/klms/LICENSE, для веб-интерфейса программы: /opt/kaspersky/klmsui/share/doc/LICENSE.

Шаг 3. Участие в Kaspersky Security Network

На этом шаге требуется отказаться от участия в Kaspersky Security Network (KSN).

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.

Участие в Kaspersky Security Network добровольное. Решение об участии вы принимаете на этапе первоначальной настройки Kaspersky Security 8 для Linux Mail Server, но можете изменить его в любой момент.

► *Чтобы отказаться от участия в Kaspersky Security Network, выполните следующие действия:*

1. Нажмите на клавишу **ENTER**.

Откроется текст Положения о Kaspersky Security Network. Для перемещения по тексту используйте клавиши управления курсором или клавишу **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**.

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

3. Введите `no` (или `n`), чтобы отказаться от участия в Kaspersky Security Network.

4. Нажмите на клавишу **ENTER**.

Шаг 4. Выбор директории резервного хранилища

На этом шаге вы можете указать директорию для хранения резервных копий сообщений электронной почты, обработанных программой Kaspersky Security 8 для Linux Mail Server, или выбрать директорию, предлагаемую по умолчанию.

► *Чтобы указать директорию резервного хранилища, выполните следующие действия:*

1. Укажите полный путь к директории, предназначенной для хранения резервных копий сообщений электронной почты.

2. Нажмите на клавишу **ENTER**.

► *Чтобы указать директорию резервного хранилища, предлагаемую по умолчанию,*

нажмите на клавишу **ENTER**.

По умолчанию предлагается путь /var/opt/kaspersky/klms/backup.

Шаг 5. Параметры подключения к резервному хранилищу

На этом шаге вы можете указать параметры для подключения программы к резервному хранилищу или указать параметры подключения, предлагаемые по умолчанию.

Вы можете использовать внешнюю базу данных в качестве резервного хранилища. Kaspersky Security 8 для Linux Mail Server поддерживает базы данных PostgreSQL версии 9.1 и выше.

► *Чтобы указать параметры подключения к резервному хранилищу, выполните следующие действия:*

1. Укажите параметры подключения к резервному хранилищу в формате:

   `[dbname=<название базы данных> user=<имя пользователя> host=<сокет базы данных>]`

2. Нажмите на клавишу **ENTER**.

► *Чтобы указать параметры подключения к резервному хранилищу, предлагаемые по умолчанию,*

нажмите на клавишу **ENTER**.

По умолчанию предлагаются параметры подключения `[dbname=backup user=kluser host=/var/run/klms]`.

Шаг 6. Выбор сокета

На этом шаге требуется указать сокет, на котором модуль управления проверкой сообщений Scan Logic ожидает входящие соединения от фильтра.

► *Чтобы указать сокет, выполните следующие действия:*

1. Введите IP-адрес и номер порта или UNIX™-сокет, на котором модуль Scan Logic ожидает входящие соединения, в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

   По умолчанию предлагается UNIX-сокет `unix:/var/run/klms/klms_scanner_sock`

2. Нажмите на клавишу **ENTER**.

Шаг 7. Использование веб-интерфейса Kaspersky Security 8 для Linux Mail Server

На этом шаге вы можете указать, надо ли использовать веб-интерфейс Kaspersky Security 8 для Linux Mail Server.

► *Чтобы использовать веб-интерфейс Kaspersky Security 8 для Linux Mail Server,*

введите `yes` (или `y`) и нажмите на клавишу **ENTER**.

По умолчанию использование веб-интерфейса Kaspersky Security 8 для Linux Mail Server отключено.

Шаг 8. Выбор TCP-порта для взаимодействия с веб-интерфейсом Kaspersky Security 8 для Linux Mail Server

Этот шаг отображается, если на предыдущем шаге вы указали, что надо использовать веб-интерфейс Kaspersky Security 8 для Linux Mail Server.

На этом шаге вы можете указать номер TCP-порта, который программа Kaspersky Security 8 для Linux Mail Server должна использовать для взаимодействия с веб-интерфейсом.

► *Чтобы указать номер TCP-порта для взаимодействия с веб-интерфейсом Kaspersky Security 8 для Linux Mail Server,*

введите номер порта и нажмите на клавишу **ENTER**.

По умолчанию предлагается использовать TCP-порт `2711`.

Шаг 9. Назначение пароля доступа к веб-интерфейсу программы

На этом шаге вы можете указать пароль учетной записи `Administrator` для доступа к веб-интерфейсу программы.

Если вы не указали пароль доступа к веб-интерфейсу программы на этом шаге, вы можете сделать это в дальнейшем с помощью утилиты `/opt/kaspersky/kav4fs/bin/kav4fs-control --set-web-admin-password`.

> Пароль доступа к веб-интерфейсу программы обязателен. Вы не сможете войти в веб-интерфейс программы без пароля.

► *Чтобы задать пароль доступа к веб-интерфейсу, выполните следующие действия:*

1. Введите `yes`.

   По умолчанию предлагается вариант `no`.

2. Нажмите на клавишу **ENTER**.

3. Укажите пароль учетной записи `Administrator`.

   Пароль должен содержать в себе как минимум восемь символов, а также удовлетворять как минимум трем из следующих четырех условий:

   - Содержать в себе минимум один символ верхнего регистра.
   - Содержать в себе минимум один символ нижнего регистра.
   - Содержать в себе минимум один специальный символ.
   - Содержать в себе минимум одну цифру.

4. Подтвердите пароль.

5. Нажмите на клавишу **ENTER**.

Шаг 10. Выбор типа интеграции с почтовым сервером

Программа Kaspersky Security 8 для Linux Mail Server может быть интегрирована со следующими почтовыми серверами:

- Exim.

- Postfix.
- Sendmail.
- QMail.

► *Чтобы выполнить автоматическую интеграцию Kaspersky Security 8 для Linux Mail Server с почтовым сервером, выполните следующие действия:*

1. Введите цифру, указанную рядом с названием почтового сервера.
2. Нажмите на клавишу **ENTER**.
3. В зависимости от того, какой почтовый сервер вы выбрали в пункте 1 инструкции, выполните дальнейшие действия, описанные в следующих разделах:
   - Интеграция с почтовым сервером Sendmail (на стр. 90).
   - Интеграция с почтовым сервером Exim (на стр. 91).
   - Интеграция с почтовым сервером Postfix (на стр. 92).
   - Интеграция с почтовым сервером QMail (на стр. 89).

Если вы не выполните автоматическую интеграцию программы с почтовым сервером на этом шаге, вы можете в дальнейшем выполнить интеграцию вручную (см. раздел "Интеграция Kaspersky Security 8 для Linux Mail Server с почтовыми серверами и интерфейсом Amavis вручную" на стр. 126).

► *Чтобы отказаться от автоматической интеграции Kaspersky Security 8 для Linux Mail Server с почтовым сервером, выполните следующие действия:*

1. Введите цифру, указанную рядом с вариантом `Manual integration`.
2. Нажмите на клавишу **ENTER**.

В этом разделе

Интеграция с почтовым сервером Qmail

Программа выполняет интеграцию с почтовым сервером QMail автоматически.

Если во время установки скрипт первоначальной настройки программы не находит путь к директории исполняемого файла qmail, требуется выполнить следующие инструкции.

► *Чтобы указать путь к директории исполняемого файла qmail, выполните следующие действия:*

1. Укажите полный путь к директории исполняемого файла qmail.
2. Нажмите на клавишу **ENTER**.

Если во время установки скрипт первоначальной настройки программы не находит стандартную учетную запись пользователя `qmailq`, требуется указать учетную запись пользователя, с правами которого должна запускаться служба qmail.

► *Чтобы указать учетную запись пользователя qmail, выполните следующие действия:*

1. Укажите учетную запись пользователя, с правами которого должна запускаться служба qmail.
2. Нажмите на клавишу **ENTER**.

Интеграция с почтовым сервером Sendmail

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Sendmail, выполните следующие действия:*

1. Выберите способ интеграции с почтовым сервером Sendmail:

   - Если вы хотите, чтобы при интеграции изменения вносились в файл с расширением mc, а затем из него был создан файл с расширением cf, введите цифру `1`.

   - Если вы хотите, чтобы при интеграции изменения вносились в конфигурационный файл с расширением cf, введите цифру `2`.

   По умолчанию предлагается вариант `1`.

2. Нажмите на клавишу **ENTER**.

3. Укажите IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

   По умолчанию предлагается UNIX-сокет `unix:/var/opt/kaspersky/klms/klms_milter`.

4. Нажмите на клавишу **ENTER**.

5. Выберите действие, которое почтовый сервер Sendmail должен выполнять над сообщением в случае ошибок фильтра:

   - Если вы хотите, чтобы Sendmail пропускал сообщение без проверки, введите `2` для выбора варианта `accept`.

   - Если вы хотите, чтобы Sendmail отклонял сообщение, введите `1` для выбора варианта `reject`.

   - Если вы хотите, чтобы Sendmail сообщал отправителю сообщения о временной неспособности принять сообщение, введите `3` для выбора варианта `tempfail`.

   По умолчанию предлагается вариант `tempfail`.

6. Нажмите на клавишу **ENTER**.

Интеграция с почтовым сервером Exim

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Exim, выполните следующие действия:*

1. Выберите тип интеграции с почтовым сервером Exim:

   - Если вы хотите выполнить before-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Exim с использованием динамически подгружаемой библиотеки (dlfunc), введите цифру `1`.

     > Убедитесь, что почтовый сервер Exim поддерживает функцию контентной фильтрации dlfunc. Для этого выполните команду `exim -bV`. Положительным ответом является результат: `Expand_dlfunc`.

   - Если вы хотите выполнить after-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Exim по протоколу SMTP методом изменения маршрутов, введите цифру `2`.

   По умолчанию предлагается вариант `1` (если почтовый сервер Exim поддерживает функцию контентной фильтрации dlfunc).

2. Нажмите на клавишу **ENTER**.

3. Если вы выбрали вариант 2, выполните следующие действия:

   a. Укажите номер порта, на котором фильтр smtp_proxy ожидает сообщения от почтового сервера.

      По умолчанию предлагается вариант `10025`.

   b. Нажмите на клавишу **ENTER**.

   c. Укажите номер порта, на который передается сообщение после проверки.

      По умолчанию предлагается вариант `10026`.

d. Нажмите на клавишу **ENTER**.

Интеграция с почтовым сервером Postfix

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Postfix, выполните следующие действия:*

1. Выберите тип интеграции с почтовым сервером Postfix:

   - Если вы хотите выполнить before-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Postfix, введите цифру `1`.
   - Если вы хотите выполнить after-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Postfix, введите цифру `2`.
   - Если вы хотите выполнить интеграцию Kaspersky Security 8 для Linux Mail Server с Postfix по протоколу Milter, введите цифру `3`.

   По умолчанию предлагается вариант `3`.

2. Нажмите на клавишу **ENTER**.

3. Укажите IP-адрес и номер порта или UNIX-сокет, на котором фильтр smtp_proxy ожидает сообщения от почтового сервера в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

   - Если на шаге 1 инструкции вы выбрали вариант 1, по умолчанию предлагается UNIX-сокет `unix`.
   - Если на шаге 2 инструкции вы выбрали вариант 2, доступен только сетевой сокет в формате `inet:<порт>@<IP-адрес>`. По умолчанию предлагается `inet:10025@127.0.0.1`.
   - Если на шаге 1 инструкции вы выбрали вариант 3, по умолчанию предлагается UNIX-сокет `unix:/var/run/klms/klms_milter_sock`.

4. Нажмите на клавишу **ENTER**.

5. Если на шаге 1 инструкции вы выбрали вариант 2, укажите номер порта, на который передается сообщение после проверки.

По умолчанию предлагается вариант `10026`.

6. Нажмите на клавишу **ENTER**.

7. Если на шаге 1 инструкции вы выбрали вариант 3, выберите действие, которое почтовый сервер Postfix должен выполнять над сообщением в случае ошибок фильтра:

   - Если вы хотите, чтобы Postfix пропускал сообщение без проверки, введите цифру `2` для выбора варианта `accept`.
   - Если вы хотите, чтобы Postfix отклонял сообщение, введите цифру `1` для выбора варианта `reject`.
   - Если вы хотите, чтобы Postfix сообщал отправителю о временной неспособности принять сообщение, введите цифру `3` для выбора варианта `tempfail`.

   По умолчанию предлагается вариант `tempfail`.

8. Нажмите на клавишу **ENTER**.

Шаг 11. Настройка параметров прокси-сервера

Если для доступа в интернет используется прокси-сервер, на этом шаге вы можете указать параметры прокси-сервера. Доступ в интернет требуется для загрузки антивирусных баз и баз Анти-Спама с серверов обновлений "Лаборатории Касперского". Если вы не настроили параметры прокси-сервера на этом шаге, вы можете настроить параметры прокси-сервера позже без использования скрипта первоначальной настройки.

Если для доступа в интернет прокси-сервер не используется, нажмите на клавишу **ENTER**.

1. Чтобы использовать прокси-сервер и настроить его параметры, выполните следующие действия:

2. Введите `yes` (или `y`) и нажмите на клавишу **ENTER**.

3. Выполните одно из следующих действий:

- Если вы хотите указать указать FQDN-имя (fully qualified domain name) и порт прокси-сервера, введите FQDN-имя прокси-сервера в формате `FQDN_прокси_сервера:порт` и нажмите на клавишу **ENTER**.

- Если вы хотите указать указать IP-адрес и порт прокси-сервера, введите адрес прокси-сервера в формате `IP_адрес_прокси_сервера:порт` и нажмите на клавишу **ENTER**.

4. Укажите, требуется ли аутентификация для подключения к прокси-серверу:

   - Если аутентификация не требуется, введите `no` (или `n`) и нажмите на клавишу **ENTER**.

   - Если аутентификация требуется, введите `yes` (или `y`) и нажмите на клавишу **ENTER**.

5. Если вы указали, что требуется аутентификация, выполните следующие действия:

   1. Введите имя пользователя прокси-сервера и нажмите на клавишу **ENTER**.

   2. Введите пароль для доступа к прокси-серверу и нажмите на клавишу **ENTER**.

Шаг 12. Добавление ключа

На этом шаге вы можете указать путь к файлу ключа. Файл ключа содержит сведения, на основании которых проверяется наличие прав на использование Kaspersky Security 8 для Linux Mail Server и определяется срок использования программы (см. раздел "О файле ключа" на стр. 48). Вы можете добавить ключ во время первоначальной настройки Kaspersky Security 8 для Linux Mail Server или добавить его позже без использования скрипта первоначальной настройки.

► *Чтобы добавить ключ во время первоначальной настройки, выполните следующие действия:*

1. Укажите полный путь к файлу ключа.

2. Нажмите на клавишу **ENTER**.

► *Чтобы не добавлять ключ, выполните следующие действия:*

1. Введите пустую строку.
2. Нажмите на клавишу **ENTER**.

Если ключ не добавлен, Kaspersky Security 8 для Linux Mail Server не обеспечивает защиту компьютера.

Шаг 13. Обновление баз

На этом шаге выполняется автоматическое обновление антивирусных баз программы.

Расписание обновления баз настроено по умолчанию и установлена периодичность обновления баз программы – один раз в 5 минут.

Запуск автоматической первоначальной настройки Kaspersky Security 8 для Linux Mail Server

Первоначальную настройку Kaspersky Security 8 для Linux Mail Server можно выполнять в автоматическом режиме.

Вы можете создать конфигурационный файл, в котором сохранятся ваши ответы на команды, с помощью параметра `--create-auto-install=<полный путь к файлу для сохранения параметров>` при запуске скрипта первоначальной настройки программы.

Возможные значения должны быть указаны в нижнем регистре символов.

► *Чтобы запустить первоначальную настройку Kaspersky Security 8 для Linux Mail Server в автоматическом режиме, выполните следующую команду:*

- для Linux:

```
/opt/kaspersky/klms/bin/klms-setup.pl \
```

```
--auto-install=<полный путь к конфигурационному файлу с сохраненными ответами>
```

- для FreeBSD:

```
/usr/local/bin/klms-setup.pl \
--auto-install=<полный путь к конфигурационному файлу с сохраненными ответами>
```

Параметры конфигурационного файла с ответами приведены в таблице ниже.

Таблица 3. Параметры конфигурационного файла первоначальной настройки Kaspersky Security 8 для Linux Mail Server с ответами

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`yes`
KSN_AGREED	Обязательный параметр. Согласие с условиями Положения о Kaspersky Security Network.	`yes | no`
KEY_FILE	Необязательный параметр. Указание пути к файлу ключа.	`<path>` Регистр символов имеет значение.
BACKUP_CUSTOM_PATH	Необязательный параметр. Указание пользовательского пути к хранилищу. При отсутствии строки с параметром путь к хранилищу остается заданным по умолчанию (/var/opt/kaspersky/klms/backup).	`<path>` Регистр символов имеет значение.

Параметр	Описание	Возможные значения
BACKUP_CUSTOM_DB	Необязательный параметр. Пользовательская строка подключения к базе данных хранилища. При отсутствии строки с параметром параметр остается заданным по умолчанию (dbname=backup user=kluser host=/var/run/klms). Kaspersky Security 8 для Linux Mail Server поддерживает базы данных PostgreSQL версии 9.1 и выше.	<connection_string> Регистр символов имеет значение.
SCANNER_SOCKET	Необязательный параметр. Устанавливает сокет, используемый сканером. При отсутствии строки с параметром параметр остается заданным по умолчанию (unix:/var/run/klms/klms_scanner_sock).	inet:port@IP | unix:<path_to_socket> Регистр символов имеет значение.
MTA	Обязательный параметр. Устанавливает тип интеграции с почтовым сервером.	postfix | exim | sendmail | qmail | manual
POSTFIX_INTEGRATION_TYPE	Обязательный параметр. Устанавливает тип интеграции с почтовым сервером Postfix.	prequeue | afterqueue | milter

Параметр	Описание	Возможные значения
POSTFIX_MILTER_SOCKET	Необязательный параметр. Устанавливает сокет, используемый для интеграции с почтовым сервером Postfix по протоколу Milter. При отсутствии строки с параметром параметр принимает значение inet:10025@127.0.0.1. Параметр игнорируется, если: • Значение параметра MTA не равно "postfix". • Значение параметра POSTFIX_INTEGRATION_TYPE не равно "milter".	`inet:port@IP | unix:<path_to_socket>` Регистр символов имеет значение.

Параметр	Описание	Возможные значения
POSTFIX_SMTP_PROXY_SOCKET	Необязательный параметр. Устанавливает сокет, используемый для интеграции с почтовым сервером Postfix с типами интеграции "после передачи сообщения в очередь" (after-queue интеграция) и "до передачи сообщения в очередь (before-queue интеграция). При отсутствии строки с параметром параметр принимает значение inet:10025@127.0.0.1. Параметр игнорируется, если: Значение параметра MTA не равно "postfix". • Значение параметра POSTFIX_INTEGRATION_TYPE равно "milter".	`inet:port@IP | unix:<path_to_socket>` Регистр символов имеет значение.
POSTFIX_FORWARD_PORT	Необязательный параметр. Устанавливает TCP-порт для пересылки проверенных сообщений при интеграции с почтовым сервером Postfix. При отсутствии строки с параметром параметр принимает значение "10026". Параметр игнорируется, если значение параметра MTA не равно "postfix".	`<port>`

Параметр	Описание	Возможные значения
POSTFIX_FAILTYPE	Необязательный параметр. Устанавливает действие над сообщением по умолчанию для интеграции с почтовым сервером Postfix по протоколу Milter. При отсутствии строки с параметром принимает значение “Tempfail”. Параметр игнорируется, если: • Значение параметра MTA не равно "postfix". • Значение параметра POSTFIX_INTEGRATION_TYPE не равно "milter".	`accept	reject	tempfail`
EXIM_INTEGRATION_TYPE	Параметр обязательный, если значение MTA равно "exim". Устанавливает тип интеграции с почтовым сервером Exim. При отсутствии строки с параметром параметр принимает значение "dlfunc" (если версия Exim скомпилирована с поддержкой динамически подгружаемой библиотеки). Параметр игнорируется, если значение параметра MTA не равно "exim".	`dlfunc	afterqueue`

Параметр	Описание	Возможные значения
EXIM_FORWARD_PORT	Необязательный параметр. Устанавливает TCP-порт для пересылки проверенных сообщений при интеграции с почтовым сервером Exim. При отсутствии строки с параметром принимает значение "10026". Параметр игнорируется, если значение параметра MTA не равно "exim".	<port>
EXIM_FILTER_PORT	Необязательный параметр. Устанавливает порт, который будет прослушиваться сканером для фильтрации сообщений, приходящих от почтового сервера Exim. При отсутствии строки с параметром принимает значение "10025". Параметр игнорируется, если значение параметра MTA не равно "exim".	<port>

Параметр	Описание	Возможные значения
SENDMAIL_USES_MC	Необязательный параметр. Устанавливает возможность изменения файла с расширением mc, его компиляции или возможность исправления файла с расширением cf. При отсутствии строки с параметром, параметр принимает значение "1". Параметр игнорируется, если значение параметра MTA не равно "sendmail".	`0 | 1`
SENDMAIL_MILTER_SOCKET	Необязательный параметр. Устанавливает сокет, используемый для интеграции с почтовым сервером Sendmail по протоколу Milter. При отсутствии строки с параметром принимает значение inet:10025@127.0.0.1. Параметр игнорируется, если: • Значение параметра MTA не равно "sendmail". • Значение параметра SENDMAIL_USES_MC не равно `1`.	`inet:port@IP | unix:<path_to_socket>` Регистр символов имеет значение.

Параметр	Описание	Возможные значения
SENDMAIL_FAILTYPE	Необязательный параметр. Устанавливает действие над сообщением по умолчанию для интеграции с почтовым сервером Sendmail по протоколу Milter. При отсутствии строки с параметром параметр принимает значение "tempfail". Параметр игнорируется, если: • Значение параметра MTA не равно "sendMail". • Значение параметра SENDMAIL_USES_MC не равно `1`.	`accept | reject | tempfail`
QMAIL_BIN_DIR	Необязательный параметр. Устанавливает путь к директории QMail. При отсутствии строки с параметром параметр принимает значение "var/qmail/bin". Параметр игнорируется, если значение параметра MTA не равно "qmail".	`<path>` Регистр символов имеет значение.

Параметр	Описание	Возможные значения
QMAIL_USER	Необязательный параметр. По умолчанию имеет значение "qmaild". Устанавливает имя пользователя службы qmaild. Строка с параметром игнорируется, если значение параметра MTA не равно "qmail".	`<login>` Регистр символов имеет значение.
USE_UI	Необязательный параметр. Устанавливает возможность использования веб-интерфейса для управления программой. При отсутствии строки с параметром принимает значение "no".	`yes | no`
WEB_UI_PORT	Необязательный параметр. Устанавливает TCP-порт для взаимодействия Kaspersky Security 8 для Linux Mail Server с веб-сервером Apache. При отсутствии строки с параметром принимает значение "2711". Параметр игнорируется, если значение параметра USE_UI равно "no".	`<port>`

Параметр	Описание	Возможные значения
WEB_UI_IFACE_ADDR	Необязательный параметр. Устанавливает IP-адрес хоста, на котором установлен веб-интерфейс Kaspersky Security 8 для Linux Mail Server. Параметр игнорируется, если значение параметра USE_UI равно "no".	

Параметр	Описание	Возможные значения
WEB_PASSWORD	Необязательный параметр. Устанавливает пароль администратора для доступа к веб-интерфейсу программы. При отсутствии строки с параметром пароль администратора не задается. Если пароль, заданный в строке, не проходит проверку, пароль администратора не задается. Пароль доступа к веб-интерфейсу программы обязателен. Вы не сможете войти в веб-интерфейс программы без пароля. Пароль не сохранится в конфигурационном файле первоначальной настройки программы с ответами, если он был задан во время работы скрипта `klms-setup.pl`.	`<password>` Регистр символов имеет значение.

Подготовка сетевой инфраструктуры вашей организации к работе Kaspersky Security 8 для Linux Mail Server

Перед использованием Kaspersky Security 8 для Linux Mail Server вам нужно подготовить сетевую инфраструктуру вашей организации и разрешить соединения по входящим и исходящим протоколам.

Входящие протоколы:

- <host>:80 (HTTP) и <host>:443 или <host>:9045 (HTTPS) – для работы веб-интерфейса программы, если он установлен и включен (дополнительный пакет klmsui).
- <host>:<port> (по умолчанию 127.0.0.1:10025) (SMTP) – для работы фильтра почтового агента MTA, если MTA-Filter настроен принимать соединения, например, с внешнего MTA, по протоколу TCP (SMTP).
- <host>:<port> (по умолчанию 127.0.0.1:10025) (Milter) – для работы фильтра почтового агента MTA, если MTA-Filter настроен принимать соединения, например, с внешнего MTA, по протоколу Milter.
- <host>:<port> (по умолчанию 127.0.0.1:2711) (FCGI/TLS) – для доступа модуля Facade к веб-интерфейсу программы.
- <host>:<port> (по умолчанию 127.0.0.1:5555) (Binary) – для работы модуля ScanLogic, если он настроен принимать соединения по протоколу TCP.

Исходящие протоколы:

- <host>:<port> (HTTPS) – для соединения с сервером активации программы для проверки лицензии.

- <host>:<port> (SNMP) – для соединения с SNMP-сервером для передачи статистики и информации о событии.
- <host>:<port> (LDAP, LDAP/TLS) – для соединения с внешним LDAP-сервером и Active Directory и авторизации пользователей.
- <host>:<port> (DNS) – для работы технологий проверки подлинности отправителей сообщений (DNSBL, SURBL, SPF) и модуля Анти-Спам.
- <host>:<port> (SMTP) – для работы фильтра почтового агента MTA, если MTA-Filter настроен отправлять сообщения электронной почты на внешний почтовый сервер по протоколу TCP.
- <host>:<port> (HTTPS) – для соединения с сервером обновлений баз программы.
- <host>:<port> (HTTPS) – для соединения модуля Moebius, предназначенного для моментального обновления баз модуля Анти-Спам, со службой быстрых обновлений баз программы.
- <host>:<port> (HTTPS) – для соединения с KSN (см. раздел "Участие в Kaspersky Security Network и использование Kaspersky Private Security Network" на стр. 210).
- <host>:<port> (HTTPS) – для соединения с сервером Kaspersky Anti Targeted Attack Platform (см. раздел "Защита KATA и интеграция Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform" на стр. 253).

Запуск и остановка программы

Запуск программы

По умолчанию Kaspersky Security 8 для Linux Mail Server запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы).

При первоначальном запуске и дальнейших перезапусках программа автоматически создает в директориях `/var/log` и `/tmp` директории, необходимые для корректного функционирования программы. Изменение этих директорий вручную может привести к некорректной работе программы.

Остановка программы

При необходимости вы можете остановить работу программы. Для остановки программы требуется сначала остановить службу klms, а затем базу данных.

- *Чтобы остановить службу klms в операционной системе Linux, выполните следующую команду:*

  ```
  # /etc/init.d/klms stop
  ```

- *Чтобы остановить базу данных в операционной системе Linux, выполните следующую команду:*

  ```
  # /etc/init.d/klmsdb stop
  ```

- *Чтобы остановить службу klms в операционной системе FreeBSD, выполните следующую команду:*

  ```
  # /usr/local/etc/rc.d/klms stop
  ```

- *Чтобы остановить базу данных в операционной системе FreeBSD, выполните следующую команду:*

  ```
  # /usr/local/etc/rc.d/klmsdb stop
  ```

Подготовка веб-интерфейса Kaspersky Security 8 для Linux Mail Server к работе

После установки веб-интерфейса Kaspersky Security 8 для Linux Mail Server требуется выполнить его первоначальную настройку.

Первоначальная настройка веб-интерфейса Kaspersky Security 8 для Linux Mail Server представляет собой последовательность шагов, которая для удобства администратора реализована в виде скрипта. После установки веб-интерфейса требуется запустить скрипт первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server. Скрипт первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server входит в пакет установки веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

Первоначальную настройку веб-интерфейса Kaspersky Security 8 для Linux Mail Server можно выполнить вручную или в автоматическом режиме.

В этом разделе

Запуск первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server вручную

► *Чтобы запустить первоначальную настройку веб-интерфейса Kaspersky Security 8 для Linux Mail Server вручную, выполните следующую команду:*

- для Linux:

  ```
  # /opt/kaspersky/klmsui/bin/klmsui-setup.pl
  ```

- для FreeBSD:

  ```
  # /usr/local/bin/klmsui-setup.pl
  ```

Для доступа к веб-интерфейсу Kaspersky Security 8 для Linux Mail Server используется учетная запись `Administrator`. Пароль этой учетной записи задается во время первоначальной настройки Kaspersky Security 8 для Linux Mail Server (см. раздел "Шаг 9. Назначение пароля доступа к веб-интерфейсу программы" на стр. 86).

Далее скрипт первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server пошагово запрашивает у вас информацию.

В этом разделе

Шаг 1. Выбор языка просмотра Лицензионного соглашения

На этом шаге вы можете выбрать язык, на котором будет отображаться текст Лицензионного соглашения. Для этого введите номер нужного языка из предложенного списка.

Выбор языка доступен, если в операционной системе установлены дополнительные пакеты локализации. Если дополнительные пакеты локализации не установлены, текст Лицензионного соглашения отображается на английском языке.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге требуется принять или отклонить условия Лицензионного соглашения.

► *Чтобы просмотреть Лицензионное соглашение, выполните следующие действия:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст Лицензионного соглашения. Для перемещения по тексту используйте клавиши управления курсором или клавишу **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**.

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

3. Выполните одно из следующих действий:

   - Если вы хотите принять условия Лицензионного соглашения, введите `yes` (или `y`).
   - Если вы хотите отклонить условия Лицензионного соглашения, введите `no` (или `n`).

4. Нажмите на клавишу **ENTER**.

   Если вы отклонили условия Лицензионного соглашения, первоначальная настройка завершается.

Вы также можете просмотреть текст Лицензионного сообщения в файле. Файл с текстом Лицензионного соглашения расположен по следующему пути:

- для программы, установленной на компьютере, работающем под управлением операционной системы Linux: /opt/kaspersky/klms/share/doc/LICENSE, для веб-интерфейса программы: /opt/kaspersky/klmsui/share/doc/LICENSE;
- для программы, установленной на компьютере, работающем под управлением операционной системы FreeBSD: /usr/local/share/doc/klms/LICENSE, для веб-интерфейса программы: /opt/kaspersky/klmsui/share/doc/LICENSE.

Шаг 3. Выбор веб-сервера Apache

Перед установкой пакета веб-интерфейса Kaspersky Security 8 для Linux Mail Server требуется установить следующие модули Apache: mod_ssl, mod_include, mod_dir и mod_expires (если они не установлены) и включить их с помощью команды `a2enmod` (если они не включены):

```
# a2enmod ssl
# a2enmod include
# a2enmod dir
# a2enmod expires
```

На этом шаге вы можете указать веб-сервер Apache, который будет использовать программа Kaspersky Security 8 для Linux Mail Server.

Скрипт первоначальной настройки веб-интерфейса программы автоматически определяет расположение конфигурационных и исполняемых файлов службы Apache и отображает информацию о найденном веб-сервере Apache.

Если скрипт первоначальной настройки веб-интерфейса программы правильно определил расположение конфигурационных и исполняемых файлов службы Apache, вам требуется подтвердить это.

Если скрипт первоначальной настройки веб-интерфейса неправильно определил расположение конфигурационных и исполняемых файлов службы Apache или если вы не

хотите использовать найденный веб-сервер Apache, вам требуется вручную указать расположение файлов службы Apache того веб-сервера Apache, который вы хотите использовать.

► *Чтобы подтвердить расположение файлов службы Apache, выполните следующие действия:*

1. Введите `yes` (или `y`).
2. Нажмите на клавишу **ENTER**.

► *Чтобы указать расположение файлов службы Apache, выполните следующие действия:*

1. Введите `no` (или `n`).
2. Нажмите на клавишу **ENTER**.
3. Укажите полный путь к исполняемому файлу службы Apache.
4. Нажмите на клавишу **ENTER**.
5. Укажите полный путь к конфигурационному файлу службы Apache.
6. Нажмите на клавишу **ENTER**.
7. Укажите полный путь к скрипту запуска службы Apache.
8. Нажмите на клавишу **ENTER**.

Шаг 4. Выбор виртуального хоста веб-сервера Apache

На этом шаге требуется указать виртуальный хост веб-сервера Apache.

► *Чтобы указать виртуальный хост веб-сервера Apache, выполните следующие действия:*

1. Выполните одно из следующих действий:
   - Если вы используете виртуальный хост веб-сервера Apache, определяемый по имени, введите `name`.

- Если вы используете виртуальный хост веб-сервера Apache, доступный только с указанием порта, введите `port`.

  Этот вариант выбран по умолчанию.

- Если вы используете виртуальный хост веб-сервера Apache, определяемый по директории, введите `dir`.

  При использовании виртуального хоста веб-сервера Apache, определяемого по директории, Kaspersky Security 8 для Linux Mail Server будет использовать параметры соединения, установленные в конфигурационном файле Apache. По умолчанию установлено небезопасное соединение http. Вы можете настроить виртуальный хост веб-сервера Apache на использование шифрованного соединения SSL самостоятельно.

2. Нажмите на клавишу **ENTER**.
3. Выполните одно из следующих действий:

   - Если на шаге 1 инструкции вы выбрали вариант `name`, введите имя виртуального хоста веб-сервера Apache.

   - Если на шаге 1 инструкции вы выбрали вариант `port`, введите порт виртуального хоста веб-сервера Apache.

     По умолчанию предлагается вариант `9045`.

   - Если на шаге 1 инструкции вы выбрали вариант `dir`, введите путь к директории, в которой будут размещаться файлы веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

     По умолчанию предлагается директория `klms`.

4. Нажмите на клавишу **ENTER**.

Шаг 5. Выбор сокета для взаимодействия с Kaspersky Security 8 для Linux Mail Server

На этом шаге требуется указать сокет (IP-адрес и порт) для взаимодействия веб-сервера Apache с Kaspersky Security 8 для Linux Mail Server.

► *Чтобы указать сокет для взаимодействия веб-сервера Apache с Kaspersky Security 8 для Linux Mail Server, выполните следующие действия:*

1. Введите IP-адрес и порт в формате `<IP-адрес>:<порт>`.

   По умолчанию предлагается сетевой сокет `127.0.0.1:2711`.

2. Нажмите на клавишу **ENTER**.

Шаг 6. Выбор сертификата для доступа к веб-интерфейсу программы

На этом шаге требуется указать сертификат для доступа к веб-интерфейсу Kaspersky Security 8 для Linux Mail Server.

Вы можете создать новый сертификат или указать путь к файлу закрытого ключа и путь к файлу уже добавленного на компьютер сертификата.

► *Чтобы создать новый сертификат для доступа к веб-интерфейсу программы, выполните следующие действия:*

1. Введите `new`.

2. Нажмите на клавишу **ENTER**.

   Будет создан новый сертификат.

► *Чтобы указать путь к файлу закрытого ключа и путь к файлу сертификата, выполните следующие действия:*

1. Введите `file` и нажмите на клавишу **ENTER**.

2. Укажите путь к файлу закрытого ключа и нажмите на клавишу **ENTER**.

3. Укажите путь к файлу сертификата и нажмите на клавишу **ENTER**.

Запуск автоматической первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server

Первоначальную настройку веб-интерфейса Kaspersky Security 8 для Linux Mail Server можно выполнять в автоматическом режиме. Вы можете создать конфигурационный файл, в котором сохранятся ваши ответы на команды, с помощью параметра `--create-auto-install=<полный путь к файлу для сохранения параметров>` при запуске скрипта первоначальной настройки программы.

Возможные значения должны быть указаны в нижнем регистре символов.

► *Чтобы запустить первоначальную настройку веб-интерфейса Kaspersky Security 8 для Linux Mail Server в автоматическом режиме, выполните следующую команду:*

- для Linux:

```
/opt/kaspersky/klmsui/bin/klmsui-setup.pl \
--auto-install=<полный путь к конфигурационному файлу с сохраненными ответами>
```

- для FreeBSD:

```
/usr/local/bin/klmsui-setup.pl \
--auto-install=<полный путь к конфигурационному файлу с сохраненными ответами>
```

Параметры конфигурационного файла с ответами приведены в таблице ниже.

Таблица 4. Параметры конфигурационного файла веб-интерфейса Kaspersky Security 8 для Linux Mail Server с ответами

Параметр	Описание	Возможные значения
WEB_EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`yes`
APACHE_BIN	Обязательный параметр. Устанавливает путь к директории веб-сервера Apache.	`<path>` Регистр символов имеет значение.
APACHE_CONF_D	Обязательный параметр. Устанавливает путь к директории настроек веб-сервера Apache.	`<path>` Регистр символов имеет значение.
APACHE_INIT_D	Обязательный параметр. Устанавливает путь к стартовому скрипту веб-сервера Apache.	`<path>` Регистр символов имеет значение.
VHOST_TYPE	Обязательный параметр. Способ настройки виртуального сервера веб-сервера Apache.	`name | port | dir`

Параметр	Описание	Возможные значения
VHOST_PORT	Обязательный параметр, если значение параметра VHOST_TYPE равно "port". Устанавливает номер порта виртуального сервера веб-сервера Apache.	`<port>`
VHOST_DIR	Обязательный параметр, если значение параметра VHOST_TYPE равно "dir". Устанавливает путь к директории, в которой будут размещаться файлы веб-интерфейса Kaspersky Security 8 для Linux Mail Server.	`<url_subdir>`
VHOST_HOST	Обязательный параметр, если значение параметра VHOST_TYPE равно "name". Устанавливает имя виртуального веб-сервера Apache.	`<hostname>`

Параметр	Описание	Возможные значения
UI_HOST	Обязательный параметр. Устанавливает сокет (IP-адрес и порт) для взаимодействия веб-сервера Apache с Kaspersky Security 8 для Linux Mail Server.	`<host:port>`
CERT_TYPE	Обязательный параметр. Устанавливает тип сертификата. Если указан тип "new", то сертификат будет создан скриптом первоначальной настройки. Тип "keep" присутствует в списке и выбран по умолчанию, если сертификат уже существует.	`new | file | keep`
CERT_KEY	Обязательный параметр, если значение параметра CERT_TYPE равно "file". Устанавливает путь к приватному ключу веб-сервера Apache.	`<path>` Регистр символов имеет значение.

Параметр	Описание	Возможные значения
CERT_CRT	Обязательный параметр, если значение параметра CERT_TYPE равно "file". Устанавливает путь к сертификату веб-сервера Apache.	`<path>` Регистр символов имеет значение.
IGNORE_APACHE_ARCH	Необязательный параметр. Указывает, игнорировать ли ошибку в случае, когда скрипт `klmsui-setup.pl` не может определить битность установленного веб-сервера Apache. Если битность веб-сервера определить не удается и значение ключа равно "yes", то интеграция продолжается.	`yes | no`

Процедура приемки

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

В этом разделе

Безопасное состояние

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

- Установка программы завершена без ошибок.
- Произведена первоначальная настройка программы (см. стр. 81);
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированной конфигурации" на стр. 405).

Проверка работоспособности. Тестовый файл EICAR

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

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

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

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

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

► *Чтобы проверить антивирусную защиту сообщений с использованием тестового файла EICAR, 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 Security 8 для Linux Mail Server.

Kaspersky Security 8 для Linux Mail Server сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

Начало работы в веб-интерфейсе программы

После установки и первоначальной настройки программы вы можете начать работу в веб-интерфейсе Kaspersky Security 8 для Linux Mail Server.

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

1. В браузере введите адрес веб-интерфейса программы, который вы задали при установке программы.

   Откроется 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 Security 8 для Linux Mail Server.

Интеграция Kaspersky Security 8 для Linux Mail Server с почтовыми серверами и интерфейсом Amavis вручную

Этот раздел содержит информацию об интеграции вручную программы Kaspersky Security 8 для Linux Mail Server с почтовыми серверами Exim, Postfix, Sendmail, QMail, а также с интерфейсом Amavis.

В этом разделе

Об интеграции программы с почтовым сервером вручную

Если во время первоначальной настройки программы вы пропустили автоматическую интеграцию программы с почтовым сервером (см. раздел "Шаг 10. Выбор типа интеграции с почтовым сервером" на стр. 87), вам требуется интегрировать программу Kaspersky Security 8 для Linux Mail Server с почтовым сервером вручную.

Вы можете вручную интегрировать Kaspersky Security 8 для Linux Mail Server со следующими почтовыми серверами:

- Exim (см. раздел "Интеграция с почтовым сервером Exim вручную" на стр. 133).
- Postfix (см. раздел "Интеграция с почтовым сервером Postfix вручную" на стр. 145).
- Sendmail (см. раздел "Интеграция с почтовым сервером Sendmail вручную" на стр. 128).
- QMail (см. раздел "Интеграция с почтовым сервером QMail вручную" на стр. 143).
- Amavis (см. раздел "Интеграция с интерфейсом Amavis вручную" на стр. 154).

Kaspersky Security 8 для Linux Mail Server поддерживает интеграцию с почтовым сервером с помощью службы klms, которая принимает от почтового сервера запросы на обработку.

В случае интеграции программы с почтовым сервером вручную требуется:

- зарегистрировать в операционной системе службу klms;
- внести изменения в конфигурационный файл почтового сервера.

В FreeBSD вы можете настроить автоматический запуск службы klms при запуске операционной системы.

► *Чтобы настроить автоматический запуск службы klms при запуске операционной системы FreeBSD,*

добавьте в конфигурационный файл /etc/rc.conf следующие строки:

```
klmsdb_enable=YES

klms_enable=YES
```

Для почтовых серверов Exim и Postfix программа Kaspersky Security 8 для Linux Mail Server поддерживает как интеграцию "до передачи в очередь" (далее – "before-queue интеграция"), так и интеграцию "после передачи в очередь" (далее – "after-queue интеграция"). При before-queue интеграции сообщения передаются на проверку программе Kaspersky Security 8 для Linux Mail Server перед размещением в очереди почтового сервера, при after-queue интеграции сообщения передаются на проверку программе Kaspersky Security 8 для Linux Mail Server после размещения в очереди почтового сервера.

Для обмена информацией между почтовым сервером и фильтром Kaspersky Security 8 для Linux Mail Server используются сокеты.

Сокеты назначаются по следующим правилам:

- `inet:<port>@<ip_address>` – для сетевого сокета;
- `unix:<socket_path>` – для UNIX-сокета.

Пример:

`scanner=inet:5555@127.0.0.1` – для сетевого сокета

`scanner=unix:/var/run/klms/scanner_sock` – для UNIX-сокета

При использовании сокета требуется соблюдать два условия:

- при определении сетевого сокета номер порта должен быть больше `1024`;
- при определении UNIX-сокета фильтр и kluser должны иметь права для доступа к этому сокету.

Интеграция с почтовым сервером Sendmail вручную

Почтовый сервер Sendmail предоставляет программный интерфейс Milter API для интеграции с фильтрами сторонних производителей. Kaspersky Security 8 для Linux Mail Server получает сообщения от почтового сервера Sendmail и передает их обратно с помощью вызовов функций программного интерфейса Milter API. Сообщения передаются на проверку до размещения в очереди почтовой системы (before-queue интеграция).

Для интеграции программы с почтовым сервером Sendmail вручную требуется внести изменения в конфигурационный файл почтового сервера Sendmail.

В файле настроек фильтров, *klms_filter.conf*, в секции `[global]` установите значение `true` для параметра `header-guard`.

Вы можете внести изменения в конфигурационный файл почтового сервера Sendmail следующими способами:

- изменить конфигурационный файл с расширением cf;
- изменить соответствующий файл с расширением mc, а затем создать из него файл с расширением cf с помощью интерпретатора m4.

Если вы внесете изменения только в файл с расширением cf, при следующем создании файла с расширением cf из файла с расширением mc все изменения будут утеряны.

В этом разделе

Интеграция с помощью файла с расширением mc

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Sendmail с помощью файла с расширением mc, выполните следующие действия:*

1. Создайте резервную копию файла с расширением mc.
2. Добавьте в файл с расширением mc следующие строки:

```
dnl #KLMS-milter-begin-filter dnl

define(`_FFR_MILTER', `true')dnl

INPUT_MAIL_FILTER(`KLMS_Milter',`S=$filter_socket,${fail_type}T=S:3m;R:5m;E:10m') \
```

```
dnl

dnl #KLMS-milter-end-filter dnl
```

где `$filter_socket` – IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета);

`${fail_type}` определяет действие почтового сервера Sendmail над сообщением в том случае, если фильтр работает некорректно. Параметр `${fail_type}` может принимать значения "F=R", "F=A," или "F=T,". `R` означает `reject`, `A` означает `accept`, а `T` означает `tempfail`. Если заменить `${fail_type}` на пустую строку, сообщение будет пропускаться. Рекомендуется использовать `tempfail`.

Пример:

```
INPUT_MAIL_FILTER(`KLMS_Milter',`S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
```

3. Скомпилируйте конфигурационный файл с расширением cf согласно параметрам вашей операционной системы.
4. Остановите службу klms.
5. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
6. В секции `[global]` укажите путь к файлу sendmail в следующей строке:

   ```
   sendmail-path=<путь к файлу sendmail>
   ```

7. В секции `[milter]` файла /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD) укажите IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в следующей строке:

   `socket=<IP-адрес и номер порта>` или `<путь к UNIX-сокету>`

Пример:

```
socket=inet:10025@127.0.0.1
```

8. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).

9. Добавьте в файл следующие строки:

   `SENDMAIL_MILTER=1`

   `SENDMAIL_USES_MC=1` или `0`, в зависимости от того, была использована компиляция файла с расширением mc или нет.

   `START_MILTER=1`

10. Запустите службу klms.

11. Перезапустите почтовый сервер Sendmail.

Интеграция с помощью файла с расширением cf

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Sendmail с помощью файла с расширением cf, выполните следующие действия:*

1. Создайте резервную копию файла sendmail.cf.

2. Добавьте следующие строки в файл sendmail.cf:

```
#KLMS-milter-begin-filter

O InputMailFilters=KLMS_Milter

O Milter.macros.connect=j, _, {daemon_name}, {if_name}, {if_addr}

O Milter.macros.helo={tls_version}, {cipher}, \

{cipher_bits}, {cert_subject}, {cert_issuer}
```

```
O Milter.macros.envfrom=i, {auth_type}, \

{auth_authen}, {auth_ssf}, {auth_author}, \

{mail_mailer}, {mail_host}, {mail_addr}

O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, {rcpt_addr}

#KLMS-milter-end-filter

#KLMS-milter-begin-socket

XKLMS_Milter, S=$filter_socket,${fail_type}T=S:3m;R:5m;E:10m

#KLMS-milter-end-socket
```

где `$filter_socket` – IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета);

`${fail_type}` определяет действие почтового сервера Sendmail над сообщением в том случае, если фильтр работает некорректно. Параметр `${fail_type}` может принимать значения "F=R", "F=A," или "F=T,". `R` означает `reject`, `A` означает `accept`, а `T` означает `tempfail`. Если заменить `${fail_type}` на пустую строку, сообщение будет пропускаться. Рекомендуется использовать `tempfail`.

Пример:

```
INPUT_MAIL_FILTER(`KLMS_Milter',`S=inet:10025@127.0.0.1,F=T,T=S:3m;
R:5m;E:10m')dnl
```

3. Остановите службу klms.
4. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
5. В секции `[global]` укажите путь к файлу sendmail в следующей строке:

   `sendmail-path=`<путь к файлу `sendmail`>

6. В секции `[milter]` файла /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD) укажите IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в следующей строке:

   `socket=inet:<порт>@<IP-адрес>` или `<UNIX-сокет>`

Пример:

`socket=inet:10025@127.0.0.1`

7. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
8. Добавьте в файл следующие строки:

   `SENDMAIL_MILTER=1`

   `SENDMAIL_USES_MC=1` или `0`, в зависимости от того, была использована компиляция файла с расширением mc или нет.

   `START_MILTER=1`

9. Запустите службу klms.
10. Перезапустите почтовый сервер Sendmail.

Интеграция с почтовым сервером Exim вручную

Для интеграции с почтовым сервером Exim вручную в Kaspersky Security 8 для Linux Mail Server предусмотрены два метода:

- Интеграция "после передачи в очередь" (after-queue интеграция) по протоколу SMTP методом изменения маршрутов. В этом случае все сообщения, проходящие через компьютер, передаются на проверку программе Kaspersky Security 8 для Linux Mail Server после размещения в очереди почтового сервера Exim.

- Интеграция "до передачи в очередь" (before-queue интеграция) с использованием динамически подгружаемой библиотеки (dlfunc). В этом случае сообщения передаются на проверку программе Kaspersky Security 8 для Linux Mail Server до размещения в очереди почтового сервера Exim.

В этом разделе

After-queue интеграция методом изменения маршрутов

При интеграции «после передачи сообщения в очередь» (after-queue интеграции) методом изменения маршрутов для передачи сообщений на проверку программе Kaspersky Security 8 для Linux Mail Server и возвращения их почтовому серверу Exim требуется соблюдение следующих условий:

- Фильтр должен быть настроен для перехвата сообщений от почтового сервера Exim по сокету `socket-in`. Этот сокет требуется задать в конфигурации программы.
- Фильтр должен передавать сообщения для проверки модулю Scan Logic по сокету `scanner`. Этот сокет требуется задать в конфигурации программы.
- Фильтр должен возвращать сообщения почтовому серверу Exim по сокету `socket-out`. Этот сокет требуется задать в конфигурации программы.

При after-queue интеграции с почтовым сервером Exim методом изменения маршрутов `socket-in`, `scanner` и `socket-out` должны указывать на сетевой сокет.

В зависимости от дистрибутива операционной системы вам требуется внести изменения в один или несколько конфигурационных файлов почтового сервера Exim. Например, в Debian и Ubuntu почтовый сервер Exim может конфигурироваться как с помощью нескольких файлов в директории /etc/exim/conf.d, так и с помощью одного файла.

► *Чтобы выполнить after-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Exim методом изменения маршрутов, выполните следующие действия:*

1. Сделайте резервную копию конфигурационного файла (файлов) Exim.

2. В секцию `[routers]` конфигурационного файла (файлов) Exim после строки

   ```
   begin routers
   ```

   добавьте следующие строки:

   ```
   #klms-filter-begin-2

   klms_dnslookup:

     driver = dnslookup

     domains = ! +local_domains

     ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8

     verify_only

     pass_router = smtp_proxy

     no_more



   klms_system_aliases:

     driver = redirect

     allow_fail

     allow_defer

     data =${lookup{$local_part}lsearch{/etc/aliases}}
   ```

```
  verify_only

  pass_router = smtp_proxy


klms_localuser:

  driver = accept

  check_local_user

  verify_only

  pass_router = smtp_proxy

  cannot_route_message = Unknown user


failed_address_router:

  driver = redirect

  verify_only

  condition = "{0}"

  allow_fail

  data = :fail: Failed to deliver to address

  no_more


smtp_proxy:

  driver = manualroute

  condition = "${if or {{eq {$interface_port}{$forward_port}} \\

      {eq {\$received_protocol}{spam-scanned}} \\
```

```
    }{0}{1}}"
  transport = smtp_proxy
  route_list = "* localhost byname"
  self = send
#klms-filter-end-2
```

где `$forward_port` – номер порта сокета, на который передается сообщение после проверки программой Kaspersky Security 8 для Linux Mail Server.

3. В секцию `[transports]` конфигурационного файла (файлов) Exim после строки

   ```
   begin transports
   ```

   добавьте следующие строки:

   ```
   #klms-filter-begin-3
   smtp_proxy:
     driver = smtp
     port = $scanner_port
     delay_after_cutoff = false
     allow_localhost
   #klms-filter-end-3
   ```

   где `$scanner_port` – порт, на котором фильтр ожидает сообщения.

4. В главном конфигурационном файле Exim (exim.conf или update-exim.conf.conf) укажите подстроку вида `127.0.0.1.$forward_port` в строке вида:

   ```
   dc_local_interfaces=<IP-адрес1>.<порт1>:127.0.0.1.$forward_port
   ```

   или

   ```
   local_interfaces=<IP-адрес1>.<порт1>:127.0.0.1.$forward_port
   ```

где подстрока `127.0.0.1.$forward_port` требуется для того, чтобы почтовый сервер Exim принимал от фильтра обработанные сообщения, ожидая данных на порту `$forward_port`.

5. Скомпилируйте конфигурационный файл (файлы) Exim согласно параметрам вашей операционной системы.
6. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
7. Добавьте в файл следующие строки:

   ```
   EXIM_INTEGRATION_TYPE= after-queue

   START_SMTP_PROXY=1
   ```

8. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
9. В секции `[smtp_proxy]` укажите следующие параметры:

   ```
   socket-in=inet:$scanner_port@127.0.0.1

   socket-out=inet: $forward_port@127.0.0.1
   ```

10. В секции `[global]` установите значение `true` для параметра `header-guard`.
11. Перезапустите службу klms.
12. Перезапустите почтовый сервер Exim.

Before-queue интеграция с использованием динамически подгружаемой библиотеки

Для использования метода интеграции "до передачи сообщения в очередь" (before-queue интеграции) при компиляции динамически подгружаемой библиотеки из исходных кодов требуется указать, что необходима поддержка dlfunc. В некоторых дистрибутивах Linux в хранилище содержатся скомпилированные версии Exim, в других случаях требуется ручная компиляция.

В случае ручной компиляции требуется добавить в Makefile следующие строки:

```
EXPAND_DLFUNC=yes

EXTRALIBS= -export-dynamic
```

При before-queue интеграции с использованием динамически подгружаемой библиотеки фильтр должен передавать сообщения для проверки модулю Scan Logic по сокету `ServiceSocket`. Этот сокет требуется задать в конфигурации программы.

В зависимости от дистрибутива операционной системы вам требуется внести изменения в один или несколько конфигурационных файлов почтового сервера Exim. Например, в Debian и Ubuntu почтовый сервер Exim может конфигурироваться как с помощью нескольких файлов в директории /etc/exim/conf.d, так и с помощью одного файла.

► *Чтобы выполнить before-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Exim с использованием динамически подгружаемой библиотеки, выполните следующие действия:*

1. Убедитесь, что почтовый сервер Exim поддерживает функцию контентной фильтрации dlfunc. Для этого выполните команду `exim -bV`.

   Положительным ответом является результат: `Expand_dlfunc`.

2. Сделайте резервную копию конфигурационных файлов Exim.

3. Внесите изменения в список контроля доступа для `acl_smtp_data`. Для этого в конфигурационном файле (файлах) Exim найдите строку вида

   `acl_smtp_data = acl_check_data` (вместо `acl_check_data` может быть указан другой список контроля доступа)

   и после строки вида

   `acl_check_data:` (или строки, содержащей другой список контроля доступа)

   добавьте следующие строки:

   ```
   #klms-filter-begin

   warn    set acl_m_klms_headers =
   ```

```
                set acl_m_klms_result =

                set                acl_m_klms_answer                =
${dlfunc{LIBDIR/libklms-exim.so}{scan}{${spool_directory}/input}}

defer   condition       = ${if eq {$acl_m_klms_answer}{}{yes}{no}}

        log_message     = LMS check failed (empty answer)

        message         = Temporary local problem - please try later

defer           condition                           =    ${if    match
{$acl_m_klms_answer}{\N^451\N}{yes}{no}}

        log_message             =   LMS   check   defer:   ${if   match
{$acl_m_klms_answer} \

{\N^451 Mail processing aborted(.+\n?.*\n)*$\N}{$1}{}}\\

                        ${if eq {$acl_m_klms_result}{}{}{, result is
\

'$acl_m_klms_result\'}}\

                        , temporary file $acl_m_klms_tempfile

        message         = Temporary local problem - please try later

defer           condition                           =    ${if    match
{$acl_m_klms_answer}{\N^452\N}{yes}{no}}

        log_message                 =    LMS    check    defer:    ${if
match{$acl_m_klms_answer} \

{\N^451 Mail processing timed out(.+\n?.*\n)*$\N}{$1}{}}\

                        ${if eq {$acl_m_klms_result}{}{}{, result is
\

'$acl_m_klms_result\'}}\

                        , temporary file $acl_m_klms_tempfile
```

```
        message         = Temporary local problem - please try later

deny            condition                       =    ${if    match
{$acl_m_klms_answer}{\N^550\N}{yes}{no}}

        log_message             =   LMS   check   reject:   ${if   match
{$acl_m_klms_answer} \

{\N^550 Rejected by malware filter(.+\n?.*\n)*$\N}{$1}{}}\

                        ${if eq {$acl_m_klms_result}{}{}{, result is
\

'$acl_m_klms_result\'}}\

                        , temporary file $acl_m_klms_tempfile

deny            condition                       =    ${if    match
{$acl_m_klms_answer}{\N^554\N}{yes}{no}}

        log_message             =   LMS   check   reject:   ${if   match
{$acl_m_klms_answer} \

{\N^554 Mail processing failed(.+\n?.*\n)*$\N}{$1}{}}\

                        ${if eq {$acl_m_klms_result}{}{}{, result is
\

'$acl_m_klms_result\'}}\

                        , temporary file $acl_m_klms_tempfile

        message         = ${if match {$acl_m_klms_answer} \

{\N^554 Mail processing failed(.+\n?.*\n)*$\N} \

{Mail processing failed:$1}{}}

warn            condition                       =    ${if    match
{$acl_m_klms_answer}{\N^250\N}{yes}{no}}

        logwrite                =   LMS   check   accept:   ${if   match
{$acl_m_klms_answer} \
```

```
{\N^250 (.+)$\N}{$1}{}} \
                        ${if eq {$acl_m_klms_result}{}{}{, result is
\
'$acl_m_klms_result\'}}
        set acl_m_klms_answer        =
warn    condition       = ${if eq {$acl_m_klms_answer}{}{no}{yes}}
        logwrite        = LMS check: $acl_m_klms_answer


#klms-filter-end
```

где LIBDIR – путь к библиотеке libklms-exim.so:

- для FreeBSD (32-bit) - /usr/local/lib/kaspersky/klms/libklms-exim.so,
- для FreeBSD (64-bit) - /usr/local/lib/kaspersky/klms/compat64/libklms-exim.so,
- для Linux (32-bit) - /opt/kaspersky/klms/lib/libklms-exim.so,
- для Linux (64-bit) - /opt/kaspersky/klms/lib64/libklms-exim.so.

4. Скомпилируйте модуль `.so` согласно параметрам вашей операционной системы (опционально).
5. Добавьте пользователя `kluser` к группе, к которой принадлежит процесс `exim`.
6. В файле настроек фильтров, *klms_filter.conf*, в секции `[global]` установите значение `false` для параметра `header-guard`.
7. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
8. Добавьте в файл следующую строку:

   ```
   EXIM_INTEGRATION_TYPE=dlfunc
   ```

9. Перезапустите службу klms.

10. Перезапустите почтовый сервер Exim.

Пакет установки Kaspersky Security 8 для Linux Mail Server содержит скомпилированную динамически подгружаемую библиотеку dlfunc для всех поддерживаемых программой операционных систем. Необходимые исходные файлы для библиотеки dlfunc находятся в директории /opt/kaspersky/klms/share/src/dlfunc (для Linux) или в директории /usr/local/share/klms/src/dlfunc (для FreeBSD).

Но в некоторых случаях требуется ручная компиляция.

► *Чтобы выполнить ручную компиляцию динамически подгружаемой библиотеки dlfunc, выполните следующие действия:*

1. Установите исходные библиотеки почтового сервера Exim.

2. Установите библиотеку libevent версии 2.0.10 или выше.

3. Установите библиотеку boost версии 1.47.0 или выше.

4. Перейдите в директорию /opt/kaspersky/klms/share/src/dlfunc (для Linux) или в директорию /usr/local/share/klms/src/dlfunc (для FreeBSD)

5. Выполните команду `./configure --with-exim=<path to exim headers> --with-boost=<path to boost> --with-libevent=<path to libevent>`

6. Выполните следующую команду: `# make`.

В текущей директории появится файл libklms-exim.so.

Интеграция с почтовым сервером QMail вручную

Почтовый сервер QMail не предоставляет средств для интеграции расширений. Интеграция Kaspersky Security 8 для Linux Mail Server с почтовым сервером QMail вручную заключается в замене оригинального исполняемого файла qmail-queue файлом /opt/kaspersky/klms/lib/bin/klms-qmail (для Linux) или /usr/local/libexec/kaspersky/klms/klms-qmail (для FreeBSD), входящим в поставку программы.

Этот файл обеспечивает фильтрацию сообщений и передает сообщения оригинальному файлу qmail-queue для дальнейшей доставки. Оригинальный файл qmail-queue требуется переименовать в qmail-queue-real.

Сообщения передаются на проверку до размещения в очереди почтовой системы (before-queue фильтрация).

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с QMail вручную, выполните следующие действия:*

1. В файле настроек фильтров, `klms_filters.conf`, в секции `[global]`, параметру `sendmail-path` присвоите значение `/var/qmail/bin/sendmail`.

2. Скопируйте файл `/var/qmail/bin/qmail-queue` в директорию `/var/qmail/bin/qmail-queue-real` с помощью следующей команды:

   ```
   #cp –fp /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue-real
   ```

3. Скопируйте файл фильтра из пакета установки Kaspersky Security 8 для Linux Mail Server в директорию `qmail` с помощью следующей команды:

   - для Linux:

     ```
     #cp -fp /opt/kaspersky/klms/libexec/qmail-queue /var/qmail/bin/qmail-queue
     ```

   - для FreeBSD:

     ```
     #cp -fp /usr/local/libexec/kaspersky/klms/qmail-queue /var/qmail/bin/qmail-queue
     ```

4. Установите следующие права доступа для файлов `qmail-queue` и `qmail-queue-real`:

   ```
   # ls -la /var/qmail/bin/qmail-queue*

   -rws--s--x 1 qmaild klusers 2287242 Фев 19 20:53 /var/qmail/bin/qmail-queue

   -rws--x--x 1 qmailq qmail 19288 Июн 27 2013 /var/qmail/bin/qmail-queue-real
   ```

5. В файле настроек фильтров, *klms_filter.conf*, в секции `[global]` убедитесь, что параметр `header-guard` имеет значение `true`.

6. Перезапустите Kaspersky Security 8 для Linux Mail Server:

   ```
   service klms restart
   ```

Интеграция с почтовым сервером Postfix вручную

Для интеграции с почтовым сервером Postfix в Kaspersky Security 8 для Linux Mail Server предусмотрены три метода:

- Интеграция "после передачи в очередь" (after-queue интеграция). В этом случае все сообщения, проходящие через защищаемый компьютер, передаются на проверку программе после размещения в очереди почтового сервера Postfix.
- Интеграция "до передачи в очередь" (before-queue интеграция). В этом случае сообщения передаются на проверку программе до размещения в очереди почтового сервера Postfix.
- Интеграция по протоколу Milter. В этом случае сообщения передаются на проверку программе по протоколу Milter.

В этом разделе

After-queue интеграция

При интеграции «после передачи сообщения в очередь» (after-queue интеграции) для

передачи сообщений на проверку программе Kaspersky Security 8 для Linux Mail Server и возвращения их почтовому серверу Postfix требуется соблюдение следующих условий:

- Фильтр должен быть настроен для перехвата сообщений от почтового сервера Postfix по сокету `socket-in`. Этот сокет требуется задать в конфигурации программы.
- Фильтр должен передавать сообщения для проверки модулю Scan Logic по сокету `scanner`. Этот сокет требуется задать в конфигурации программы.
- Фильтр должен возвращать сообщения почтовому серверу Postfix по сокету `socket-out`. Этот сокет требуется задать в конфигурации программы.

При интеграции Kaspersky Security 8 для Linux Mail Server с почтовым сервером Postfix `socket-in`, `scanner` и `socket-out` могут указывать как на сетевой, так и на локальный сокет.

► *Чтобы выполнить after-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Postfix, выполните следующие действия:*

1. Откройте конфигурационный файл main.cf.
2. В конец файла main.cf добавьте следующие строки:

   ```
   #klms-begin-afterqueue-filter

   content_filter =klms_postfix-afterqueue:$sock_postfix_format

   #klms-end-afterqueue-filter
   ```

   где `$sock_postfix_format` – IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в формате `inet:<IP-адрес>:<порт>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

3. Откройте конфигурационный файл master.cf.
4. В конец файла master.cf добавьте следующие строки:

   ```
   #klms-begin-afterqueue-filter

   klms_postfix-afterqueue\tunix - - \n - 10 smtp
   ```

```
-o smtp_send_xforward_command=yes

127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd

-o content_filter=

-o receive_override_options=no_unknown_recipient_checks,\

no_header_body_checks,no_address_mappings

-o smtpd_helo_restrictions=

-o smtpd_client_restrictions=

-o smtpd_sender_restrictions=

-o smtpd_recipient_restrictions=permit_mynetworks,reject

-o mynetworks=127.0.0.0/8,[::1]/128

-o smtpd_authorized_xforward_hosts=127.0.0.0/8,[::1]/128

#klms-end-afterqueue-filter
```

где строка

`127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd` требуется для того, чтобы почтовый сервер Postfix принимал от фильтра обработанные сообщения, ожидая данных на порту `$forward_port`.

5. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
6. Добавьте в файл следующие строки:

```
POSTFIX_INTEGRATION_TYPE=afterqueue

START_SMTP_PROXY =1
```

7. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
8. В секции `[global]` установите значение `false` для параметра `header-guard`.

9. В секции `[smtp_proxy]` укажите следующие параметры:

   `socket-in=<IP-адрес и номер порта>` или `<UNIX-сокет>`, указанные в пункте 2 инструкции для `$sock_postfix_format`

   `socket-out=inet: $forward_port@127.0.0.1`

   в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

Пример:

```
socket-in=inet:10025@127.0.0.1

socket-out=inet: 10026@127.0.0.1
```

10. Перезапустите службу klms.

11. Перезапустите почтовый сервер Postfix.

Before-queue интеграция

При интеграции «после передачи сообщения в очередь» (before-queue интеграции) для передачи сообщений на проверку программе Kaspersky Security 8 для Linux Mail Server и возвращения их почтовому серверу Postfix требуется соблюдение следующих условий:

- Фильтр должен быть настроен для перехвата сообщений от почтового сервера Postfix по сокету `socket-in`. Этот сокет требуется задать в конфигурации программы.

- Фильтр должен передавать сообщения для проверки модулю Scan Logic по сокету `scanner`. Этот сокет требуется задать в конфигурации программы.

- Фильтр должен возвращать сообщения почтовому серверу Postfix по сокету `socket-out`. Этот сокет требуется задать в конфигурации программы.

При интеграции Kaspersky Security 8 для Linux Mail Server с почтовым сервером Postfix `socket-in`, `scanner` и `socket-out` могут указывать как на сетевой, так и на локальный сокет.

► *Чтобы выполнить before-queue интеграцию Kaspersky Security 8 для Linux Mail Server с Postfix, выполните следующие действия:*

1. Откройте конфигурационный файл master.cf.

2. В файл master.cf после строки вида

   ```
   smtp inet n - n - - smtpd
   ```

   добавьте следующие строки:

   ```
   #klms-postfix-prequeue-start

   -o smtpd_proxy_filter=$sock_postfix_format

   -o smtpd_proxy_options=speed_adjust
   ```
   (для интеграции с Postfix 2.7 или выше)

   ```
   #klms-postfix-prequeue-end
   ```

   где `$sock_postfix_format` – IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в формате `inet:<IP-адрес>:<порт>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

3. В конец конфигурационного файла master.cf добавьте следующие строки:

   ```
   #klms-begin

   klms_postfix-prequeue unix - - n - 10 smtp

   -o smtp_send_xforward_command=yes

   127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd

   -o receive_override_options=no_unknown_recipient_checks, \

   no_header_body_checks,no_address_mappings

   -o smtpd_helo_restrictions=
   ```

```
-o smtpd_client_restrictions=

-o smtpd_sender_restrictions=

-o smtpd_recipient_restrictions=permit_mynetworks,reject

-o mynetworks=127.0.0.0/8,[::1]/128

-o smtpd_authorized_xforward_hosts=127.0.0.0/8,[::1]/128

#klms-end
```

где строка

`127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd` требуется для того, чтобы почтовый сервер Postfix принимал от фильтра обработанные сообщения, ожидая данных на порту `$forward_port`.

4. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
5. Добавьте в файл следующие строки:

   ```
   POSTFIX_INTEGRATION_TYPE= prequeue

   START_SMTP_PROXY =1
   ```

6. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
7. В секции `[global]` установите значение `false` для параметра `header-guard`.
8. В секции `[smtp_proxy]` укажите следующие параметры:

   `socket-in=<IP-адрес и номер порта>` или `<UNIX-сокет>`, указанные в пункте 2 инструкции для `$sock_postfix_format`

   ```
   socket-out=inet: $forward_port@127.0.0.1
   ```

   в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

Пример:

```
socket-in=inet:10025@127.0.0.1

socket-out=inet: 10026@127.0.0.1
```

9. Перезапустите службу klms.

10. Перезапустите почтовый сервер Postfix.

Интеграция по протоколу Milter

При интеграции Kaspersky Security 8 для Linux Mail Server с почтовым сервером Postfix по протоколу Milter для передачи сообщений на проверку программе Kaspersky Security 8 для Linux Mail Server и возвращения их почтовому серверу Postfix требуется соблюдение следующих условий:

- Фильтр должен быть настроен для перехвата сообщений от почтового сервера Postfix по сокету `socket`. Этот сокет требуется задать в конфигурации программы.
- Фильтр должен передавать сообщения для проверки модулю Scan Logic по сокету `scanner`. Этот сокет требуется задать в конфигурации программы.

При интеграции Kaspersky Security 8 для Linux Mail Server с почтовым сервером Postfix `socket` и `scanner` могут указывать как на сетевой, так и на локальный сокет.

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Postfix по протоколу Milter, выполните следующие действия:*

1. Выполните следующую команду:

   ```
   postconf -e $milter_socket
   ```

   где `$milter_socket` – IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

2. Откройте конфигурационный файл main.cf.

3. В конец файла main.cf добавьте следующие строки:

```
#lms-milter-begin

milter_connect_macros = j _ {daemon_name} {if_name} {if_addr}

milter_helo_macros = {tls_version} {cipher} {cipher_bits}
{cert_subject} \

{cert_issuer}

milter_mail_macros = i {auth_type} {auth_authen} {auth_ssf}
{auth_author} \

{mail_mailer} {mail_host} {mail_addr}

milter_rcpt_macros = {rcpt_mailer} {rcpt_host} {rcpt_addr}

milter_default_action = $fail_type

milter_protocol = 3

milter_connect_timeout=180

milter_command_timeout=180

milter_content_timeout=600

#lms-milter-end
```

где `$fail_type` может принимать значения `reject`, `accept` или `tempfail`.

Параметр `$fail_type` определяет действие почтового сервера Postfix над сообщением в том случае, если фильтр недоступен:

- `reject` – отклонять;
- `accept` – пропускать без проверки;
- `tempfail` – отправлять отправителю сообщения уведомление о временной ошибке.

Рекомендуется использовать `tempfail`.

4. Откройте файл /var/opt/kaspersky/klms/installer.dat (для Linux) или /var/db/kaspersky/klms/installer.dat (для FreeBSD).
5. Добавьте в файл следующие строки:

   ```
   POSTFIX_INTEGRATION_TYPE= milter

   START_MILTER=1
   ```

6. Откройте файл /etc/opt/kaspersky/klms/klms_filters.conf (для Linux) или /usr/local/etc/kaspersky/klms/klms_filters.conf (для FreeBSD).
7. В секции `[milter]` укажите IP-адрес и номер порта или UNIX-сокет, на котором фильтр ожидает входящие соединения, в следующей строке:

   `socket=<IP-адрес и номер порта>` или `<UNIX-сокет>`, указанные в пункте 1 инструкции для `$milter_socket`

   в формате `inet:<порт>@<IP-адрес>` (для сетевого сокета) или `unix:<путь к UNIX-сокету>` (для UNIX-сокета).

Пример:

```
socket=inet:10025@127.0.0.1
```

8. В секции `[global]` установите значение `false` для параметра `header-guard`.
9. Перезапустите службу klms.
10. Перезапустите почтовый сервер Postfix.

Интеграция с интерфейсом Amavis вручную

► *Чтобы интегрировать Kaspersky Security 8 для Linux Mail Server с Amavis вручную, выполните следующие действия:*

1. Добавьте учетную запись пользователя kluser в группу пользователей amavis (или в группу, указанную в параметре `$daemon_group` конфигурационного файла /etc/amavisd.conf) с помощью следующей команды:

   ```
   gpasswd -a kluser amavis
   ```

2. Добавьте учетную запись пользователя amavis (или пользователя, указанного в параметре `$daemon_user` конфигурационного файла amavisd.conf (далее /etc/amavis.conf)) в группу пользователей klusers с помощью следующей команды:

   ```
   gpasswd -a amavis klusers
   ```

3. Откройте файл amavisd (далее - /usr/sbin/amavisd)

4. В секции `@spam_scanners` закомментируйте следующую строку:

   ```
   @spam_scanners = (

   #['SpamdClient', 'Amavis::SpamControl::SpamdClient' ],
   ```

5. Для операционной системы SUSE Linux 11 SP2 добавьте учетную запись пользователя kluser в группу пользователей vscan. Группа пользователей vscan должна быть основной группой для учетной записи пользователя kluser.

6. Для операционной системы SUSE Linux 11 SP2 добавьте учетную запись пользователя vscan в группу пользователей klusers. Группа пользователей klusers должна быть основной группой для учетной записи пользователя vscan.

7. В файле /usr/sbin/amavisd для Perl-модуля SpamdClient укажите сокет rds_asp, на котором задача KLRDS ожидает входящие сообщения, в следующих строках:

   ```
   package Amavis::SpamControl::SpamdClient ...

   my($spamd_handle) = Amavis::IO::RW->new(
   ```

```
[ '/var/run/klms/rds_asp' ], Eol => "\015\012", Timeout => 30);
```

8. Откройте конфигурационный файл amavisd.conf (далее /etc/amavisd.conf)

9. Внесите следующие изменения в секции `@av_scanners` и `@spam_scanners` конфигурационного файла:

```
@av_scanners = (

['Kaspersky Security 8.0 for Linux Mail Server',

  \&ask_daemon, ["nCONTSCAN {}\n", "/var/run/klms/rds_av"],

  qr/\bOK$/m, qr/\bFOUND$/m,

  qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ], ); ...

@spam_scanners = (

['SpamdClient',  'Amavis::SpamControl::SpamdClient' ], );
```

10. Рекомендуется установить ограничение в 1500 КБ на максимальный размер сообщения при использовании проверки на спам. Для этого установите следующее значение в строке:

```
$sa_mail_body_size_limit = 1500000;
```

11. Перезапустите службу amavisd с помощью следующей команды:

```
/etc/init.d/amavisd restart
```

При интеграции с интерфейсом Amavis вы можете установить параметры Kaspersky Security 8 для Linux Mail Server только с помощью командной строки. Параметры, установленные через веб-интерфейс Kaspersky Security 8 для Linux Mail Server (например, время ожидания ответа от KSN) не будут применены.

Мониторинг Kaspersky Security 8 для Linux Mail Server

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 Security 8 для Linux Mail Server, 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.

Работа с правилами обработки сообщений

Правило обработки сообщений (далее также "правило") – заданное множество пар адресов отправителей и получателей, сообщения электронной почты которых Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server просматривает комбинацию адресов *отправитель-получатель* каждого правила, начиная с правила с наивысшим приоритетом (1). Если совпадение не найдено, Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server.
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 Security 8 для Linux Mail Server для правила:

  - **Анти-Спам**.
  - **Антивирус** (см. раздел "**Включение и отключение антивирусной проверки для правила**" на стр. 241).
  - **Защита KATA** (см. раздел "**Включение и отключение защиты KATA для правила**" на стр. 264).
  - **Анти-Фишинг**.
  - **Контентная фильтрация**.
  - **Уведомления** (см. раздел "**Настройка уведомлений о событиях проверки сообщений для правила**" на стр. 296).
  - **Примечание к сообщению** (см. раздел "**Добавление примечания к событиям проверки сообщений для правила**" на стр. 313).
  - **Предупреждение о небезопасном сообщении** (см. раздел "**Добавление предупреждения о небезопасном сообщении для правила**" на стр. 314).
  - **Проверка подлинности отправителей сообщений** (см. раздел "**Включение и отключение проверки подлинности отправителей для правила**" на стр. 220).

- **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** (см. раздел "**Добавление примечания к событиям проверки сообщений для правила**" на стр. 313), 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 Security 8 для Linux Mail Server, требуется настроить список отправителей сообщений (см. раздел "Добавление адресов электронной почты" на стр. 164) 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. 162).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176). 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 Security 8 для Linux Mail Server.
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 Security 8 для Linux Mail Server для этого правила (см. раздел "Создание правила обработки сообщений" на стр. 159).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176). 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 Security 8 для Linux Mail Server, 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. 167) 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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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. 173).

► *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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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 Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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.

Хранилище

Хранилище предназначено для копий сообщений, которые Kaspersky Security 8 для Linux Mail Server сохраняет во время обработки. Копии сообщений хранятся в хранилище в недоступном для чтения виде и поэтому не угрожают безопасности вашего компьютера.

Kaspersky Security 8 для Linux Mail Server помещает в Хранилище копии сообщений:

- которым модуль Антивирус присвоил один из статусов проверки (см. раздел "О статусах антивирусной проверки сообщений" на стр. 240) и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями при антивирусной проверке" на стр. 245);
- которым модуль Анти-Спам присвоил один из статусов проверки и перед выполнением над ними действий;
- 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 (см. раздел "О статусах проверки сообщений в KATA" на стр. 254) и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями по результатам проверки KATA" на стр. 265);
- которым по результатам проверки подлинности отправителей сообщений присвоен один из статусов проверки (см. раздел "О статусах проверки подлинности отправителей сообщений" на стр. 216) и перед выполнением над ними действий (см. раздел "Настройка действий над сообщениями при DMARC-, SPF- и DKIM-проверке" на стр. 229);
- адреса отправителей которых обнаружены в персональном черном списке адресов (см. раздел "Настройка параметров персонального черного списка адресов" на стр. 270) 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 Security 8 для Linux Mail Server.

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. 184) зараженных сообщений из Хранилища получателям.

   - **Нет**, если вы хотите запретить доставку (см. раздел "Доставка сообщения из Хранилища получателям" на стр. 184) зараженных сообщений из Хранилища получателям.

   > Этот параметр применяется для учетной записи HelpDesk (см. раздел "Настройка параметров учетной записи HelpDesk" на стр. 340). Пользователь под учетной записью Administrator может доставлять сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища получателям" на стр. 184) 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 Security 8 для Linux Mail Server, 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. 182) 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. 178) (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. 182) 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 Security 8 для Linux Mail Server.

   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. 182) 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 Security 8 для Linux Mail Server

Этот раздел содержит информацию о работе с очередями сообщений в KATA-карантине и Анти-Спам карантине, а также о том, как отсортировать, отфильтровать, принудительно отправить сообщения или выполнить поиск сообщений в очереди.

В этом разделе

Просмотр информации об очереди сообщений

► *Чтобы просмотреть информацию об очереди сообщений,*

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 Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform" на стр. 253).

- **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 Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform" на стр. 253).

- **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.

- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине 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:
   - **Анти-Спам карантин**.
   - **KATA-карантин**.
4. Нажмите на кнопку **Применить**.

В рабочей области раздела **Очередь сообщений** главного окна веб-интерфейса Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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.
   - **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 Security 8 для Linux Mail Server не будет ждать результата проверки этих сообщений. Эти сообщения не будут отображаться в очереди на проверку.

Отчеты о работе Kaspersky Security 8 для Linux Mail Server

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 Security 8 для Linux Mail Server

Вы можете получить информацию о результатах работы Kaspersky Security 8 для Linux Mail Server за определенный период из отчетов о работе Kaspersky Security 8 для Linux Mail Server.

Отчеты содержат следующую информацию о работе Kaspersky Security 8 для Linux Mail Server:

1. Суммарный отчет по обнаружениям. Отчет о результатах работы модулей Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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. 158).

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 Security 8 для Linux Mail Server

► Чтобы просмотреть отчеты о работе *Kaspersky Security 8 для Linux Mail Server*, 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 Security 8 для Linux Mail Server.

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.

Обновление баз Kaspersky Security 8 для Linux Mail Server

Этот раздел содержит информацию об обновлении антивирусных баз.

В этом разделе

Об обновлении баз

Базы модуля Антивирус (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.

Если вы настроили автоматическое обновление баз, Kaspersky Security 8 для Linux Mail Server выполняет его по расписанию (с периодичностью один раз в пять минут).

По умолчанию если антивирусные базы Kaspersky Security 8 для Linux Mail Server не обновляются в течение суток с момента, когда "Лаборатория Касперского" опубликовала последние пакеты обновлений, Kaspersky Security 8 для Linux Mail Server записывает в журнал событий событие *Базы устарели*. Если антивирусные базы не обновляются в течение недели, Kaspersky Security 8 для Linux Mail Server записывает событие *Базы сильно устарели*. Вы можете настроить уведомления администратора об этих событиях.

Об источниках обновлений

Источник обновлений – это ресурс, содержащий обновления баз Kaspersky Security 8 для Linux Mail Server.

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. 208).

Чтобы уменьшить интернет-трафик, вы можете настроить обновление баз Kaspersky Security 8 для Linux Mail Server из *пользовательского источника обновлений.* Пользовательским источником обновлений могут служить указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

Если Kaspersky Security 8 для Linux Mail Server 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:

   - **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.

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. 207).
   - **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 **25.05.2018** и **15:00**, то

обновление баз запускается каждые три часа, начиная с 15 часов 25 мая 2018 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 Security 8 для Linux Mail Server.

   - **Нет**, если вы хотите отключить использование прокси-сервера в работе Kaspersky Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server.
   - Выключите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы не хотите использовать прокси-сервер в работе Kaspersky Security 8 для Linux Mail Server.

Вы можете включить использование прокси-сервера только после того, как настроите параметры соединения с прокси-сервером.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и использовании Kaspersky Private Security Network.

В этом разделе

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

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, 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.

Проверка подлинности отправителей сообщений

Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры вашей организации от спама и фишинга.

Kaspersky Security 8 для Linux Mail Server использует следующие технологии проверки подлинности отправителей сообщений:

- SPF-проверку (Sender Policy Framework).
- DKIM-проверку (DomainKeys Identified Mail).
- DMARC-проверку (Domain-based Message Authentication, Reporting and Conformance).

SPF-проверка подлинности отправителей сообщений – сопоставление IP-адресов отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

Kaspersky Security 8 для Linux Mail Server получает списки возможных источников сообщений с DNS-сервера.

Включайте SPF-проверку, если Kaspersky Security 8 для Linux Mail Server принимает сообщения напрямую из интернета. Отключайте SPF-проверку, если Kaspersky Security 8 для Linux Mail Server принимает сообщения с внутреннего промежуточного сервера.

DKIM-проверка подлинности отправителей сообщений – проверка цифровой подписи к сообщениям.

К сообщениям добавляется цифровая подпись, связанная с именем домена организации. Kaspersky Security 8 для Linux Mail Server проверяет эту цифровую подпись.

DMARC-проверка подлинности отправителей сообщений – проверка, определяющая политику и действия над сообщениями по результатам SPF- и DKIM-проверок подлинности отправителей сообщений.

После того, как сообщение прошло SPF- и DKIM-проверки, выполняется проверка того, что домен, содержащий адрес отправителя в поле От заголовка сообщения электронной почты, соответствует идентификаторам SPF и DKIM.

Для выполнения SPF-, DKIM- и DMARC-проверок подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу (см. раздел "Подключение к DNS-серверу для проверки подлинности отправителей" на стр. 217). Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

Если по результатам SPF-, DKIM- или DMARC-проверок подлинности отправителей сообщений Kaspersky Security 8 для Linux Mail Server обнаруживает нарушения, считается, что при SPF-, DKIM- или DMARC-проверках обнаружены *нарушения подлинности отправителей сообщений*.

В этом разделе

О статусах проверки подлинности отправителей сообщений

По результатам всех проверок подлинности отправителей сообщений программа присваивает сообщению один из следующих статусов:

- *ViolationNotFound* – нарушения подлинности отправителя сообщения не обнаружены.
- *ViolationFound* – обнаружено одно или несколько нарушений подлинности отправителя сообщения.

По результатам DMARC-проверки подлинности отправителей сообщений программа присваивает сообщению один из следующих статусов:

- *Pass* – нарушение подлинности отправителя сообщения не обнаружено.
- *Fail* – обнаружено нарушение подлинности отправителя сообщения.
- *TempError* – временная ошибка проверки подлинности отправителя сообщения.
- *PermError* – постоянная ошибка проверки подлинности отправителя сообщения.

По результатам DKIM-проверки подлинности отправителей сообщений программа присваивает сообщению один из следующих статусов:

- *Pass* – нарушение подлинности отправителя сообщения не обнаружено.
- *Fail* – обнаружено нарушение подлинности отправителя сообщения.
- *TempError* – временная ошибка проверки подлинности отправителя сообщения.
- *PermError* – постоянная ошибка проверки подлинности отправителя сообщения.
- *Neutral* – сообщение содержит цифровую подпись некорректного формата.

По результатам SPF-проверки подлинности отправителей сообщений программа присваивает сообщению один из следующих статусов:

- *Pass* – нарушение подлинности отправителя сообщения не обнаружено.
- *Fail* – обнаружено нарушение подлинности отправителя сообщения.

- *SoftFail* – обнаружено незначительное нарушение подлинности отправителя сообщения.
- *TempError* – временная ошибка проверки подлинности отправителя сообщения.
- *PermError* – постоянная ошибка проверки подлинности отправителя сообщения.
- *Neutral* – сообщение содержит цифровую подпись некорректного формата.

Подключение к DNS-серверу для проверки подлинности отправителей

Для выполнения проверки подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу. Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

Вы также можете задать максимальное время ожидания ответа от DNS-сервера, по истечении которого DNS-сервер будет считаться недоступным, и сообщение будет обработано Kaspersky Security 8 для Linux Mail Server без проверки подлинности отправителей. Значение по умолчанию: 10 сек.

► *Чтобы разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу, 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 **Разрешить подключение к DNS-серверу** откройте окно **Внешние службы**.
3. В списке справа от названия параметра **Разрешить подключение к DNS-серверу** выберите **Да**.
4. Нажмите на кнопку **Применить**.

► *Чтобы задать максимальное время ожидания ответа от DNS-сервера, 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 **Разрешить подключение к DNS-серверу** откройте окно **Внешние службы**.

3. В поле справа от названия параметра **Ждать ответ от DNS-сервера** укажите максимальное время ожидания ответа от DNS-сервера в секундах.

   Значение по умолчанию: 10 сек.

4. Нажмите на кнопку **Применить**.

Включение и отключение SPF-проверки подлинности отправителей

► *Чтобы включить или отключить SPF-проверку подлинности отправителей сообщений, 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 **Включить SPF-проверку подлинности отправителей** откройте окно **Внешние службы**.

3. В списке справа от названия параметра **Включить SPF-проверку подлинности отправителей** выберите один из следующих вариантов:

   - **Да**, если вы хотите включить SPF-проверку подлинности отправителей сообщений.

   - **Нет**, если вы хотите отключить SPF-проверку подлинности отправителей сообщений.

4. Нажмите на кнопку **Применить**.

Для выполнения SPF-проверки подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу (см. раздел "Подключение к DNS-серверу для проверки подлинности отправителей" на стр. 217). Если подключение к DNS-серверу запрещено, SPF-проверка подлинности отправителей сообщений будет отключена.

Включение и отключение DKIM-проверки подлинности отправителей

► *Чтобы включить или отключить DKIM-проверку подлинности отправителей сообщений, 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 **Включить DKIM-проверку подлинности отправителей** откройте окно **Внешние службы**.
3. В списке справа от названия параметра **Включить DKIM-проверку подлинности отправителей** выберите один из следующих вариантов:
   - **Да**, если вы хотите включить DKIM-проверку подлинности отправителей сообщений.
   - **Нет**, если вы хотите отключить DKIM-проверку подлинности отправителей сообщений.
4. Нажмите на кнопку **Применить**.

Для DKIM-проверки подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу (см. раздел "Подключение к DNS-серверу для проверки подлинности отправителей" на стр. 217). Если подключение к DNS-серверу запрещено, DKIM-проверка подлинности отправителей сообщений будет отключена.

Включение и отключение DMARC-проверки подлинности отправителей

► *Чтобы включить или отключить DMARC-проверку подлинности отправителей сообщений, 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 **Включить DMARC-проверку подлинности отправителей** откройте окно **Внешние службы**.
3. В списке справа от названия параметра **Включить DMARC-проверку подлинности отправителей** выберите один из следующих вариантов:
   - **Да**, если вы хотите включить DMARC-проверку подлинности отправителей сообщений.
   - **Нет**, если вы хотите отключить DMARC-проверку подлинности отправителей сообщений.
4. Нажмите на кнопку **Применить**.

Для DMARC-проверки подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security 8 для Linux Mail Server к DNS-серверу (см. раздел "Подключение к DNS-серверу для проверки подлинности отправителей" на стр. 217). Если подключение к DNS-серверу запрещено, DMARC-проверка подлинности отправителей сообщений будет отключена.

Включение и отключение проверки подлинности отправителей для правила

Вы можете включить или отключить проверку подлинности отправителей сообщений для одного или нескольких правил.

Перед тем как включить проверку подлинности отправителей сообщений для правила, убедитесь, что как минимум одна проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение SPF-проверки подлинности отправителей" на стр. 218, "Включение и отключение DKIM-проверки подлинности отправителей" на стр. 219, "Включение и отключение DMARC-проверки подлинности отправителей" на стр. 220).

► *Чтобы включить или отключить проверку подлинности отправителей 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 проверку подлинности отправителей сообщений.
3. Выберите блок **Проверка подлинности отправителей сообщений**.
4. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если вы хотите включить проверку подлинности отправителей сообщений.
   - Выключите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если вы хотите отключить проверку подлинности отправителей сообщений.
5. В нижней части рабочей области нажмите на кнопку **Применить**.

Настройка обнаружения ошибок TempError и PermError при проверке подлинности отправителей

Если вы хотите, чтобы наличие временной ошибки TempError считалось нарушением подлинности отправителей сообщений, вы можете указать это для одного или нескольких правил.

Перед тем как указать, считать ли временную ошибку TempError нарушением подлинности отправителей сообщений, убедитесь, что как минимум одна проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение SPF-проверки подлинности отправителей" на стр. 218, "Включение и отключение DKIM-проверки подлинности отправителей" на стр. 219, "Включение и отключение DMARC-проверки подлинности отправителей" на стр. 220).

► *Чтобы указать, считать ли временную ошибку TempError нарушением подлинности 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, для которого вы хотите указать, считать ли временную ошибку TempError нарушением подлинности отправителей сообщений.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Выполните одно из следующих действий:

   - Установите флажок рядом с названием параметра **Считать временные ошибки (TempError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал временные ошибки TempError нарушением подлинности отправителя сообщений.

   - Снимите флажок рядом с названием параметра **Считать временные ошибки (TempError) нарушением подлинности отправителя**, если вы не хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал временные ошибки TempError нарушением подлинности отправителя сообщений.

5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием параметра **Считать постоянные ошибки (PermError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал постоянные ошибки PermError нарушением подлинности отправителя сообщений.

- Снимите флажок рядом с названием параметра **Считать постоянные ошибки (PermError) нарушением подлинности отправителя**, если вы не хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал постоянные ошибки PermError нарушением подлинности отправителя сообщений.

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

Настройка дополнительных параметров DMARC-проверки для правила

Вы можете настроить дополнительные параметры DMARC-проверки подлинности отправителей сообщений для одного или нескольких правил.

Перед тем как настроить дополнительные параметры DMARC-проверки сообщений для правила, убедитесь, что DMARC-проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение SPF-проверки подлинности отправителей" на стр. 218).

► *Чтобы настроить дополнительные параметры DMARC-проверки 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 дополнительные параметры DMARC-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **DMARC-проверка подлинности отправителей** выполните одно из следующих действий:

   - Установите флажок рядом с названием параметра **Считать результат DMARC-проверки приоритетным**, если вы хотите, чтобы Kaspersky Security 8

для Linux Mail Server определял нарушение подлинности отправителя сообщений по результатам DMARC-проверки.

- Снимите флажок рядом с названием параметра **Считать результат DMARC-проверки приоритетным**, если вы не хотите, чтобы Kaspersky Security 8 для Linux Mail Server определял нарушение подлинности отправителя сообщений по результатам DMARC-проверки.

Если флажок установлен, нарушение подлинности отправителя сообщений определяется по результатам DMARC-проверки. Если флажок снят, результаты SPF-, DKIM- и DMARC-проверок считаются равнозначными. Нарушение при любой из этих проверок считается нарушением подлинности отправителя. При нарушении по нескольким проверкам одновременно, над сообщением выполняется самое строгое из заданных действий над сообщением (см. раздел "Настройка действий над сообщениями при DMARC-, SPF- и DKIM-проверке" на стр. 229) при SPF-, DKIM- или DMARC-нарушениях подлинности отправителя.

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

Настройка дополнительных параметров SPF-проверки для правила

Вы можете настроить дополнительные параметры SPF-проверки подлинности отправителей сообщений для одного или нескольких правил.

Перед тем как настроить дополнительные параметры SPF-проверки сообщений для правила, убедитесь, что SPF-проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение SPF-проверки подлинности отправителей" на стр. 218).

► *Чтобы настроить дополнительные параметры SPF-проверки 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 дополнительные параметры SPF-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **SPF-проверка подлинности отправителей** выполните одно из следующих действий:

   - Установите флажок рядом с названием параметра **Считать SPF softfail нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал ошибку SPF softfail, обнаруженную при SPF-проверке, нарушением подлинности отправителя сообщений.

   - Снимите флажок рядом с названием параметра **Считать SPF softfail нарушением подлинности отправителя**, если вы не хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал ошибку SPF softfail, обнаруженную при SPF-проверке, нарушением подлинности отправителя сообщений.

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

Настройка дополнительных параметров DKIM-проверки для правила

Вы можете настроить дополнительные параметры DKIM-проверки подлинности отправителей сообщений для одного или нескольких правил.

Перед тем как настроить дополнительные параметры DKIM-проверки сообщений для правила, убедитесь, что DKIM-проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение DKIM-проверки подлинности отправителей" на стр. 219).

► *Чтобы настроить дополнительные параметры DKIM-проверки 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 дополнительные параметры DKIM-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **DKIM-проверка подлинности отправителей** выполните одно из следующих действий:

   - Установите флажок рядом с названием параметра **Считать отсутствие DKIM-подписи нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал отсутствие DKIM-подписи к сообщению, обнаруженное при DKIM-проверке, нарушением подлинности отправителя сообщения.

   - Снимите флажок рядом с названием параметра **Считать отсутствие DKIM-подписи нарушением подлинности отправителя**, если вы не хотите, чтобы Kaspersky Security 8 для Linux Mail Server считал отсутствие DKIM-подписи к сообщению, обнаруженное при DKIM-проверке, нарушением подлинности отправителя сообщения.

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

Настройка меток к теме сообщений по результатам SPF-проверки

► *Чтобы настроить метки, добавляемые Kaspersky Security 8 для Linux Mail Server к теме сообщений по результатам SPF-проверки подлинности 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, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам SPF-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **SPF-проверка подлинности отправителей** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения нарушения при SPF-проверке**.

6. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщения при SPF-нарушении подлинности отправителя сообщения.

7. Нажмите на кнопку **ОК**.

   Окно **Метка для обозначения нарушения при SPF-проверке** закроется.

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

Настройка меток к теме сообщений по результатам DKIM-проверки

► *Чтобы настроить метки, добавляемые Kaspersky Security 8 для Linux Mail Server к теме сообщений по результатам DKIM-проверки подлинности 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, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам DKIM-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **DKIM-проверка подлинности отправителей** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения нарушения при DKIM-проверке**.

6. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщения при DKIM-нарушении подлинности отправителя сообщения.

7. Нажмите на кнопку **ОК**.

   Окно **Метка для обозначения нарушения при DKIM-проверке** закроется.

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

Настройка меток к теме сообщений по результатам DMARC-проверки

► *Чтобы настроить метки, добавляемые Kaspersky Security 8 для Linux Mail Server к теме сообщений по результатам DMARC-проверки подлинности 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, для которого вы хотите настроить метки, добавляемые к теме сообщений по результатам DMARC-проверки.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке параметров **Если обнаружено DMARC-нарушение** по ссылке справа от названия параметра **Добавлять к теме сообщения текст** откройте окно **Метка для обозначения нарушения при DMARC-проверке**.

6. В поле под названием окна введите текст, который вы хотите добавить в начало темы сообщения при DMARC-нарушении подлинности отправителя сообщения.

7. Нажмите на кнопку **ОК**.

   Окно **Метка для обозначения нарушения при DMARC-проверке** закроется.

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

Настройка действий над сообщениями при DMARC-, SPF- и DKIM-проверке

Вы можете настроить действия над сообщениями при DMARC-, SPF- и DKIM-проверке подлинности отправителей сообщений для одного или нескольких правил.

Перед тем как настроить действия над сообщениями при DMARC-, SPF- и DKIM-проверке, убедитесь, что соответствующая проверка подлинности отправителей сообщений включена в параметрах Kaspersky Security 8 для Linux Mail Server (см. раздел "Включение и отключение DMARC-проверки подлинности отправителей" на стр. 220).

► *Чтобы настроить действия над сообщениями при DMARC-, SPF- и DKIM-проверке подлинности 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, для которого вы хотите настроить действия над сообщениями при DMARC-проверке.

3. Выберите блок **Проверка подлинности отправителей сообщений**.

4. Включите переключатель рядом с названием блока параметров **Проверка подлинности отправителей сообщений**, если он выключен.

5. В блоке **DMARC-проверка подлинности отправителей** в раскрывающемся списке **Если обнаружено DMARC-нарушение** выберите одно из следующих действий над сообщениями, DMARC-проверка которых выявила нарушение подлинности отправителя сообщений:

   - **Применить DMARC-политику**.

     DMARC-политика задается администратором почтового сервера на DNS-сервере.

   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

6. Установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**, если вы хотите настроить автоматическое сохранение копий сообщений в Хранилище перед их обработкой.

7. В блоке **SPF-проверка подлинности отправителей** в раскрывающемся списке **Если обнаружено SPF-нарушение** выберите одно из следующих действий над сообщениями, SPF-проверка которых выявила нарушение подлинности отправителя сообщений:

   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

8. Установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**, если вы хотите настроить автоматическое сохранение копий сообщений в Хранилище перед их обработкой.

9. В блоке **DKIM-проверка подлинности отправителей** в раскрывающемся списке **Если обнаружено DKIM-нарушение** выберите одно из следующих действий над сообщениями, DKIM-проверка которых выявила нарушение подлинности отправителя сообщений:

   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

10. Установите флажок рядом с названием параметра **Предварительно поместить копию в хранилище**, если вы хотите настроить автоматическое сохранение копий сообщений в Хранилище перед их обработкой.

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

Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений

Для того чтобы удаленный почтовый сервер мог проверить подлинность отправителя сообщений, если отправителем сообщений является Kaspersky Security 8 для Linux Mail Server (подлинность отправителя исходящих сообщений), вам нужно добавить SPF- и DMARC-записи в параметры вашего DNS-сервера.

► *Чтобы добавить SPF- и DMARC-записи 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 проверку подлинности отправителя исходящих сообщений.

   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 проверку подлинности отправителя исходящих сообщений.

4. В списке записей формата TXT добавьте SPF-запись для определенного домена следующего содержания:

   ```
   <имя домена, для адресов которого вы хотите настроить SPF-проверку подлинности отправителя исходящих сообщений> IN TXT "v=<версия SPF> +all>"
   ```

   Например, вы можете добавить строку:

   ```
   example.com IN TXT "v=spf1 +all"
   ```

   > Подробнее о назначении параметров SPF-записи см. в документе RFC 4408.

5. В списке записей формата TXT добавьте DMARC-запись для определенного домена следующего содержания:

   ```
   _dmarc.<имя домена, для адресов которого вы хотите настроить DMARC-проверку подлинности отправителя исходящих сообщений>. IN TXT "v=<версия DMARC>; p=<действие, которое удаленный почтовый сервер будет производить над всеми сообщениями электронной почты, не удовлетворяющими требованиям DMARC>;"
   ```

   Например, вы можете добавить строку:

   ```
   _dmarc.example.com. IN TXT "v=DMARC1; p=quarantine;"
   ```

   > Подробнее о назначении параметров DMARC-записи см. в документации DMARC.

6. Сохраните изменения.

> Синтаксис примеров SPF- и DMARC-записей приведен для добавления в параметры DNS-сервера BIND. Синтаксис SPF- и DMARC-записей, добавляемых в параметры других DNS-серверов, может незначительно отличаться от приведенных примеров.

Антивирусная защита сообщений

Kaspersky Security 8 для Linux Mail Server 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. 242) некоторых легальных программ (см. раздел "О защите компьютеров от некоторых легальных программ" на стр. 235) модулем Антивирус.

По результатам антивирусной проверки модуль Антивирус присваивает сообщению один из статусов антивирусной проверки (см. раздел "О статусах антивирусной проверки сообщений" на стр. 240) и добавляет метку, содержащую статус, в начало темы сообщения.

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. 245), которые программа выполняет над сообщениями с определенным статусом, и настраивать метки (см. раздел "Настройка меток к теме сообщений по результатам антивирусной проверки" на стр. 248) 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. 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. 241) или отключить антивирусную проверку сообщений для любого правила (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 241).

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.

Тип	Название	Описание
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.

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

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 Security 8 для Linux Mail Server 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. 235) 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 Security 8 для Linux Mail Server.
   - **Нет**, если вы хотите отключить обнаружение таких программ Kaspersky Security 8 для Linux Mail Server.
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 Security 8 для Linux Mail Server выполняет следующие действия:
   - Прерывает проверку сообщения.
   - Выполняет действие над сообщением, которое вы настроили (см. раздел "Настройка действий над сообщениями при антивирусной проверке" на стр. 245).
   - Присваивает сообщению статус *Error.*

- Добавляет запись следующего содержания в журнал событий /var/log/maillog:

  ```
  <дата и время проверки> <имя хоста Kaspersky Security 8 для Linux Mail Server>: 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 241), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Настройка меток к теме сообщений по результатам антивирусной проверки

► *Чтобы настроить метки, добавляемые Kaspersky Security 8 для Linux Mail Server 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 заголовок 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 заголовок 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 заголовок 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 заголовок 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 заголовок 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 Security 8 для Linux Mail Server, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 241), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

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 **Имена, исключенные из проверки**.

    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 **Имена, исключенные из проверки** 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 **Типы вложений, исключенные из проверки**.

    b. Установите флажки рядом с теми форматами вложенных объектов, которые вы хотите исключить из антивирусной проверки.

    c. Нажмите на кнопку **Закрыть**.

    Окно **Типы вложений, исключенные из проверки** закроется.

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

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security 8 для Linux Mail Server, убедитесь, что антивирусная проверка сообщений для правила включена (см. раздел "Включение и отключение антивирусной проверки для правила" на стр. 241), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Защита KATA и интеграция Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform

Вы можете настроить интеграцию Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server может блокировать отдельные сообщения.

В этом разделе

О статусах проверки сообщений в KATA

В результате проверки сообщений в KATA программа присваивает сообщению один из следующих статусов:

- *Detected (Обнаружено)* – программа KATA обнаружила событие, на которое администратору Kaspersky Security 8 для Linux Mail Server рекомендуется обратить внимание.
- *NotDetected (Не обнаружено)* – программа KATA не обнаружила событие, на которое администратору Kaspersky Security 8 для Linux Mail Server рекомендуется обратить внимание.

- *Error (Ошибка проверки)* – проверка сообщения завершена с ошибкой.

Ввод параметров интеграции на стороне Kaspersky Security 8 для Linux Mail Server

► *Чтобы ввести параметры интеграции Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Security 8 для Linux Mail Server, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server попытается установить соединение с сервером Kaspersky Anti Targeted Attack Platform с компонентом Central Node.

Перейдите к подтверждению интеграции Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server. Строка неподтвержденного соединения отмечена "звездочкой".

8. Нажмите на клавишу **ENTER**.

   Отобразится окно с отпечатками открытых сертификатов соединения Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform.

9. Убедитесь, что сертификат Kaspersky Security 8 для Linux Mail Server соответствует отпечатку сертификата в веб-интерфейсе Kaspersky Security 8 для Linux Mail Server.

10. Выберите **Accept KSMG Sensor**.

11. Нажмите на клавишу **ENTER**.

    Вы вернетесь в окно **Configure KSMG Sensor connections**. Строка с IP-адресом сервера Kaspersky Security 8 для Linux Mail Server не будет отмечена "звездочкой".

Интеграция Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Anti Targeted Attack Platform будет подтверждена.

Проверка соединения Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform

► *Чтобы проверить соединение Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform.

   Рядом с названием параметра **Отпечаток сертификата KLMS** отобразится отпечаток сертификата Kaspersky Security 8 для Linux Mail Server.

   Рядом с названием параметра **Отпечаток сертификата 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 Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform **Connected**, интеграция Kaspersky Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform настроена верно и соединение между серверами установлено.

Настройка отправки сообщений Kaspersky Security 8 для Linux Mail Server на проверку Kaspersky Anti Targeted Attack Platform

► *Чтобы настроить отправку сообщений электронной почты Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 заголовок 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Security 8 для Linux Mail Server, выполните следующие действия:*

1. В главном окне веб-интерфейса Kaspersky Security 8 для Linux Mail Server 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. 262).

► *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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, убедитесь, что защита KATA для правила включена (см. раздел "Включение и отключение защиты KATA для правила" на стр. 264), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Настройка меток к теме сообщений по результатам проверки KATA

► *Чтобы настроить метки, добавляемые Kaspersky Security 8 для Linux Mail Server 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 заголовок 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 Security 8 для Linux Mail Server, убедитесь, что защита KATA для правила включена (см. раздел "Включение и отключение защиты KATA для правила" на стр. 264), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Черные и белые списки адресов

Этот раздел содержит информацию о черных и белых списках адресов электронной почты, которые можно создавать и редактировать в Kaspersky Security 8 для Linux Mail Server.

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. 158). 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 Security 8 для Linux Mail Server необходимо подключится к LDAP-серверу (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 276).

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 Security 8 для Linux Mail Server необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 277).

Для работы с персональными черным и белыми списками адресов из веб-интерфейса Kaspersky Security 8 для Linux Mail Server необходимо подключится к LDAP-серверу (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 276).

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 Security 8 для Linux Mail Server необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 277) и подключиться к нему (см. раздел "Подключение и отключение от LDAP-сервера" на стр. 276).

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 Security 8 для Linux Mail Server с LDAP-сервером и о настройке параметров и фильтров соединения с LDAP-сервером.

В этом разделе

О соединении с LDAP-сервером

Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server возможность выполнять следующие задачи:

- Добавлять отправителей или получателей (см. раздел "Добавление учетных записей LDAP в списки отправителей и получателей сообщений" на стр. 167) 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. 271) пользователей локальной сети организации.
- Просматривать копии сообщений пользователей локальной сети организации в Хранилище (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 182).

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 Security 8 для Linux Mail Server.

   - **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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

11. Нажмите на кнопку **Проверить**.

    Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

11. Нажмите на кнопку **Проверить**.

    Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server протокол SNMP используется следующим образом:

1. *SNMP-агент* – программный модуль сетевого управления Kaspersky Security 8 для Linux Mail Server, который отслеживает информацию о работе Kaspersky Security 8 для Linux Mail Server.

2. Kaspersky Security 8 для Linux Mail Server 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

Security 8 для Linux Mail Server:

- общим сведениям;
- статистике работы Kaspersky Security 8 для Linux Mail Server с момента установки программы;
- данным о событиях, возникающих в ходе работы Kaspersky Security 8 для Linux Mail Server.

Например, Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server.

Доступ предоставляется только на чтение информации.

Включение и отключение использования SNMP в Kaspersky Security 8 для Linux Mail Server

► *Чтобы включить или отключить использование SNMP в работе Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server, 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.

Почтовые уведомления Kaspersky Security 8 для Linux Mail Server

Этот раздел содержит информацию о почтовых уведомлениях Kaspersky Security 8 для Linux Mail Server и настройке их параметров.

В этом разделе

О почтовых уведомлениях

Почтовое уведомление (далее также "уведомление") – это сообщение электронной почты с описанием события программы или события проверки сообщений, которое Kaspersky Security 8 для Linux Mail Server отправляет на заданные адреса электронной почты.

Вы можете настроить отправку уведомлений на следующие адреса электронной почты:

- администратора почтового сервера;
- отправителя сообщений;
- получателя сообщений;
- дополнительные адреса электронной почты.

При настройке отправки уведомлений получателю сообщений вы можете выбрать отправку уведомления с оригиналом сообщения во вложении (см. раздел "Настройка уведомлений о событиях проверки сообщений для правила" на стр. 296).

Уведомления о событиях Kaspersky Security 8 для Linux Mail Server содержат информацию о параметрах программы, ошибках, возникающих во время работы программы, а также о том, что отправленное сообщение не было доставлено получателю в случае невозможности доставить сообщение.

Вы можете настроить отправку почтового уведомления **Сообщение не доставлено** отправителю недоставленного сообщения.

Вы можете настроить отправку почтовых уведомлений администратору почтового сервера о следующих событиях Kaspersky Security 8 для Linux Mail Server:

- **Базы модуля Анти-Спам устарели**.
- **Базы модуля Антивирус устарели**.
- **Базы модуля Анти-Фишинг устарели**.
- **Ошибка помещения сообщений в хранилище**.
- **Ошибка очистки хранилища**.
- **Хранилище почти заполнено**.
- **Отправка уведомлений о персональном хранилище**.
- **Срок действия лицензии скоро истечет**.
- **Срок действия лицензии истек**.
- **Ключ заблокирован**.
- **Льготный период**.
- **Лицензия обновлена**.
- **Ошибка соединения с LDAP-сервером**.

Уведомления о событиях проверки сообщений содержат информацию об обработанном сообщении и удаленных из него объектах. В уведомления для получателя программа также включает заголовки исходного сообщения электронной почты.

Вы можете настроить отправку почтовых уведомлений администратору, отправителю, получателю сообщений или другим адресатам о следующих событиях проверки сообщений:

- **Обнаружены вредоносные объекты**.
- **Обнаружены зашифрованные объекты**.
- **Обнаружены ошибки проверки**.
- **Сработала контентная фильтрация**.
- **Обнаружены фишинговые сообщения**.
- **Обнаружен макрос во вложении**.

Изменение шаблонов уведомлений

► *Чтобы изменить шаблон почтового уведомления, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Уведомления**.
2. Выберите блок с типом уведомления, шаблон которого вы хотите изменить.

   Например, вы можете выбрать блок **Базы модуля Анти-Спам устарели**.
3. В выбранном блоке по одной из ссылок **Тема сообщения** или **Сообщение** откройте окно **Параметры уведомления**.

   Например, если вы хотите изменить шаблон уведомлений об устаревших базах модуля Анти-Спам, перейдите по одной из ссылок **Тема сообщения об устаревших базах** или **Сообщение об устаревших базах**.

   Откроется окно **Параметры уведомления**.

4. В поле **Тема** введите тему уведомления, шаблон которого вы хотите изменить.

5. В поле **Сообщение** введите текст уведомления, шаблон которого вы хотите изменить.

6. Нажмите на кнопку **Сохранить**.

   Окно **Параметры уведомления** закроется.

Настройка отправки уведомлений о персональном хранилище

► *Чтобы настроить отправку уведомлений о персональном Хранилище, выполните следующие действия:*

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

2. Выберите блок **Отправка уведомлений о персональном хранилище**.

3. По одной из ссылок **Тема сообщения**, **Сообщение**, **Расписание** или **Не отправлять на адреса** откройте окно **Параметры уведомления**.

4. В поле **Тема** введите тему уведомления о персональном Хранилище. Например, вы можете ввести тему "Weekly Backup".

5. В поле **Сообщение** введите текст уведомления о персональном Хранилище. Например, вы можете использовать текст уведомления о персональном Хранилище по умолчанию.

6. В полях **Отправлять уведомления в** укажите день недели и время для отправки уведомлений о персональном Хранилище.

7. Если вы хотите исключить какие-либо адреса из рассылки уведомлений о персональном Хранилище, выполните следующие действия для каждого адреса, который вы хотите исключить:

   a. В поле **Не отправлять на адреса** 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.

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

8. Нажмите на кнопку **Сохранить**.

Настройка уведомлений о событиях проверки сообщений для правила

Вы можете настроить отправку почтовых уведомлений о событиях проверки сообщений для одного или нескольких правил.

Вы можете настроить отправку почтовых уведомлений администратору, отправителю, получателю сообщений или другим адресатам о следующих событиях проверки сообщений:

- **Обнаружены вредоносные объекты**.
- **Обнаружены зашифрованные объекты**.
- **Обнаружены ошибки проверки**.
- **Сработала контентная фильтрация**.
- **Обнаружены фишинговые сообщения**.
- **Обнаружен макрос во вложении**.

► Чтобы настроить отправку уведомлений о событиях проверки 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, для которого вы хотите настроить отправку уведомлений.

3. Выберите блок **Уведомления**.

4. Выберите событие проверки сообщений, отправку уведомлений о котором вы хотите настроить.

   Например, вы можете выбрать событие **Обнаружены вредоносные объекты**.

5. В блоке параметров с названием выбранного события (например, **Обнаружены вредоносные объекты**) установите флажки рядом с названиями параметров:

   - **Уведомлять администратора**, если вы хотите включить отправку уведомлений о выбранном событии на адрес администратора (см. раздел "Настройка адресов электронной почты администратора" на стр. 338) Kaspersky Security 8 для Linux Mail Server.

   - **Уведомлять отправителя**, если вы хотите включить отправку уведомлений о выбранном событии на адреса отправителей сообщений.

   - **Уведомлять получателя**, если вы хотите включить отправку уведомлений о выбранном событии на адреса получателей сообщений.

   - **Дополнительные адреса**, если вы хотите включить отправку уведомлений о выбранном событии на дополнительные адреса электронной почты.

6. Если вы включили отправку уведомлений на адреса получателей сообщений, настройте параметры отправки уведомлений получателям сообщений. Для этого выполните следующие действия:

   a. По ссылке справа от названия параметра **Уведомлять получателя** откройте окно **Параметры отправки уведомлений получателю**.

   b. Выберите один из следующих вариантов:

- **Только уведомление**, если вы хотите настроить отправку уведомления получателям без оригинала сообщения.
- **Уведомление с оригиналом сообщения во вложении**, если вы хотите настроить отправку уведомления получателям с оригиналом сообщения во вложении.

c. Нажмите на кнопку **ОК**.

Окно **Параметры отправки уведомлений получателю** закроется.

7. Если вы включили отправку уведомлений на дополнительные адреса электронной почты, укажите дополнительные адреса электронной почты получателей уведомлений. Для этого выполните следующие действия:

a. По ссылке справа от названия параметра **Дополнительные адреса** откройте окно **Адреса для отправки уведомлений**.

b. В поле **Адреса для отправки уведомлений** введите адрес электронной почты получателя уведомлений.

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 добавления записей справа от поля ввода.

В поле под кнопкой добавления записей сформируется список дополнительных адресов электронной почты получателей уведомлений.

d. Нажмите на кнопку **ОК**.

Окно **Адреса для отправки уведомлений** закроется.

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

Включение и отключение отправки уведомлений о событиях программы

► *Чтобы включить или отключить отправку уведомлений о событиях Kaspersky Security 8 для Linux Mail Server, выполните следующие действия:*

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

2. В блоке с типом уведомления, отправку которого вы хотите включить или отключить, выполните одно из следующих действий:

   - Включите переключатель рядом с названием выбранного блока (например, **Базы модуля Анти-Спам устарели**), если вы хотите включить отправку уведомлений об этом событии.

   - Выключите переключатель рядом с названием выбранного блока (например, **Базы модуля Анти-Спам устарели**), если вы хотите отключить отправку уведомлений об этом событии.

Использование макросов в шаблонах почтовых уведомлений о событиях

Макрос – это элемент подстановки, используемый в шаблонах уведомлений о событиях. В формируемом на основе шаблона тексте уведомления макрос заменяется на некоторое значение.

Синтаксис макроса: `%ИМЯ_МАКРОСА%`

В текстах уведомлений о событиях можно использовать следующие макросы (см. таблицу ниже).

Таблица 5. Макросы для шаблонов уведомлений о событиях

Макрос	Описание	Событие, для которого используется макрос
%SERVER_NAME%	Имя почтового сервера.	*antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete, messageBackupFailed, severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed, backupAlmostFull, licenseExpiresSoon, licenseExpired, licenseBlacklisted*
%PRODUCT_NAME%	Название программы.	*antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete, messageBackupFailed, severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed, backupAlmostFull, licenseExpiresSoon, licenseExpired, licenseBlacklisted*
%BASES_ISSUE_DATE%	Дата выпуска антивирусных баз или баз Анти-Спама.	*antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete*

Макрос	Описание	Событие, для которого используется макрос
%OUTDATED_DAYS%	Количество дней с момента последнего обновления антивирусных баз или баз Анти-Спама.	*antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesObsolete*
%OUTDATED_HOURS%	Количество часов с момента последнего обновления баз Анти-Спама.	*antiSpamBasesOutOfDate*
%SMTP_MESSAGE_ID%	Заголовок сообщения.	*messageBackupFailed, scanStatusAlertForAdmin, scanStatusAlertForOthers*
%MESSAGES_COUNT%	Количество сообщений, которые не удалось поместить в хранилище или общее количество сообщений в хранилище.	*severalMessagesBackupFailed, backupAlmostFull*

Макрос	Описание	Событие, для которого используется макрос
%MINUTES%	Время, в течение которого произошли попытки помещения сообщений в хранилище или автоматического удаления сообщений из него.	*severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed*
%ATTEMPTS%	Количество попыток автоматического удаления сообщений из хранилища.	*severalBackupCleanupAttemptsFailed*
%MESSAGES_SIZE%	Общий размер сообщений в хранилище в мегабайтах.	*backupAlmostFull*
%MAX_BACKUP_SIZE%	Максимальный размер хранилища.	*backupAlmostFull*
%LICENSE_NUMBER%	Ключ, связанный с лицензией.	*licenseExpiresSoon, licenseExpired, licenseBlacklisted*
%EXPIRATION_DAYS%	Количество дней до окончания срока действия лицензии.	*licenseExpiresSoon*
%EXPIRATION_DATE%	Дата окончания срока действия лицензии.	*licenseExpired*

Макрос	Описание	Событие, для которого используется макрос
%SENDER%	Адрес отправителя сообщения.	*scanStatusAlertForAdmin, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%ALL_RECIPIENTS%	Адреса всех получателей исходного сообщения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForOthers*
%AFFECTED_RECIPIENTS%	Адреса получателей исходного сообщения, имеющие отношение к событию, описанному в уведомлении.	*scanStatusAlertForAdmin, scanStatusAlertForOthers, messageBounce*
%AFFECTED_RULES%	Правила обработки исходного сообщения, имеющие отношение к событию, описанному в уведомлении.	*scanStatusAlertForAdmin, scanStatusAlertForOthers*
%MESSAGE_ID%	Идентификационный номер сообщения в программе.	*scanStatusAlertForAdmin, scanStatusAlertForOthers*

Макрос	Описание	Событие, для которого используется макрос
%SUBJECT%	Тема исходного сообщения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%DATE%	Дата обработки сообщения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%MESSAGE_ACTION%	Действие программы над сообщением.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*

Макрос	Описание	Событие, для которого используется макрос
%DATA_BEGIN%	Служебный макрос для обозначения начала списка макросов для вложения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%DATA_END%	Служебный макрос для обозначения конца списка макросов для вложения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%OBJECT_NAME%	Имя вложения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%OBJECT_SIZE%	Размер вложения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%STATUS%	Статус сообщения.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*
%OBJECT_ACTION%	Действие программы над вложением.	*scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForRecipient, scanStatusAlertForOthers*

Ограничение трафика Kaspersky Security 8 для Linux Mail Server

► *Чтобы перевести Kaspersky Security 8 для Linux Mail Server в режим* ограниченного трафика*, 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. Выберите **Не использовать KSN / KPSN**.

4. Нажмите на кнопку **Применить**.

   Окно **Использование KSN / KPSN** закроется.

5. В блоке **Внешние службы** по ссылке **Разрешить подключение к DNS-серверу** откройте окно **Внешние службы**.

6. В списке справа от названия параметра **Разрешить подключение к DNS-серверу** выберите **Нет**.

7. Нажмите на кнопку **Применить**.

   Окно **Внешние службы** закроется.

8. 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**.

9. В блоке параметров **Внешние службы** в раскрывающемся списке **Использовать службу Enforced Anti-Spam Updates** выберите **Нет**.

10. Нажмите на кнопку **Применить**.

    Окно **Параметры модуля Анти-Спам** закроется.

11. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Параметры**, подраздел **Обновление баз**.

12. В блоке **Параметры обновления баз программы** по ссылке **Источник обновлений** откройте окно **Параметры обновления баз программы**.

13. В блоке параметров **Источник обновлений** выберите **Kaspersky Security Center**.

14. Снимите флажок **При недоступности использовать серверы "Лаборатории Касперского"**.

15. Нажмите на кнопку **ОК**.

    Окно **Параметры обновления баз программы** закроется.

Kaspersky Security 8 для Linux Mail Server начнет работать в режиме ограниченного трафика.

Примечания и предупреждения Kaspersky Security 8 для Linux Mail Server

Этот раздел содержит информацию о примечаниях и предупреждениях Kaspersky Security 8 для Linux Mail Server и настройке их параметров.

В этом разделе

О примечаниях к сообщениям и предупреждениях о небезопасном сообщении

Примечание к сообщениям (далее также "примечание") – это текст, который Kaspersky Security 8 для Linux Mail Server может добавлять в начале или в конце сообщения электронной почты.

Вы можете настроить шаблоны примечаний, задать формат отображения примечаний в сообщениях, включить или отключить использование примечаний для одного или нескольких правил обработки сообщений.

Предупреждение о небезопасном сообщении (далее также "предупреждение") – это текст, который Kaspersky Security 8 для Linux Mail Server может добавлять в начале или в конце сообщений электронной почты, имеющих один из следующих статусов проверки модулями Kaspersky Security 8 для Linux Mail Server:

- *Encrypted (Зашифрованное)*.
- *Phishing (Фишинг)*.
- *Infected (Зараженное)*.
- *Error (Ошибка проверки)*.

Вы можете настроить шаблоны предупреждений, задать формат отображения предупреждений в сообщениях, включить или отключить использование предупреждений для одного или нескольких правил обработки сообщений.

Создание шаблона примечания или предупреждения

► *Чтобы создать шаблон примечания или предупреждения, выполните следующие действия:*

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

   Откроется новый шаблон примечания или предупреждения.
3. В поле **Имя шаблона** введите имя шаблона.

   По этому имени вы можете выбрать шаблон для использования в настройке параметров правил обработки сообщений.
4. В раскрывающемся списке **Положение** выберите расположение примечания или предупреждения. Вы можете настроить отображение примечания или предупреждения перед сообщением или после сообщения.
5. Над полем **Текст сообщения** выберите одну из следующих закладок:

- **Без разметки**, если вы хотите, чтобы сообщение отображалось в текстовом формате.
- **HTML**, если вы хотите, чтобы сообщение отображалось в формате HTML.

  Kaspersky Security 8 для Linux Mail Server по умолчанию устанавливает формат текста в зависимости от формата сообщений электронной почты.

  В сообщение электронной почты формата **HTML** Kaspersky Security 8 для Linux Mail Server добавит примечание или предупреждение в формате **HTML**.

  В сообщение электронной почты формата **Без разметки** Kaspersky Security 8 для Linux Mail Server добавит примечание или предупреждение в формате **Без разметки**.

6. В поле **Текст сообщения** введите текст примечания или предупреждения.
7. Если вы ввели текст примечания или предупреждения в формате HTML, под полем **Текст сообщения** перейдите по ссылке **Просмотр** и просмотрите, как будет выглядеть сообщение.
8. Установите флажок **Только текстовый**, если вы хотите, чтобы сообщение содержало только текст.

   При добавлении примечания или предупреждения формата **Только текстовый** в сообщение электронной почты формата **HTML** формат сообщения может отображаться некорректно.

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

Созданный вами шаблон примечания или предупреждения отобразится в списке шаблонов примечаний и предупреждений в рабочей области главного окна веб-интерфейса программы.

Изменение шаблона примечания или предупреждения

► *Чтобы изменить шаблон примечания или предупреждения, выполните следующие действия:*

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

2. В рабочей области в списке шаблонов примечаний и предупреждений в рабочей области выберите шаблон примечания или предупреждения, который вы хотите изменить.

3. В поле **Имя шаблона** измените имя шаблона.

   По этому имени вы можете выбрать шаблон для использования в настройке параметров правил обработки сообщений.

4. В раскрывающемся списке **Положение** измените расположение примечания или предупреждения. Вы можете настроить отображение примечания или предупреждения перед сообщением или после сообщения.

5. Над полем **Текст сообщения** выберите одну из следующих закладок:

   - **Без разметки**, если вы хотите, чтобы сообщение отображалось в текстовом формате.

   - **HTML**, если вы хотите, чтобы сообщение отображалось в формате HTML.

6. В поле **Текст сообщения** измените текст примечания или предупреждения.

7. Если вы ввели текст примечания или предупреждения в формате HTML, под полем **Текст сообщения** перейдите по ссылке **Просмотр** и просмотрите, как будет выглядеть сообщение.

8. Установите флажок **Только текстовый**, если вы хотите, чтобы сообщение содержало только текст.

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

Удаление шаблона примечания или предупреждения

► *Чтобы удалить шаблон примечания или предупреждения, выполните следующие действия:*

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

2. Установите флажок в строках с названиями одного или нескольких шаблонов примечаний и предупреждений, которые вы хотите удалить.

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

Выбранные вами шаблоны примечаний и предупреждений будут удалены.

Включение и отключение примечаний к сообщениям для правила

Вы можете включить или отключить добавление примечаний к сообщениям для одного или нескольких правил. По умолчанию добавление примечаний к сообщениям отключено.

► *Чтобы включить или отключить добавление примечаний к сообщениям 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 добавление примечаний к сообщениям.

3. Выберите блок **Примечание к сообщению**.

4. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием блока параметров **Примечание к сообщению**, если вы хотите включить добавление примечаний к сообщениям для правила.

- Выключите переключатель рядом с названием блока параметров **Примечание к сообщению**, если вы хотите отключить добавление примечаний к сообщениям для правила.

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

Добавление примечания к событиям проверки сообщений для правила

► *Чтобы добавить примечание к событию 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 добавить примечание к событию проверки сообщений.

3. Выберите блок **Примечание к сообщению**.

4. Включите переключатель рядом с названием блока параметров **Примечание к сообщению**, если он выключен.

5. В блоке параметров **Добавить примечание** перейдите по ссылке справа от названия параметра **Шаблон примечания**.

6. Откроется окно **Шаблон примечания**.

7. В списке **Шаблон примечания** выберите шаблон примечания, которое вы хотите добавить к событию проверки сообщений для правила.

8. Нажмите на кнопку **ОК**.

   Окно **Шаблон примечания** закроется.

   Добавленное вами примечание отобразится в блоке **Примечание к сообщению** в рабочей области главного окна веб-интерфейса программы.

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

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security 8 для Linux Mail Server, убедитесь, что добавление примечаний к сообщениям для правила включено (см. раздел "Включение и отключение примечаний к сообщениям для правила" на стр. 312), и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Добавление предупреждения о небезопасном сообщении для правила

► Чтобы добавить предупреждение о небезопасном сообщении 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 добавить предупреждение о небезопасном сообщении.

3. Выберите блок **Предупреждение о небезопасном сообщении**.

4. Установите флажки рядом с одним или несколькими из следующих типов сообщений, к которым вы хотите добавить предупреждение:

   - **добавлять к зашифрованным сообщениям**, если вы хотите добавить предупреждение к сообщениям со статусом проверки модулями Kaspersky Security 8 для Linux Mail Server *Encrypted (Зашифрованное)*.

   - **добавлять к фишинговым сообщениям**, если вы хотите добавить предупреждение к сообщениям со статусом проверки модулями Kaspersky Security 8 для Linux Mail Server *Phishing (Фишинг)*.

   - **добавлять к зараженным сообщениям**, если вы хотите добавить предупреждение к сообщениям со статусом проверки модулями Kaspersky Security 8 для Linux Mail Server *Infected (Зараженное)*.

- **добавлять к сообщениям с ошибками проверки**, если вы хотите добавить предупреждение к сообщениям со статусом проверки модулями Kaspersky Security 8 для Linux Mail Server *Error (Ошибка проверки)*.

5. В блоке параметров **Добавить предупреждение** перейдите по ссылке справа от названия параметра **Шаблон предупреждения**.

6. Откроется окно **Шаблон предупреждения**.

7. В списке **Шаблон предупреждения** выберите шаблон предупреждения о небезопасном сообщении, которое вы хотите добавить для правила.

8. Нажмите на кнопку **ОК**.

   Окно **Шаблон предупреждения** закроется.

   Добавленное вами предупреждение отобразится в блоке **Предупреждение о небезопасном сообщении** в рабочей области главного окна веб-интерфейса программы.

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

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security 8 для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 176).

Журнал аудита Kaspersky Security 8 для Linux Mail Server

Kaspersky Security 8 для Linux Mail Server регистрирует события, связанные с проверкой сообщений электронной почты, в журнале аудита.

Этот раздел содержит информацию о работе с журналом аудита Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server, выполните следующие действия,*

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

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 Security 8 для Linux Mail Server, выполните следующие действия:*

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

   Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке с информацией о событии, которое вы хотите просмотреть, откройте окно с информацией об этом событии.

3. 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 аудита**.

   Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. 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 Security 8 для Linux Mail Server. Например, **Проверка сообщений**.

- **ID субъекта** – идентификатор субъекта. Например, доменное имя сервера Kaspersky Security 8 для Linux Mail Server.
- **Результат** – результат события Kaspersky Security 8 для Linux Mail Server. 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 аудита**.

   Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке **Время события** раскройте список интервалов для поиска событий.
3. Выберите один из следующих интервалов:
   - **Прошедший час**.
   - **Прошедший день**.
   - **Прошедшая неделя**.
   - **Пользовательский**.

4. 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 аудита**.

    Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке **Тип события** откройте окно настройки фильтрации событий.

3. В раскрывающемся списке **Тип события** выберите тип события. Например, вы можете ввести **Проверка сообщений**.

4. 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 аудита**.

   Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке **ID субъекта** откройте окно настройки фильтрации событий.

3. В поле **ID субъекта** введите несколько символов или все символы идентификатора субъекта. Например, вы можете ввести доменное имя сервера Kaspersky Security 8 для Linux Mail Server.

4. 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 аудита**.

   Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке **Результат** раскройте список результатов события.

3. Выберите один из следующих результатов события:

   - **Успешно**.
   - **Сбой**.

4. 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 аудита**.

Откроется таблица событий в журнале аудита Kaspersky Security 8 для Linux Mail Server.

2. По ссылке **Описание** откройте окно настройки фильтрации событий.
3. В поле **Описание** введите несколько символов описания события.
4. 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.

Информация о системе для Службы технической поддержки

Вы можете сформировать архив с информацией о системе (работе Kaspersky Security 8 для Linux Mail Server) для отправки в Службу технической поддержки "Лаборатории Касперского". Архив может содержать данные о вашей организации, которые вы считаете конфиденциальными. Администратору Kaspersky Security 8 для Linux Mail Server 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 **Информация о системе**.

2. Нажмите на кнопку **Создать**.

   Откроется окно **Создать архив с информацией о системе**.

Через несколько секунд архив с информацией о работе Kaspersky Security 8 для Linux Mail Server 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 **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.

2. 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 Security 8 для Linux Mail Server.

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 **Информация о системе**.

2. Установите флажки слева от имени каждого из архивов, который вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. Если вы хотите полностью очистить список архивов с информацией о системе, нажмите на кнопку **Удалить все**.

Архивы с информацией о системе будут удалены.

Удаление отчетов о работе Kaspersky Security 8 для Linux Mail Server

► Чтобы удалить один или несколько отчетов о работе *Kaspersky Security 8 для Linux Mail Server*, 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 Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server.

   - Выключите переключатель рядом с названием блока **Формирование ежедневного отчета**, если вы хотите отключить формирование ежедневных отчетов о работе Kaspersky Security 8 для Linux Mail Server.

Настройка параметров ежедневного отчета

► *Чтобы настроить параметры ежедневного отчета о работе Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server отправлял ежедневный отчет на адреса электронной почты администратора Kaspersky Security 8 для Linux Mail Server.

    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 Security 8 для Linux Mail Server.

Сформированные отчеты о работе Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server.

   - Выключите переключатель рядом с названием блока **Формирование еженедельного отчета**, если вы хотите отключить формирование еженедельных отчетов о работе Kaspersky Security 8 для Linux Mail Server.

Настройка параметров еженедельного отчета

► *Чтобы настроить параметры еженедельного отчета о работе Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server отправлял еженедельный отчет на адреса электронной почты администратора Kaspersky Security 8 для Linux Mail Server.

   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 Security 8 для Linux Mail Server.

Сформированные отчеты о работе Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server.

   - Выключите переключатель рядом с названием блока **Формирование ежемесячного отчета**, если вы хотите отключить формирование ежемесячных отчетов о работе Kaspersky Security 8 для Linux Mail Server.

Настройка параметров ежемесячного отчета

► *Чтобы настроить параметры ежемесячного отчета о работе Kaspersky Security 8 для Linux Mail Server, 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server отправлял ежемесячный отчет на адреса электронной почты администратора Kaspersky Security 8 для Linux Mail Server.

   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 Security 8 для Linux Mail Server.

Сформированные отчеты о работе Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server отправил пользовательский отчет на адреса электронной почты администратора Kaspersky Security 8 для Linux Mail Server.

   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 Security 8 для Linux Mail Server отобразятся в списке в рабочей области главного окна веб-интерфейса программы.

Общие параметры Kaspersky Security 8 для Linux Mail Server

Этот раздел содержит информацию о настройке общих параметров Kaspersky Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server.

   - **Нет**, если вы хотите отключить использование прокси-сервера в работе Kaspersky Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server.
   - Выключите переключатель рядом с названием блока параметров **Использовать прокси-сервер**, если вы не хотите использовать прокси-сервер в работе Kaspersky Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server, 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 Security для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server под учетной записью HelpDesk, учетная запись HelpDesk должна быть активирована (см. раздел "Активация и деактивация учетной записи HelpDesk" на стр. 341), 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. 342).

Пользователю HelpDesk доступны следующие операции в веб-интерфейсе Kaspersky Security 8 для Linux Mail Server:

- 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. 178).
- 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 для {UserName}**.

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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server. 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 Security 8 для Linux Mail Server передает информацию о себе в Kaspersky Security Center. На основании этой информации Kaspersky Security Center объединяет все виртуальные машины Kaspersky Security 8 для Linux Mail Server 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 Security 8 для Linux Mail Server.

4. Нажмите на кнопку **ОК**.

Изменение пути к каталогу для распаковывания архивов

Программа проверяет архивы, вложенные в сообщения электронной почты для обнаружения вредоносных файлов. Для выполнения проверки программа распаковывает архивы в каталог, расположенный в локальной файловой системе сервера, на который установлена программа.

По умолчанию программа распаковывает архивы в каталог /tmp/klmstmp. Вы можете изменить каталог, в который программа распаковывает архивы перед проверкой.

► *Чтобы изменить каталог, в который программа распаковывает архивы перед проверкой, выполните следующие действия:*

1. В любом текстовом редакторе откройте конфигурационный файл /var/opt/kaspersky/apps/1463.

2. Измените значение параметра tmp секции [paths]. Для этого в качестве значения параметра tmp укажите путь к каталогу в локальной файловой системе сервера, на который установлена программа:

   ```
   tmp=<путь к каталогу в локальной файловой системе сервера>
   ```

3. Сохраните изменения в файле.

4. Перезапустите программу.

Журнал трассировки

Этот раздел содержит информацию о журнале трассировке и настройке его параметров.

В этом разделе

О журнале трассировки

Если в работе Kaspersky Security 8 для Linux Mail Server возникла проблема (например, Kaspersky Security 8 для Linux Mail Server или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать журнал трассировки, в который сохраняются все события, возникающие во время работы программы, для отправки в Службу технической поддержки.

По умолчанию файлы журнала трассировки хранятся в директории /var/log/kaspersky/klms. Вы можете указать местонахождение журнала трассировки на жестком диске (см. раздел "Настройка местонахождения журнала трассировки" на стр. 353).

Вы можете указать уровень детализации журнала трассировки (см. раздел "Настройка уровня детализации журнала трассировки" на стр. 352).

Для выбора доступны следующие уровни детализации журнала трассировки:

- `Fatal` – критические события.

- `Error` – события об ошибках в работе программы.
- `Warning` – важные события. В журнал трассировки попадает значение smtp заголовка, если его не удалось декодировать.
- `Info` – информационные события.
- `Debug` – отладочная информация. В журнал трассировки попадают темы сообщений и адреса отправителей и получателей, имена вложений и прочая информацию об обрабатываемых сообщениях; полная информация о поступающих запросах на поиск сообщений. Также в журнал попадают данные, которые берутся из внешних источников, и все ссылки на веб-ресурсы, содержащиеся в сообщениях. При использовании *milter* в журнал трассировки попадают все заголовки писем.

Наиболее подробным является уровень детализации `Debug`, при котором в журнал трассировки записываются все события, а наименее подробным является уровень детализации `Fatal`, при котором в журнал трассировки записываются только критические события. По умолчанию установлен уровень детализации `Error`.

Журнал трассировки с уровнем детализации `Debug` может занимать большой объем дискового пространства и содержать конфиденциальную информацию пользователя.

Включение ведения журнала трассировки

► *Чтобы включить или отключить ведение журнала трассировки, выполните следующие действия:*

1. Экспортируйте общие параметры программы в XML-файл с помощью команды:

   `# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <имя файла>`

2. Откройте XML-файл параметров на изменение.
3. В секции `<tracerSettings>` укажите одно из следующих значений в качестве значения параметра <`Enable`>:

- `1`, если вы хотите включить ведение журнала трассировки;
- `0`, если вы хотите отключить ведение журнала трассировки.

4. Сохраните внесенные изменения.
5. Импортируйте общие параметры программы из XML-файла с помощью команды:

   `# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <имя файла>`

6. Перезапустите программу. Для этого выполните следующую команду:

   `# /etc/init.d/klms restart`

Настройка уровня детализации журнала трассировки

► *Чтобы настроить уровень детализации журнала трассировки, выполните следующие действия:*

1. Экспортируйте общие параметры программы в XML-файл с помощью команды:

   `# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <имя файла>`

2. Откройте XML-файл параметров на изменение.
3. Укажите уровень детализации журнала трассировки. Для этого в секции `<tracerSettings>` укажите одно из следующих значений в качестве значения параметра `<level>`:
   - `Fatal` – критические события.
   - `Error` – события об ошибках в работе программы.
   - `Warning` – важные события.
   - `Info` – информационные события.

- `Debug` – отладочная информация.

4. Сохраните внесенные изменения.
5. Импортируйте общие параметры программы из XML-файла с помощью команды:

   `# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <имя файла>`

6. Перезапустите программу. Для этого выполните следующую команду:

   `# /etc/init.d/klms restart`

Настройка местонахождения журнала трассировки

► *Чтобы настроить местонахождение журнала трассировки, выполните следующие действия:*

1. Экспортируйте общие параметры программы в XML-файл с помощью команды:

   `# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <имя файла>`

2. Откройте XML-файл параметров на изменение.
3. Укажите местонахождение журнала трассировки на жестком диске. Для этого в секции `<tracerSettings>` укажите одно из следующих значений в качестве значения параметра <`destination`>:

   - `Files`, если вы хотите, чтобы программа вела журнал трассировки в отдельном файле в директории /var/log/kaspersky/klms (это значение указано по умолчанию).
   - `Syslog`, если вы хотите, чтобы программа записывала все события в системный журнал операционной системы.

4. Сохраните внесенные изменения.
5. Импортируйте общие параметры программы из XML-файла с помощью команды:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <имя файла>
```

6. Перезапустите программу. Для этого выполните следующую команду:

```
# /etc/init.d/klms restart
```

Настройка параметров ротации файлов трассировки

Вы можете настроить параметры ротации файлов трассировки, такие как максимальный размер файла трассировки и количество сохраняемых файлов трассировки. При превышении указанных значений старые файлы трассировки заменяются новыми файлами. Параметры ротации файлов трассировки дают возможность ограничить объем памяти, который может быть занят журналом трассировки.

► *Чтобы настроить параметры ротации файлов трассировки, выполните следующие действия:*

1. Экспортируйте общие параметры программы в XML-файл с помощью команды:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <имя файла>
```

2. Откройте XML-файл параметров на изменение.

3. Укажите параметры ротации файлов трассировки. Для этого в секции `<tracerSettings>` укажите значения следующих параметров:

   a. В подсекции `<rotationPeriod>` укажите одно из следующих значений:

   - `NoRotation`. Старые файлы трассировки заменяются новыми при превышении значений параметров `<rotationFileSize>` или `<maxFileCount>`.
   - `Monthly`. Старые файлы трассировки заменяются новыми ежемесячно или при превышении значений параметров `<rotationFileSize>` или `<maxFileCount>`.

- `Weekly`. Старые файлы трассировки заменяются новыми еженедельно или при превышении значений параметров `<rotationFileSize>` или `<maxFileCount>`.
- `Daily`. Старые файлы трассировки заменяются новыми ежедневно или при превышении значений параметров `<rotationFileSize>` или `<maxFileCount>`.
- `Hourly`. Старые файлы трассировки заменяются новыми каждый час или при превышении значений параметров `<rotationFileSize>` или `<maxFileCount>`.

По умолчанию указано значение `NoRotation`.

b. В подсекции `<rotationFileSize>` укажите максимальный размер файла трассировки (в байтах). При превышении указанного значения старый файл трассировки заменяется новым файлом трассировки.

По умолчанию указано значение `100` МБ.

c. В подсекции `<maxFileCount>` укажите максимальное количество файлов трассировки, которые могут храниться одновременно. Когда количество файлов трассировки превысит указанное значение, файлы трассировки заменяются новыми файлами.

По умолчанию указано значение `10`.

4. Сохраните внесенные изменения.
5. Импортируйте общие параметры программы из XML-файла с помощью команды:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <имя файла>
```

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Security 8 для Linux Mail Server через Kaspersky Security Center.

В этом разделе

Об управлении программой через Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения административных задач по управлению и мониторингу почтовыми серверами с установленной программой Kaspersky Security 8 для Linux Mail Server. Kaspersky Security Center поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

Kaspersky Security Center позволяет выполнять следующие функции по управлению программой Kaspersky Security 8 для Linux Mail Server, установленной на почтовых серверах:

- добавлять активный и дополнительный ключ;

- запускать задачу обновления баз Kaspersky Security 8 для Linux Mail Server;
- отображать информацию о состоянии защиты кластера почтовых серверов;
- запускать и останавливать Kaspersky Security 8 для Linux Mail Server.

Настройка управления программой через Kaspersky Security Center

Чтобы настроить управление программой Kaspersky Security 8 для Linux Mail Server через Kaspersky Security Center, необходимо выполнить следующие действия:

1. Установить Агент администрирования Kaspersky Security Center (см. раздел "Установка Агента администрирования" на стр. 358). Агент администрирования поставляется в отдельном установочном пакете вместе с установочным пакетом Kaspersky Security 8 для Linux Mail Server.
2. Настроить параметры Агента администрирования с помощью скрипта первоначальной настройки (см. раздел "Настройка параметров Агента администрирования" на стр. 358).
3. Установить плагин управления Kaspersky Security 8 для Linux Mail Server (см. раздел "Установка плагина управления Kaspersky Security 8 для Linux Mail Server" на стр. 359).

В этом разделе

Установка Агента администрирования

Запускать установку Агента администрирования требуется с правами учетной записи `root`.

► *Чтобы установить Агент администрирования из пакета формата RPM, выполните следующую команду:*

```
# rpm -i klnagent-<номер_версии>.i386.rpm
```

► *Чтобы установить Агент администрирования из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:*

```
# dpkg -i klnagent_<номер_версии>_i386.deb
```

► *Чтобы установить Агент администрирования из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:*

```
# dpkg -i --force-architecture klnagent_<номер_версии>_i386.deb
```

После выполнения команды установка Агента администрирования происходит автоматически.

После установки требуется настроить параметры Агента администрирования (см. раздел "Настройка параметров Агента администрирования" на стр. 358).

Настройка параметров Агента администрирования

► *Чтобы настроить параметры Агента администрирования, выполните следующие действия:*

1. Выполните команду

   ```
   # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl.
   ```

   Запустится скрипт первоначальной настройки Агента администрирования.

2. В процессе работы скрипта выполните следующие действия:

    a. Укажите DNS-имя или IP-адрес Сервера администрирования Kaspersky Security Center.

    b. Укажите номер порта Сервера администрирования или порт по умолчанию (14000).

    c. Укажите номер SSL-порта Сервера администрирования или порт по умолчанию (13000).

    d. Укажите, использовать ли SSL-соединение для передачи данных. По умолчанию SSL-соединение включено.

    e. Указать, нужно ли использовать Агент администрирования в качестве шлюза для соединения с Kaspersky Security Center. По умолчанию соединение с Kaspersky Security Center будет установлено напрямую без использования шлюза.

Подробную информацию о настройке Агента администрирования см. *Руководство администратора Kaspersky Security Center*.

Установка плагина управления Kaspersky Security 8 для Linux Mail Server

► *Чтобы установить плагин управления Kaspersky Security 8 для Linux Mail Server, выполните следующие действия:*

1. Из папки с установочным пакетом Kaspersky Security 8 для Linux Mail Server запустите файл klcfginst.msi.

2. Дождитесь завершения работы мастера установки.

Проверка соединения с Kaspersky Security Center

После установки Агента администрирования и его настройки вы можете проверить соединение программы Kaspersky Security 8 для Linux Mail Server с Сервером администрирования Kaspersky Security Center с помощью утилиты `klnagchk`.

► *Чтобы проверить соединение с Kaspersky Security Center, выполните следующую команду:*

```
# /opt/kaspersky/klnagent/bin/klnagchk
```

Утилита `klnagchk` отобразит результаты проверки соединения.

Если при проверке соединения возникли проблемы, для получения информации об их решении см. *Руководство Администратора Kaspersky Security Center*.

Запуск и остановка Kaspersky Security 8 для Linux Mail Server на клиентском компьютере

► *Чтобы запустить или остановить Kaspersky Security 8 для Linux Mail Server на клиентском компьютере, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В панели результатов выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить или остановить Kaspersky Security 8 для Linux Mail Server.
5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   Откроется окно свойств клиентского компьютера.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.

7. Выберите программу Kaspersky Security 8 для Linux Mail Server.

8. Выполните следующие действия:

   - Если вы хотите запустить Kaspersky Security 8 для Linux Mail Server, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:

     a. По правой клавише мыши откройте контекстное меню программы Kaspersky Security 8 для Linux Mail Server и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

     Откроется окно **Параметры программы Kaspersky Security 8 для Linux Mail Server** на закладке **Общие**.

     b. Нажмите на кнопку **Запустить**.

   - Если вы хотите остановить работу Kaspersky Security 8 для Linux Mail Server, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:

     a. По правой клавише мыши откройте контекстное меню программы Kaspersky Security 8 для Linux Mail Server и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

     Откроется окно **Параметры программы Kaspersky Security 8 для Linux Mail Server** на закладке **Общие**.

     b. Нажмите на кнопку **Остановить**.

Управление задачами

Этот раздел содержит информацию об управлении задачами для Kaspersky Security 8 для Linux Mail Server. Подробнее о концепции управления задачами через Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

В этом разделе

О задачах для Kaspersky Security 8.0 для Linux Mail Server

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на клиентских компьютерах, с помощью задач.

Для работы с Kaspersky Security 8 для Linux Mail Server через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в одну или разные группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи клиентских компьютеров. Если в набор компьютеров, для которого сформирована задача, добавлены новые клиентские компьютеры, то для них эта задача не выполняется. В этом случае требуется создать новую задачу или изменить параметры уже существующей задачи.

Удаленно управляя программой Kaspersky Security 8 для Linux Mail Server через Kaspersky Security Center, вы можете работать с задачей добавления ключа. В процессе выполнения задачи программа добавляет ключ, в том числе дополнительный, для активации программы.

Вы можете выполнять следующие действия над задачами:

- запускать выполнение задач;

  Если на клиентском компьютере запущена программа Kaspersky Security 8 для Linux Mail Server, вы можете запустить выполнение задачи на этом клиентском компьютере через Kaspersky Security Center. Если программа Kaspersky Security 8 для Linux Mail Server остановлена, выполнение запущенных задач прекращается, а управлять запуском задач через Kaspersky Security Center становится невозможным.

- создавать новые задачи;
- изменять параметры задач.

Создание локальной задачи

► *Чтобы создать локальную задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В панели результатов выберите закладку **Компьютеры**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.
5. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   Откроется окно свойств клиентского компьютера.
6. Выберите закладку **Задачи**.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► *Чтобы создать групповую задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Управляемые компьютеры** дерева консоли.
3. В панели результатов выберите закладку **Задачи**.
4. Выполните одно из следующих действий:
   - Нажмите на кнопку **Создать задачу**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Создать** → **Задачу**.

   Запустится мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

Создание задачи для набора компьютеров

► *Чтобы создать задачу для набора компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Задачи для наборов компьютеров** дерева консоли.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Создать задачу**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Создать** → **Задачу**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Просмотр общей информации о работе Kaspersky Security 8 для Linux Mail Server для кластера

► *Чтобы просмотреть общую информацию о работе Kaspersky Security 8 для Linux Mail Server для кластера, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку **Security for Linux Mail Server**.
3. Откройте папку **Кластеры и массивы серверов**.
4. В панели результатов выберите кластер, для компьютеров которого вы хотите посмотреть информацию о работе Kaspersky Security 8 для Linux Mail Server.
5. По правой клавише мыши откройте контекстное меню кластера. Выберите пункт **Свойства**.

Откроется окно свойств кластера.

6. Выберите раздел **Сводная информация**.

   В правой части окна отобразится таблица с информацией о работе Kaspersky Security 8 для Linux Mail Server для каждого компьютера кластера.Подробнее о работе с кластерами вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Публикация событий программы в SIEM-систему

Kaspersky Security 8 для Linux Mail Server может публиковать события, происходящие во время работы программы, в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

SIEM-система (Security Information and Event Management) – решение для управления информацией и событиями в системе безопасности организации.

Информация о каждом событии программы передается как отдельное syslog-сообщение формата CEF (далее также "CEF-сообщение").

CEF-сообщение с информацией о событии передается сразу после появления события. Исключение – классы событий группы ScanLogic, все CEF-сообщения этих классов передаются после обработки сообщений электронной почты модулем ScanLogic.

По умолчанию экспорт CEF-сообщений в программе отключен.

В этом разделе

Извлечение параметров из Kaspersky Security 8 для Linux Mail Server в XML-файл

► *Чтобы извлечь параметры из Kaspersky Security 8 для Linux Mail Server в XML-файл, выполните следующую команду:*

```
# sudo /opt/kaspersky/klms/bin/klms-control \

--get-settings EventLogger -n [-f|--file <file-name>]
```

После выполнения команды параметры экспорта CEF-сообщений будут извлечены в XML-файл. Параметр `-f|--file <file-name>` указывает XML-файл, содержащий эти параметры.

Включение экспорта событий в формате CEF

Перед включением экспорта событий в формате CEF рекомендуется указать такую категорию (facility) для syslog, которая не используется другими программами на сервере.

► *Чтобы включить экспорт событий в формате CEF, выполните следующие действия:*

1. Откройте XML-файл с извлеченными параметрами утилиты klms-control.
2. Если вы хотите выбрать категорию (facility) для syslog, в которую будут экспортироваться события, в открывшемся файле в блоке `<siemSettings>` укажите одно из следующих значений параметра `<facility>`:
   - `Auth`.
   - `Authpriv`.
   - `Cron`.

- `Daemon`.
- `Ftp`.
- `Lpr`.
- `Mail`.
- `News`.
- `Syslog`.
- `User`.
- `Uucp`.
- `Local0`.
- `Local1`.
- `Local2`.
- `Local3`.
- `Local4`.
- `Local5`.
- `Local6`.
- `Local7`.

По умолчанию установлено значение `Mail`.

Пример:

```
<siemSettings>

    <enabled>0</enabled>

    <facility>Local0</facility>
```

3. В открывшемся файле в блоке `<siemSettings>` установите значение параметра `<enabled>` равным `1`.

Пример:

```
<siemSettings>

    <enabled>1</enabled>
```

Содержание и свойства syslog-сообщений в формате CEF

Информация о каждом обнаруженном событии передается как отдельное syslog-сообщение формата CEF, имеющее кодировку UTF-8.

Сообщение в формате CEF состоит из *тела сообщения* и *заголовка*. В заголовке сообщения содержится версия формата CEF и общая информация о событии: производитель, название и версия программы, имя, важность и класс обнаруженного события, время, в которое событие было обнаружено. Тело сообщения представляет собой последовательность пар `<ключ>=<значение>`.

Пример:

```
July 16, 2017 10:34:23 host.avp.ru \

CEF:0|AO Kaspersky Lab|Kaspersky Linux \

Mail Security|8.0MP2|LMS_EV_SETTINGS_CHANGED|\

task settings changed|Low|cn1=taskId \

cn1Label=TaskId cs1=taskName csLabel=TaskName \

act=created
```

Максимальный размер syslog-сообщения об обнаруженном событии зависит от значений параметров syslog на сервере, на котором установлен Kaspersky Security 8 для Linux Mail Server. Вы можете настроить пересылку syslog-сообщений только на один внешний syslog-сервер единовременно.

Значения полей тела CEF-сообщений классов событий группы Settings

В теле CEF-сообщений классов событий группы Settings допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 6. Допустимые значения полей классов событий группы Settings

Ключ	Значение
cn1	Номер задачи (из klms-control).
cn1Label	Всегда имеет значение `TaskId`.
cs1	Имя задачи (из klms-control).

Ключ	Значение
cs1Label	Всегда имеет значение `TaskName`.
duser	Пользователь, чьи параметры были изменены.
suser	Пользователь, который изменил параметры.
act	Действие, выполненное с параметрами. Допустимые значения: `created`, `changed`, `deleted`.

В каждом классе событий группы Settings допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 7. Релевантные ключи для классов событий группы Settings

Класс событий	Релевантные ключи
LMS_EV_SETTINGS_CHANGED	cn1, cn1Label, cs1, cs1Label, act
LMS_EV_ALL_SETTINGS_CHANGED	suser
LMS_EV_PERSONAL_SETTINGS_CHANGED	suser, duser

Значения полей тела CEF-сообщений классов событий группы Tasks

В теле CEF-сообщений классов событий группы Tasks допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 8. Допустимые значения полей классов событий группы Tasks

Ключ	Значение
deviceProcessName	Имя задачи (из klms-control).
cnt	Количество сбоев за последние 5 минут.
reason	Описание ошибки.
outcome	Описание результата.
cs1	Режим работы программы (`real time scan` / `configuration mode`).
cs1Label	Всегда имеет значение `Mode`.

В каждом классе событий группы Tasks допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 9. Релевантные ключи для классов событий группы Tasks

Класс событий	Релевантные ключи
LMS_EV_PROCESS_CRASHED	deviceProcessName, cnt
LMS_EV_RESTARTED	deviceProcessName, cnt
LMS_EV_PRODUCT_STARTED	cs1, cs1Label

Значения полей тела CEF-сообщений классов событий группы Import / Export Settings

В теле CEF-сообщений классов событий группы Import / Export Settings допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 10. Допустимые значения полей классов событий группы Import / Export Settings

Ключ	Значение
cs1	Список категорий импортированных параметров.
cs1Label	Всегда имеет значение `ImportedAreas`.
reason	Описание ошибки.
outcome	Результат импорта / экспорта.

В каждом классе событий группы Import / Export Settings допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 11. Релевантные ключи для классов событий группы Import / Export Settings

Класс событий	Релевантные ключи
LMS_EV_EXPORT_SETTINGS	outcome, reason
LMS_EV_IMPORT_SETTINGS	outcome, reason, cs1, cs1Label

Значения полей тела CEF-сообщений классов событий группы Backup

В теле CEF-сообщений классов событий группы Backup допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 12. Допустимые значения полей для классов событий группы Backup

Ключ	Значение
cn1	Размер сообщения.
cn1Label	Всегда имеет значение `MessageSize`.
cn2	Максимальный размер хранилища.
cn2Label	Всегда имеет значение `MaxBackupSize`.
cn3	Количество сообщений в хранилище.
cn3Label	Всегда имеет значение `MessageCount`.
cs1	ID сообщения в хранилище.
cs1Label	Всегда имеет значение `MessageId`.
cnt	Количество ошибок за последние 10 минут.
act	Действие над сообщением в хранилище (доставить / удалить).
suser	Пользователь, который выполнил действие с сообщением в хранилище.

Ключ	Значение
cs2	Статус антивирусной проверки.
cs2Label	Всегда имеет значение `AvStatus`.
cs3	Статус проверки на спам.
cs3Label	Всегда имеет значение `AsStatus`.
cs4	Статус проверки на фишинг.
cs4Label	Всегда имеет значение `ApStatus`.
cs5	Имя вредоносного объекта.
cs5Label	Всегда имеет значение `Threat`.
cs6	Статус контентной фильтрации.
cs6Label	Всегда имеет значение `CfStatus`.
duser	Список получателей сообщения.
reason	Описание ошибки.
outcome	Результат события *Backup Digest*: `no messages`, `success` или `failed`.

В каждом классе событий группы Backup допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 13. Релевантные ключи для классов событий группы Backup

Класс событий	Релевантные ключи
LMS_EV_BACKUP_ADD_ERROR	cs1, cs1Label, cnt
LMS_EV_BACKUP_ROTATE_ERROR	reason, cnt
LMS_EV_BACKUP_ALMOST_FULL	cn1, cn1Label, cn2, cn2Label, cn3Label
LMS_EV_BACKUP_MESSAGE_RESTORE	cs1, cs1Label, act, suser, cs2, cs2Label, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, duser

Значения полей тела CEF-сообщений классов событий группы Report

В теле CEF-сообщений классов событий группы Report допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 14. Допустимые значения полей классов событий группы Report

Ключ	Значение
cs1	Тип отчета.
cs1Label	Всегда имеет значение `ReportType`.
cs2	Период.
cs2Label	Всегда имеет значение `PeriodInfo`.
fname	Имя файла отчета.

В каждом классе событий группы Report допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 15. Релевантные ключи для классов событий группы Report

Класс событий	Релевантные ключи
LMS_EV_REPORT_CREATING_ERROR	cs1, cs1Label, cs2, cs2Label
LMS_EV_REPORT_CREATED	cs2, cs2Label, fname

Значения полей тела CEF-сообщений классов событий группы License

В теле CEF-сообщений классов событий группы License допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 16. Допустимые значения полей классов событий группы License

Ключ	Значение
cs1	Серийный номер лицензии.
cs1Label	Всегда имеет значение `LicenseID`.
cs2	Режим работы Kaspersky Security 8 для Linux Mail Server в соответствии с лицензией.
cs2Label	Всегда имеет значение `FunctionalityLevel`.
cs3	Тип лицензии.
cs3Label	Всегда имеет значение `KeyType`.

Ключ	Значение
cn1	Количество дней до истечения срока действия лицензии.
cn1Label	Всегда имеет значение `DaysLeft`.
reason	Описание ошибки.
deviceCustomDate1	Дата истечения срока действия лицензии.
deviceCustomDate1Label	Всегда имеет значение `ExpirationDate`.

В каждом классе событий группы License допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 17. Релевантные ключи для классов событий группы License

Класс событий	Релевантные ключи
LMS_EV_LICENSE_OK	cs1, cs1Label, cs2, cs2Label
LMS_EV_LICENSE_INVALID	cs1, cs1Label, reason
LMS_EV_NO_LICENSE	Нет значения
LMS_EV_LICENSE_BLACKLISTED	cs1, cs1Label
LMS_EV_LICENSE_TRIAL_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_ERROR	reason
LMS_EV_LICENSE_INSTALLED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label
LMS_EV_LICENSE_UPDATED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_GRACE_PERIOD	cs1, cs1Label, cn1, cn1Label
LMS_EV_LICENSE_REVOKED	cs1, cs1Label
LMS_EV_LICENSE_EXPIRES_SOON	cs1, cs1Label, cn1, cn1Label

Значения полей тела CEF-сообщений классов событий группы Rules

В теле CEF-сообщений классов событий группы Rules допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 18. Допустимые значения полей классов событий группы Rules

Ключ	Значение
cs1	Имя правила.
cs1Label	Всегда имеет значение `RuleName`.
cn1	ID правила.
cn1Label	Всегда имеет значение `RuleId`.
act	Действие с правилом (`created` / `settings changed` / `deleted` / `priotity changed`).

В каждом классе событий группы Rules допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 19. Релевантные ключи для классов событий группы Rules

Класс событий	Релевантные ключи
LMS_EV_RULE_CHANGED	cs1, cs1Label, cn1, cn1Label, act
LMS_EV_ALL_RULES_IMPORTED	Нет значения

Значения полей тела CEF-сообщений классов событий группы Auth

В теле CEF-сообщений классов событий группы Auth допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 20. Допустимые значения полей классов событий группы Auth

Ключ	Значение
cs1	Тип интеграции (LDAP).
cs1Label	Всегда имеет значение `IntegrationType`.
cn1	Сколько секунд сервер был недоступен.
cn1Label	Всегда имеет значение `Seconds`.
reason	Описание ошибки.
start	Начало периода недоступности LDAP-сервера.
end	Окончание периода недоступности LDAP-сервера.
rt	Время первого события.
deviceServiceName	Имя службы.

В каждом классе событий группы Auth допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 21. Релевантные ключи для классов событий группы Auth

Класс событий	Релевантные ключи
LMS_EV_EXT_DIR_REPORT_FOR_PERIOD	rt, cs1, cs1Label, deviceServiceName, start, end
LMS_EV_EXT_DIR_SERVICE_ERROR	cs1, cs1Label, deviceServiceName, reason, cn1, cn1Label
LMS_EV_EXT_DIR_SERVICE_UP	Нет значения
LMS_EV_EXT_DIR_SERVICE_DISABLED	Нет значения

Значения полей тела CEF-сообщений классов событий группы Quarantine

В теле CEF-сообщений классов событий группы Quarantine допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 22. Допустимые значения полей классов событий группы Quarantine

Ключ	Значение
cs1	ID сообщения.
cs1Label	Всегда имеет значение `MessageId`.
cs2	Список правил через запятую.
cs2Label	Всегда имеет значение `Rules`.
cs3	Учетная запись, под которой было выполнено действие над сообщением.

Ключ	Значение
cs3Label	Всегда имеет значение `Account`.
src	IP-адрес, с которого получено сообщение.
duser	Список получателей сообщения.
suser	Отправитель сообщения.
act	Действие над сообщением (`proceed` / `delete`).

В каждом классе событий группы Quarantine допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 23. Релевантные ключи для классов событий группы Quarantine

Класс событий	Релевантные ключи
LMS_EV_ASP_QUARANTINE	cs1, cs1Label, src, suser, cs3, cs3Label, act
LMS_EV_KATA_QUARANTINE	cs1, cs1Label, cs2, cs2Label, suser, duser, act, cs3, cs3Label

Значения полей тела CEF-сообщений классов событий группы Update

В теле CEF-сообщений классов событий группы Update допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 24. Допустимые значения полей классов событий группы Update

Ключ	Значение
reason	Причина возникновения события.
cn1	Количество дней.
cn1Label	Всегда имеет значение `Days`.
cn2	Количество часов.
cn2Label	Всегда имеет значение `Hours`.
cnt	Количество записей в базах.
deviceCustomDate1	Дата публикации баз.
deviceCustomDate1Label	Всегда имеет значение `PublishingTime`.
deviceCustomDate2	Дата публикации индекса.
deviceCustomDate2Label	Всегда имеет значение `IndexPublishingTime`.

В каждом классе событий группы Update допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 25. Релевантные ключи для классов событий группы Update

Класс событий	Релевантные ключи
LMS_EV_ANTIVIRUS_BASES_UPDATED	reason
LMS_EV_ANTISPAM_BASES_UPDATED	Нет значения
LMS_EV_BASES_NOTHING_TO_UPDATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIPHISHING_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTISPAM_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTISPAM_BASES_OUT_OF_DATE	cn2, cn2Label
LMS_EV_ANTIVIRUS_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTISPAM_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIVIRUS_BASES_APPLIED	deviceCustomDate2, deviceCustomDate2Label, cnt, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTISPAM_BASES_APPLIED	deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTIPHISHING_BASES_APPLIED	deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTIVIRUS_BASES_ERROR	reason
LMS_EV_ANTISPAM_BASES_ERROR	reason

Класс событий	Релевантные ключи
LMS_EV_ANTIPHISHING_BASES_ERROR	reason

Значения полей тела CEF-сообщений классов событий группы ScanLogic

В теле CEF-сообщений классов событий группы ScanLogic допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 26. Допустимые значения полей классов событий группы ScanLogic

Класс событий	Ключ	Значение
Все классы группы ScanLogic	cs1	ID сообщения.
	cs1Label	Всегда имеет значение `MessageId`.
	src	IP-адрес сервера, от которого получено сообщение.
	act	Действие.
	fsize	Размер сообщения.
	suser	Отправитель сообщения.
	duser	Список получателей сообщения.
	reason	Причина возникновения события.
	cs2	Список правил.

Класс событий	Ключ	Значение
	cs2Label	Всегда имеет значение `Rules`.
	outcome	Статус проверки.
	cs3	Список получателей обнаруженного сообщения (с действием Skip).
	cs3Label	Всегда имеет значение `UnsafeRecipients`.
	fname	Имя файла.
LMS_EV_SCAN_LOGIC_AS_STATUS LMS_EV_SCAN_LOGIC_AP_STATUS	cs4	Метод обнаружения.
	cs4Label	Всегда имеет значение `Method`.
LMS_EV_SCAN_LOGIC_MA_STATUS	cs4	Заключение SPF.
	cs4Label	Всегда имеет значение `SpfVerdict`.
	cs5	Заключение DKIM.
	cs5Label	Всегда имеет значение `DkimVerdict`.
	cs6	Заключение DMARC.
	cs6Label	Всегда имеет значение `DmarcVerdict`.
LMS_EV_SCAN_LOGIC_KT_STATUS	suser	Имя учетной записи пользователя,

Класс событий	Ключ	Значение
		который извлек сообщение из KATA-карантина.
	cs4	Причина пропуска сканирования.
	cs4Label	Всегда имеет значение `SkipReason`.
LMS_EV_SCAN_LOGIC_CF_STATUS	cs4	`BannedFileFormat` или `BannedFileName`.
	cs4Label	Всегда имеет значение `BannedEntity`.
LMS_EV_SCAN_LOGIC_PART_RESULT	cn1	Количество объектов.
	cn1Label	Всегда имеет значение `ObjectsNumber`.
	cs2	Список правил.
	cs2Label	Всегда имеет значение `Rules`.
	cs3	Непроверенные файлы.
	cs3Label	Всегда имеет значение `AvExclude`.
	cs4	Имена угроз.
	cs4Label	Всегда имеет значение `Threats`.
	cs5	Имя заблокированного файла.

Класс событий	Ключ	Значение
	cs5Label	Всегда имеет значение `BannedFileName`.
	cs6	Формат заблокированного файла.
	cs6Label	Всегда имеет значение `BannedFileFormat`.

В каждом классе событий группы ScanLogic допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 27. Релевантные ключи для классов событий группы ScanLogic

Класс событий	Релевантные ключи
LMS_EV_SCAN_LOGIC_ALL_NOT_PROCESSED	cs1, cs1Label, src, act, fsize, suser, duser
LMS_EV_SCAN_LOGIC_AS_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label
LMS_EV_SCAN_LOGIC_AV_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, outcome
LMS_EV_SCAN_LOGIC_AP_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, outcome
LMS_EV_SCAN_LOGIC_KT_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, suser, outcome
LMS_EV_SCAN_LOGIC_MA_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, outcome
LMS_EV_SCAN_LOGIC_CF_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, outcome
LMS_EV_SCAN_LOGIC_PART_RESULT	cs1, cs1Label, cn1, cn1Label, fname, act, cn2, cn2Label, reason, cs2, cs2Label, cs3, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, outcome
LMS_EV_SCAN_LOGIC_MESSAGE_BACKUP	cs1, cs1Label, src, act, fsize, suser, duser, reason, cs2, cs2Label

Отключение экспорта событий в формате CEF

► *Чтобы отключить экспорт событий в формате CEF, выполните следующие действия:*

1. Откройте XML-файл с извлеченными параметрами утилиты управления программой klms-control.
2. В открывшемся файле в блоке `<siemSettings>` установите значение параметра `<enabled>` равным `0`.

Пример:

```
<siemSettings>

    <enabled>0</enabled>
```

Применение новых значений параметров Kaspersky Security 8 для Linux Mail Server

► *Чтобы применить параметры из XML-файла к Kaspersky Security 8 для Linux Mail Server, выполните следующую команду:*

```
# sudo /opt/kaspersky/klms/bin/klms-control \

--set-settings EventLogger -n [-f|--file <file-name>]
```

После выполнения команды параметры экспорта CEF-сообщений будут применены к Kaspersky Security 8 для Linux Mail Server. Параметр `-f|--file <file-name>` указывает XML-файл, содержащий эти параметры.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (http://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (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. 396).

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. 23), 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 (https://support.kaspersky.ru/support/rules#ru_ru).

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

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2c) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2c).

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

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

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

Портал Kaspersky CompanyAccount доступен на следующих языках:

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

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

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией о работе Kaspersky Security 8 для Linux Mail Server и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

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

Расширенная диагностика работы программы

Для расширенной диагностики проблем, связанных с работой программы, возможно использование некоторых команд для управления программой. Эти команды не описаны в Руководстве администратора Kaspersky Security 8 для Linux Mail Server. Сотрудники Службы технической поддержки сообщат об этих командах в случае необходимости.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

Схема расположения файлов программы на компьютере под управлением Linux

После установки Kaspersky Security 8 для Linux Mail Server на компьютер под управлением операционной системы Linux по умолчанию файлы программы располагаются следующим образом:

/etc/opt/kaspersky/klms – директория, содержащая конфигурационные файлы Kaspersky Security 8 для Linux Mail Server:

kavscanner_defaults.conf – конфигурационный файл утилиты kavscanner;

klms_filters.conf – конфигурационный файл фильтров почтового агента.

/opt/kaspersky/klms/ – основная директория Kaspersky Security 8 для Linux Mail Server, включающая:

/opt/kaspersky/klms/bin/ – директория исполняемых файлов компонентов Kaspersky Security 8 для Linux Mail Server:

klms-setup.pl – скрипт первоначальной настройки Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/lib/ – директория хранения библиотек Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/lib64/ – директория хранения дополнительных 64-битных библиотек Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/libexec/ – директория хранения служебных исполняемых файлов Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/libexec/cleanup.sh – скрит для удаления данных, оставшихся после удаления Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/share/ – директория хранения файлов шрифтов, файлов справочной системы Kaspersky Security 8 для Linux Mail Server (manual pages), локализационных пакетов, исходных файлов модулей Kaspersky Security 8 для Linux Mail Server, MIB-файлов, файлов с текстом Лицензионного соглашения:

/opt/kaspersky/klms/share/man/ – директория хранения файлов справочной системы Kaspersky Security 8 для Linux Mail Server (manual pages);

/opt/kaspersky/klms/share/locale – директория хранения локализационных пакетов;

/opt/kaspersky/klms/share/src/ – директория хранения исходного кода модулей Kaspersky Security 8 для Linux Mail Server;

/opt/kaspersky/klms/share/snmp-mibs/ – директория хранения MIB-файлов Kaspersky Security 8 для Linux Mail Server.

/opt/kaspersky/klmsui/lib/ – директория хранения библиотек веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

/opt/kaspersky/klmsui/bin/klmsui-setup.pl – скрипт первоначальной настройки веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

/opt/kaspersky/klmsui/share/htdocs – директория хранения всех hml-ресурсов веб-интерфейса Kaspersky Security 8 для Linux Mail Server.

/opt/kaspersky/klmsui/libexec/ – директория хранения служебных исполняемых файлов веб-интерфейса Kaspersky Security 8 для Linux Mail Server:

- /opt/kaspersky/klmsui/libexec/cleanup.sh – скрипт для удаления данных, оставшихся после удаления веб-интерфейса Kaspersky Security 8 для Linux Mail Server;
- /opt/kaspersky/klmsui/libexec/mod_klwi.so – модуль веб-сервера Apache.

/var/opt/kaspersky/klms/ – директория хранения данных Kaspersky Security 8 для Linux Mail Server:

- /var/opt/kaspersky/klms/backup – хранилище для хранения копий сообщений;
- /var/opt/kaspersky/klms/reports/ – отчеты по требованию;
- /var/opt/kaspersky/klms/reports/weekly – отчеты по расписанию за неделю;
- /var/opt/kaspersky/klms/reports/daily – отчеты по расписанию за день;
- /var/opt/kaspersky/klms/reports/monthly – отчеты по расписанию за месяц;
- /var/opt/kaspersky/klms/postgresql/ – база данных Kaspersky Security 8 для Linux Mail Server;
- /var/opt/kaspersky/klms/update/ – директория хранения пакетов обновлений Kaspersky Security 8 для Linux Mail Server;
  - /var/opt/kaspersky/klms/update/avbases – директория хранения пакетов обновлений антивирусных баз, загруженных из источников обновлений;
  - /var/opt/kaspersky/klms/update/avbases-backup – директория хранения резервных копий пакетов обновлений антивирусных баз.

/var/log/kaspersky/klms/ – директория хранения файлов трассировки Kaspersky Security 8 для Linux Mail Server.

/var/run/klms/ – директория хранения служебных файлов Kaspersky Security 8 для Linux Mail Server.

Схема расположения файлов программы на компьютере под управлением FreeBSD

После установки Kaspersky Security 8 для Linux Mail Server на компьютер под управлением операционной системы FreeBSD по умолчанию файлы программы располагаются следующим образом:

/usr/local/libexec/kaspersky/klms – директория хранения библиотек Kaspersky Security 8 для Linux Mail Server;

/usr/local/lib/kaspersky/klms – директория хранения библиотек Kaspersky Security 8 для Linux Mail Server;

/usr/local/bin/ – директория хранения исполняемых файлов компонентов Kaspersky Security 8 для Linux Mail Server:

- /usr/local/bin/kavscanner – конфигурационный файл утилиты kavscanner;
- /usr/local/bin/klms-disable_content_reputation.pl – скрипт отключения контентной фильтрации и очистки карантина.
- /usr/local/bin/klms-setup.pl – скрипт первоначальной настройки Kaspersky Security 8 для Linux Mail Server;
- /usr/local/bin/klms-uninstall_filters.pl – скрипт деинтеграции с почтовым сервером;
- /usr/local/etc/rc.d/klms – скрипт запуска программы;
- /usr/local/etc/rc.d/klmsdb – скрипт запуска базы данных;

/usr/local/man/ – директория хранения файлов справочной системы Kaspersky Security 8 для Linux Mail Server (manual pages);

/usr/local/share/doc/klms/ – директория хранения файлов шрифтов, рисунков, локализационных пакетов, файлов с текстом Лицензионного соглашения, MIB-файлов, исходного кода модулей:

- /usr/local/share/klms/fonts – директория хранения файлов шрифтов;

/usr/local/share/klms/images – директория хранения рисунков;

/usr/local/share/klms/locale – директория хранения локализационных пакетов;

/usr/local/share/klms/snmp-mibs – директория хранения MIB-файлов Kaspersky Security 8 для Linux Mail Server;

/usr/local/share/klms/srcsrc/ – директория хранения исходного кода модулей Kaspersky Security 8 для Linux Mail Server.

/var/db/kaspersky – директория хранения файлов и данных программы:

/var/db/kaspersky/klms/cleanup.sh – скрипт для удаления данных, оставшихся после удаления Kaspersky Security 8 для Linux Mail Server;

/var/db/kaspersky/klms/backup – директория хранения копий сообщений хранилища;

/var/db/kaspersky/klms/postgresql – база данных Kaspersky Security 8 для Linux Mail Server;

/var/db/kaspersky/klms/reports – отчеты по требованию;

/var/db/kaspersky/klms/reports/daily – отчеты по расписанию за день;

/var/db/kaspersky/klms/reports/monthly – отчеты по расписанию за месяц;

/var/db/kaspersky/klms/reports/weekly – отчеты по расписанию за неделю.

/var/db/kaspersky/klms/update – директория хранения пакетов обновлений Kaspersky Security 8 для Linux Mail Server:

/var/db/kaspersky/klms/update/avbases – директория хранения пакетов обновлений антивирусных баз, загруженных из источников обновлений;

/var/db/kaspersky/klms/update/avbases-backup – директория хранения резервных копий пакетов обновлений антивирусных баз.

/var/log/kaspersky/klms/ – директория хранения файлов трассировки Kaspersky Security 8 для Linux Mail Server.

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 28. 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	
		Включить DMARC-проверку подлинности отправителей	
	Антивирус	Антивирус	Вкл.

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
		Использовать KSN	**Нет**
		Использовать эвристический анализ	
	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
Правила / Изменить правило для правила **Default**	**Общие параметры правила**	**Режим работы правила**	**Использовать параметры модулей проверки**
	Анти-Спам	**Проверка на спам**	**Вкл.**

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
	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.
	Уведомления	Все параметры блока параметров	Не отправлять

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
	Проверка подлинности отправителей сообщений	Проверка подлинности отправителей сообщений	Выкл.

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

SCL-оценка

Spam Confidence Level, специальная метка сообщения, которая используется почтовыми серверами Microsoft Exchange для определения вероятности того, что сообщение является спам-сообщением. SCL-оценка может принимать значения от 0 (вероятность спама минимальна) до 9 (сообщение, скорее всего, является спам-сообщением). Значение SCL-оценки сообщения может быть изменено программой Kaspersky Security 8 для Linux Mail Server в соответствии с результатами проверки сообщения.

SNMP-агент

Программный модуль сетевого управления Kaspersky Security 8 для Linux Mail Server, отслеживает информацию о работе Kaspersky Security 8 для Linux Mail Server.

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 Security 8 для Linux Mail Server, предназначенный для обнаружения вирусов в сообщениях электронной почты и вложениях в сообщения электронной почты.

Анти-Спам

Компонент Kaspersky Security 8 для Linux Mail Server, предназначенный для обнаружения сообщений, которые классифицируются как спам.

Анти-Фишинг

Компонент Kaspersky Security 8 для Linux Mail Server, 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.

B

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

И

Интернационализованный адрес

Адрес электронной почты, который содержит символы национальных (нелатинских) алфавитов (например, кириллица, арабский алфавит).

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 Security 8 для Linux Mail Server 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.

Спуфинг

Вид компьютерного мошенничества. Целью спуфинга является получение незаконного доступа к персональным данным путем фальсификации программы или веб-сайта. Например, злоумышленники могут создать точную копию официального веб-сайта какой-либо компании и при помощи спам-технологий рассылать сообщения от имени этой компании. В таких сообщениях, как правило, содержится ссылка на фальсифицированный веб-сайт, где у пользователя запрашиваются конфиденциальные данные.

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

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google Chrome – товарный знак Google, Inc.

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

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Active Directory, 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 и Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Sendmail и другие наименования и названия продуктов – товарные знаки или зарегистрированные товарные знаки Sendmail, Inc.

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

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

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

Предметный указатель

A

B

D

E

F

L

M

P

Q

S

T

А

Д

Ж

Л

М

О

П

Р

Т

У

Ф

Соответствие терминов

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

Таблица 29. 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