kaspersky

Kaspersky Security для Linux Mail Server

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 10.0.0.7427

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 15.08.2023

Обозначение документа: 643.46856491.00061-08 90 01

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

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

Об этом документе

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

Подготовительные процедуры изложены в разделах «Установка приложения», «Подготовка Kaspersky Security для Linux Mail Server к работе» и «Процедура приемки» и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе «Требования» приведены минимально необходимые системные требования для безопасной установки приложения.

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

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security для Linux Mail Server, а также поддержка организаций, использующих Kaspersky Security для Linux Mail Server.

kaspersky

Источники информации о приложении

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

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Security для Linux Mail Server:

- страница Kaspersky Security для Linux Mail Server на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Security для Linux Mail Server на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

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

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

На странице Kaspersky Security для Linux Mail Server (https://www.kaspersky.ru/small-to-medium-business-security/linux-mail-server) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

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

Страница Kaspersky Security для Linux Mail Server в Базе знаний

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

На странице в Базе знаний (https://support.kaspersky.ru/klms/10) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security для Linux Mail Server, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

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

С помощью веб-интерфейса вы можете управлять Kaspersky Security для Linux Mail Server через браузер. Справка (https://support.kaspersky.com/KLMS/10/ru-RU/100512.htm) содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя через веб-интерфейс Kaspersky Security для Linux Mail Server (далее также "веб-интерфейс").

Документация

В комплект поставки Kaspersky Security для Linux Mail Server включен настоящий документ "Kaspersky Security для Linux Mail Server. Подготовительные процедуры и руководство по эксплуатации", с помощью которого вы можете установить программу и произвести настройку параметров программы.

kaspersky

О Kaspersky Security для Linux Mail Server

Kaspersky Security для Linux Mail Server обеспечивает защиту входящей и исходящей почты от вредоносных объектов и спама, выполняет контентную фильтрацию сообщений, а также, при интеграции с приложением Kaspersky Anti Targeted Attack Platform (далее также "KATA"), обеспечивает защиту почты от целевых атак на IT-инфраструктуру организации.

Kaspersky Security для Linux Mail Server 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 для Linux Mail Server, 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 Kaspersky Security для Linux Mail Server реализованы следующие функции безопасности:

- Разграничение доступа к управлению приложением.
- Управление работой приложения.
- Управление параметрами приложения.
- Управление установкой обновлений (актуализации) БД ПКВ приложения.
- Аудит безопасности.
- Выполнение проверок объектов воздействия.
- Обработка объектов воздействия.
- Сигнализация приложения.
- Выполнение проверок сообщений электронной почты.
- Идентификация и аутентификация.

Основные возможности Kaspersky Security для Linux Mail Server перечислены ниже.

Технологии защиты

- Проверка сообщений модулем Антивирус.

  Проверка сообщений электронной почты на наличие вирусов и вредоносных программ, макросов (например, файлов форматов Microsoft® Office с макросами); зашифрованных объектов, архивов.

- Проверка сообщений модулем Анти-Спам:
  - Проверка сообщений на наличие спама, предполагаемого спама, массовых рассылок (в том числе с использованием технологии распознавания поддельных доменов и проверки репутации IP-адресов).
  - Обнаружение сообщений с Юникод-спуфингом.

    В случае обнаружения Юникод-спуфинга сообщение считается спамом. Приложение добавляет метку unicode_spoof к заголовку сообщения X-KLMS-AntiSpam-Method.
  - Добавление в сообщения X-заголовков X-MS-Exchange-Organization-SCL, содержащих SCL-оценку, по результатам проверки на спам.

    - Помещение сообщения в Анти-Спам карантин, управление Анти-Спам карантином в веб-интерфейсе.
- Проверка сообщений модулем Анти-Фишинг.
- Проверка сообщений на наличие вредоносных или рекламных ссылок, а также ссылок, относящихся к легальному ПО.
- Контентная фильтрация сообщений:
    - размеру сообщения;
    - по имени вложений;
    - по типу вложений.

      Kaspersky Security для Linux Mail Server позволяет определять истинный формат и тип вложения, независимо от его расширения, в том числе внутри архивов и составных объектов.
- Проверка подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC.

Управление Хранилищем

- Сохранение в Хранилище оригиналов сообщений по результатам их обработки модулями Антивирус, Анти-Спам, Анти-Фишинг, а также контентной фильтрации и проверки сообщений KATA.
- Сохранение сообщений из Хранилища в файл.
- Пересылка сообщений получателям.
- Предоставление пользователям доступа к персональному Хранилищу.
- Настройка рассылки дайджеста персонального Хранилища пользователей.

Правила

- Обработка сообщений электронной почты согласно правилам, заданным для групп отправителей и получателей.
- Добавление примечаний к исходящим и входящим сообщениям, а также предупреждений о небезопасном сообщении.
- Списки запрещенных и разрешенных адресов, позволяющие более точно настроить реакцию почтовой системы на сообщения с определенных адресов.
- Возможность указать пользователей и группы пользователей из Microsoft Active Directory® в правилах фильтрации сообщений электронной почты.
- Уведомление отправителя, получателей и администратора об обнаружении сообщений, содержащих зараженные, защищенные паролем и недоступные для проверки объекты.

Управление приложением

- Настройка параметров и управление работой приложения через веб-интерфейс.
- Обновление баз приложения с серверов обновлений "Лаборатории Касперского", серверов Kaspersky Security Center и пользовательских ресурсов (HTTP- и HTTPS-серверов, локальных и сетевых папок) по расписанию и по требованию.
- Создание и просмотр отчетов о результатах обработки сообщений и событиях работы приложения.
- Управление доступом пользователей к функциям приложения с помощью ролевой системы.
- Помещение сообщений в Анти-Спам карантин и KATA-карантин, управление Анти-Спам карантином и KATA-карантином в веб-интерфейсе.
- Получение информации о пользователях из разных доменов.
- Настройка аутентификации с помощью технологии единого входа.

- Создание кластера для масштабирования решения (как горизонтально, так и вертикально) с возможностью централизованного управления всеми серверами кластера через веб-интерфейс приложения.

Интеграция

- Использование информации из Kaspersky Security Network, чтобы увеличить скорость реакции на новые угрозы.
- Интеграция с Kaspersky Private Security Network (далее также KPSN) для тех организаций, в которых доступ в интернет ограничен внутренними правилами и политиками.

  После интеграции с KPSN Kaspersky Security для Linux Mail Server может использовать репутационные базы KSN, не отправляя данные за пределы организации.

  По вопросам приобретения приложения Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

- Интеграция с Kaspersky Anti Targeted Attack Platform (далее также KATA) для обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (APT).

  После интеграции с KATA Kaspersky Security для Linux Mail Server может отправлять копии сообщений на проверку в KATA. По результатам проверки KATA Kaspersky Security для Linux Mail Server может блокировать отдельные сообщения.

  По вопросам приобретения приложения Kaspersky Anti Targeted Attack Platform вы можете связаться со специалистами отдела продаж "Лаборатории Касперского".

- Интеграция с Active Directory для получения информации о пользователях домена.

Мониторинг работы приложения

- Мониторинг состояния почтового трафика, просмотр списков последних обнаруженных угроз в веб-интерфейсе приложения.
- Просмотр журнала событий в веб-интерфейсе приложения.
- Получение статистики работы приложения по протоколу SNMP, включение и отключение отправки SNMP-ловушек.
- Публикация событий, происходящих во время работы приложения, в SIEM-систему, используемую в организации, по протоколу Syslog.

  Информация о каждом событии приложения передается как отдельное syslog-сообщение формата CEF.

- Создание и просмотр отчетов о результатах обработки сообщений электронной почты.
- Создание архива с диагностической информацией о работе Kaspersky Security для Linux Mail Server для отправки в Службу технической поддержки "Лаборатории Касперского".

kaspersky

В этом разделе

О действиях приложения над объектами

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

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

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

- `Пропустить` – доставить сообщение получателю, не изменяя его.
- `Отклонить` – 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.
- `Удалить сообщение` – удалить сообщение. Если выбрано это действие, почтовый сервер-отправитель сообщения получит уведомление о доставке сообщения, однако получателю сообщение доставлено не будет.
- `Удалить вложение` – удалить вложение (применяется только по результатам антивирусной проверки).
- `Вылечить` – лечить зараженный объект (применяется только по результатам антивирусной проверки). Если выбрано это действие, приложение пытается вылечить зараженный объект. Если лечение невозможно, к объекту применяется действие `Отклонить`, `Удалить сообщение` или `Удалить вложение`, заданное в параметрах правила. Если администратор не задал действие в параметрах правила, приложение выполняет действие `Удалить вложение`.

Комплект поставки

Kaspersky Security для Linux Mail Server входит в состав следующих комплексных решений "Лаборатории Касперского" для обеспечения безопасности и системного администрирования:

- Kaspersky TOTAL Security для бизнеса (http://www.kaspersky.ru/business-security/total).
- Kaspersky Security для почтовых серверов (http://www.kaspersky.ru/business-security/mail-server).

Для выбора комплексного решения, наиболее подходящего для вашей организации, проконсультируйтесь со специалистами компании-партнера "Лаборатории Касперского". Контактная информация и адреса партнеров представлены на сайте "Лаборатории Касперского" в разделе https://partnersearch.kaspersky.com https://partnersearch.kaspersky.com.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется приложение.

При покупке Kaspersky Security для Linux Mail Server вы копируете приложение с сайта компании-партнера или "Лаборатории Касперского". Информация, необходимая для активации приложения, высылается вам по электронной почте после оплаты.

Об информационных X-заголовках

По результатам проверки приложение добавляет к заголовку сообщения специальные информационные X-заголовки, например:

- X-KLMS-Rule-ID – список идентификаторов правил обработки сообщений.
- X-KLMS-Message-Action – действие приложения над сообщением, а также сработавший модуль приложения.
- X-KLMS-AntiVirus – заголовок для сообщений, обработанных модулем Антивирус (содержит название и версию приложения, а также дату выпуска антивирусных баз).
- X-KLMS-AntiVirus-Status – статус, присвоенный сообщению модулем Антивирус по результатам проверки.
- X-KLMS-AntiSpam-Lua-Profiles – версия Анти-Спам баз, а также информация о присвоенном спам-рейтинге.
- X-KLMS-AntiSpam-Method – сработавший метод распознавания спама.
- X-KLMS-AntiSpam-Rate – рейтинг, присвоенный сообщению модулем Анти-Спам.
- X-KLMS-AntiSpam-Status – статус, присвоенный сообщению модулем Анти-Спам по результатам проверки.
- X-KLMS-AntiSpam-Envelope-From – отправитель сообщения.
- X-KLMS-AntiSpam-Auth – статус, присвоенный сообщению по результатам проверки подлинности отправителей с помощью технологий SPF, DKIM, DMARC.
- X-KLMS-AntiSpam-Version – версия модуля Анти-Спам.
- X-KLMS-AntiSpam-Info – критерии, по которым модуль Анти-Спам присвоил сообщению статус.
- X-KLMS-AntiSpam-Moebius-Timestamps – информация о сигнатурах службы Moebius.
- X-KLMS-AntiPhishing – заголовок для сообщений, обработанных модулем Анти-Фишинг (содержит результат проверки).
- X-KLMS-LinksScanning – заголовок для сообщений, обработанных модулем проверки ссылок (содержит результат проверки и дату выпуска антивирусных баз).
- X-KLMS-AntiSpam-Interceptor-Info – результат проверки сообщения.

Заголовок может содержать следующие значения:

- not scanned – модуль Анти-Спам отключен;
- timeout expired – проверка не была завершена из-за превышения времени ожидания;
- scan successful – проверка сообщения выполнена успешно;
- fallback – проверка не была завершена из-за возникшей ошибки.

kaspersky

Ограничение трафика приложения

► *Чтобы перевести Kaspersky Security для Linux Mail Server в режим ограниченного трафика:*

1. В главном окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN** и выберите вкладку **Параметры KSN/KPSN**.
2. В раскрывающемся списке **Использование KSN/KPSN** выберите значение **Не использовать**.
3. Нажмите на кнопку **Сохранить**.

   Откроется окно подтверждения.
4. Нажмите на кнопку **Отключить**.
5. В дереве консоли управления выберите раздел **Параметры** → **Общие** → **Защита** и выберите вкладку **Внешние службы**.
6. Выключите переключатель **Разрешить подключение к DNS-серверу**.
7. Выберите вкладку **Анти-Спам** и выключите переключатель **Использовать службу Moebius**.
8. Нажмите на кнопку **Сохранить**.
9. В дереве консоли управления выберите раздел **Параметры** → **Внешние службы** → **Обновление баз** и выберите вкладку **Параметры обновления**.
10. В раскрывающемся списке **Источник** выберите значение **Kaspersky Security Center**.
11. Нажмите на кнопку **Сохранить**.

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

Используемые сетевые доступы

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

В таблице не указаны сетевые доступы для работы почтового сервера, SNMP-сервера, Syslog-сервера. Администратор операционной системы должен настроить их самостоятельно.

kaspersky

Таблица 1. Сетевые доступы, необходимые для работы приложения

Функциональность	Протокол	Порт	Направление	Назначение соединения
Работа с приложением через веб-интерфейс (см. раздел "Интерфейс Kaspersky Security для Linux Mail Server" на стр. 87)	TCP	443	Входящее	Компьютер администратора приложения
Взаимодействие между узлами кластера (см. раздел "Управление кластером" на стр. 136)	TCP	По умолчанию 9045 (возможно изменить при установке)	Входящее и исходящее	Другие узлы кластера
DNS-запросы	UDP, TCP	53	Исходящее	DNS-серверы, указанные вручную администратором
Соединение с прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 256)	TCP	По умолчанию 8080 (возможно изменить в веб-интерфейсе приложения)	Исходящее	Прокси-сервер
Активация приложения (см. раздел "Добавление кода активации" на стр. 55)	TCP	443	Исходящее	Серверы "Лаборатории Касперского": • activation-v2.kaspersky.com • eu.activation-v2.kaspersky.com • americas.activation-v2.kaspersky.com • apac.activation-v2.kaspersky.com • china.activation-v2.kaspersky.com • activation-v2.geo.kaspersky.com • activate.activation-v2.kaspersky.com

Функциональность	Протокол	Порт	Направление	Назначение соединения
Обновление баз приложения (см. раздел "Обновление баз" на стр. 257)	TCP	80, 443	Исходящее	Серверы "Лаборатории Касперского". Вы можете посмотреть список серверов в Базе знаний https://support.kaspersky.ru/common/start/, статья 6105.
KSN (см. раздел "Настройка участия в Kaspersky Security Network" на стр. 267)	TCP	443	Исходящее	Серверы "Лаборатории Касперского": • ds.kaspersky.com • ksn-file-geo.kaspersky-labs.com • ksn-verdict-geo.kaspersky-labs.com • ksn-url-geo.kaspersky-labs.com • ksn-kas-geo.kaspersky-labs.com • ksn-a-stat-geo.kaspersky-labs.com • ksn-info-geo.kaspersky-labs.com • ksn-cinfo-geo.kaspersky-labs.com • dc1.ksn.kaspersky-labs.com • dc1-file.ksn.kaspersky-labs.com • dc1-kas.ksn.kaspersky-labs.com • dc1-st.ksn.kaspersky-labs.com
KPSN (см. раздел "Настройка использования Kaspersky Private Security Network" на стр. 268)	TCP	443	Исходящее	Сервер KPSN
Служба Moebius (см. стр. 249)	TCP	443	Исходящее	Серверы "Лаборатории Касперского": • moebius.kaspersky-labs.com • moebius-new.kaspersky-labs.com
Соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272)	TCP	389	Исходящее	Серверы Active Directory

Функциональность	Протокол	Порт	Направление	Назначение соединения
Kerberos-аутентификация в Active Directory (см. раздел "Настройка Kerberos-аутентификации" на стр. 333)	UDP, TCP	88	Исходящее	Серверы Active Directory
NTLM-аутентификация с помощью технологии единого входа (см. раздел "Настройка NTLM-аутентификации" на стр. 334)	TCP	445 (возможно изменить в веб-интерфейсе приложения)	Исходящее	Серверы Active Directory
Защита KATA (на стр. 277)	TCP	По умолчанию 443 (возможно изменить в веб-интерфейсе приложения)	Исходящее	Сервер KATA

kaspersky

Требования

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

В этом разделе

Аппаратные и программные требования

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

- Минимальные аппаратные требования:
  - 8 ядер процесса;
  - 16 ГБ оперативной памяти;
  - 200 ГБ на жестком диске для установки приложения и хранения временных файлов и файлов журналов.
- Программные требования:

  Одна из следующих операционных систем:
  - Astra Linux Special Edition РУСБ.10015-01, очередное обновление 1.6 с оперативным обновлением 12 (БЮЛЛЕТЕНЬ № 20221220SE16), ядро generic.
  - Astra Linux Special Edition РУСБ.10015-01 очередное обновление 1.7 с оперативным обновлением 1.7.3 (БЮЛЛЕТЕНЬ № 2022-1110SE17), ядро generic.

Kaspersky Security для Linux Mail Server поддерживает интеграцию с почтовым сервером Exim из состава пакета exim4-daemon-heavy (с поддержкой dlfunc) из репозиториев, поставляемых на установочном диске и диске с кумулятивным обновлением Astra Linux. Требования к версии Exim:

- Для Astra Linux Special Edition 1.6 – версия 4.89 и выше;
- Для Astra Linux Special Edition 1.7 – версия 4.92 и выше.

Kaspersky Security для Linux Mail Server поддерживает интеграцию с СУБД PostgreSQL из состава пакета установки приложения или из состава операционной системы. Пользователям сертифицированной версии Kaspersky Security для Linux Mail Server следует использовать СУБД PostgreSQL из состава операционной системы Astra Linux Special Edition. Требования к версии СУБД PostgreSQL:

- Для Astra Linux Special Edition 1.6 – версия 9.6.24 и выше;
- Для Astra Linux Special Edition 1.7 – версия 11.17 и выше.

Kaspersky Security для Linux Mail Server поддерживает обновление баз без подключения к интернету через Kaspersky Security Center. На все компьютеры, где требуется обновление баз Kaspersky Security для Linux Mail Server через Kaspersky Security Center, необходимо установить Агент администрирования версии 14.0.0.4490.

На компьютере администратора приложения должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ 90 и выше.
- Microsoft Edge® 114 и выше.
- Google Chrome™ 114 и выше.

На всех компьютерах, на которых планируется установка Kaspersky Security для Linux Mail Server, должны быть выполнены следующие условия:

- Установлен веб-сервер Apache:
  - Для Astra Linux Special Edition 1.6 – версия 2.4.46 и выше;
  - Для Astra Linux Special Edition 1.7 – версия 2.4.52 и выше.
- Установлен пакет postgresql из состава Astra Linux Special Edition, если вы хотите использовать СУБД PostgreSQL из состава операционной системы вместо СУБД, поставляемой в составе Kaspersky Security для Linux Mail Server.
- В операционной системе установлена локаль en_US.UTF-8.
- В параметрах операционной системы настроена синхронизация времени и установлен один и тот же часовой пояс.

Указания по эксплуатации и требования к среде

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

11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя 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.

Разделение доступа к функциям программы по пользовательским ролям

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

- Учетная запись суперпользователя приложения Administrator.

  Учетная запись администратора веб-интерфейса программы Administrator создается при установке программы и обладает всем набором прав на управление программой. Эта учетная запись предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Security для Linux Mail Server через веб-интерфейс программы.

- Учетные записи привилегированных пользователей веб-интерфейса.

  Пользователь Administrator может назначить роль с ограниченным набором прав на управление программой другим сотрудникам, например офицеру безопасности.

  Пользователям, которым назначена хотя бы одна роль, доступен просмотр веб-интерфейса в режиме привилегированного пользователя. В меню отображаются те разделы, на которые у пользователя есть права.

- Учетные записи персональных пользователей.

  Режим персонального пользователя доступен всем пользователям домена Active Directory, для которого настроена аутентификация с помощью технологии единого входа (SSO) (см. раздел "Аутентификация с помощью технологии единого входа" на стр. 330). Для просмотра веб-интерфейса в режиме персонального пользователя требуется войти в приложение (см. раздел "Подключение к веб-интерфейсу приложения" на стр. 89), используя доменную учетную запись. В меню отображаются разделы с персональным Хранилищем и персональными списками разрешенных и запрещенных адресов, если доступ к этим разделам разрешен администратором. В этих разделах доступна информация только о сообщениях и адресах текущего пользователя.

Об обработке сообщений в режиме мандатного управления доступом

В режиме поддержки мандатного управления доступом приложение снимает мандатную метку перед обработкой некоторых сообщений и проставляет метку снова после обработки.

Мандатная метка не сохраняется для сообщений, отправляемых из карантина и из Хранилища.

kaspersky

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Security для Linux Mail Server.

В сертифицированной версии Kaspersky Security для Linux Mail Server допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния приложения.

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 приложение.

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Security для Linux Mail Server.
- Прочитав документ license.txt. Этот документ включен в комплект поставки приложения.

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

О лицензии

Лицензия – это ограниченное по времени право на использование приложения, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security для Linux Mail Server прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Security для Linux Mail Server вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

kaspersky

О ключе

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

Вы можете добавить ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*.

Добавленный лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности.

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

Для Kaspersky Security для Linux Mail Server используются ключи следующих типов:

- *Полнофункциональный ключ*. При добавлении ключа приложение работает в режиме полной функциональности, осуществляются проверки на спам, фишинг, вирусы и другие программы, представляющие угрозу, проверка ссылок, контентная фильтрация, проверка подлинности отправителей сообщений и проверка сообщений в Kaspersky Anti Targeted Attack Platform.
- *Ключ для антивирусной защиты*. При добавлении ключа приложение производит поиск вирусов и других программ, представляющих угрозу, выполняет проверку ссылок, проверку подлинности отправителя сообщений, контентную фильтрацию и проверку сообщений в Kaspersky Anti Targeted Attack Platform. Приложение не производит проверку на спам и фишинг. Статус, присвоенный приложением сообщению при проверке этими модулями, содержит информацию об ограниченной функциональности.

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

О коде активации

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

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

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

kaspersky

О файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security для Linux Mail Server или после заказа пробной версии Kaspersky Security для Linux Mail Server.

Чтобы активировать приложение 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 к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

О подписке

Подписка на Kaspersky Security для Linux Mail Server – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств).

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

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

Чтобы использовать Kaspersky Security для Linux Mail Server по подписке, требуется применить код активации. После применения кода активации устанавливается ключ, определяющий лицензию на использование приложения по подписке.

О предоставлении данных

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

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

- В Лицензионном соглашении.

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

  - тип, версия и локализация приложения;

- версии установленных обновлений;
- код активации и уникальный идентификатор активации текущего лицензионного кода активации;
- идентификатор компьютера и идентификатор установки приложения;
- тип, версия и разрядность операционной системы;
- название виртуальной среды;
- идентификаторы компонентов приложения, активных на момент предоставления данных.

Вы можете просмотреть Лицензионное соглашение при установке Kaspersky Security для Linux Mail Server или в папке /opt/kaspersky/klms/share/doc.

- В Политике конфиденциальности.
- В Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network.

  При участии в Kaspersky Security Network и при отправке KSN-статистики в "Лабораторию Касперского" может передаваться информация, полученная в результате работы приложения. Перечень передаваемых данных указан в Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network. Вы можете просмотреть эти Положения в веб-интерфейсе в разделе **Параметры** → **Внешние службы** → **KSN/KPSN** → **Параметры KSN/KPSN**.

Защита данных

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

Оперативная память Kaspersky Security для Linux Mail Server может содержать любые обрабатываемые данные пользователей приложения. Администратору Kaspersky Security для Linux Mail Server необходимо обеспечить безопасность этих данных с использованием сертифицированной ОС Astra Linux Special Edition.

По умолчанию доступ к персональным данным пользователей имеют следующие учетные записи:

- Учетные записи операционной системы:
  - Пользователь с привилегиями root.
  - kluser.
  - Пользователи, от имени которых запускаются процессы приложения:
    - Exim (далее – пользователь Exim);
    - Apache (далее – пользователь Apache);
  - Учетные записи, входящие в одну из следующих групп:
    - klusers;

  - kl_web_users;
  - kl_var_users.
- Учетная запись привилегированного пользователя Kaspersky Security для Linux Mail Server Administrator.

Учетные записи пользователей Exim, Apache не являются частью приложения. Эти учетные записи создаются на компьютере администратора, когда администратор самостоятельно устанавливает стороннее ПО Exim и Apache.

Приложение не предоставляет возможностей для ограничения прав учетных записей пользователей операционной системы, на которой установлено приложение. Доступ к месту хранения данных ограничен средствами файловой системы. Администратору рекомендуется контролировать доступ к персональным данным других пользователей любыми системными средствами на его усмотрение.

Пользователь Administrator имеет возможность предоставить доступ к веб-интерфейсу. Доступ к персональным данным предоставляется согласно правам доступа для роли, которая привязана к учетной записи.

Передача данных между узлами кластера осуществляется по зашифрованному каналу (по протоколу HTTPS с использованием авторизации с помощью сертификата безопасности). Передача данных в веб-интерфейс осуществляется по зашифрованному каналу по протоколу HTTPS. Привилегированные пользователи с локальной учетной записью авторизуются с помощью пароля, остальные пользователи веб-интерфейса проходят авторизацию по протоколу Kerberos или NTLM.

Подключение к Active Directory осуществляется по зашифрованному каналу (SASL) с авторизацией по протоколу Kerberos.

Работа с приложением из командной строки сервера, на котором установлено приложение, под учетной записью суперпользователя позволяет управлять параметрами дампа. Дамп формируется при сбоях приложения и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные, включая фрагменты анализируемых файлов. По умолчанию формирование дампа в Kaspersky Security для Linux Mail Server отключено.

Доступ к этим данным может быть осуществлен из командной строки сервера, на котором установлено приложение, под учетной записью суперпользователя.

При передаче диагностической информации в Службу технической поддержки "Лаборатории Касперского" администратору Kaspersky Security для Linux Mail Server необходимо обеспечить безопасность дампов и файлов трассировки самостоятельно. Администратор Kaspersky Security для Linux Mail Server несет ответственность за доступ к этой информации.

Состав данных, которые могут храниться в приложении

Для ознакомления с полным перечнем данных пользователей, которые могут храниться в Kaspersky Security для Linux Mail Server, см. таблицу ниже.

Таблица 2. Данные пользователей, которые могут храниться в Kaspersky Security для Linux

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Основная функциональность приложения				
• Имена учетных записей администратора и пользователей приложения. • Права доступа учетных записей приложения. • Хеш пароля локальных учетных записей привилегированных пользователей. • Имя учетной записи и пароль подключения приложения к прокси-серверу. • Keytab-файлы и параметры для подключения к LDAP-серверу. • Keytab-файлы для подключения по SSO Kerberos и параметры для подключения к NTLM-серверу. • Комментарии.	Конфигурация приложения	/var/opt/kaspersky/klms	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр параметров приложения и права на просмотр учетных записей.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• Имена учетных записей пользователей и контактов в LDAP, другие LDAP-атрибуты. • Адреса электронной почты отправителей и получателей сообщений. • IP-адреса отправителей сообщений. • Комментарии.	Правила обработки сообщений и пользовательские списки	/var/opt/kaspersky/klms	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр правил обработки сообщений.
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений.	Статистика работы приложения	/var/opt/kaspersky/klms	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр отчетов и раздела **Мониторинг**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Имена и размер почтовых вложений. • Тема сообщения.	Журнал событий обработки сообщений	/var/opt/kaspersky/klms	Согласно параметрам, заданным пользователем приложения. По умолчанию устанавливается срок хранения 3 дня или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события обработки почтового трафика**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
		Зависит от настроек syslog из состава операционной системы. Пример места хранения: /var/log/messages	Зависит от настроек syslog из состава операционной системы	• Пользователь root имеет доступ к месту хранения информации. • Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями syslog. Права доступа выдает администратор операционной системы. Если будет выдан доступ группе klusers, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события обработки почтового трафика**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• Имя учетной записи пользователя, инициировавшего событие. • IP-адрес и порт узла, на котором произошло событие.	Журнал событий приложения	/var/opt/kaspersky/klms	Согласно параметрам, заданным пользователем приложения. По умолчанию устанавливается срок хранения 1100 дней или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события приложения**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
		Зависит от настроек syslog из состава операционной системы. Пример места хранения /var/log/messages	Зависит от настроек syslog из состава операционной системы.	• Пользователь root имеет доступ к месту хранения информации. • Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями syslog. Права доступа выдает администратор операционной системы. Если будет выдан доступ группе klusers, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события обработки почтового трафика**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений. Данные об обновлениях приложения:	Файлы трассировки	/var/log/kaspersky/klms	Бессрочно. При достижении объема 150 МБ для каждого потока трассировки более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на получение диагностической информации.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. Информация об учетных записях пользователей: • Имена учетных записей администраторов и пользователей веб-интерфейса приложения. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.		Зависит от настроек syslog из состава операционной системы. Пример места хранения: /var/log/messages	Зависит от настроек syslog из состава операционной системы.	• Пользователь root имеет доступ к месту хранения информации. • Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями syslog. Права доступа выдает администратор операционной системы. Если будет выдан доступ группе klusers, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события обработки почтового трафика**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
		/var/log/kaspersky/extra	Бессрочно. При достижении объема 400 МБ для каждого файла трассировки более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право **Просматривать события обработки почтового трафика**.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело и размер сообщения. • Служебные заголовки сообщения. • Имена, размер и тела почтовых вложений.	Хранилище	/var/opt/kaspersky/klms	Бессрочно. При достижении объема 7 ГБ более старые записи удаляются. Администратор может изменить это значение.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователь Exim имеет доступ к сообщениям во время их доставки из Хранилища. • Пользователи веб-интерфейса приложения, имеющие права на просмотр Хранилища.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело и размер сообщения. • Служебные заголовки сообщения. • Имена, размер и тела почтовых вложений.	Анти-Спам карантин	/var/opt/kaspersky/klms	Бессрочно. При достижении объема 1 ГБ более старые записи удаляются. Администратор может изменить это значение.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр очереди сообщений.
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело и размер сообщения. • Служебные заголовки сообщения. • Имена, размер и тела почтовых вложений. • URL-адреса, содержащиеся в сообщении.	KATA-карантин	/var/opt/kaspersky/klms	Бессрочно. При достижении объема 1 ГБ или 5000 сообщений (значения настраиваются администратором) новые письма не помещаются в KATA-карантин.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр очереди сообщений.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений.	Временные файлы	• /tmp/klmstmp • /tmp/klms_filter (если в конфигурационном файле Exim параметр PrivateTmp имеет значение yes). • /var/opt/kaspersky/klms/tmp/klms_filter (если в конфигурационном файле Exim параметр PrivateTmp имеет значение no).	Зависит от операционной системы и ее настроек.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Exim имеет доступ к обработанным сообщениям во время их доставки.
Интеграция с Active Directory				

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Атрибуты User Object: • distinguishedName • sAMAccountName • msDS-PrincipalName • userPrincipalName • canonicalName • displayName • cn • primaryGroupID • proxyAddresses • mail • memberOf Атрибуты Contacts Object: • distinguishedName • displayName • cn • proxyAddresses • mail • memberOf Атрибуты Group Object: • distinguishedName • canonicalName • objectSid • proxyAddresses • mail • memberOf	• Правила обработки сообщений. • Аутентификация с помощью технологии единого входа. • Автозаполнение учетных записей при работе с ролями и правами пользователей, а также при настройке правил обработки сообщений и пользовательских списков.	• /var/opt/kaspersky/klms/ldap/cache.dbm • /var/opt/kaspersky/klms/ldap/storage	Бессрочно. Данные регулярно обновляются. При отключении интеграции приложения с Active Directory данные удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр разделов приложения, где есть элемент интерфейса с функцией автозаполнения учетных записей.
Интеграция с решением Kaspersky Anti Targeted Attack Platform (KATA)				

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из электронной почты: • IP-адреса отправителей. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений. • URL-адреса, содержащиеся в сообщении.	Отправка объектов для проверки на сервере KATA	Данные не сохраняются.	Данные не сохраняются.	Нет доступа.

Состав данных, передаваемых в службу Kaspersky Security Network

Данные передаются на серверы KSN в зашифрованном виде. По умолчанию доступ к данным имеют специалисты "Лаборатории Касперского", учетная запись root, а также ученая запись kluser, от имени которой работают компоненты приложения.

Для ознакомления с полным перечнем данных пользователей, передаваемых в службу KSN, см. таблицу ниже.

Указанные данные передаются только в случае согласия на участие в Kaspersky Security Network (см. раздел "Настройка участия в Kaspersky Security Network" на стр. 267).

Таблица 3. Данные, передаваемые в службу Kaspersky Security Network

Тип данных	Где используются данные	Место хранения	Срок хранения
• Контрольные суммы (MD5, SHA2-256) проверяемого объекта; • URL-адрес, репутация которого запрашивается; • идентификатор протокола соединения и номер используемого порта; • идентификатор антивирусных баз и идентификатор записи в антивирусных базах, которые использовались для проверки объекта; • информация о сертификате подписанного файла (отпечаток сертификата и контрольная сумма (SHA256) публичного ключа сертификата); • идентификатор и полная версия установленного ПО; • идентификатор службы KSN, к которой обращается ПО; • дата и время отправки объекта на проверку; • идентификатор компонента ПО; • идентификатор сценария, в рамках которого объект отправлен на проверку.	Отправка KSN-запросов	KSN-серверы	Бессрочно. Максимальное количество хранимых записей составляет 360 тысяч. При достижении этого ограничения удаляются записи, к которым дольше всего не было обращений.

• Информация об операционной системе, установленной на компьютере (тип; версия; разрядность). • Информация об установленном приложении и компьютере (уникальный идентификатор компьютера, на котором установлено приложение; уникальный идентификатор установки приложения на компьютере; название, локализация, идентификатор и полная версия установленного приложения; дата и время установки ПО). • Информация о проверяемых объектах (идентификатор баз приложения и идентификатор записи в базах приложения; название обнаруженной угрозы согласно классификации АО "Лаборатория Касперского"; контрольная сумма (MD5, SHA256); размер, название и тип проверяемого объекта; полный путь к проверяемому объекту; дата и время проверки объекта; IP-адрес пользователя; результат проверки файлов и URL-адресов; метаданные проверяемых объектов; проверяемый URL-адрес; заголовок Referrer; контрольная сумма проверяемого URL-адреса; контрольная сумма и размер пакера и контейнера проверяемого объекта; дата и время последнего установленного обновления баз; флаг, поясняющий, является ли обнаружение отладочным). • Информация о проверяемых сообщениях электронной почты (идентификатор сообщения; время получения сообщения; цель атаки (название организации, веб-сайт); весовой уровень атаки; значение уровня доверия; IP-адрес отправителя из SMTP-сессии; информация из заголовков сообщения; IP-адреса промежуточных почтовых агентов; данные из SMTP-сессии; использованные методы обнаружения; фрагмент DKIM-подписи сообщения; информация о результатах проверки подлинности отправителя сообщения; информация о подключениях к DNS-серверу; информация из сообщения для обнаружения спама; размер сообщения в байтах; размер вложения в байтах; контрольная сумма и тип вложения; размер темы письма в байтах; имя кодировки письма; информация о том, что сообщение находилось в Анти-Спам карантине; информация об html-разметке сообщения; контрольная сумма и размер MIME-партов).	Отправка KSN-статистики	KSN-серверы	До отправки статистики в KSN. После отключения отправки KSN-статистики в параметрах приложения данные удаляются при следующей попытке отправки.

Тип данных	Где используются данные	Место хранения	Срок хранения
• Информация о работе компонента Updater (версия компонента Updater; статус завершения задачи обновления компонента Updater; тип и идентификатор ошибки при обновлении компонента Updater в случае ее возникновения; код завершения задачи обновления компонента Updater; количество аварийных завершений работы компонента Updater при выполнении задач обновления за время работы этого компонента). • Информация об ошибках, возникших в работе компонентов ПО (информация о компонентах ПО, в работе которых произошла ошибка; идентификатор типа ошибки; фрагменты отчетов о работе компонентов). • Информация о версии пакета статистики, дате и времени начала получения статистики, дате и времени окончания получения статистики. • Информация о лицензии, по которой используется ПО (идентификатор лицензии, идентификатор партнера, у которого приобретена лицензия, серийный номер лицензионного ключа, дата и время добавления лицензионного ключа, признак принятия Положения о KSN).			

При обновлении баз приложения с серверов «Лаборатории Касперского» передается следующая информация:

- тип и версия приложения;
- уникальный идентификатор действующего лицензионного ключа;
- уникальный идентификатор установки приложения;
- идентификатор сессии обновления.

Добавление файла ключа

Рекомендуется активировать приложение с помощью кода активации (см. раздел "Добавление кода активации" на стр. 55).

► *Чтобы добавить файл ключа:*

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

2. Нажмите на кнопку **Добавить лицензионный ключ**.

   Откроется окно **Добавление лицензионного ключа**.

3. В раскрывающемся списке **Тип лицензионного ключа** выберите **Файл ключа**.
4. В блоке **Файл лицензионного ключа** нажмите на кнопку **Обзор**.

   Откроется окно выбора файла.

5. Выберите файл ключа, который вы хотите добавить, и нажмите на кнопку **Open**.
6. Нажмите на кнопку **Активировать**.

Файл ключа будет добавлен, приложение будет активировано. Вы можете проверить состояние лицензионного ключа (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 56) на узлах кластера.

Добавление кода активации

► *Чтобы добавить код активации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Общие → Лицензирование**.
2. Нажмите на кнопку **Добавить лицензионный ключ**.

   Откроется окно **Добавление лицензионного ключа**.

3. В раскрывающемся списке **Тип лицензионного ключа** выберите **Код активации**.
4. В поле **Код активации** введите код активации приложения в формате XXXXX-XXXXX-XXXXX-XXXXX, где X может быть буквами латинского алфавита (A-Z) или цифрами (0-9).
5. Нажмите на кнопку **Активировать**.

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

Если введенный код неверен, в рабочей области отобразится сообщение о том, что приложение не активировано. Вы можете повторить попытку ввода кода активации в этом же окне.

Если введенный код верен, отобразится сообщение об успешной активации приложения. Вы можете проверить состояние лицензионного ключа (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 56) на узлах кластера.

Вы также можете активировать приложение с помощью файла ключа (см. раздел "Добавление файла ключа" на стр. 54).

kaspersky

Удаление ключа

Если вы удалите лицензионный ключ, вы не сможете использовать приложение в режиме той функциональности, которую предусматривает ваша лицензия.

► *Чтобы удалить ключ:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. Нажмите на кнопку **Удалить лицензионный ключ**.
3. В окне подтверждения нажмите на кнопку **ОК**.

Лицензионный ключ будет удален на всех узлах кластера.

Мониторинг статуса лицензионного ключа

Чтобы отслеживать проблемы, связанные с лицензионным ключом, вы можете просматривать сводную информацию о состоянии лицензирования на всех узлах кластера на информационной панели **Лицензирование** в разделе **Узлы**.

Возможны следующие статусы лицензионного ключа:

- *Без ошибок* – добавлен действующий лицензионный ключ.
- *Предупреждения* – срок действия лицензионного ключа скоро истекает.

  Вы можете настроить, за сколько дней до истечения будет отображаться этот статус в параметрах лицензирования (см. раздел "Настройка предупреждений о скором истечении лицензионного ключа" на стр. 57).

- *Ошибки* – лицензионный ключ не добавлен или возникли ошибки лицензирования (например, истек срок действия ключа или ключ находится в списке запрещенных).

В правой части информационной панели указано количество узлов кластера по каждому статусу.

► *Чтобы просмотреть детальную информацию о состоянии лицензионного ключа на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Лицензирование** перейдите в раздел **Параметры** → **Лицензирование** → **Статус лицензионного ключа**.

В верхней части раздела отображается блок параметров с информацией о добавленном лицензионном ключе:

- Состояние лицензионного ключа (например, *Активный лицензионный ключ* или *Ключ в списке запрещенных*).
- **Тип лицензии** – тип лицензии (пробная или коммерческая).
- **Уровень функциональности** – режим работы приложения.

- **Серийный номер** – уникальная последовательность из латинских букв и цифр.
- **Приложение** – название приложения, для которого предназначен лицензионный ключ.

В нижней части раздела отображается таблица узлов кластера с информацией о статусе лицензионного ключа на каждом узле:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Статус лицензионного ключа** – подробное описание статуса лицензионного ключа на узле кластера.
- **Серийный номер** – уникальная последовательность из латинских букв и цифр.
- **Дата истечения** – дата и время, когда текущая лицензия перестанет действовать.

  Если вы используете коммерческий лицензионный ключ, то начиная с указанного времени приложение будет выполнять проверку сообщений на основе последних загруженных баз, но перестанет получать обновления баз. Если вы используете пробный лицензионный ключ, то с указанного времени функциональность приложения будет полностью отключена.

Таблица отображается при наличии у пользователя прав **Просматривать информацию об узлах** и/или **Создавать/изменять/удалять узлы**, а также **Просматривать параметры** и/или **Изменять параметры**.

Вы также можете просмотреть сведения о добавленном лицензионном ключе в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).

Настройка предупреждений о скором истечении лицензионного ключа

Вы можете настроить предупреждения о скором истечении лицензионного ключа в веб-интерфейсе приложения. Когда до истечения срока действия остается заданное количество дней, администратору отображается предупреждение в следующих разделах веб-интерфейса:

- в разделе **Узлы** на информационной панели **Лицензирование** (см. раздел "**Мониторинг статуса лицензионного ключа**" на стр. 56);
- в окне просмотра информации об узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138);
- в таблице о состоянии лицензионного ключа на узлах кластера (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 56) в разделе **Параметры → Лицензирование → Статус лицензионного ключа**.

► *Чтобы настроить предупреждения о скором истечении лицензионного ключа:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Лицензирование → Параметры**.
2. В поле **Предупреждать о скором истечении лицензионного ключа (в днях)** укажите, за сколько дней до истечения срока действия лицензионного ключа вы хотите получать предупреждение в веб-интерфейсе приложения.

Если вы хотите, чтобы предупреждения не отображались, установите значение 0.

Возможные значения – целые числа от 0 до 99. Значение по умолчанию – 30.

3. Нажмите на кнопку **Сохранить**.

Предупреждения о скором истечении лицензионного ключа будут настроены.

Приобретение лицензии

Kaspersky Security для Linux Mail Server входит в состав следующих комплексных решений "Лаборатории Касперского" для обеспечения безопасности и системного администрирования:

- Kaspersky TOTAL Security для бизнеса (http://www.kaspersky.ru/business-security/total).
- Kaspersky Security для почтовых серверов (http://www.kaspersky.ru/business-security/mail-server).

Для выбора комплексного решения, наиболее подходящего для вашей организации, проконсультируйтесь со специалистами компании-партнера "Лаборатории Касперского". Контактная информация и адреса партнеров представлены на сайте "Лаборатории Касперского" в разделе https://partnersearch.kaspersky.com https://partnersearch.kaspersky.com.

kaspersky

Установка приложения

Установка приложения состоит из следующих этапов:

1. **Подготовка к установке приложения (на стр. 60)**
2. **Установка пакета Kaspersky Security для Linux Mail Server (на стр. 63)**

   Запускать процесс установки пакета Kaspersky Security для Linux Mail Server требуется с правами учетной записи `root`.
3. **Установка пакета локализации Kaspersky Security для Linux Mail Server (на стр. 63)**

   Установка этого пакета требуется, если вам нужна русская локализация веб-интерфейса.

В этом разделе

kaspersky

Подготовка к установке приложения

Перед установкой пакета Kaspersky Security для Linux Mail Server выполните следующие действия:

1. Убедитесь, что сервер удовлетворяет аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 25).
2. С сайта "Лаборатории Касперского" или компании-партнера загрузите следующие файлы на сервер:
   - Пакет установки Kaspersky Security для Linux Mail Server в формате DEB.
   - Пакет локализации Kaspersky Security для Linux Mail Server в формате DEB.
   - Файл с ключом для работы в режиме замкнутой программной среды в формате GPG.
3. Удалите приложение Kaspersky Security для Linux Mail Server более ранней версии или версии 10 (см. раздел "Удаление приложения" на стр. 74), если такая версия уже была установлена.

   При удалении приложения необходимо учесть следующее:

   - Если при установке приложения вы выполняли ручную интеграцию почтового сервера Exim, необходимо вручную привести конфигурационные файлы почтового сервера в исходное состояние.
   - Если в предыдущей версии приложения использовалась интеграция с Kaspersky Security Center, необходимо удалить Агент администрирования предыдущей версии.
4. Проверьте, что в операционной системе установлена английская локаль, и при необходимости установите ее.
   a. Выполните команду:

      ```
      locale -a
      ```

   b. Проверьте, есть ли списке локаль en_US.UTF-8 или en_US.utf8.

      Если локаль уже установлена, дополнительных действий не требуется.

   c. Если локаль не установлена, выполните команду:

      ```
      dpkg-reconfigure locales
      ```

      Запустится интерактивный мастер.

   d. На первом шаге мастера выберите локаль en_US.UTF-8.

   e. Пройдите остальные шаги мастера.

      После завершения работы мастера локаль будет добавлена в операционную систему.

   f. Проверьте, что локаль была успешно добавлена, повторно вызвав команду:

      ```
      locale -a
      ```

5. Если вы хотите использовать СУБД PostgreSQL из состава операционной системы вместо СУБД, поставляемой в составе Kaspersky Security для Linux Mail Server, установите пакет postgresql из состава Astra Linux Special Edition.

   Для этого на сервере, на который вы планируете установить Kaspersky Security для Linux Mail Server, выполните команду:

   ```
   apt install postgresql
   ```

6. Установите и включите следующие модули Apache:

- headers;
- proxy;
- proxy_http;
- deflate;
- ssl;
- socache_shmcb.

Чтобы включить необходимые модули на операционных системах Astra Linux Special Edition 1.6 и 1.7:

a. Выполните команду:

```
a2enmod headers proxy proxy_http deflate ssl socache_shmcb
```

b. Перезапустите службу веб-сервера с помощью команды:

```
systemctl restart apache2
```

Kaspersky Security для Linux Mail Server работает в режиме отключенного AstraMode. Если для использования веб-сервисов, отличных от Kaspersky Security для Linux Mail Server, вам нужен Apache с режимом AstraMode, вы можете оставить включенным AstraMode в настройках Apache. Это не влияет на работоспособность Kaspersky Security для Linux Mail Server, Apache и веб-сервисов, работающих под управлением Apache.

7. При необходимости выполните команды по настройке Astra Linux Special Edition для установки Kaspersky Security для Linux Mail Server в режиме замкнутой программной среды (см. раздел "Подготовка к установке в Astra Linux Special Edition в режиме замкнутой программной среды" на стр. 62).
8. Если вы хотите, чтобы приложение Kaspersky Security для Linux Mail Server работало в режиме поддержки мандатного управления доступом, убедитесь, что режим мандатного управления доступом включен в настройках операционной системы.

   Если вы не планируете работать в режиме мандатного управления доступом, отключите этот режим в настройках операционной системы. Отключить режим мандатного управления доступом можно только в Astra Linux Special Edition 1.7.
9. Скрипт первоначальной настройки приложения автоматически ищет веб-сервер Apache на вашем компьютере. Чтобы обнаружение прошло успешно, убедитесь, что параметры веб-сервера соответствуют условиям, перечисленным в таблице ниже.

Таблица 4. Параметры веб-сервера Apache

Описание параметра	Условие обнаружения параметра
Имя сервиса Apache	В ответе утилиты systemctl cat есть одно из следующих имен: • httpd • apache2
Утилита для управления веб-сервером Apache	1. Утилита which с одной из следующих команд возвращает путь к исполняемому файлу: • httpd • apachectl 2. Не возникает ошибок при вызове исполняемого файла с каждой из следующих опций: • -S (показ конфигурационных опций) • -t (проверка синтаксиса конфигурационных файлов) • -M (показ доступных расширений)
Путь к директории с сайтами	В одной из следующих директорий есть директория sites-enabled или conf.d: • /etc/apache2/ • /etc/httpd/ • /etc/httpd/conf/
Пользователь, от имени которого запущен процесс Apache	В ответе утилиты <путь к исполняемому файлу, полученный в результате вызова `which httpd` или `which apachectl`> -S есть запись вида `User: name=<имя пользователя>`

Подготовка к установке в Astra Linux Special Edition в режиме замкнутой программной среды

Администратору требуется выполнить подготовительные действия для установки Kaspersky Security для Linux Mail Server в операционной системе Astra Linux Special Edition 1.6 или 1.7 в режиме замкнутой программной среды.

► *Чтобы установить Kaspersky Security для Linux Mail Server в режиме замкнутой программной среды:*

1. Создайте директорию для ключа Kaspersky Security для Linux Mail Server с помощью команды:

   ```
   mkdir -p /etc/digsig/keys/kaspersky/
   ```

2. Скопируйте файл kaspersky_klms_pub_key_339cc887.gpg из состава дистрибутива приложения в директорию, созданную на предыдущем шаге, с помощью команды:

   ```
   cp kaspersky_klms_pub_key_339cc887.gpg /etc/digsig/keys/kaspersky/
   ```

3. Обновите образ initramfs с помощью команды:

```
update-initramfs -u -k all
```

4. Перезагрузите сервер.

В результате приложение Kaspersky Security для Linux Mail Server может быть установлено в режиме замкнутой программной среды.

Установка пакета Kaspersky Security для Linux Mail Server

Kaspersky Security для Linux Mail Server распространяется в пакете формата DEB.

Запускать установку Kaspersky Security для Linux Mail Server требуется с правами учетной записи root.

► *Чтобы установить Kaspersky Security для Linux Mail Server, выполните следующую команду:*

```
dpkg -i klms_10.0.0-XXXX_amd64.deb
```

После установки приложения отобразится путь к скрипту настройки setup.py.

Установка пакета локализации Kaspersky Security для Linux Mail Server

Английская локализация включена в состав приложения. Для остальных языков требуется установка языкового пакета.

► *Чтобы установить пакет русской локализации из пакета формата DEB, выполните следующую команду:*

```
dpkg -i klms-l10n-ru_XXXX_all.deb
```

kaspersky

Подготовка приложения к работе

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

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

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

В этом разделе

Запуск первоначальной настройки вручную

Запускать процесс первоначальной настройки Kaspersky Security для Linux Mail Server требуется с правами учетной записи root.

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

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

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

Чтобы ввести значение по умолчанию, предложенное скриптом, нажмите на клавишу **ENTER**.

Чтобы просмотреть справку по функциям скрипта, используйте команду запуска скрипта первоначальной настройки с параметром `--help`.

Шаг 1. Выбор языка просмотра Лицензионного соглашения и Политики конфиденциальности

На этом шаге вы можете выбрать язык, на котором будут отображаться тексты Лицензионного соглашения и Политики конфиденциальности.

► *Чтобы выбрать язык:*

1. Введите номер нужного языка из предложенного списка.
2. Нажмите на клавишу **ENTER**.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге требуется принять или отклонить условия Лицензионного соглашения. Использовать приложение без принятия Лицензионного соглашения невозможно.

► *Чтобы просмотреть Лицензионное соглашение:*

1. Нажмите на клавишу **ENTER**.
2. Откроется текст Лицензионного соглашения. Для перемещения по тексту используйте клавиши управления курсором.
3. Нажмите на клавишу **Q** для выхода из режима просмотра.
4. Выполните одно из следующих действий:
   - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.
   - Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.
5. Нажмите на клавишу **ENTER**.

   Если вы отклонили условия Лицензионного соглашения, первоначальная настройка прерывается.

Вы можете в любой момент просмотреть текст Лицензионного сообщения в файле. Файл с текстом Лицензионного соглашения расположен по пути: /opt/kaspersky/klms/share/doc/LICENSE.<язык>.

Шаг 3. Просмотр Политики конфиденциальности

На этом шаге требуется принять или отклонить условия Политики конфиденциальности. Использовать приложение без принятия Политики конфиденциальности невозможно.

► *Чтобы просмотреть Политику конфиденциальности:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст Политики конфиденциальности. 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 Политики конфиденциальности, введите `yes`.
   - Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.
4. Нажмите на клавишу **ENTER**.

   Если вы отклонили условия Политики конфиденциальности, первоначальная настройка прерывается.

Вы можете в любой момент просмотреть текст Политики конфиденциальности в файле. Файл с текстом Политики конфиденциальности расположен по пути: opt/kaspersky/klms/share/doc/LICENSE_privacy_policy.<язык>.

kaspersky

Шаг 4. Выбор веб-сервера

На этом шаге вы можете выбрать веб-сервер для работы веб-интерфейса Kaspersky Security для Linux Mail Server из списка веб-серверов, автоматически обнаруженных в операционной системе.

► *Чтобы выбрать веб-сервер:*

1. Укажите номер нужного веб-сервера из списка.

   Если нужный веб-сервер не найден, введите цифру, соответствующую опции прерывания настройки **Abort setup**, исправьте проблему обнаружения веб-сервера (например, установите пакет веб-сервера) и запустите скрипт первоначальной настройки Kaspersky Security для Linux Mail Server заново (см. раздел "Запуск первоначальной настройки вручную" на стр. 64).
2. Нажмите на клавишу **ENTER**.
3. Проверьте параметры веб-сервера и подтвердите предложенную конфигурацию вводом цифры, соответствующей опции **Continue setup**.

   Если параметры веб-сервера определены неверно, введите цифру, соответствующую опции **Abort setup**, измените конфигурацию веб-сервера и повторно запустите скрипт первоначальной настройки Kaspersky Security для Linux Mail Server.

Шаг 5. Ввод параметров узла

На этом шаге вы можете указать IP-адрес узла, номер порта для межмашинного взаимодействия в кластере и номер порта, по которому будет доступен веб-интерфейс Kaspersky Security для Linux Mail Server.

Скрипт предлагает следующие номера портов по умолчанию: 9045 для межмашинного взаимодействия и 443 для веб-интерфейса. Если эти порты заняты, скрипт не будет предлагать значение по умолчанию, вам нужно вручную указать номера свободных портов.

Если вы хотите использовать значения по умолчанию, для каждого параметра нажмите на клавишу **ENTER**.

► *Чтобы указать параметры узла Kaspersky Security для Linux Mail Server:*

1. Укажите IP-адрес текущего узла и нажмите на клавишу **ENTER**.

   Этот IP-адрес будет использоваться для межмашинного взаимодействия в кластере.
2. Укажите номер порта текущего узла и нажмите на клавишу **ENTER**.

   Этот порт будет использоваться для межмашинного взаимодействия в кластере.
3. Укажите номер порта текущего узла для предоставления доступа к веб-интерфейсу Kaspersky Security для Linux Mail Server и нажмите на клавишу **ENTER**.

   Значение, отличное от номера порта по умолчанию, требуется, если веб-сервер используется для предоставления доступа к веб-интерфейсу разных систем, и стандартный порт уже занят.

Шаг 6. Выбор СУБД

На этом шаге вы можете выбрать, какую СУБД PostgreSQL будет использовать Kaspersky Security для Linux Mail Server: из пакета установки приложения или из состава операционной системы.

Использование СУБД PostreSQL из состава операционной системы может потребоваться для выполнения требований по сертификации. В таком случае вам необходимо предварительно установить пакет PostgreSQL (см. раздел "Подготовка к установке приложения" на стр. 60).

Если вы хотите использовать значения по умолчанию, для каждого параметра нажмите на клавишу **ENTER**.

► *Чтобы выбрать экземпляр СУБД PostgreSQL:*

1. Введите цифру, указанную рядом с нужным вариантом:
   - **INTERNAL** – использовать СУБД PostgreSQL из состава пакета приложения.

     Вариант по умолчанию.
   - **EXTERNAL** – использовать СУБД PostgresSQL из состава операционной системы.
2. Нажмите на клавишу **ENTER**.
3. Если вы выбрали вариант **EXTERNAL**, проверьте автоматически обнаруженные параметры СУБД:
   - Если все верно, подтвердите конфигурацию вводом цифры, соответствующей значению **Yes**.
   - Если обнаруженные параметры некорректны:
     a. Введите цифру, соответствующую опции **Change utility path**.
     b. Укажите путь к утилите psql и нажмите на клавишу **ENTER**.
     c. Укажите путь к утилите pg_ctl и нажмите на клавишу **ENTER**.
     d. Подтвердите конфигурацию.
   - Если параметры СУБД не удалось определить автоматически:
     a. Укажите путь к утилите psql и нажмите на клавишу **ENTER**.
     b. Укажите путь к утилите pg_ctl и нажмите на клавишу **ENTER**.
     c. Подтвердите конфигурацию.

Шаг 7. Выбор типа интеграции с почтовым сервером

Вы можете выполнить автоматическую или ручную before-queue-интеграцию Kaspersky Security для Linux Mail Server с Exim с использованием динамически подгружаемой библиотеки (dlfunc).

Интеграция с почтовым сервером вручную поддерживается только при работе в Astra Linux Special Edition 1.7 с выключенным режимом мандатного управления доступом.

Скрипт первоначальной настройки устанавливает пути к рабочим директориям в зависимости от значения параметра PrivateTmp в настройках systemd-сервиса Exim:

- Если PrivateTmp установлен в значение `true`, почтовые сообщения Kaspersky Security для Linux Mail Server будут сохраняться в директории /var/opt/kaspersky/klms/tmp/klms_filter.
- Если PrivateTmp установлен в значение `false` или не указан, почтовые сообщения Kaspersky Security для Linux Mail Server будут сохраняться в директории /tmp/klms_filter.

После выполнения интеграции изменение значения параметра PrivateTmp не допускается, так как это может нарушить нормальную работу почтового сервера.

► *Чтобы выполнить автоматическую интеграцию Kaspersky Security для Linux Mail Server с почтовым сервером:*

1. Введите цифру, указанную рядом с названием почтового сервера Exim.
2. Нажмите на клавишу **ENTER**.
3. Если вы хотите подтвердить выбранную конфигурацию почтового сервера, введите цифру, указанную рядом со значением **yes**.
4. Если вы хотите изменить параметры конфигурации почтового сервера, введите цифру, указанную рядом со значением **Change MTA**.

   Вы вернетесь к пункту 1 и сможете выбрать интеграцию вручную, чтобы указать нужные вам параметры конфигурации почтового сервера.

► *Чтобы выбрать ручную интеграцию Kaspersky Security для Linux Mail Server с почтовым сервером:*

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

В дальнейшем вы можете выполнить ручную интеграцию с почтовым сервером (см. раздел "Интеграция с почтовым сервером Exim вручную" на стр. 71).

В ходе автоматической интеграции будут созданы резервные копии конфигурационных файлов Exim вида *klms-install.backup. Вы можете найти резервные файлы конфигурации с помощью команды:
`find /etc/exim* -type f -name *klms-install.backup=`

Шаг 8. Поддержка режима мандатного управления доступом

Вы можете указать, требуется ли включить поддержку режима мандатного управления доступом в Kaspersky Security для Linux Mail Server. Этот шаг отображается, если на предыдущем шаге вы выбрали автоматическую интеграцию с Exim.

Поддержка режима мандатного управления доступом позволяет приложению Kaspersky Security для Linux Mail Server проверять почтовые сообщения с ненулевыми мандатными метками уровня и категории конфиденциальности в операционных системах Astra Linux Special Edition. Подробнее см. по ссылке https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362553.

Если в Astra Linux Special Edition 1.7 используется мандатное управление доступом, вам нужно включить поддержку режима мандатного управления доступом в Kaspersky Security для Linux Mail Server.

В Astra Linux Special Edition 1.6 всегда включен режим мандатного управления доступом. Поэтому для Astra Linux Special Edition 1.6 включение поддержки режима мандатного управления доступом на этом шаге обязательно.

► *Чтобы включить поддержку режима мандатного управления доступом:*

1. Введите значение `yes`.
2. Нажмите на клавишу **ENTER**.

Шаг 9. Назначение пароля доступа к веб-интерфейсу приложения

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

Пароль доступа к веб-интерфейсу Kaspersky Security для Linux Mail Server обязателен. Вы не сможете войти в веб-интерфейс приложения без пароля.

► *Чтобы задать пароль доступа к веб-интерфейсу:*

1. Укажите пароль учетной записи Administrator.

   Пароль должен содержать не менее 15 символов, а также удовлетворять следующим условиям:

   - Содержать хотя бы один символ верхнего регистра.
   - Содержать хотя бы один символ нижнего регистра.
   - Содержать хотя бы один специальный символ.
   - Содержать хотя бы одну цифру.
2. Нажмите на клавишу **ENTER**.
3. Подтвердите пароль.
4. Нажмите на клавишу **ENTER**.

   На этом первоначальная настройка приложения будет завершена.

После завершения настройки станет доступен веб-интерфейс Kaspersky Security для Linux Mail Server (см. раздел "Начало работы с приложением" на стр. 88).

Запуск первоначальной настройки в автоматическом режиме

Вы можете выполнять первоначальную настройку Kaspersky Security для Linux Mail Server в автоматическом режиме.

Сценарий выполнения первоначальной настройки в автоматическом режиме состоит из следующих этапов:

1. **Создание конфигурационного файла с ответами на вопросы скрипта первоначальной настройки**

   Для этого используется команда:

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

   Создание конфигурационного файла с ответами невозможно запустить на узле, на котором была выполнена первоначальная настройка вручную (см. раздел "Запуск первоначальной настройки вручную" на стр. 64).

2. **Изменение адреса настраиваемого узла**

   В конфигурационном файле с ответами записаны сетевые параметры того узла, на котором этот файл был создан (см. раздел "Шаг 5. Ввод параметров узла" на стр. 66). Чтобы настроить Kaspersky Security для Linux Mail Server на других узлах, вам нужно вручную в конфигурационном файле изменить IP-адрес текущего узла на значение IP-адреса настраиваемого узла. При необходимости нужно также изменить номера портов узла.

3. **Запуск настройки Kaspersky Security для Linux Mail Server в автоматическом режиме**

   Для этого используется команда:

   ```
   /opt/kaspersky/klms/bin/setup.py --auto-install=<полный путь к файлу с сохраненными параметрами>
   ```

   Если для учетной записи администратора вы хотите использовать пароль из переменной окружения ADMINISTRATOR_PASSWORD, выполните команду:

   ```
   /opt/kaspersky/klms/bin/setup.py --auto-install=<полный путь к файлу с сохраненными параметрами> --administrator-password-from-environment
   ```

kaspersky

Интеграция с почтовым сервером Exim вручную

Если во время первоначальной настройки приложения вы пропустили автоматическую интеграцию программы с почтовым сервером, вам требуется интегрировать приложение Kaspersky Security для Linux Mail Server с почтовым сервером вручную.

Вы можете настроить интеграцию с почтовым сервером вручную только при работе в Astra Linux Special Edition 1.7 с выключенным режимом мандатного управления доступом.

Вы можете вручную интегрировать Kaspersky Security для Linux Mail Server с почтовым сервером Exim методом «до передачи сообщения в очередь» (before-queue-интеграция) с использованием динамически подгружаемой библиотеки (dlfunc). В этом случае сообщения передаются на проверку приложению Kaspersky Security для Linux Mail Server до размещения в очереди почтового сервера Exim.

В зависимости от дистрибутива операционной системы вам требуется внести изменения в один или несколько конфигурационных файлов почтового сервера Exim. В Astra Linux Special Edition версии 1.6 и 1.7 почтовый сервер Exim может быть настроен как с помощью нескольких файлов в подкаталогах /etc/exim4/conf.d, так и с помощью одного файла.

► *Чтобы выполнить before-queue-интеграцию Kaspersky Security для Linux Mail Server с Exim:*

1. Убедитесь, что почтовый сервер Exim поддерживает функции динамически загружаемой библиотеки 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 другая переменная или макрос)

   и после строки вида

   `acl_check_data:` (или строки, содержащей другую переменную или макрос)

   добавьте следующие строки:

```
# Manual klms-exim-filter-dlfunc begin
#
warn    set acl_m_klms_input_directory = ${spool_directory}/input
            set acl_m_klms_lookup_result = ${lookup {$message_id-D}
dsearch {$acl_m_klms_input_directory}}
warn    condition       = ${if eq
{$acl_m_klms_lookup_result}{}{yes}{no}}
            # A split_spool_directory option is set
            set acl_m_klms_input_directory =
```

```
${spool_directory}/input/${substr{5}{1}{$message_id}}
warn    set acl_m_klms_answer =
${dlfunc{DLFUNC_LIBRARY_FULLPATH}{scan}{$acl_m_klms_input_directory}}
defer   condition       = ${if eq {$acl_m_klms_answer}{}{yes}{no}}
            log_message     = KLMS check failed (empty answer)
            message         = Temporary local problem - please try
later
warn    set acl_m_klms_result_code = ${if match
{$acl_m_klms_answer}{\N^([0-9]{3}) .*\N}{$1}{}}
            set acl_m_klms_result_message = ${if match
{$acl_m_klms_answer}{\N^[0-9]{3} (.*)\N}{$1}{}}
            # Anything except details in brackets
            set acl_m_klms_result_short_message = ${if match
{$acl_m_klms_result_message}{\N^([^\(]+)( \(.+\))?$\N}{$1}{}}
defer   condition       = ${if match
{$acl_m_klms_result_code}{^[245]}{no}{yes}}
            log_message     = KLMS check failed,  unexpected answer:
$acl_m_klms_answer
            message         = Temporary local problem - please try
later
defer   condition       = ${if eq
{${substr_0_1:$acl_m_klms_result_code}}{4}{yes}{no}}
            log_message     = KLMS check defer: $acl_m_klms_answer
            message         = $acl_m_klms_result_code
$acl_m_klms_result_short_message
deny    condition       = ${if eq
{${substr_0_1:$acl_m_klms_result_code}}{5}{yes}{no}}
            log_message     = KLMS check reject: $acl_m_klms_answer
            message         = $acl_m_klms_result_code
$acl_m_klms_result_short_message
warn    condition       = ${if eq
{${substr_0_1:$acl_m_klms_result_code}}{2}{yes}{no}}
            logwrite        = KLMS check accept: $acl_m_klms_answer
#
# Manual klms-exim-filter-dlfunc ends here
```

где DLFUNC_LIBRARY_FULLPATH – путь к библиотеке dlfunc. Если используется exim daemon heavy из состава ОС Astra Linux Special Edition, путь выглядит следующим образом:

- для Exim с версии 4.96 до версии 5.0 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi60.so
- для Exim с версии 4.94 до версии 4.96 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi41.so
- для Exim с версии 4.93 до версии 4.94 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi31.so
- для Exim с версии 4.90 до версии 4.93 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi20-2.so
- для Exim с версии 4.86 до версии 4.90 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi20-1.so

- для Exim с версии 4.64 до версии 4.86 невключительно – /opt/kaspersky/klms/lib/libklms-exim-abi11.so

4. После завершения правок конфигурационного файла при необходимости перегенерируйте основной файл конфигурации Exim.
5. Добавьте пользователя `kluser` к группе, в которую входит пользователь, от имени которого запускается процесс `exim`.

   В Astra Linux Special Edition 1.6 и 1.7 по умолчанию такой группой является `Debian-exim`.
6. Добавьте пользователя, от имени которого запускается процесс exim, к группам `klusers` и `kl_var_users`.

   В Astra Linux Special Edition 1.6 и 1.7 по умолчанию таким пользователем является `Debian-exim`.
7. В файле параметров фильтров /etc/opt/kaspersky/klms/filters.conf в секции `[global]` установите следующие значения параметров:

   ```
   scanner=unix:/var/run/klms/klms_scanner_sock
   header-guard=false
   ```

   - Если в Unit-файле Exim параметр `PrivateTmp` установлен в `false` или не указан:

     ```
     workdir=/tmp
     ```

   - Если в Unit-файле Exim параметр `PrivateTmp` установлен в `true`:

     ```
     workdir=/var/opt/kaspersky/klms/tmp
     ```
8. Откройте файл /var/opt/kaspersky/klms/installer.dat
9. Добавьте в файл следующие строки:

   ```
   MTA_INTEGRATION_METHOD=dlfunc
   MTA_INTEGRATION_MODE=prequeue
   filters_workdir=<значение в зависимости от условий в п. 7>
   mta=manual
   START_SMTP_PROXY=0
   START_MILTER=0
   ```
10. Перезапустите службу klms.
11. Перезапустите почтовый сервер Exim.

Интеграция с Exim будет завершена.

kaspersky

Удаление приложения

Узел с удаляемым приложением должен быть предварительно удален из кластера (см. раздел "Удаление узла из кластера" на стр. 141).

Вы можете удалить приложение Kaspersky Security для Linux Mail Server полностью или частично.

Полное удаление

При полном удалении приложения с сервера удаляются все файлы и директории. Системные пользователи и группы не удаляются.

► *Чтобы удалить приложение полностью:*

1. Выполните команды:

   ```
   dpkg -r klms-l10n-ru
   dpkg -r klms
   ```

2. Запустите скрипт для удаления данных приложения с помощью команды:

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

3. Введите `yes`, чтобы подтвердить удаление данных, оставшихся после удаления Kaspersky Security для Linux Mail Server.
4. После завершения работы скрипта выполните команду:

   ```
   dpkg -P klms
   ```

Данные приложения будут удалены с сервера.

Частичное удаление

При частичном удалении на сервере останутся данные, созданные и используемые приложением для работы, а также системные пользователи и группы.

Частичное удаление Kaspersky Security для Linux Mail Server может быть полезно использовать, если в дальнейшем потребуется вновь установить Kaspersky Security для Linux Mail Server. В таком случае Kaspersky Security для Linux Mail Server в процессе настройки обнаружит и восстановит следующие данные:

- правила обработки сообщений;
- параметры работы приложения;
- содержимое Хранилища;
- содержимое Карантина;
- журналы событий.

► *Чтобы удалить приложение частично, выполните команды:*

```
dpkg -r klms-l10n-ru
dpkg -r klms
```

Если потребуется, вы можете позже удалить все файлы и директории, оставшиеся после удаления приложения, с помощью скрипта cleanup.sh. Скрипт поставляется в составе пакета установки Kaspersky Security для Linux Mail Server.

Удаление данных приложения с помощью скрипта

После частичного удаления Kaspersky Security для Linux Mail Server на сервере остаются данные, такие как база данных параметров работы приложения, сообщения в Хранилище, служебные исполняемые файлы, файлы man-страниц (справочных страниц), обновления баз, созданные отчеты, файлы журналов приложения, сокеты, созданные и используемые приложением для работы.

► *Чтобы удалить данные, оставшиеся после частичного удаления приложения:*

1. Выполните команду:

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

2. Введите `yes`, чтобы подтвердить удаление данных, оставшихся после удаления Kaspersky Security для Linux Mail Server.
3. После завершения работы скрипта выполните команду:

   `dpkg -P klms`

Данные приложения будут удалены с сервера.

kaspersky

Обновление приложения до версии 10

Возможны следующие варианты обновления приложения до версии 10:

- Установка на новый сервер (см. раздел "Обновление с установкой приложения на новый сервер" на стр. 76)

  Установка на новый сервер является рекомендуемым вариантом миграции.

  В этом варианте необходимо подготовить новый почтовый сервер, установить на него новую версию приложения Kaspersky Security для Linux Mail Server, после чего постепенно перенести на этот сервер функции обработки почтового трафика. Сервер с предыдущей версией приложения необходимо сохранять в работоспособном состоянии до тех пор, пока требуется доступ к данным, которые на нем хранились: содержимому Хранилища, карантинов, журналу аудита, отчетам.

- Установка на существующий сервер (см. раздел "Обновление с установкой приложения на существующий сервер" на стр. 77)

  В этом варианте требуется сохранить параметры работы и данные предыдущей версии приложения Kaspersky Security для Linux Mail Server. После этого приложение нужно будет удалить, так как установка новой версии приложения поверх предыдущей невозможна. Затем необходимо установить и настроить новую версию приложения, после чего восстановить функции обработки почтового трафика на этом сервере.

В этом разделе

Обновление с установкой приложения на новый сервер

► *Чтобы обновить приложение Kaspersky Security для Linux Mail Server с установкой на новый сервер:*

1. Установите и настройте почтовый сервер Exim для выполнения функций маршрутизации почтового трафика.

   Используйте те же параметры настройки Exim, что на сервере, с которого осуществляется миграция.

2. Сохраните параметры работы и данные предыдущей версии приложения Kaspersky Security для Linux Mail Server с сервера, с которого осуществляется миграция.

3. Выполните шаги установки новой версии приложения (см. раздел "Порядок установки новой версии приложения" на стр. 77).

Обновление с установкой приложения на существующий сервер

Условия, при которых возможна установка новой версии приложения на существующий почтовый сервер:

- Сервер соответствует аппаратным требованиям новой версии приложения (см. раздел "Аппаратные и программные требования" на стр. 25): количество ядер процессора, размер оперативной памяти, свободное место на диске.
- Сервер соответствует программным требованиям новой версии приложения: тип и версия операционной системы, тип и версия MTA.
- На этом сервере можно прервать обработку почтового трафика на период установки и настройки новой версии приложения.
- Не требуется сохранять доступ к данным предыдущей версии приложения: содержимому Хранилища, карантинов, журналу событий, отчетам. Эти данные будут удалены.

► *Чтобы установить Kaspersky Security для Linux Mail Server на существующий сервер:*

1. Выведите сервер из обработки почтового трафика, например, перераспределив нагрузку на другие серверы.
2. Сохраните параметры и данные предыдущей версии приложения Kaspersky Security для Linux Mail Server, установленной на этом сервере (см. раздел "Миграция параметров из более старой версии" на стр. 265).
3. Удалите предыдущую версию приложения Kaspersky Security для Linux Mail Server.
4. Удалите параметры интеграции с предыдущей версией приложения из конфигурационных файлов почтового сервера и веб-сервера.
5. Выполните шаги установки новой версии приложения (см. раздел "Порядок установки новой версии приложения" на стр. 77).

Порядок установки новой версии приложения

► *Чтобы установить новую версию приложения:*

1. Установите пакеты дополнительного программного обеспечения согласно программным требованиям приложения Kaspersky Security для Linux Mail Server.
2. Установите ключи для работы приложения и Агента администрирования в режиме замкнутой программной среды, если планируется работа операционной системы в этом режиме.
3. Если требуется интеграция с Kaspersky Security Center, установите Агент администрирования.
4. Установите пакеты новой версии приложения и выполните первоначальную настройку приложения (см. раздел "Подготовка приложения к работе" на стр. 64).
5. Выполните настройку приложения в зависимости от роли узла кластера:

- Управляющий узел кластера (устанавливается и настраивается первым).

  Авторизуйтесь в веб-интерфейсе под учетной записью администратора, создайте кластер и выполните настройку приложения (см. раздел "Порядок настройки приложения" на стр. 92).

- Подчиненный узел кластера (второй и последующие узлы).

  Добавьте узел в кластер, используя веб-интерфейс Управляющего узла. Параметры приложения будут автоматически синхронизированы на Подчиненный узел.

6. Для применения обновлений баз перезагрузите операционную систему.
7. Настройте службы операционной системы для работы с приложением:
   - Служба системных журналов (rsyslog) – параметры хранения и ротации журналов приложения, параметры экспорта событий во внешнюю SIEM-систему.
   - Служба SNMP-сервера (snmpd) – для взаимодействия с внешней системой мониторинга по протоколу SNMP (см. раздел "Работа с приложением по протоколу SNMP_VerticalLayout" на стр. 289).
   - Служба локального балансировщика (haproxy) – если требуется взаимодействие с серверами KATA по отказоустойчивой схеме (см. раздел "Защита KATA" на стр. 277).
8. Отправьте тестовые сообщения, чтобы проверить работу почтового сервера.
9. Введите почтовый сервер в обработку почтового трафика.

Экспорт параметров из Kaspersky Security 8 для Linux Mail Server

► *Чтобы сохранить параметры при наличии веб-интерфейса:*

1. Экспортируйте правила и пользовательские списки в файл.
2. Для сохранения информации о прочих параметрах приложения снимите скриншоты соответствующих разделов веб-интерфейса или выпишите значения настроек в текстовый файл.
3. При необходимости сохраните сообщения из Хранилища (см. раздел "Скачивание сообщения из Хранилища" на стр. 197).

► *Чтобы сохранить параметры без веб-интерфейса:*

1. Для экспорта правил и пользовательских списков выполните команду:

   ```
   /opt/kaspersky/klms/bin/klms-control --export-all-settings KLMS_settings.kz
   ```

2. Для сохранения информации о прочих параметрах выполните команду:

   ```
   /opt/kaspersky/klms/bin/klms-control --export-settings --file settings.xml
   ```

   Информация из полученного файла settings.xml не может быть импортирована в новую версию приложения, требуется настройка всех параметров вручную.

3. При необходимости сохраните сообщения из Хранилища, используя функцию утилиты klms-control.

kaspersky

Категории данных для миграции

Параметры, которые могут быть перенесены с помощью процедуры экспорта и импорта данных:

- Правила обработки почтового трафика.
- Шаблоны уведомлений об обнаружениях.
- Тексты предупреждений и примечаний, используемые в правилах.
- Пользовательские списки разрешенных и запрещенных адресов.

Параметры, которые не могут быть перенесены автоматически, их потребуется указать заново через веб-интерфейс:

- Данные лицензии (код активации или ключ).
- Параметры подключения к прокси-серверу.
- Параметры обновления баз.
- Параметры защиты.
- Параметры Хранилища.
- Параметры взаимодействия с KSN.
- Параметры подключения к серверам KATA.
- Параметры подключения к LDAP-серверам.
- Параметры административных ролей и пользователей.
- Параметры прав доступа для персональных пользователей.
- Параметры дайджеста персонального Хранилища.
- Параметры журнала аудита, журналов Syslog и SIEM.
- Параметры мониторинга по протоколу SNMP.
- Параметры уведомлений о сбоях в работе приложения.
- Параметры отправки отчетов со статистикой работы приложения.

Данные, которые не могут быть перенесены в новую версию приложения:

- Содержимое Хранилища (копии почтовых сообщений).
- Содержимое карантинов.
- Записи журнала событий.
- Отчеты со статистикой работы приложения.

Известные ограничения Kaspersky Security для Linux Mail Server

В таблице ниже приведены ограничения версии 10.0 по сравнению с версией 8.0 MR3, которые необходимо учитывать перед тем, как начинать миграцию.

Таблица 5. Ограничения версии 10.0

Ограничение	Комментарии
Повышены минимальные аппаратные требования.	Минимальные требования: 8 ядер процессора, 16 ГБ памяти, 200 ГБ свободного места на диске.
Ограничен список поддерживаемых операционных систем.	Поддерживается работа только на следующих операционных системах: • Astra Linux Special Edition 1.6 (оперативное обновление 12 и выше) • Astra Linux Special Edition 1.7 (оперативное обновление 3 и выше) Работа на других операционных системах не поддерживается.
Ограничен список поддерживаемых MTA и способов интеграции.	Поддерживается интеграция только с почтовым сервером Exim и только методом before-queue с использованием динамически подгружаемой библиотеки. Интеграция методом after-queue не поддерживается.
Не поддерживается управление приложением через командную строку.	Управление работой приложения осуществляется только через веб-интерфейс. Утилита klms-control может быть использована только для просмотра текущих параметров настройки, но не для их изменения.
Ограничена функциональность интеграции с Kaspersky Security Center.	Поддерживается только обновление баз из репозитория, не поддерживается добавление лицензионного ключа и мониторинг, не предусмотрен плагин для управления приложением. Невозможно изменить название кластера. Для добавления данных лицензии и мониторинга работы нужно использовать веб-интерфейс приложения.
Не поддерживается добавление резервного лицензионного ключа.	Для замены недействительного лицензионного ключа необходимо удалить действующий лицензионный ключ, затем добавить новый.
Не поддерживается база данных для Хранилища на внешнем сервере.	База данных Хранилища может располагаться только на том же сервере, где установлено приложение.
Не поддерживается хранение объектов Хранилища в локальной или сетевой папке.	Изменился способ хранения объектов Хранилища – теперь они хранятся в базе данных, а не в файловой системе.

Не поддерживается интеграция со службами каталогов, отличными от Microsoft Active Directory.	Службы каталогов, использующие схему, отличную от Microsoft Active Directory, (например, OpenLDAP) не поддерживаются. Обязательно использование аутентификации по протоколу Kerberos с созданием keytab-файлов.
Не поддерживается использование протокола LDAPS и механизма STARTTLS для интеграции со службой каталогов.	Для интеграции со службой каталогов необходимо обеспечить возможность подключения по протоколу LDAP (порт 389). Для шифрования передаваемых данных используется механизм SASL.
Не поддерживается непосредственное указание адреса сервера и порта для подключения к службе каталогов по протоколу LDAP.	Приложение получает адреса серверов и номера портов для подключения к службе каталогов по протоколу LDAP из соответствующих SRV-записей на DNS-сервере.
Не поддерживается указание пользовательских списков SURBL и DNSBL в модуле Анти-Спам.	Для фильтрации по SURBL- и DNSBL-спискам можно использовать встроенные функции почтового сервера Exim.
Невозможно отключить добавление информационных X-заголовков	Приложение всегда добавляет X-заголовки в проверенные письма, эту функцию невозможно отключить.
Не поддерживается настройка шаблона для уведомления о доставке сообщения из Хранилища в виде вложения, замещающего текста для удаленного вложения, шаблона отчета о недоставленном сообщении.	Приложение использует предустановленные шаблоны на английском языке, их редактирование не предусмотрено.
Нет почтовых уведомлений о достижении порогового значения заполненности Хранилища, об истечении срока действия лицензии.	Мониторинг заполненности Хранилища и срока действия лицензии можно осуществлять по протоколу SNMP.

Действия в случае ошибочного обновления приложения

Установка Kaspersky Security для Linux Mail Server на компьютер с уже установленным Kaspersky Security 8 для Linux Mail Server не поддерживается. Если администратор попытается выполнить такую установку, это приведет к потере работоспособности Kaspersky Security 8 для Linux Mail Server.

Если вам нужно установить Kaspersky Security для Linux Mail Server, сначала нужно полностью удалить Kaspersky Security 8 для Linux Mail Server, а затем установить Kaspersky Security для Linux Mail Server (см. раздел "Установка пакета Kaspersky Security для Linux Mail Server" на стр. 63).

► *Чтобы восстановить работоспособность Kaspersky Security 8 для Linux Mail Server после ошибочного обновления приложения:*

1. Определите состояние пакета Kaspersky Security 8 для Linux Mail Server с помощью команды:

   ```
   dpkg -s klms
   ```

2. В зависимости от значения поля **Status** выполните следующие действия:

   - Если в поле **Status** отображается `install ok installed`:

     a. Выполните следующие команды:

     ```
     update-rc.d klms defaults
     update-rc.d klmsdb defaults
     systemctl restart klmsdb
     systemctl restart klms
     ```

     b. Перезагрузите сервер.

   - Если в поле **Status** отображается `deinstall ok config-files`, приложение Kaspersky Security 8 для Linux Mail Server было частично удалено, остались только данные приложения.

     При необходимости вы можете установить Kaspersky Security 8 для Linux Mail Server. Новый экземпляр приложения будет использовать оставшиеся данные.

kaspersky

Процедура приемки

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

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

В этом разделе

Безопасное состояние приложения

Приложение находится в безопасном состоянии (сертифицированной конфигурации), если параметры приложения находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. стр. 391).

Проверка работоспособности

Перед началом проверки убедитесь, что выполнены следующие условия:

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

Проверка антивирусной защиты сообщений с использованием тестового файла EICAR

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

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

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: https://www.eicar.org/download-anti-malware-testfile/.
2. Сохраните тестовый файл EICAR.
3. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Security для Linux Mail Server.

4. Получите почтовое сообщение и проверьте вложения.

   Kaspersky Security для Linux Mail Server сообщит вам об обнаружении угрозы и удалит из сообщения зараженный объект.

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

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: https://www.eicar.org/download-anti-malware-testfile/.
2. Сохраните тестовый файл EICAR.
3. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.
4. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.
5. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Security для Linux Mail Server.
6. Получите почтовое сообщение и проверьте вложения.

   Kaspersky Security для Linux Mail Server сообщит вам об обнаружении угрозы и удалит из сообщения зараженный объект.

Проверка работоспособности модуля Анти-Спам

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

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

► *Чтобы проверить работоспособность модуля Анти-Спам:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Спам**.
3. Включите модуль Анти-Спам с помощью переключателя **Использовать Анти-Спам**.
4. В левой панели выберите раздел **Правила**.
5. Выберите правило, которое вы хотите использовать для проверки работоспособности модуля Анти-Спам.

   Откроется окно **Просмотреть правило**.
6. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
7. В левой панели выберите раздел **Анти-Спам**.
8. Включите проверку модулем Анти-Спам сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.
9. В блоке параметров **Если обнаружен спам** установите флажок **Поместить сообщение в Хранилище**.

10. Запустите утилиту SwithMail.
11. Укажите адрес отправителя, назначения, а также адрес программы.
12. Откройте закладку Email Content.
13. В поле Email Subject введите gtube.
14. В поле Email Body введите строку GTUBE.
15. Нажмите на кнопку Test Settings.

    Тестовое спам-сообщение будет отправлено.
16. Перейдите в почтовый ящик пользователя, адрес электронной почты которого вы указали в качестве адреса назначения.
17. Убедитесь, что отправленное вами письмо было доставлено с меткой *[Spam]*.
18. В окне веб-интерфейса программы выберите раздел **Хранилище**.
19. Убедитесь, что в таблице объектов Хранилища появилась запись об отправленном тестовом спам-сообщении.

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

kaspersky

Интерфейс Kaspersky Security для Linux Mail Server

Работа с Kaspersky Security 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 приложения;
- рабочую область в правой части главного окна веб-интерфейса приложения.

Дерево консоли управления Kaspersky Security для Linux Mail Server

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

- **Мониторинг**. Содержит графики и информационные панели, позволяющие отслеживать работу приложения.
- **Правила**. Позволяет создавать и настраивать правила обработки сообщений.
- **Пользовательские списки**. Позволяет создавать и настраивать персональные пользовательские списки разрешенных и запрещенных адресов.
- **Узлы**. Позволяет управлять узлами кластера.
- **События**. Содержит информацию о событиях, обнаруженных в почтовом трафике, а также о событиях приложения.
- **Хранилище**. Содержит информацию о сообщениях, которых были помещены в Хранилище по результатам проверки модулями приложения, а также фильтр поиска сообщений в Хранилище.
- **Очередь сообщений**. Содержит информацию об Анти-Спам карантине и KATA-карантине (при настроенной интеграции с KATA), а также фильтр поиска сообщений.
- **Отчеты**. Позволяет формировать отчеты о работе приложения, а также отправлять их по электронной почте.
- **Учетные записи и роли**. Содержит информацию об учетных записях пользователей приложения и их разрешениях.
- **Параметры**. Содержит разделы **Общие**, **Персональные учетные записи**, **Внешние службы**, **Журналы и события**, **Мониторинг**, **Доступ к приложению**, в которых вы можете настраивать параметры приложения.

Рабочая область окна веб-интерфейса Kaspersky Security 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 приложения.

Для разделов, предусматривающих работу с параметрами Kaspersky Security для Linux Mail Server, в рабочей области главного окна параметры сгруппированы в блоки параметров.

kaspersky

Начало работы с приложением

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

Администратору Kaspersky Security для Linux Mail Server требуется самостоятельно обеспечить защиту передачи данных между браузером и Управляющим узлом. Для обеспечения безопасности также рекомендуется настроить Kerberos-аутентификацию с использованием технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 333).

Чтобы управлять параметрами приложения, вам требуется подключиться к Управляющему узлу. При подключении к Подчиненным узлам вам доступно изменение роли узла в кластере (на стр. 142) и просмотр состояния других подключенных серверов.

В этом разделе

Режимы просмотра веб-интерфейса приложения

В приложении доступно два режима просмотра веб-интерфейса:

- Режим персонального пользователя.

  Режим персонального пользователя доступен всем пользователям домена Active Directory, для которого настроена аутентификация с помощью технологии единого входа (SSO) (см. раздел "Аутентификация с помощью технологии единого входа" на стр. 330).

  Персональные пользователи могут просматривать персональное Хранилище и персональные списки разрешенных и запрещенных адресов, если доступ к этим разделам разрешен администратором в параметрах **Параметры** → **Персональные учетные записи**. Персональным пользователям доступна информация только о своих сообщениях и адресах.

  Для просмотра этой информации требуется настроить интеграцию с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 270). Иначе пользователю будут доступны разделы, но вместо информации о сообщениях и адресах будет отображаться сообщение об ошибке.

- Режим привилегированного пользователя.

  Режим привилегированного пользователя доступен пользователям приложения, для которых создана учетная запись (см. раздел "Создание учетной записи" на стр. 158) и назначена хотя бы одна роль (см. раздел "Назначение роли" на стр. 173). Привилегированный пользователь может авторизоваться с помощью SSO или используя локальную учетную запись. Привилегированным

пользователям доступны те разделы приложения, на которые у пользователей есть разрешения в соответствии с типовыми задачами и служебными обязанностями.

Если пользователю с SSO-аутентификацией назначена роль в приложении, по умолчанию после входа приложение открывается в режиме привилегированного пользователя. При необходимости вы можете переключиться в режим персонального пользователя для текущей учетной записи (см. раздел "Изменение режима просмотра веб-интерфейса" на стр. 91).

Время бездействия в режиме привилегированного пользователя ограничено 10 минутами. За минуту до окончания этого времени появляется предупреждение о скором завершении сессии. Пользователь может продлить текущую сессию или выйти из приложения. Если никаких действий не предпринято, текущая сессия будет прервана после истечения времени ожидания, отобразится страница авторизации веб-интерфейса.

Подключение к веб-интерфейсу приложения

Если вы подключаетесь к веб-интерфейсу впервые после установки приложения, перед началом работы вам потребуется создать новый кластер (см. раздел "Создание нового кластера" на стр. 136).

В зависимости от учетной записи, под которой вы подключаетесь к веб-интерфейсу, вам будут доступны для просмотра и изменения разные параметры приложения:

- Локальные учетные записи (см. раздел "Работа с учетными записями и ролями пользователей" на стр. 158) привилегированных пользователей имеют набор разрешений, определенный их ролями. Учетная запись привилегированного пользователя Administrator, созданная во время установки приложения, имеет полный набор разрешений.
- Пользователи с доменной учетной записью могут подключаться к веб-интерфейсу в режиме привилегированного пользователя или в режиме персонального пользователя и просматривать разделы в соответствии с заданными в приложении разрешениями.

► *Чтобы подключиться к веб-интерфейсу приложения под локальной учетной записью привилегированного пользователя:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или полное доменное имя (FQDN) Управляющего сервера>:<порт подключения к веб-интерфейсу>`

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

   В поле **Имя пользователя** введите имя учетной записи, например `Administrator`.

2. В поле **Пароль** введите пароль учетной записи.

   Пароль учетной записи Administrator задается во время первоначальной настройки приложения.

   Если вы введете неверный пароль пять раз, возможность авторизации под учетной записью привилегированного пользователя будет заблокирована на пять минут. Возможность авторизации под доменной учетной записью по протоколу NTLM останется доступной.

3. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса приложения.

► *Чтобы подключиться к веб-интерфейсу приложения под учетной записью пользователя с SSO-аутентификацией,*

в браузере введите следующий адрес:

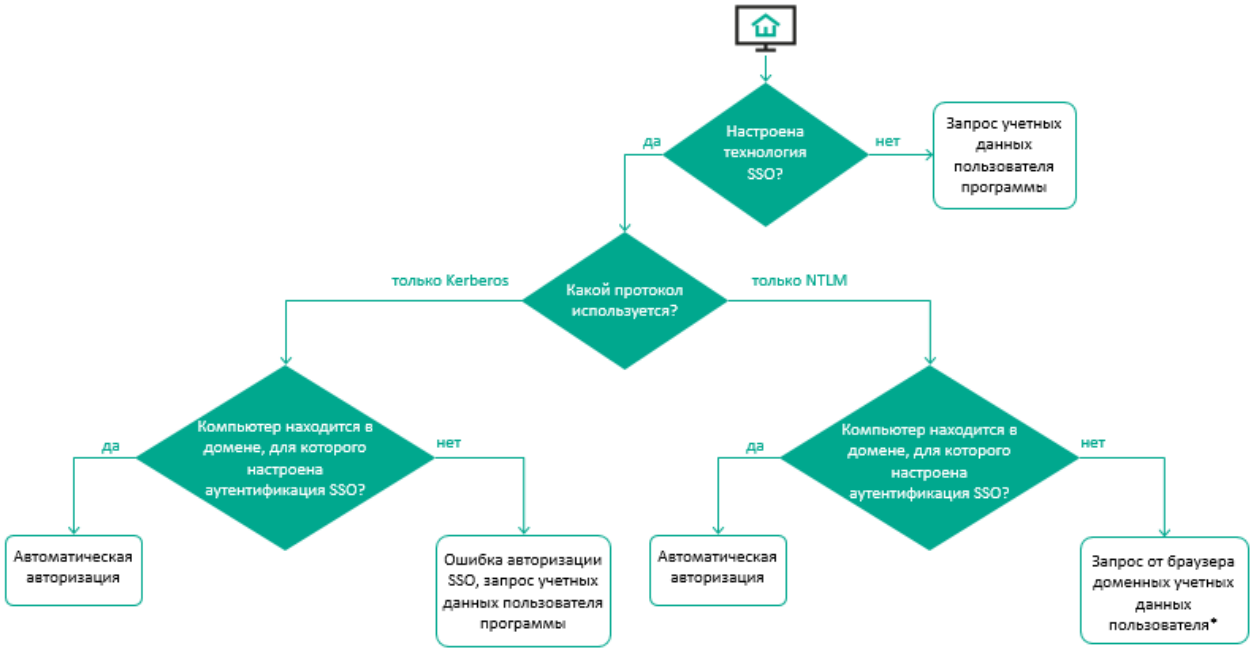
```
https://<IP-адрес или полное доменное имя (FQDN) Управляющего
сервера>:<порт подключения к веб-интерфейсу>
```

Если вы настроили аутентификацию с помощью технологии единого входа по протоколу Kerberos, требуется вводить адрес только в формате FQDN.

Дальнейшая процедура авторизации зависит от следующих факторов:

- какой протокол используется для аутентификации;
- находится ли компьютер в домене Active Directory, для которого настроена аутентификация SSO.

Алгоритм авторизации в зависимости от перечисленных факторов представлен на рисунке ниже.



* Если при запросе от браузера доменных учетных данных пользователя вы введете неверный пароль пять раз, возможность NTLM-аутентификации будет заблокирована на пять минут. Возможность авторизации под учетной записью привилегированного пользователя останется доступной.

Если в приложении настроено одновременное использование Kerberos- и NTLM-аутентификации, то процедура авторизации будет выглядеть следующим образом:

1. Попытка авторизации по протоколу Kerberos.
2. В случае неудачи попытка авторизации по протоколу NTLM.
3. В случае неудачи запрос на ввод учетных данных пользователя приложения.

Для корректной работы автоматической авторизации на компьютерах, входящих в домен Active Directory, для которого настроена аутентификация с помощью технологии SSO, требуется провести дополнительную настройку (см. раздел "Дополнительная настройка в операционной системе и браузере" на стр. 335) в операционной системе и в свойствах браузера.

В результате успешной авторизации откроется главное окно веб-интерфейса приложения. Если пользователю с SSO-аутентификацией в соответствии с его правами доступны разные режимы просмотра веб-интерфейса, он сможет переключаться между ними (см. раздел "Изменение режима просмотра веб-интерфейса" на стр. 91).

Изменение режима просмотра веб-интерфейса

Режим персонального пользователя доступен только для пользователей, которые используют SSO-аутентификацию для входа в Kaspersky Security для Linux Mail Server.

► *Чтобы перейти из режима привилегированного пользователя в режим персонального пользователя:*

1. Внизу левой панели меню нажмите на имя текущего пользователя.
2. В раскрывшейся справа панели включите переключатель **Персональный пользователь**.

Откроется главное окно веб-интерфейса приложения в режиме персонального пользователя для текущей учетной записи.

► *Чтобы перейти из режима персонального пользователя в режим привилегированного пользователя:*

1. Внизу левой панели меню нажмите на имя текущего пользователя.
2. В раскрывшейся справа панели выключите переключатель **Персональный пользователь**.

Откроется главное окно веб-интерфейса приложения в режиме привилегированного пользователя для текущей учетной записи.

► *Чтобы выйти из учетной записи с SSO-аутентификацией и войти с локальной учетной записью:*

1. Внизу левой панели меню нажмите на имя текущего пользователя.
2. В раскрывшейся справа панели выберите **Войти как локальный пользователь**.

3. На странице авторизации веб-интерфейса введите логин и пароль учетной записи привилегированного пользователя.

   При необходимости на странице авторизации веб-интерфейса вы можете вернуться к действующей SSO-сессии по ссылке **На главную страницу**.

Откроется главное окно веб-интерфейса приложения в режиме привилегированного пользователя для локальной учетной записи.

► *Чтобы выйти из локальной учетной записи и войти с SSO-аутентификацией:*

1. Внизу левой панели меню нажмите на имя текущего пользователя.
2. В раскрывшейся справа панели выберите **Выйти**.

   Откроется страница авторизации веб-интерфейса Kaspersky Security для Linux Mail Server.
3. Обновите страницу с помощью клавиши **F5**.

Откроется главное окно веб-интерфейса приложения для учетной записи с SSO-аутентификацией. Если пользователю с SSO-аутентификацией назначена роль в приложении, по умолчанию после входа приложение открывается в режиме привилегированного пользователя.

Порядок настройки приложения

Вы можете настроить приложение через веб-интерфейс Управляющего узла кластера. Новые параметры будут автоматически распространены на Подчиненные узлы.

Сценарий настройки работы приложения состоит из следующих этапов:

1. **Настройка параметров подключения к прокси-серверу (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 256)**

   Этот этап следует выполнять, если на узле нет прямого доступа в интернет для активации приложения, обновления баз и для взаимодействия с "Лабораторией Касперского".
2. **Активация приложения**

   Активируйте Kaspersky Security для Linux Mail Server с помощью кода активации (см. раздел "Добавление кода активации" на стр. 55) или, если нет доступа в интернет, добавьте лицензионный ключ с помощью файла ключа (см. раздел "Добавление файла ключа" на стр. 54).
3. **Настройка обновления баз приложения (см. раздел "Настройка расписания и параметров обновления баз" на стр. 258)**

   Если нет доступа в интернет, настройте обновление баз приложения через Kaspersky Security Center или другой источник обновлений, расположенный в локальной сети.
4. **Запуск обновления баз вручную (на стр. 260)**

   Дождитесь завершения задачи обновления. Для применения обновления баз перезагрузите операционную систему.
5. **Настройка параметров защиты (см. раздел "Общие параметры защиты" на стр. 238)**
6. **Настройка параметров Хранилища (на стр. 180)**
7. **Настройка участия в Kaspersky Security Network (на стр. 267)**

Если вы хотите иметь доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров, вы можете настроить использование Kaspersky Private Security Network.

8. **Настройка интеграции с сервером KATA (см. раздел "Защита KATA" на стр. 277)**

   Этот этап следует выполнять, если в вашей организации развернуто приложение KATA.

9. **Настройка интеграции с внешней службой каталогов по протоколу LDAP (см. раздел "Интеграция с внешней службой каталогов" на стр. 270)**

10. **Настройка аутентификации пользователей с помощью единого входа (SSO) (см. раздел "Аутентификация с помощью технологии единого входа" на стр. 330)**

    Этот этап требуется для работы персональных и привилегированных пользователей с доменными учетными записями.

11. **Создание учетных записей и ролей пользователей (см. раздел "Работа с учетными записями и ролями пользователей" на стр. 158)**

    Назначьте пользователям нужные роли.

    Если в предыдущей версии приложения использовалась учетная запись helpdesk, создайте роль с аналогичными разрешениями: просмотр сообщений Хранилища, доставка сообщений из Хранилища, управление адресами в персональных списках разрешенных и запрещенных адресов.

12. **Настройка работы приложения для персональных пользователей**

    Настройте параметры персональных учетных записей (см. раздел "Настройка параметров персональных списков" на стр. 132), параметры персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182), расписание отправки дайджеста персонального Хранилища (см. раздел "Настройка расписания рассылки дайджеста Хранилища" на стр. 199).

13. **Перенос правил обработки сообщений и персональных списков пользователей из предыдущей версии приложения**

    При обновлении приложения с предыдущей версии вы можете экспортировать правила и персональные списки пользователей (см. раздел "Экспорт параметров" на стр. 263) из своей версии приложения, а затем импортировать их в новую версию (см. раздел "Импорт параметров" на стр. 264).

    Для импорта параметров укажите путь к файлу KLMS_settings.kz, полученному в результате экспорта параметров приложения из предыдущей версии.

14. **Настройка правил обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 101)**

    Этот этап требуется выполнять, если данных для импорта правил нет или нужны дополнительные правила.

15. **Настройка параметров системного журнала (см. раздел "Настройка параметров журнала событий" на стр. 219)**

16. **Настройка экспорта событий во внешнюю SIEM-систему (см. раздел "Публикация событий приложения в SIEM-систему" на стр. 345)**

17. **Настройка мониторинга работы приложения по протоколу SNMP (см. раздел "Работа с приложением по протоколу SNMP" на стр. 289)**

18. **Настройка параметров почтовых уведомлений о событиях в работе приложения (см. раздел "Настройка уведомлений о событиях в работе приложения" на стр. 323)**

19. **Настройка параметров расписания отправки отчетов со статистикой работы приложения (см. раздел "Настройка параметров отчетов по расписанию" на стр. 228).**

kaspersky

Мониторинг работы приложения

Вы можете осуществлять мониторинг работы приложения с помощью графиков и информационных панелей. Вы можете фильтровать данные мониторинга (см. раздел "Фильтрация данных мониторинга" на стр. 100) по интервалу времени и узлам кластера.

В разделе **Мониторинг** веб-интерфейса приложения доступна следующая информация:

1. **Работоспособность системы**. Диаграмма ошибок в работе кластера. По ссылке **Перейти в раздел Узлы** вы можете перейти в раздел **Узлы** и посмотреть более подробные сведения о работоспособности каждого узла кластера.
2. **Обработано**. График, показывающий статистику действий приложения, примененных ко всем обработанным сообщениям электронной почты:
   - **Удалены вложения**.
   - **Удалено**.
   - **Вылечено**.
   - **Помещено в Карантин**.
   - **Отклонено**.
   - **Пропущено**.

   С помощью кнопок **Размер** и **Количество** вы можете переключать отображение на графике суммарного размера или количества всех обработанных сообщений соответственно.
3. **Обнаружено**. График количества обнаруженных объектов, сгруппированных по модулям защиты:
   - **Анти-Фишинг**.
   - **Анти-Спам**.
   - **Антивирус**.
   - **Контентная фильтрация**.
   - **Проверка подлинности**.
   - **Проверка ссылок**.
   - **KATA**.

     Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

   Если в одном сообщении было обнаружено несколько объектов одним модулем защиты, то в статистике для этого модуля защиты считается только один объект. Если в одном сообщении было обнаружено несколько объектов разными модулями защиты, то в статистике считается по одному объекту для каждого модуля защиты.

   По ссылке в правом верхнем углу информационной панели вы можете перейти в раздел **События**, чтобы просмотреть связанные события с информацией об обнаружениях за выбранный период (см. раздел "Фильтрация данных мониторинга" на стр. 100).
4. Графики, которые показывают количество сообщений, проверенных определенным модулем и сгруппированных по результату проверки:

- **Антивирус**.
- **Анти-Спам**.
- **Анти-Фишинг**.
- **Контентная фильтрация**.
- **Проверка ссылок**.
- **Проверка подлинности**.

По умолчанию отображается только график **Антивирус**. Вы можете создать новую схему расположения графиков (см. раздел "Создание новой схемы расположения графиков" на стр. 98) или изменить текущую (см. раздел "Изменение схемы расположения графиков" на стр. 99), чтобы добавить нужные вам графики.

На всех графиках со статистикой по модулям защиты отображаются следующие статусы проверки:

- **Обнаружено** – в сообщении обнаружен объект, удовлетворяющий критериям применения правила.
- **Не обнаружено** – сообщение проверено и не содержит угроз и других объектов.
- **Документ с макросом** – в сообщении есть вложение, содержащее документ с макросом.

  Применимо только к графику **Антивирус**.
- **Помещено в Карантин** – сообщение помещено в Анти-Спам карантин.

  Применимо только к графику **Анти-Спам**.
- **Не обработано** – группа статусов, присваиваемых сообщению, если оно не было проверено по одной из следующих причин:
  - **Зашифровано** – не удалось проверить объект из-за того, что он зашифрован.

    Применимо только к графику **Антивирус**.
  - **Ошибка** – при проверке сообщения произошла ошибка.
  - **Ошибка баз** – не удалось проверить сообщение из-за того, что базы приложения не загружены (см. раздел "Мониторинг состояния баз приложения" на стр. 260).
  - **Ограничения лицензирования** – не удалось проверить сообщение из-за ограничений, связанных с лицензированием приложения (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 56) (например, истек срок действия лицензионного ключа).
- **Отключено в параметрах** – группа статусов, присваиваемых сообщению, если оно не было проверено согласно одному из следующих параметров приложения, заданных администратором:
  - **Список разрешенных адресов** – сообщение доставлено без проверки, т.к. адрес отправителя сообщения находится в глобальном списке разрешенных адресов (см. раздел "Списки разрешенных и запрещенных адресов" на стр. 130).
  - **Список запрещенных адресов** – сообщение отклонено без проверки, т.к. адрес отправителя сообщения находится в глобальном списке запрещенных адресов (см. раздел "Списки разрешенных и запрещенных адресов" на стр. 130).
  - **Превышен уровень вложенности** – превышен максимальный уровень вложенности архивов, заданный в общих параметрах защиты (см. раздел "Общие параметры защиты" на стр. 238).

    Применимо только к графику **Антивирус**.

- **Персональный список разрешенных адресов** – сообщение не было проверено модулем Анти-Спам, т.к. адрес отправителя находится в персональном списке разрешенных адресов (см. раздел "Формирование персональных списков" на стр. 134) получателя.

  Применимо только к графику **Анти-Спам**.

- **Персональный список запрещенных адресов** – адрес отправителя находится в персональном списке запрещенных адресов получателя. К сообщению применено действие, заданное в параметрах персональных списков (см. раздел "Настройка параметров персональных списков" на стр. 132).

  При подсчете не учитываются сообщения, помещенные в Хранилище согласно параметрам персональных списков. Такие сообщения попадают в статистику по другим статусам в соответствии с результатом проверки.

- **Локальная политика** – сообщение было отправлено с локального IP-адреса.

  Применимо только к графику **Проверка подлинности**.

- **Отключено в параметрах защиты** – модуль отключен в общих параметрах защиты или в правиле обработки сообщений.

- **Обработано ранее другим модулем** – сообщение не было проверено данным модулем, т.к. ранее была выполнена проверка другим модулем защиты и к сообщению уже применено действие **Отклонить** или **Удалить сообщение** (при этом сообщение не было помещено в Хранилище).

5. **Последние угрозы**. Таблица с информацией о недавних обнаруженных угрозах:

   - **Время** – время обнаружения угрозы.
   - **Название угрозы** – название угрозы, обнаруженной в объекте.
   - **Результат** – действие, выполненное с объектом.

   > Отображаются сведения, доступные в приложении на текущий момент. Критерии фильтрации по времени (см. раздел "Фильтрация данных мониторинга" на стр. 100) не применяются.

6. **Сообщения**. График, который показывает объем исходящего и входящего почтового трафика, обработанного приложением.

   > При подсчете исходящих сообщений не учитываются уведомления, отправляемые приложением, и сообщения со статусами проверки **Удалено**, **Отклонено** и **Помещено в Карантин**.

   С помощью кнопок **Размер** и **Количество** вы можете переключать отображение на графике суммарного размера или количества исходящих и входящих сообщений соответственно.

7. **Топ сработавших правил**. Таблица с информацией о правилах, которые наиболее часто применялись при обработке сообщений:

   - **Название правила** – название примененного правила, заданное администратором.
   - **Количество** – количество срабатываний правила.

   > Если правило было удалено администратором, то оно не отображается на этой информационной панели.

По умолчанию отображаются не все информационные панели. Вы можете создать новую схему расположения (см. раздел "Создание новой схемы расположения графиков" на стр. 98) и добавить на нее необходимые панели, а затем переключаться между доступными схемами (см. раздел "Выбор схемы расположения графиков из списка" на стр. 100).

В этом разделе

Создание новой схемы расположения графиков

После установки приложения в разделе **Мониторинг** отображается только схема расположения по умолчанию. Вы можете создать новую схему и настроить отображение информационных панелей на ней.

► *Чтобы создать новую схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывшемся списке выберите **Новая схема**.

   Отобразится набор графиков по умолчанию.
4. Если вы хотите изменить стандартное название схемы, выполните следующие действия:
   a. В верхней части рабочей области рядом с названием **Новая схема #** нажмите на значок  .
   b. В открывшемся окне в поле **Название схемы расположения графиков** введите новое название.
   c. Нажмите на кнопку **Сохранить**.
5. Если вы хотите добавить графики на схему, выполните следующие действия:
   a. Нажмите на кнопку **Добавить график**.

      Откроется окно **Добавить график**.
   b. Установите флажки рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   c. Нажмите на кнопку **Добавить**.
6. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
7. Если вы хотите удалить график со схемы, нажмите на значок ✕ в правом верхнем углу панели.

8. Если вы хотите изменить масштаб графика, нажмите на значок  в правом верхнем углу панели и в раскрывшемся списке выберите нужное значение.
9. Если вы хотите отключить отображение какой-либо категории данных на графике, нажмите на цветовой индикатор слева от этой категории (например,  для объектов со статусом **Не обнаружено**).
10. Если требуется, измените способ отображения информации (гистограмма или график) с помощью переключателя  в правом верхнем углу панели.
11. Нажмите на кнопку **Сохранить**.

Новая схема будет добавлена в список схем расположения графиков в разделе **Мониторинг**. Вы сможете выбрать ее из списка доступных схем (см. раздел "Выбор схемы расположения графиков из списка" на стр. 100).

Изменение схемы расположения графиков

► *Чтобы изменить схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите изменить.
3. Нажмите на кнопку  и в раскрывшемся списке выберите **Изменить схему**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет изменена.

Удаление схемы расположения графиков

► *Чтобы удалить схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите удалить.
3. Нажмите на кнопку  и в раскрывшемся списке выберите **Удалить схему**.

Схема расположения графиков будет удалена.

kaspersky

Выбор схемы расположения графиков из списка

► *Чтобы выбрать схему расположения графиков из списка доступных:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите открыть.

Выбранная схема отобразится в рабочей области.

Фильтрация данных мониторинга

► *Чтобы отфильтровать данные, отображаемые на графиках:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. Если вы хотите отфильтровать данные по интервалу времени, в правом верхнем углу рабочей области в левом раскрывающемся списке выберите один из следующих вариантов:
   - **Прошедший час**.
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.
   - **Прошедший месяц**.
   - **Прошедший год**.

   По умолчанию отображаются данные за последний час.
3. Если вы хотите отфильтровать данные по узлам кластера, в среднем раскрывающемся списке выберите IP-адрес нужного узла.

   По умолчанию отображаются данные обо всех узлах.

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

kaspersky

Работа с правилами обработки сообщений

Правило обработки сообщений (далее также "правило") – это набор параметров и действий, применяемых приложением к сообщениям, удовлетворяющим заданным критериям. Принадлежность сообщения к правилу определяется наличием в этом правиле как адреса отправителя, так и адреса получателя.

По умолчанию в приложении предусмотрены следующие предустановленные правила обработки сообщений:

- **AllowList** – обработка сообщений из глобального списка разрешенных адресов.
- **DenyList** – обработка сообщений из глобального списка запрещенных адресов.
- **Default** – обработка сообщений по предустановленным "Лабораторией Касперского" параметрам.

Правила **AllowList** и **DenyList** по умолчанию отключены.

Обрабатывая сообщение электронной почты, Kaspersky Security для Linux Mail Server применяет правила согласно их приоритету – в порядке расположения в таблице правил сверху вниз. Если комбинация адресов *отправитель-получатель* не совпадает, приложение переходит к следующему правилу. Как только комбинация адресов отправитель-получатель найдена в каком-либо правиле, к сообщению применяются параметры обработки, заданные в этом правиле, и поиск совпадения завершается.

Если одному адресу электронной почты соответствует несколько учетных записей LDAP, то правило применяется, если хотя бы одна из этих учетных записей попадает под его критерии. Для каждой пары отправитель-получатель срабатывает строго одно правило.

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

Если в сообщении есть DKIM-подпись, она может быть повреждена при применении тех правил обработки, в результате работы которых происходят изменение темы или тела сообщения, удаление вложений сообщения, лечение найденных вредоносных объектов, добавление примечаний к телу сообщения.

Для каждого правила вы можете задать собственные критерии обработки сообщений электронной почты и выбрать действие, применяемое к сообщениям. Если по результатам проверки сработало несколько модулей приложения и для них заданы разные действия, то будет выполнено более строгое действие (**Удалить сообщение** → **Отклонить** → **Удалить вложение** → **Пропустить**).

Рекомендуется устанавливать действие **Отклонить**, только если приложение Kaspersky Security для Linux Mail Server встроено в почтовую инфраструктуру напрямую, то есть выступает в роли пограничного шлюза. Если приложение встроено за сторонним пограничным шлюзом, то есть выступает в роли внутреннего шлюза, то в случае применения действия **Отклонить** пограничный шлюз будет формировать уведомления о недоставке (DSN, Delivery status notification). Рассылка таких уведомлений на несуществующие адреса электронной почты может привести к снижению репутации пограничного шлюза в сети Интернет.

kaspersky

В этом разделе

Просмотр таблицы правил

► *Чтобы просмотреть таблицу правил,*

в окне веб-интерфейса приложения выберите раздел **Правила**.

В таблице отображается следующая информация о правилах:

- **Приоритет**.

  Номер, соответствующий приоритету, задает последовательность применения правил. Правила применяются в порядке их расположения в таблице сверху вниз, то есть от наивысшего приоритета к низшему.

- **Название правила**.

  Название правила, заданное пользователем.

- **Статус**.

  Переключатель для включения и отключения правила.

- **Режим**.

  Правило может работать в одном из следующих режимов:

  -  – **Использовать параметры модулей проверки**.
  -  – **Отклонять без проверки**.
  -  – **Удалять без уведомления отправителя**.
  -  – **Пропускать без проверки**.

- **Описание**.

Любая дополнительная информация о правиле, указанная пользователем.

По ссылке **Уведомления об обнаружениях** вы можете настроить общие параметры почтовых уведомлений об обнаружениях (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 324), применимые ко всем правилам. После этого требуется включить уведомления для каждого правила (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 123), о срабатывании которого вы хотите получать сообщения от приложения.

Настройка отображения таблицы правил

► *Чтобы настроить отображение таблицы правил:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Нажмите на кнопку  .

   Откроется окно **Настроить таблицу**.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы правил будет настроено.

Сценарий настройки правил обработки сообщений

Вы можете изменить общие параметры защиты (на стр. 238), применяемые ко всем правилам обработки сообщений, в разделе **Параметры** → **Общие**.

1. **Создание правила (см. раздел "Создание правила обработки сообщений" на стр. 105)**

   При создании правила необходимо задать адреса отправителей и получателей, сообщения которых будут обрабатываться согласно параметрам этого правила, а также режим обработки сообщений. Остальные общие параметры правила являются опциональными.
2. **Антивирусная защита сообщений (см. раздел "Настройка антивирусной защиты" на стр. 109)**

   Kaspersky Security для Linux Mail Server проверяет сообщения электронной почты на вирусы и другие программы, представляющие угрозу, с помощью модуля Антивирус.

   Вы можете включить или отключить антивирусную проверку сообщений для правила. Если в правиле включена антивирусная проверка, то вы можете настроить параметры проверки в зависимости от типа объекта:

   - зараженные и возможно зараженные объекты, а также легальные программы, которые могут быть использованы злоумышленниками;
   - объекты, во время проверки которых возникли ошибки;
   - зашифрованные объекты;

- вложения с макросами.

3. **Проверка ссылок (см. раздел "Настройка проверки ссылок" на стр. 112)**

   Kaspersky Security для Linux Mail Server проверяет, являются ли ссылки в тексте сообщения вредоносными, т.е. ведущими на веб-ресурсы, которые распространяют вредоносное ПО. Вы также можете включить обнаружение рекламных ссылок и ссылок, относящихся к легальным программам (см. раздел "Настройка параметров проверки ссылок" на стр. 248).

4. **Защита сообщений от спама (см. раздел "Настройка защиты от спама" на стр. 113)**

   Kaspersky Security для Linux Mail Server фильтрует сообщения, проходящие через почтовый сервер, от нежелательной почты (спама) с помощью модуля Анти-Спам.

   Вы можете включить или отключить защиту от спама для правила. Если в правиле включена защита от спама, то вы можете настроить параметры проверки в зависимости от типа объекта:

   - спам;
   - предполагаемый спам;
   - массовая рассылка.

5. **Защита сообщений от фишинга (см. раздел "Настройка защиты от фишинга" на стр. 115)**

   Kaspersky Security для Linux Mail Server фильтрует сообщения, проходящие через почтовый сервер, от фишинга с помощью модуля Анти-Фишинг.

   Вы можете включить или отключить защиту от фишинга для правила.

6. **Контентная фильтрация сообщений (см. раздел "Настройка контентной фильтрации" на стр. 116)**

   Kaspersky Security для Linux Mail Server выполняет контентную фильтрацию сообщений, проходящих через почтовый сервер.

   Вы можете включить или отключить контентную фильтрацию для правила. Если в правиле включена контентная фильтрация, вы можете ограничить пересылку почтовым сервером сообщений по следующим критериям:

   - размер сообщения;
   - маска имен вложенных файлов;
   - формат вложенных файлов.

7. **Проверка подлинности отправителей сообщений (на стр. 120)**

   Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры вашей организации от спама и фишинга.

   Kaspersky Security 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).

8. **Уведомления о результатах проверки сообщений (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 123)**

   Вы можете настроить отправку почтовых уведомлений о событиях проверки сообщений на адреса из заданного общего списка, отправителю, получателям сообщения или другим адресатам.

9. **Предупреждения о небезопасных сообщениях (см. раздел "Добавление предупреждения о небезопасном сообщении" на стр. 124)**

   Вы можете настроить шаблон предупреждения, текст которого будет добавляться в тело сообщения, имеющего один из следующих статусов проверки:

   - *Зашифровано*;
   - *Заражено*;
   - *Ошибка*;
   - *Фишинг*;
   - *Проверка ссылок*.

10. **Примечания к сообщениям (см. раздел "Добавление примечания к событиям проверки сообщений" на стр. 125)**

    Примечание к сообщениям (далее также "примечание") – это текст, который приложение может добавлять в конце сообщения электронной почты.

    Вы можете включить или отключить использование примечаний для одного или нескольких правил обработки сообщений, а также настроить шаблоны примечаний.

11. **Защита KATA (см. раздел "Настройка защиты KATA" на стр. 126)**

    Kaspersky Security для Linux Mail Server может интегрироваться с Kaspersky Anti Targeted Attack Platform и отправлять сообщения для проверки на сервер KATA.

    Вы можете включить или отключить защиту KATA для правила. Если в правиле включена защита KATA, то вы можете выбрать действие для сообщений, в которых обнаружены объекты, указать, должно ли приложение помещать сообщения в Хранилище, а также настроить метку в теме сообщений.

Создание правила обработки сообщений

► *Чтобы создать правило обработки сообщений:*

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

   Откроется новое правило обработки сообщений.
3. В левой панели выберите раздел **Общие**.
4. В поле **Название правила** введите название нового правила.

   Название правила должно быть уникальным в списке правил Kaspersky Security для Linux Mail Server.
5. В поле **Описание** введите описание правила.
6. В блоке параметров **Режим** выберите один из следующих вариантов обработки сообщений, соответствующих критериям этого правила:

   - **Использовать параметры модулей проверки** – использовать параметры модулей Антивирус, Анти-Спам, Анти-Фишинг и параметры контентной фильтрации.

     В левой панели станут доступны разделы, в которых вы можете настроить параметры модулей, применяемые в этом правиле.

- **Отклонять без проверки** – отклонять сообщения без проверки модулями Антивирус, Анти-Спам, Анти-Фишинг и без применения к ним параметров контентной фильтрации.
- **Удалять без уведомления отправителя** – удалять сообщения без проверки модулями Антивирус, Анти-Спам, Анти-Фишинг и без применения к ним параметров контентной фильтрации и не уведомлять отправителя о том, что сообщение не было доставлено.
- **Пропускать без проверки** – доставлять сообщения, не выполняя их проверку.

7. Если вы хотите изменить приоритет создаваемого правила, в блоке **Приоритет правила** задайте позицию создаваемого правила в таблице правил.

   По умолчанию правилу присваивается наивысший приоритет из всех ранее созданных правил.

8. В блоке параметров **Отправитель** укажите отправителей сообщения, для которых должно применяться это правило:

   - **Email**

     1. На закладке **Адреса эл. почты** добавьте адреса электронной почты в список:

        - Чтобы указать адрес вручную, нажмите на кнопку **Добавить**, введите адрес электронной почты и нажмите на значок ✓. Кнопка доступна, если формат введенного текста соответствует формату адреса электронной почты.

          При необходимости повторите действия для остальных адресов.

        - Чтобы вставить адреса из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена адреса электронной почты, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.

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

        > Регулярные выражения нечувствительны к регистру.

     2. Если вы хотите изменить ранее добавленный адрес, нажмите на него в поле ввода, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.

     3. Если вы хотите удалить адрес из списка, нажмите на значок 🗑 справа от адреса. Чтобы очистить список, нажмите на кнопку **Удалить все**.

        Поддерживается добавление до 100000 адресов.

   - **IP**

     1. Перейдите на закладку **IP** и добавьте IP-адреса отправителей сообщений в список:

        - Чтобы указать IP-адрес вручную, нажмите на кнопку **Добавить**, введите IP-адрес и нажмите на значок ✓. Кнопка доступна, если формат введенного значения соответствует формату IP-адреса.

          При необходимости повторите действия для остальных IP-адресов.

        - Чтобы вставить IP-адреса из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена IP-адреса, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.

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).

2. Если вы хотите изменить ранее добавленный IP-адрес, нажмите на него в списке, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.
3. Если вы хотите удалить IP-адрес из списка, нажмите на значок 🗑 справа от IP-адреса. Чтобы очистить список, нажмите на кнопку **Удалить все**.

   Поддерживается добавление до 100000 IP-адресов.

- **LDAP: DN**

  1. Перейдите на закладку **LDAP:DN** и добавьте учетные записи LDAP в список:
     - Чтобы указать учетную запись вручную, нажмите на кнопку **Добавить**, введите значение и нажмите на значок ✓. При вводе значения отображается подсказка с учетными записями из LDAP-кеша, которые содержат указанные символы.

       Подсказка для учетных записей контактов отображается, если включено получение почтовых адресов контактов в параметрах соединения с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272).

       Если в имени учетной записи LDAP используется специальный символ, при вводе значения следует экранировать специальный символ с помощью символа обратной косой черты ("\"). В противном случае подсказка для записи не будет отображена. Например, имя учетной записи `exa,mple` следует вводить в виде `exa\,mple`. Более подробную информацию и полный список экранируемых символов см. в документации компании Microsoft https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names.

       При необходимости повторите действия для остальных учетных записей LDAP.
     - Чтобы вставить учетную запись LDAP из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена учетные записи, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.
  2. Если вы хотите изменить ранее добавленную запись, нажмите на нее в списке, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.
  3. Если вы хотите удалить запись из списка, нажмите на значок 🗑 справа от учетной записи LDAP. Чтобы очистить список, нажмите на кнопку **Удалить все**.

Для того чтобы правило применялось, необходимо указать хотя бы одного отправителя.

9. В блоке параметров **Получатель** укажите получателей сообщения, для которых должно применяться это правило:

   - **Email**

     1. На закладке **Адреса эл. почты** добавьте адреса электронной почты в список:

- Чтобы указать адрес вручную, нажмите на кнопку **Добавить**, введите адрес электронной почты и нажмите на значок ✓. Кнопка доступна, если формат введенного текста соответствует формату адреса электронной почты.

  При необходимости повторите действия для остальных адресов.

- Чтобы вставить адреса из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена адреса электронной почты, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.

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

> Регулярные выражения нечувствительны к регистру.

2. Если вы хотите изменить ранее добавленный адрес, нажмите на него в поле ввода, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.
3. Если вы хотите удалить адрес из списка, нажмите на значок 🗑 справа от адреса. Чтобы очистить список, нажмите на кнопку **Удалить все**.

   Поддерживается добавление до 100000 адресов.

- **LDAP: DN**

1. Перейдите на закладку **LDAP:DN** и добавьте учетные записи LDAP в список:
   - Чтобы указать учетную запись вручную, нажмите на кнопку **Добавить**, введите значение и нажмите на значок ✓. При вводе значения отображается подсказка с учетными записями из LDAP-кеша, которые содержат указанные символы.

     > Подсказка для учетных записей контактов отображается, если включено получение почтовых адресов контактов в параметрах соединения с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272).

     Если в имени учетной записи LDAP используется специальный символ, при вводе значения следует экранировать специальный символ с помощью символа обратной косой черты ("\"). В противном случае подсказка для записи не будет отображена. Например, имя учетной записи `exa,mple` следует вводить в виде `exa\,mple`. Более подробную информацию и полный список экранируемых символов см. в документации компании Microsoft https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names.

     При необходимости повторите действия для остальных учетных записей LDAP.

   - Чтобы вставить учетную запись LDAP из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена учетные записи, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.
2. Если вы хотите изменить ранее добавленную запись, нажмите на нее в списке, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.

3. Если вы хотите удалить запись из списка, нажмите на значок справа от учетной записи LDAP. Чтобы очистить список, нажмите на кнопку **Удалить все**.

Для того чтобы правило применялось, необходимо указать хотя бы одного получателя.

10. Нажмите на кнопку **Сохранить**.

Если хотя бы один из элементов списка в блоках параметров **Отправитель** и **Получатель** указан в недопустимом формате, сохранение правила недоступно. Исправьте все значения, выделенные красным фоном, и повторите операцию сохранения.

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

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, требуется включить правило (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128). По умолчанию новое правило отключено и не используется в работе приложения.

Настройка антивирусной защиты

Перед тем как настроить параметры антивирусной защиты в правиле обработки сообщений, убедитесь, что модуль Антивирус включен в общих параметрах защиты.

► *Чтобы настроить параметры антивирусной защиты в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры антивирусной защиты.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Антивирус**.
5. Включите или отключите проверку модулем Антивирус сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию антивирусная защита сообщений включена.
6. Если на предыдущем шаге вы включили антивирусную проверку, настройте параметры модуля Антивирус, применяемые по результатам проверки к следующим типам объектов:

   - Зараженные и возможно зараженные объекты, а также легальные программы, которые могут быть использованы злоумышленниками.

1. В блоке параметров **Если обнаружен зараженный объект** в раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:
   - **Пропустить**.
   - **Вылечить**.
   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Вылечить**.
2. Если на предыдущем шаге вы выбрали действие **Вылечить**, в раскрывающемся списке **Если вылечить не удалось** выберите одно из следующих действий над зараженными сообщениями, вылечить которые не удалось:
   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Удалить вложение**.
3. Если вы хотите по результатам антивирусной проверки автоматически помещать в Хранилище сообщения с обнаруженными объектами, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.
4. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы зараженных и вылеченных сообщений, укажите текст меток в полях ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию добавлены метки *[Infected]* и *[Cured]*.

- Объекты, во время проверки которых произошли ошибки.
  1. В раскрывающемся списке **Если обнаружены ошибки проверки модулем Антивирус** выберите действие, применяемое к сообщениям, при проверке которых произошли ошибки:
     - **Пропустить**.
     - **Удалить вложение**.
     - **Удалить сообщение**.
     - **Отклонить**.

     По умолчанию выбрано действие **Пропустить**.
  2. Если вы хотите автоматически помещать в Хранилище сообщения, при проверке которых произошли ошибки, установите флажок **Поместить сообщение в Хранилище**.

     По умолчанию флажок снят.
  3. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы сообщений, при проверке которых произошли ошибки, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.
- Зашифрованные объекты.
  1. В раскрывающемся списке **Если обнаружен зашифрованный объект** выберите действие, применяемое к сообщениям, содержащим зашифрованные объекты:

- **Пропустить**.
- **Удалить вложение**.
- **Удалить сообщение**.
- **Отклонить**.

По умолчанию выбрано действие **Пропустить**.

2. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения с зашифрованными объектами, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок снят.

3. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы сообщений, содержащих зашифрованные объекты, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

- Вложения с макросами.

1. В блоке параметров **Если обнаружен макрос** установите флажок **Обрабатывать вложения с макросами** если вы хотите, чтобы приложение обрабатывало вложения с макросами.
2. В раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:

   - **Пропустить**.
   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Удалить вложение**.

3. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, содержащие вложения с макросами, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок снят.

4. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы сообщений, содержащих вложения с макросами, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию добавлена метка *[Attachments with Macros]*.

7. Если требуется, настройте список исключений из проверки. Для этого в блоке параметров **Исключения из проверки** выполните следующие действия:

   a. Если вы хотите исключить из антивирусной проверки архивы, установите флажок **Не проверять архивы**.

   b. Если вы хотите исключить из антивирусной проверки вложенные в сообщение объекты с определенными именами, в поле **Не проверять вложения по маскам имени** укажите маску имени и нажмите на клавишу **ENTER**.

      Вводите маски по одной. Повторите указанные действия для каждой добавляемой маски.

      Маски нечувствительны к регистру и могут содержать любые символы.

8. Нажмите на кнопку **Сохранить**.

Антивирусная защита будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что антивирусная проверка сообщений для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Настройка проверки ссылок

Перед тем как настроить параметры проверки ссылок в правиле обработки сообщений, убедитесь, что проверка ссылок включена (см. раздел "Настройка параметров проверки ссылок" на стр. 248) в общих параметрах защиты.

► *Чтобы настроить параметры проверки ссылок в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры антивирусной защиты.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Проверка ссылок**.
5. Включите или отключите проверку ссылок в сообщениях, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию проверка ссылок включена.
6. Если на предыдущем шаге вы включили проверку ссылок, настройте параметры, применяемые по результатам проверки к вредоносным или рекламным ссылкам, а также к ссылкам, относящимся к легальным программам:

   a. В раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:

      - **Удалить сообщение**.
      - **Отклонить**.
      - **Пропустить**.

      По умолчанию выбрано действие **Отклонить**.

   b. Если вы хотите чтобы по результатам проверки сообщения с обнаруженными объектами автоматически помещались в Хранилище, установите флажок **Поместить сообщение в Хранилище**.

По умолчанию флажок установлен.

c. Если вы хотите, чтобы по результатам проверки приложение добавляло метку в начало темы сообщений, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

По умолчанию добавлена метка *[Malicious|Adware|Legitimate links]*.

7. Нажмите на кнопку **Сохранить**.

Настройка защиты от спама

Перед тем как настроить параметры защиты от спама в правиле обработки сообщений, убедитесь, что модуль Анти-Спам включен в общих параметрах защиты.

► *Чтобы настроить параметры защиты от спама в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры защиты от спама.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Анти-Спам**.
5. Включите или отключите проверку модулем Анти-Спам сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита сообщений от спама включена.
6. Если на предыдущем шаге вы включили защиту от спама, настройте параметры модуля Анти-Спам, применяемые по результатам проверки к следующим типам объектов:

   - Спам.
7. В блоке параметров **Если обнаружен спам** выберите одно из следующих действий над сообщениями, содержащими спам:

   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Пропустить**.
8. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, признанные спамом, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок снят.
9. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, содержащих спам, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

По умолчанию добавлена метка *[Spam]*.

- Предполагаемый спам.

10. В блоке параметров **Если обнаружен предполагаемый спам** выберите одно из следующих действий над сообщениями, содержащими предполагаемый спам:

    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Пропустить**.

11. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, содержащие предполагаемый спам, установите флажок **Поместить сообщение в Хранилище**.

    По умолчанию флажок снят.

12. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, содержащих предполагаемый спам, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

    По умолчанию добавлена метка *[Probable spam]*.

    - Массовая рассылка.

13. В блоке параметров **Если обнаружена массовая рассылка** выберите одно из следующих действий над сообщениями, являющимися массовой рассылкой:

    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Пропустить**.

14. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, признанные массовой рассылкой, установите флажок **Поместить сообщение в Хранилище**.

    По умолчанию флажок снят.

15. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, являющихся массовой рассылкой, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

    По умолчанию добавлена метка *[MASSMAIL]*.

16. В блоке параметров **Дополнительные параметры** установите флажки рядом с названиями параметров, которые вы хотите включить:

    a. **Использовать технологии обработки графических изображений**, если вы хотите использовать технологию GSG, позволяющую идентифицировать изображения, содержащие текст, чтобы затем определить, является ли текст спамом. Текст распознается вне зависимости от того, был ли он модифицирован, повернут на изображении, "зашумлен" или подвергнут любой другой обработке, скрывающей назначение отправленного изображения.

    b. **Защита от Юникод-спуфинга**, если вы хотите включить защиту от Юникод-спуфинга. В случае обнаружения Юникод-спуфинга сообщение считается спамом. Приложение добавляет метку `unicode_spoof` к заголовку сообщения `X-KLMS-AntiSpam-Method`.

Приложение проверяет наличие Юникод-спуфинга только в заголовках Mail From SMTP-конверта, а также в заголовках сообщения From, Sender, Reply-To.

17. Нажмите на кнопку **Сохранить**.

Защита от спама будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что защита от спама для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Настройка защиты от фишинга

Перед тем как настроить параметры защиты от фишинга в правиле обработки сообщений, убедитесь, что модуль Анти-Фишинг включен (см. раздел "Настройка параметров модуля Анти-Фишинг" на стр. 251) в общих параметрах защиты.

► *Чтобы настроить параметры защиты от фишинга в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры защиты от фишинга.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Анти-Фишинг**.
5. Включите или отключите проверку модулем Анти-Фишинг сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита сообщений от фишинга включена.
6. Если на предыдущем шаге вы включили защиту от фишинга, в раскрывающемся списке выберите одно из следующих действий над сообщениями, содержащими фишинг:
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Отклонить**.
7. Если вы хотите чтобы по результатам проверки сообщения, содержащие фишинг, автоматически помещались в Хранилище, установите флажок **Поместить сообщение в Хранилище**.

По умолчанию флажок снят.

8. Если вы хотите, чтобы по результатам проверки приложение добавляло метки в начало темы сообщений, содержащих фишинг, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию добавлена метка *[Phishing]*.

9. Нажмите на кнопку **Сохранить**.

Защита от фишинга будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что защита от фишинга для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Настройка контентной фильтрации

Перед тем как настроить параметры контентной фильтрации в правиле обработки сообщений, убедитесь, что контентная фильтрация включена (см. раздел "Настройка параметров контентной фильтрации" на стр. 251) в общих параметрах защиты.

► *Чтобы настроить параметры контентной фильтрации в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры контентной фильтрации.

   Откроется окно **Просмотреть правило**.

3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Контентная фильтрация**.
5. Включите или отключите контентную фильтрацию сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию контентная фильтрация сообщений отключена.

6. Если на предыдущем шаге вы включили контентную фильтрацию, настройте параметры фильтрации по следующим критериям:

   - по размеру сообщений;

     1. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты определенного размера, в блоке параметров **Если превышен допустимый размер сообщения** в раскрывающемся списке выберите действие, которое будет применяться к сообщениям:

        - **Пропустить**.

- **Удалить сообщение**.
- **Отклонить**.

По умолчанию выбрано действие **Отклонить**.

2. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, содержащие вложенные объекты определенного размера, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.

3. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы для сообщений, содержащих вложенные объекты определенного размера, укажите текст меток в полях ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию метка не задана.

4. В поле **Размер сообщения** введите максимальный размер объектов в диапазоне от 0 КБ до 1048576 КБ (1 ГБ).

   Если установлено значение 0 КБ, ограничения размера объектов отсутствуют.

- по формату вложения;

  1. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты определенного формата, в блоке параметров **Тип вложения** сформируйте список форматов вложений, к которым должно применяться правило. Для этого выполните следующие действия:

     a. Выберите способ формирования списка:

        - **Вложения, тип которых указан в списке**, если вы хотите указать форматы вложений, которые требуется добавить в список.

          К сообщениям, содержащим вложения указанных форматов, будут применяться параметры контентной фильтрации.

        - **Вложения, тип которых НЕ указан в списке**, если вы хотите указать форматы вложений, которые требуется исключить из списка.

          К сообщениям, содержащим вложения указанных форматов, не будут применяться параметры контентной фильтрации.

     b. По ссылке **Изменить** откройте список возможных форматов вложений.

     c. Установите флажки рядом с форматами вложений, которые вы хотите добавить в список или исключить из списка:

        - архивы: 7Z (в том числе тома архивов с расширением вида 7Z*), ACR, ARJ, BZ, BZ2, TBZ, TBZ2, CAB, DMG, SMI, IMG, GZ, TGZ, ISO, JAR, RAR, TAR, XAR, ZIP;
        - базы данных: ACCDB, ACCDE, ACCDP, ACCDR, ACCDC, MDB, MDT;
        - исполняемые файлы: APK, SCPT, APPLESCRIPT, BAT, CMD, DEB, DEX, ODEX, ELF, CLASS, JS, O, DYLIB, MSI, PYC, PYO, RPM, SH, PL, VBS, EXE, DLL, OCX, SCR, LNK;
        - графические файлы:
          - анимированные файлы: SWF;
          - растровые графические файлы: BMP, GIF, JPG, JPE, JPEG, JFIF, PNG, APNG, TIF, TIFF;
          - векторные графические файлы: CDR, EMF, WMF, EPS, PSD;

- файлы мультимедиа:
  - аудиофайлы: AAC, M4A, AC3, APE, CDA, FLAC, MID, MIDI, MKA, MP3, OGG, RM, RA, RAVB, WAV, WMA;
  - видеофайлы: 3GP, 3G2, 3GP2, 3P2, ASF, WMV, AVI, BIK, F4V, FLV, MKV, MOV, QT, DIVX, MP4, RM, RMVB, RTMP, VOB, DAT, MPG, MPEG;
- файлы документов:
  - документы: DOC, DOCM, DOCX, DOT, DOTM, DOTX, ODT, PDF, RTF, SXW, XPS;
  - презентации: POTM, POTX, PPSM, PPSX, PPT, POT, PPS, PPTM, SLDM, PPTX, SLDX, ODP;
  - специализированные: PUB, MSG, OFT, ONE, ONEPKG, VDX, VSX, VTX, VSD, VSS, VST, XSN;
  - электронные таблицы: XLAM, XLS, XLT, XLSB, XLSM, XLSX, XLTM, XLTX, ODS;
- прочие файлы: CAT, CSV, HTML, HTM, TXT, CHM, REG.

d. Внизу окна настройки нажмите на кнопку **ОК**.

2. В раскрывающемся списке **В случае обнаружения** выберите действие, которое будет применяться к сообщениям:
   - **Пропустить**.
   - **Удалить сообщение**.
   - **Удалить вложение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Отклонить**.
3. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, содержащие вложения указанных форматов, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.
4. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы для сообщений, содержащих вложенные объекты определенного формата, укажите текст меток в полях ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию метка не задана.

- по имени вложения.

1. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты с определенными именами, в блоке параметров **Имя вложения** в поле **Имена вложений** введите имена таких вложенных объектов.

   В качестве имени вложенного объекта могут использоваться маски и регулярные выражения. Имена могут содержать любые символы. Разделяйте имена знаком ";".

   > Маски и регулярные выражения нечувствительны к регистру.

   Например, вы можете ввести маску имени `*.exe` и ограничить пересылку сообщений, содержащих вложенные объекты с расширением EXE.

Чтобы ограничить пересылку сообщений, содержащих исполняемые файлы распространенных форматов, вы можете использовать следующие регулярные выражения:

```
re:.*\.(scr|cpl|com|bat|cmd|vbs|pif|lnk|url|exe|bvs|spl|dll)$;
re:^[^\t\n]*\.[A-Za-z0-9]+\.(exe|vbs|cpl|dll)[. ]*$
```

2. В раскрывающемся списке **В случае обнаружения** выберите действие, которое нужно применять к сообщениям:

   - **Пропустить**.
   - **Удалить сообщение**.
   - **Удалить вложение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Отклонить**.

3. Если вы хотите по результатам проверки автоматически помещать в Хранилище сообщения, содержащие вложения с указанными именами, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.

4. Если вы хотите по результатам проверки автоматически добавлять метку в начало темы для сообщений, содержащих вложенные объекты определенного формата, укажите текст меток в полях ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию метка не задана.

7. Если вы хотите проверять наличие запрещенных форматов или имен файлов внутри составных объектов (в том числе внутри архивов), установите флажок **Проверять составные объекты**.

   Если вы включите проверку составных объектов, флажок **Проверять форматы и имена файлов внутри архивов** будет установлен автоматически, так как архивы являются разновидностью составных объектов.

8. Если на предыдущем шаге вы не включили проверку составных объектов и хотите проверять наличие запрещенных форматов или имен файлов только внутри архивов, установите флажок **Проверять форматы и имена файлов внутри архивов**.
9. Нажмите на кнопку **Сохранить**.

Контентная фильтрация будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что контентная фильтрация сообщений для правила включена и правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

kaspersky

Проверка подлинности отправителей сообщений

Перед тем как настроить параметры проверки подлинности в правиле обработки сообщений, убедитесь, что соответствующая проверка подлинности отправителей включена в общих параметрах защиты.

► *Чтобы настроить проверку подлинности отправителей сообщений в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить проверку подлинности отправителей сообщений.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Проверка подлинности**.
5. Включите или отключите проверку подлинности отправителей сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию проверка подлинности отключена.
6. Если на предыдущем шаге вы включили проверку подлинности, настройте общие параметры для всех типов проверок:
   - Установите флажок **Считать временные ошибки (TempError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security для Linux Mail Server считал временные ошибки TempError нарушением подлинности отправителя сообщений.
   - Установите флажок **Считать постоянные ошибки (PermError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Security для Linux Mail Server считал постоянные ошибки PermError нарушением подлинности отправителя сообщений.
7. Настройте параметры проверок следующих типов:
   - DMARC-проверка.

     Перед тем как настроить параметры DMARC-проверки сообщений для правила, убедитесь, что DMARC-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

     1. В блоке параметров **DMARC-проверка подлинности отправителей** установите флажок **Считать результат DMARC-проверки приоритетным**, если вы хотите определять нарушение подлинности отправителя сообщений только по результатам DMARC-проверки, не учитывая результаты SPF- и DKIM-проверок.

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. Если выявлены нарушения по нескольким проверкам одновременно, над сообщением выполняется самое строгое из заданных действий при SPF-, DKIM- или DMARC-нарушениях подлинности отправителя.

2. 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 на DNS-сервере. Если администратор установил политику None или Quarantine, приложение выполнит действие **Пропустить**. Политике Reject соответствует действие приложения **Отклонить**.

   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

   По умолчанию выбрано действие **Применить DMARC-политику**.

3. Если вы хотите автоматически помещать в Хранилище сообщения, DMARC-проверка которых выявила нарушение подлинности, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок снят.

4. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, DMARC-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию метка не задана.

- SPF-проверка.

Перед тем как настроить параметры SPF-проверки сообщений для правила, убедитесь, что SPF-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

1. В блоке параметров **SPF-проверка подлинности отправителей** установите флажок **Считать SPF softfail нарушением подлинности отправителя**, если вы хотите считать ошибку SPF softfail, обнаруженную при SPF-проверке, нарушением подлинности отправителя сообщений.
2. 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**.

По умолчанию выбрано действие **Пропустить**.

3. Если вы хотите автоматически помещать в Хранилище сообщения, SPF-проверка которых выявила нарушение подлинности, установите флажок **Поместить сообщение в Хранилище**.

По умолчанию флажок снят.

4. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, SPF-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

По умолчанию метка не задана.

- DKIM-проверка.

Перед тем как настроить параметры DKIM-проверки сообщений для правила, убедитесь, что DKIM-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

1. В блоке параметров **DKIM-проверка подлинности отправителей** установите флажок **Считать отсутствие DKIM-подписи нарушением подлинности отправителя**, если вы хотите считать отсутствие DKIM-подписи к сообщению, обнаруженное при DKIM-проверке, нарушением подлинности отправителя сообщения.
2. В раскрывающемся списке **Режим сопоставления** выберите режим аутентификации:
   - **Расслабленный**.
   - **Строгий**.
3. 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**.

   По умолчанию выбрано действие **Пропустить**.
4. Если вы хотите автоматически помещать в Хранилище сообщения, DKIM-проверка которых выявила нарушение подлинности, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок снят.
5. Если вы хотите по результатам проверки автоматически добавлять метки в начало темы сообщений, DKIM-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию метка не задана.

8. Нажмите на кнопку **Сохранить**.

Проверка подлинности отправителей сообщений будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что проверка подлинности для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Настройка уведомлений о событиях проверки сообщений

Вы можете настроить отправку почтовых уведомлений о событиях проверки сообщений для одного или нескольких правил.

Доступно, если отправка уведомлений включена в общих параметрах (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 324) почтовых уведомлений.

Вы можете настроить отправку почтовых уведомлений адресатам из общего списка, отправителю, получателю сообщений или другим адресатам о следующих событиях проверки сообщений:

- **Обнаружены вредоносные объекты**.
- **Обнаружены зашифрованные объекты**.
- **Обнаружены ошибки проверки модулем Антивирус**.
- **Обнаружены проблемы с контентной фильтрацией**.
- **Обнаружены сообщения, содержащие фишинг**.
- **Обнаружен макрос во вложении**.
- **Обнаружены вредоносные ссылки**.
- **Если KATA сервер обнаружил объект**.

  Настройка отправки уведомлений об обнаружениях KATA доступна только при интеграции с Kaspersky Anti Targeted Attack Platform (см. раздел "Защита KATA" на стр. 277).

► Чтобы настроить отправку уведомлений о событиях проверки сообщений:

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить уведомления о событиях проверки.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Уведомления**.
5. В блоке параметров с названием выбранного события (например, **Обнаружены вредоносные объекты**) установите флажки рядом с названиями параметров:

- **Уведомить получателей из общего списка**, если вы хотите включить отправку уведомлений о выбранном событии на адреса из общего списка.

  Если флажок установлен, вам требуется задать список адресов, перейдя по ссылке **Настроить** в общие параметры почтовых уведомлений (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 324).

- **Уведомить отправителя**, если вы хотите включить отправку уведомлений о выбранном событии на адреса отправителей сообщений.
- **Уведомить 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, выберите один из следующих вариантов:
   - **Только уведомлять**, если вы хотите настроить отправку уведомления без оригинала сообщения.
   - **Уведомлять с оригиналом сообщения во вложении**, если вы хотите настроить отправку уведомления с оригиналом сообщения во вложении.
7. Если вы включили отправку уведомлений на дополнительные адреса электронной почты, укажите адрес в поле ввода и нажмите на клавишу **ENTER**.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.
8. Если требуется, по ссылке **Настроить шаблоны уведомлений** в правом верхнем углу окна измените шаблоны уведомлений (см. раздел "Настройка шаблонов уведомлений" на стр. 325).
9. Нажмите на кнопку **Сохранить**.

Уведомления о событиях проверки сообщений будут настроены.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Добавление предупреждения о небезопасном сообщении

► Чтобы добавить предупреждение о небезопасном сообщении:

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить предупреждение о небезопасном сообщении.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Предупреждение о небезопасном сообщении**.
5. В раскрывающемся списке **Шаблон предупреждения** выберите шаблон предупреждения о небезопасном сообщении, которое вы хотите добавить.
6. Установите флажки рядом с одним или несколькими из следующих типов сообщений, к которым вы хотите добавить предупреждение:
   - **Для зашифрованных сообщений**.
   - **Для фишинговых сообщений**.
   - **Для зараженных сообщений**.
   - **Для сообщений с ошибками проверки модулем Антивирус**.
   - **Для сообщений, содержащих ссылки**.
7. Нажмите на кнопку **Сохранить**.

Предупреждения будут добавляться в текст сообщений согласно заданным параметрам.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Добавление примечания к событиям проверки сообщений

► *Чтобы добавить примечание к событию проверки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить примечание к событию проверки сообщений.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Примечание к сообщению**.
5. Включите или отключите добавление примечания к событию проверки сообщений с помощью переключателя справа от названия раздела.

   По умолчанию добавление примечания отключено.
6. В раскрывающемся списке **Добавить примечание** выберите шаблон примечания, которое вы хотите добавить к событию проверки сообщений.
7. Нажмите на кнопку **Сохранить**.

Добавление примечания к событиям проверки сообщений будет настроено.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что добавление примечаний к сообщениям для правила включено, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Настройка защиты KATA

Перед тем как настроить параметры защиты KATA в правиле обработки сообщений, убедитесь, что интеграция с KATA настроена (см. раздел "Защита KATA" на стр. 277) в общих параметрах защиты.

► *Чтобы настроить защиту KATA в правиле обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить защиту KATA.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Защита KATA**.
5. Включите или отключите защиту KATA для сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита KATA отключена.
6. Если на предыдущем шаге вы включили защиту KATA, в раскрывающемся списке **В случае обнаружения** выберите действие, которое будет применяться к сообщениям:
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Удалить сообщение**.
7. Если вы хотите чтобы по результатам проверки на сервере KATA сообщения с обнаруженными объектами автоматически помещались в Хранилище, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.
8. Если вы хотите, чтобы по результатам проверки приложение добавляло метку в начало темы для сообщений, в которых обнаружены объекты по результатам проверки KATA, укажите текст метки в поле ввода под флажком **Поместить сообщение в Хранилище**.

   По умолчанию добавлена метка *[KATA detect]*.
9. Нажмите на кнопку **Сохранить**.

Защита KATA будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Security для Linux Mail Server, убедитесь, что защита KATA для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

Примеры настройки правил обработки сообщений

В этом разделе приведены примеры настройки правил обработки сообщений для решения задач организации.

- Настройка правил для отправки внешних сообщений только пользователями указанной группы AD

  Для этого создайте следующий набор правил:

  1. Создайте правило обработки исходящих сообщений, отправленных пользователями определенной группы Active Directory.
     a. Установите режим **Использовать параметры модулей проверки**.
     b. В списке отправителей укажите группу пользователей Active Directory, которым разрешена отправка сообщений на внешние почтовые адреса.
     c. В списке получателей укажите значение `*`.
  2. Создайте правило обработки сообщений, которые отправляют друг другу пользователи домена.

     Если такой почтовый трафик не проходит через Kaspersky Security для Linux Mail Server, то пропустите этот шаг.
     a. Установите режим **Использовать параметры модулей проверки**.
     b. В списке отправителей укажите все локальные домены.
     c. В списке получателей укажите все локальные домены.
  3. Создайте правило, которое будет отклонять отправку исходящих сообщений от всех внутренних почтовых доменов компании на любой почтовый адрес.
     a. В зависимости от политики вашей организации установите режим **Отклонять без проверки** или **Удалять без уведомления отправителя**.
     b. В списке отправителей укажите все почтовые домены вашей организации.
     c. В списке получателей укажите значение `*`.

  Для обработки входящих сообщений используется предустановленное правило.

  В результате будут настроены правила обработки сообщений, которые разрешают отправку внешних сообщений пользователям определенной группы Active Directory и запрещают остальным пользователям.

- Настройка правил для отключения фильтрации исходящих сообщений

  Для этого создайте правило со следующими параметрами:

  1. Установите режим **Использовать параметры модулей проверки** и отключите ненужные модули проверки.

В целях информационной безопасности не рекомендуется использовать вместо этого режим **Пропускать без проверки**.

2. В списке отправителей укажите IP-адреса внутренних почтовых серверов или локальные домены, сообщения с которых не нужно проверять.
3. В списке получателей на закладке **Адреса эл. почты** укажите значение `*`.

В результате будет настроено правило, которое отключит фильтрацию исходящих сообщений. При этом входящие сообщения с других доменов будут фильтроваться.

Просмотр информации о правиле

► *Чтобы просмотреть информацию о правиле:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Выберите правило, информацию о котором вы хотите просмотреть.

   Откроется окно **Просмотреть правило**.

Окно содержит следующие разделы:

- **Общие**.
- **Антивирус**.
- **Проверка ссылок**.
- **Анти-Спам**.
- **Анти-Фишинг**.
- **Контентная фильтрация**.
- **Проверка подлинности**.
- **Уведомления**.
- **Предупреждение о небезопасном сообщении**.
- **Примечание к сообщению**.
- **Защита KATA**.

  Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

Включение и отключение правила обработки сообщений

► *Чтобы включить или отключить правило обработки сообщений:*

1. В окне веб-интерфейса приложения 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.

kaspersky

Изменение параметров правила

► *Чтобы изменить параметры правила:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Выберите правило, параметры которого вы хотите изменить.

   Откроется окно **Просмотреть правило**.
3. В нижней части окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Удаление правил обработки сообщений

► *Чтобы удалить правило обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Выберите правило, которое вы хотите удалить.

   Откроется окно **Просмотреть правило**.
3. В нижней части окна нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **ОК**.

Правило обработки сообщений будет удалено.

kaspersky

Списки разрешенных и запрещенных адресов

Списки разрешенных и запрещенных адресов предоставляют возможность более точно настроить реакцию почтовой системы на сообщения с определенных адресов. Например, вы можете добавить в список разрешенных адреса источников, не являющиеся спамом официально, но определяемые приложением как массовые рассылки (к примеру, сообщения с новостных порталов).

Вы можете настроить списки разрешенных и запрещенных адресов следующими способами:

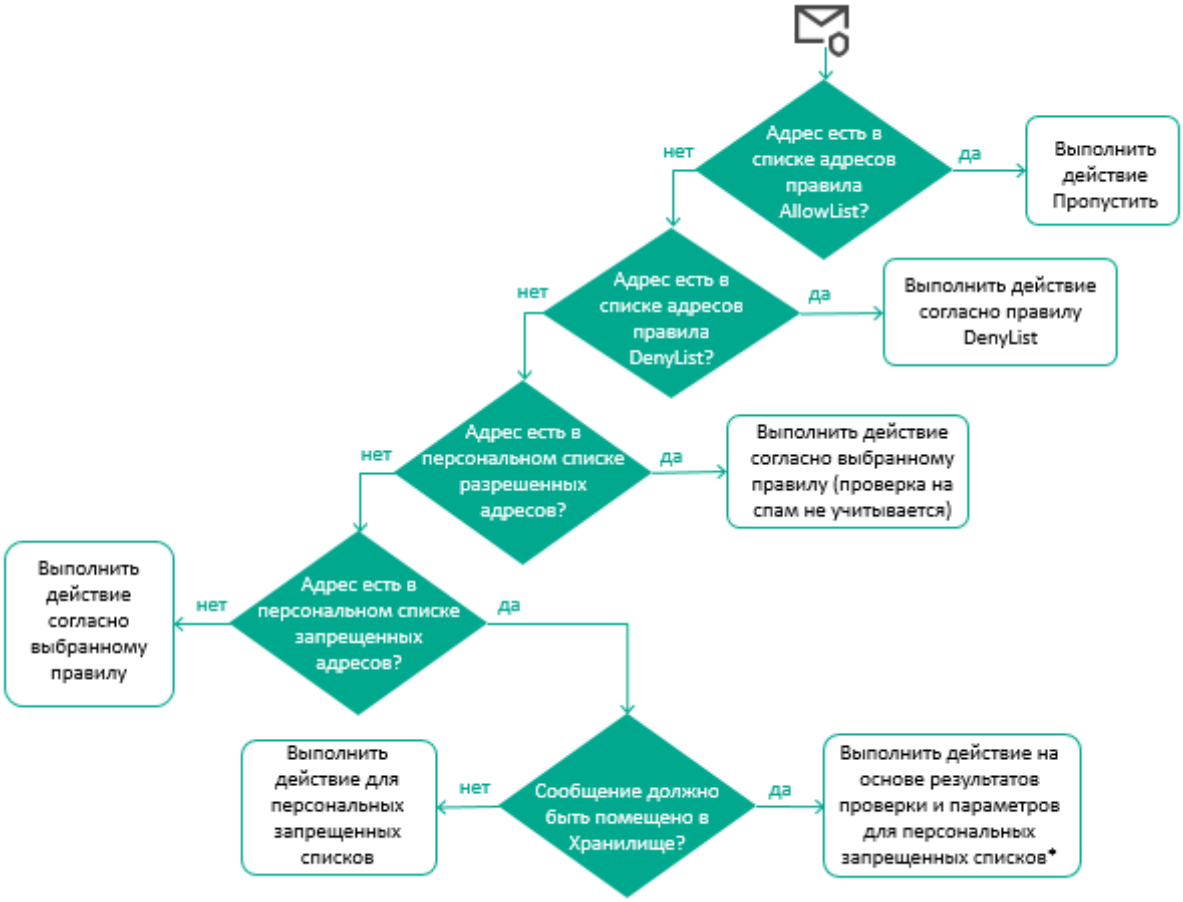
- С помощью предустановленных правил обработки сообщений AllowList и DenyList. Вы также можете создать свои правила с указанием адресов отправителей и получателей, к сообщениям от которых нужно применять заданное действие, и изменить их приоритет.

  По умолчанию правила AllowList и DenyList отключены, и в них не указаны адреса отправителей и получателей. Вам требуется сформировать в этих правилах списки адресов (см. раздел "Изменение параметров правила" на стр. 129) и включить их использование (см. раздел "Включение и отключение правила обработки сообщений" на стр. 128).

- С помощью персональных списков разрешенных и запрещенных адресов, которые содержат адреса отправителей сообщений для одного получателя. Персональный список разрешенных адресов пропускает сообщения без проверки на спам. При этом выполняется проверка на фишинг, вирусы и другие программы, представляющие угрозу, а также выполняется контентная фильтрация.

Алгоритм обработки сообщений согласно спискам разрешенных и запрещенных адресов, установленный по умолчанию, схематически представлен на рисунке ниже. Вы можете изменять действие для правила DenyList (**Отклонить** или **Удалить сообщение**), а также изменять приоритет правил, перемещая правила

AllowList и DenyList в таблице правил. В этом случае алгоритм применения действий приложения будет отличаться от описанного ниже.



Обработка сообщения, адреса отправителя и получателей которого состоят в списке разрешенных или запрещенных адресов в правилах обработки сообщений, выполняется следующим образом:

- Если адреса отправителя и получателей сообщения состоят в списке разрешенных адресов в правиле AllowList, по умолчанию приложение пропускает сообщение без проверки.
- Если адреса не указаны в правиле AllowList, выполняется проверка по списку запрещенных адресов в правиле DenyList. Если адреса отправителя и получателей найдены в списке, по умолчанию приложение отклоняет сообщение, не выполняя проверку. Вы можете изменить действие правила DenyList.

Если сообщение не попадает под действие списков разрешенных и запрещенных адресов в правилах обработки сообщений, то приложение проверяет, находится ли адрес отправителя сообщения в персональных списках получателя:

- Если адрес отправителя содержится в персональном списке разрешенных адресов, то проверка модулем Анти-Спам не выполняется. Сообщение обрабатывается согласно результатам проверки других модулей приложения.
- Если адрес отправителя сообщения не состоит в персональном списке разрешенных адресов получателя этого сообщения, то выполняется проверка по персональному запрещенному списку. В случае совпадения сообщение не доставляется получателю – владельцу персонального списка запрещенных адресов. В зависимости от указанного действия (см. раздел "Настройка параметров

персональных списков" на стр. 132) приложение удаляет или отклоняет сообщение. Также приложение может поместить сообщение в Хранилище.

> * Перед тем, как поместить сообщение в Хранилище, приложение проверяет его с помощью всех модулей защиты. По результатам проверки приложение выполняет над сообщением наиболее строгое действие. Например, если в результате проверки должно быть применено правило, в котором задано действие **Удалить сообщение**, а для персональных запрещенных списков задано действие **Отклонить**, то будет выполнено действие **Удалить сообщение** как более строгое (см. раздел "Работа с правилами обработки сообщений" на стр. 101), т.е. сообщение будет удалено согласно параметрам правила, а не отклонено согласно параметрам для персональных запрещенных списков.
> Сообщения, помещенные в Хранилище, не учитываются при подсчете сообщений со статусом *Персональный список запрещенных адресов* на графиках в разделе **Мониторинг**.

Если адреса не указаны ни в одном из списков ни в правилах обработки сообщений, ни в персональных списках получателя, то сообщение обрабатывается согласно выбранному правилу. Алгоритм выбора правила более подробно описан в главе про работу правил обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 101).

В этом разделе

Настройка параметров персональных списков

> Параметры этого раздела применяются ко всем персональным учетным записям.

► *Чтобы настроить параметры персональных списков разрешенных и запрещенных адресов:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Персональные учетные записи** → **Списки запрещенных и разрешенных адресов**.
2. Включите или отключите отображение и использование списков разрешенных и/или запрещенных адресов с помощью переключателей **Список разрешенных адресов** и **Список запрещенных адресов**.

   > При включении персонального списка разрешенных или запрещенных адресов он становится доступным для просмотра и используется при обработке почтового трафика.

3. В раскрывающемся списке **Если адрес отправителя в списке запрещенных** выберите одно из следующих действий над сообщениями:

- **Удалить сообщение**, если вы хотите удалять сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов.
- **Отклонить**, если вы хотите отклонять сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов.

4. Если вы хотите помещать в Хранилище сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов, установите флажок **Поместить сообщение в Хранилище**.

   По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Параметры персональных списков разрешенных и запрещенных адресов будут настроены.

Просмотр персональных списков разрешенных и запрещенных адресов

Для работы с персональными списками разрешенных и запрещенных адресов из веб-интерфейса приложения необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272).

В режиме привилегированного пользователя вы можете просмотреть персональные списки разрешенных и запрещенных адресов всех пользователей, данные об учетных записях которых сохранены в LDAP-кеше.

В режиме персонального пользователя отображаются только персональные списки текущего пользователя, если администратор включил отображение и использование персональных списков (см. раздел "Настройка параметров персональных списков" на стр. 132) в параметрах приложения.

► *Чтобы просмотреть персональные списки разрешенных и запрещенных адресов в режиме привилегированного пользователя:*

1. Подключитесь к веб-интерфейсу приложения, используя учетную запись привилегированного пользователя (см. раздел "Работа с учетными записями и ролями пользователей" на стр. 158).
2. В окне веб-интерфейса приложения выберите раздел **Пользовательские списки**.
3. В поле ввода укажите имя пользователя в формате distinguishedName в службе каталогов LDAP.

   Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.

4. Нажмите на LDAP-запись пользователя, списки которого вы хотите просмотреть.
5. Нажмите на кнопку **Найти** справа от поля ввода.

В рабочей области отобразятся списки разрешенных и запрещенных адресов выбранного пользователя.

► *Чтобы просмотреть персональные списки разрешенных и запрещенных адресов в режиме персонального пользователя:*

1. Подключитесь к веб-интерфейсу приложения, используя доменные учетные данные пользователя.

2. Выберите раздел **Пользовательские списки**.

В рабочей области отобразятся списки разрешенных и запрещенных адресов текущего пользователя.

Если для учетной записи пользователя обнаружен дубликат в LDAP-кеше, персональные списки разрешенных и запрещенных адресов отправителей перестают применяться для этого пользователя и становятся недоступны в веб-интерфейсе. Следующие данные проверяются на наличие дубликатов:

- Имена пользователей домена.
- Учетные записи пользователей Kerberos.
- Учетные записи пользователей NTLM.
- Адреса электронной почты пользователей домена.

Формирование персональных списков

Для получения доступа к персональным спискам разрешенных и запрещенных адресов из веб-интерфейса приложения необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272).

В режиме привилегированного пользователя вы можете добавлять, изменять и удалять адреса в персональных списках всех пользователей, данные об учетных записях которых сохранены в LDAP-кеше.

В режиме персонального пользователя вы можете просматривать и изменять персональные списки только текущего пользователя.

Регулярные выражения в адресах персональных списков, созданных в предыдущих версиях Kaspersky Security для Linux Mail Server, не работают. Максимальное количество записей в списках разрешенных и запрещенных адресов – 500.

► *Чтобы сформировать персональные списки разрешенных и запрещенных адресов:*

1. Если вы находитесь в режиме привилегированного пользователя, выполните следующие действия:
   a. В окне веб-интерфейса приложения выберите раздел **Пользовательские списки**.
   b. В поле ввода укажите имя пользователя в формате distinguishedName в службе каталогов LDAP.

      Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.

      Если в имени учетной записи LDAP используется специальный символ, при вводе значения следует экранировать специальный символ с помощью символа обратной косой черты ("\"). В противном случае подсказка для записи не будет отображена. Например, имя учетной записи `exa,mple` следует вводить в виде `exa\,mple`. Более подробную информацию и полный список экранируемых символов см. в документации компании Microsoft https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names.
   c. Нажмите на LDAP-запись пользователя, списки которого вы хотите изменить.
   d. Нажмите на кнопку **Найти** справа от поля ввода.

2. Если вы находитесь в режиме персонального пользователя, выберите раздел **Пользовательские списки**.

   В рабочей области отобразятся персональные списки – в левой части список разрешенных адресов, в правой части список запрещенных адресов.

   > Выполните шаги 3-5 для каждого персонального списка.

3. Если вы хотите добавить в персональный список новый адрес, выполните следующие действия:

   - Чтобы указать адрес вручную, нажмите на кнопку **Добавить**, введите адрес электронной почты и нажмите на значок ✓. Кнопка доступна, если формат введенного текста соответствует формату адреса электронной почты.

     При необходимости повторите действия для остальных адресов.

   - Чтобы вставить адреса из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена адреса электронной почты, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.

   Вы можете использовать символы "*" и "?" для создания масок адресов.

   Поддерживается добавление интернационализированных адресов.

4. Если вы хотите изменить ранее добавленный адрес, нажмите на него в поле ввода, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.

5. Если вы хотите удалить адрес из списка, нажмите на значок 🗑 справа от адреса. Чтобы очистить список, нажмите на кнопку **Удалить все**.

6. Нажмите на кнопку **Сохранить**.

   > Если хотя бы один из адресов указан в недопустимом формате, сохранение списков недоступно. Исправьте все адреса, выделенные красным фоном, и повторите операцию сохранения еще раз.

Персональные списки разрешенных и запрещенных адресов будут сформированы.

kaspersky

Управление кластером

После установки и первоначальной настройки вы можете настраивать параметры в веб-интерфейсе приложения. Для этого требуется объединить все узлы с установленным приложением Kaspersky Security для Linux Mail Server в кластер. Вы можете добавлять узлы в кластер (см. раздел "Добавление узла в кластер" на стр. 140) и удалять узлы из кластера (см. раздел "Удаление узла из кластера" на стр. 141). Вы можете назначить роль Управляющего узла любому из узлов, входящих в кластер. Остальные серверы в кластере получат роль Подчиненный узел. Независимо от роли все узлы кластера будут осуществлять обработку трафика.

Все узлы должны быть добавлены в кластер по IP-адресу одинакового формата (только IPv4 или только IPv6).

Таблица узлов кластера отображается в веб-интерфейсе приложения в разделе **Узлы**.

В этом разделе

Создание нового кластера

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

► *Чтобы создать новый кластер:*

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

2. Через несколько минут обновите страницу браузера.

   Откроется веб-интерфейс Управляющего узла.

Кластер будет создан. После этого вы можете добавлять в кластер Подчиненные узлы (см. раздел "Добавление узла в кластер" на стр. 140).

Просмотр таблицы узлов кластера

► *Чтобы просмотреть таблицу узлов кластера,*

в окне веб-интерфейса приложения выберите раздел **Узлы**.

В таблице отображается следующая информация об узлах кластера:

- **IP-адрес:порт** – IP-адрес и порт подключения узла кластера.
- **Роль** – роль узла в кластере.
- **Статус** – информация о наличии проблем на узле.

  При отображении статуса учитывается следующая информация об узле:

  - состояние подключения к серверам KSN/KPSN;
  - статус лицензионного ключа;
  - актуальность баз приложения;
  - дата и время, а также результат выполнения последней задачи обновления;
  - состояние синхронизации времени с Управляющим узлом (для Подчиненных узлов);
  - наличие дубликатов учетных записей и адресов электронной почты пользователей, контактов и групп в домене сервера LDAP.

  Возможны следующие статусы:

  - *Синхронизирован* – на узле нет проблем ни с одним из перечисленных параметров.
  - *Узел недоступен* – нет соединения с узлом (также указывается время, с которого узел стал недоступен).
  - *Невозможно обеспечить отказоустойчивость приложения: нет серверов с ролью Подчиненный узел*.
  - *Отсутствует SPN-идентификатор для службы единого входа Kerberos*.
  - *Требуется перезагрузить операционную систему*.
  - *Данные с контроллера домена устарели или отсутствуют*.

  При наличии ошибок или предупреждений по какому-либо параметру в столбце перечисляются все статусы (например, *Базы устарели, Уровень защиты снижен, Действие лицензии временно приостановлено*).
- **Комментарий** – любая дополнительная информация об узле.

При необходимости вы можете просмотреть детальную информацию (см. раздел "Просмотр информации об узле кластера" на стр. 138) о каждом узле кластера.

kaspersky

Настройка отображения таблицы узлов кластера

► *Чтобы настроить отображение таблицы узлов кластера:*

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

   Откроется таблица узлов кластера.

2. В таблице справа нажмите на кнопку  .

   Откроется меню настройки таблицы узлов кластера.

3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   > Должен быть установлен хотя бы один флажок.

Отображение таблицы узлов кластера будет настроено.

Просмотр информации об узле кластера

► *Чтобы просмотреть информацию об узле кластера:*

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

   Откроется окно с информацией об узле.

Окно содержит следующую информацию в зависимости от типа сервера:

1. Блок параметров **Информация об узле**:
   - **Отпечаток сертификата** – отпечаток сертификата сервера.
   - **Комментарий** – дополнительная информация об узле. Необязательный параметр.
   - **Роль текущего сервера** – роль текущего узла в кластере.
   - **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.
2. Блок параметров **Параметры**:
   - Для Управляющего узла:
     - **Применены** – время последнего успешного применения параметров к модулям приложения.
   - Для Подчиненного узла:
     - **Синхронизирован** – время последнего успешного получения параметров от Управляющего узла. Если параметры получены, вы можете назначить этому Подчиненному узлу роль Управляющего без потери заданных параметров.
     - **Применены** – время последнего успешного применения параметров к модулям приложения.
3. Блок параметров **Информация о базах**:
   - **Обновление баз** – состояние баз приложения, а также результат и время их последнего успешного обновления.

- **Антивирус** – состояние баз модуля Антивирус.
- **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
- **Анти-Спам** – состояние баз модуля Анти-Спам.

Возможны следующие значения:

- *Базы обновлены*.
- *Базы устарели*.
- *Базы сильно устарели*.
- *Ошибка баз*.

4. Блок параметров **Внешние службы**:
   - **Состояние соединения с KSN/KPSN** – состояние соединения со службами KSN / KPSN.
   - **KATA статус** – состояние подключения к серверу KATA (отображается только при настроенной интеграции с KATA).
   - **Состояние keytab-файла Kerberos** – наличие SPN-записей обо всех Подчиненных узлах в keytab-файле (отображается только при включенной Kerberos-аутентификации).
   - Блок параметров **Состояние LDAP** (отображается только при настроенной интеграции с доменом Active Directory):
     - **Подключение** – дата и время последнего успешного подключения к контроллеру домена Active Directory.
     - **Данные для подбора правил** – дата и время последнего успешного обновления данных об учетных записях, используемых для подбора правил обработки трафика.
     - **Автозаполнение учетных записей** – дата и время последнего успешного обновления данных, используемых для автозаполнения имен пользователей в веб-интерфейсе приложения.

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

     Если после успешной синхронизации с доменом Active Directory в учетных записях обнаружены дублирующиеся данные, в таблице узлов кластера и в блоке параметров **Состояние LDAP** отображается предупреждение. Следующие данные проверяются на наличие дубликатов:

     - Имена всех пользователей домена. Для пользователей с дублирующимися именами не работают защита от спуфинга Active Directory и персональные списки разрешенных и запрещенных адресов отправителей, сообщения не помещаются в персональное Хранилище; персональное Хранилище и персональные списки становятся недоступны в приложении.
     - Группы, в которых состоят пользователи домена. Для групп с дублирующимися именами отключена защита от спуфинга Active Directory.
     - Контакты Active Directory. Для контактов с дублирующимися именами отключена защита от спуфинга Active Directory.
     - Учетные записи пользователей Kerberos. Для пользователей с дублирующимися именами Kerberos не работают персональные списки разрешенных и запрещенных адресов отправителей, сообщения не помещаются в персональное Хранилище; персональное Хранилище и персональные списки становятся недоступны в приложении.

- Учетные записи пользователей NTLM. Для пользователей с дублирующимися именами NTLM не работают персональные списки разрешенных и запрещенных адресов отправителей, сообщения не помещаются в персональное Хранилище; персональное Хранилище и персональные списки становятся недоступны в приложении.
- Адреса электронной почты пользователей домена. Сообщения, предназначенные для дублирующихся адресов, не помещаются в персональное Хранилище пользователей, и к таким адресам не применяются персональные списки разрешенных и запрещенных адресов отправителей.

Вы можете сохранить данные дублирующихся учетных записей в файл. Для этого в области предупреждения нажмите на кнопку **Сохранить дубликаты в файле CSV**.

5. Блок параметров **Дата и время** (отображается только для Подчиненных узлов):
   - **Время** – состояние синхронизации времени:
     - с сервером, на котором установлен Управляющий узел;
     - с гипервизором;
     - с NTP-сервером.

   Если статус имеет значение *Ошибка*, вы можете скопировать информацию об ошибке в буфер обмена по кнопке справа от статуса.
6. Блок параметров **Информация о лицензии**:
   - **Дата окончания срока действия лицензии**.
   - **Лицензия** – информация о состоянии лицензионного ключа (для активного лицензионного ключа указывается также дата окончания срока действия и количество дней до его истечения).
   - **Приложение** – название приложения, для которой предназначен добавленный лицензионный ключ.
   - **Уровень функциональности** – режим работы приложения в зависимости от добавленного лицензионного ключа.
   - **Тип лицензии** – тип лицензии (пробная, коммерческая или подписочная).
   - **Серийный номер** – серийный номер лицензионного ключа.

Добавление узла в кластер

► *Чтобы добавить узел в кластер:*

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

   Откроется окно **Добавить узел**.
3. В поля **IP-адрес** и **Порт** введите IP-адрес и порт сервера с установленным приложением, который вы хотите добавить в качестве узла кластера.
4. Если требуется, в поле **Комментарий** укажите дополнительную информацию о добавляемом узле.
5. В поле **Количество потоков проверки** укажите, сколько потоков трафика может обрабатывать почтовый сервер одновременно.

   Значение по умолчанию – 16.

6. Нажмите на кнопку **Далее**.
7. Сравните отпечаток сертификата в окне **Проверка узла** с отпечатком сертификата сервера. Если отпечатки сертификата совпадают, нажмите на кнопку **Подтвердить**.

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

Прежде чем направить на добавленный узел почтовый трафик, требуется обновить базы приложения (см. раздел "Запуск обновления баз вручную" на стр. 260) и выполнить LDAP-синхронизацию (см. раздел "Запуск синхронизации с контроллером домена Active Directory вручную" на стр. 275). В противном случае приложение не сможет обеспечить должный уровень защиты, не сможет помещать сообщения электронной почты в Персональное Хранилище, а правила, в которых указаны атрибуты учетных записей Active Directory, не будут применены.

Изменение параметров узла

Вы можете изменить IP-адрес и порт сервера, на котором установлено приложение, с помощью скрипта изменения сетевых параметров узла кластера (см. раздел "Изменение сетевых параметров узла кластера" на стр. 151).

► *Чтобы изменить параметры узла:*

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

   Откроется окно параметров узла.
3. В нижней части окна нажмите на кнопку **Изменить**.

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

     Рекомендуемое значение: количество ядер процессора, умноженное на два.
5. Нажмите на кнопку **Сохранить**.

Параметры узла будут изменены.

Удаление узла из кластера

Удаление Управляющего узла недоступно.

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

► *Чтобы удалить узел из кластера:*

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

   Откроется окно параметров узла.
3. В нижней части окна нажмите на кнопку **Удалить**.

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

Узел будет удален из кластера. Информация об узле не будет отображаться в таблице узлов кластера. Объекты, помещенные на карантин, объекты Хранилища, обновления баз, журналы событий, отчеты, а также полученная диагностическая информация сохраняются на сервере с установленным приложением.

Изменение роли узла в кластере

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

► *Чтобы назначить Управляющему узлу роль Подчиненный узел:*

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

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

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

► *Чтобы назначить Подчиненному узлу роль Управляющий узел:*

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

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

   В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль привилегированного пользователя приложения.

   Откроется веб-интерфейс Подчиненного узла.
5. Нажмите на кнопку **Изменить роль на Управляющий узел**.

6. В окне подтверждения нажмите на кнопку **ОК**.

Подчиненный узел станет Управляющим узлом.

Удаление кластера

Удаление кластера возможно только при отсутствии Подчиненных узлов.

► *Чтобы удалить кластер:*

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

   Откроется окно параметров узла.
3. В нижней части окна нажмите на кнопку **Удалить кластер**.

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

Кластер будет удален. Отобразится веб-интерфейс сервера с установленным приложением, не входящего в кластер.

Управление SSL-сертификатом узла кластера

По умолчанию Kaspersky Security для Linux Mail Server в качестве SSL-сертификата узла кластера использует самоподписанный сертификат, который генерируется автоматически при развертывании узла кластера. При входе в веб-интерфейс приложения с этим сертификатом в браузере отображается предупреждение о том, что соединение небезопасно. Для повышения удобства и безопасности при работе в веб-интерфейсе приложения вы можете заменить сертификат узла, который используется по умолчанию, на сертификат, выписанный доверенным центром сертификации.

Для замены SSL-сертификата узла кластера вам потребуются следующие файлы:

- Файл сертификата формата X.509 с расширением PEM или файл-контейнер с цепочкой сертификатов формата X.509 с расширением PEM.
- Файл приватного ключа RSA с расширением PEM (без парольной фразы).

Вы можете подготовить файл приватного ключа и сертификат для подписи самостоятельно или можете получить готовые файлы от удостоверяющего центра.

Этапы замены SSL-сертификата узла кластера при самостоятельном создании файлов приватного ключа и сертификата

1. **Создание файла приватного ключа и запроса на подпись сертификата (Certificate Signing Request) (см. раздел "Создание файла запроса на подпись SSL-сертификата" на стр. 144)**

   Вы получите от удостоверяющего центра один из следующих файлов:

- файл подписанного сертификата формата X.509 с расширением CER или CRT;
- файл цепочки сертификатов в формате PKCS#7 с расширением P7B. Файл включает подписанный по вашему запросу сертификат сайта и сертификаты промежуточных центров сертификации.

2. **Конвертация полученных файлов в PEM-кодировку**

   В зависимости от типа файла, полученного на предыдущем этапе, следует выполнить одно из следующих действий:

   - Конвертировать сертификат из кодировки DER в PEM-кодировку (см. раздел "Конвертация сертификата из кодировки DER в PEM-кодировку" на стр. 146).
   - Извлечь цепочку сертификатов из контейнера PKCS#7 (см. раздел "Извлечение цепочки сертификатов из контейнера PKCS#7" на стр. 146).

3. **Замена SSL-сертификата узла кластера (на стр. 147)**

Этапы замены SSL-сертификата узла кластера при предоставлении файлов приватного ключа и сертификата удостоверяющим центром

1. **Получение файлов приватного ключа и сертификата от удостоверяющего центра**

   Приватный ключ и сертификат предоставляются в виде PFX-контейнера (формат PKCS#12, файл с расширением PFX или P12).

   Если в качестве удостоверяющего центра в вашей организации используется стандартная служба Active Directory Certification Services, следует использовать шаблон **Web Server** для создания сертификата. Вам нужно сохранить результат в виде цепочки сертификатов (certificate chain) в DER-кодировке.

2. **Извлечение файлов сертификата и приватного ключа из PFX-контейнера (на стр. 147)**
3. **Замена SSL-сертификата узла кластера (на стр. 147)**

Создание файла запроса на подпись SSL-сертификата

Вы можете создать файл запроса на подпись сертификата (Certificate Signing Request) самостоятельно с помощью утилиты *openssl* или воспользоваться онлайн-сервисами.

► *Чтобы создать файл запроса на выписку сертификата самостоятельно с помощью утилиты openssl:*

1. Подготовьте текстовый файл request.config следующего содержания (примеры параметров см. в таблице ниже):

```
[req]
default_bits=2048
prompt=no
default_md=sha256
req_extensions=req_ext
distinguished_name=dn
[dn]
```

```
C=<двухбуквенный код страны>
ST=<регион>
L=<город>
O=<название организации>
OU=<название отдела организации>
emailAddress=<адрес электронной почты администратора>
CN=<доменное имя управляющего узла кластера>
[req_ext]
subjectAltName=@alt_names
[alt_names]
DNS.1=<доменное имя управляющего узла кластера>
DNS.2=<доменное имя подчиненного узла кластера>
DNS.3=<доменное имя подчиненного узла кластера>
```

2. Создайте приватный ключ RSA с расширением PEM (без парольной фразы) с помощью команды:

   ```
   openssl genrsa -out key.pem 2048
   ```

3. Создайте файл запроса на подпись сертификата с помощью команды:

   ```
   openssl req -new -sha256 -key key.pem -out request.csr -config
   request.config
   ```

В результате будут созданы следующие файлы:

- key.pem – файл приватного ключа RSA с расширением PEM. Вам нужно сохранить этот файл, чтобы использовать его для замены сертификата на узле кластера (см. раздел "Замена SSL-сертификата узла кластера" на стр. 147).
- request.csr – файл запроса на подпись сертификата в формате PKCS#10. Вам нужно передать этот файл в удостоверяющий центр.

Примеры параметров конфигурационного файла request.config

Параметр	Пример
C	RU
ST	Moscow
L	Moscow
O	Organization name
OU	IT department
emailAddress	administrator@example.com
CN	klms01.example.com
DNS.1	klms01.example.com
DNS.<номер>	klms<номер>.example.com

Конвертация сертификата из кодировки DER в PEM-кодировку

После выполнения запроса на выписку сертификата удостоверяющий центр может предоставить подписанный сертификат в формате X.509 (файл с расширением CER или CRT).

Файл сертификата в формате X.509 может быть представлен в двух кодировках:

- DER encoded (DER-кодировка).
- Base64 encoded (PEM-кодировка).

Если сертификат представлен в DER-кодировке, необходимо конвертировать его в кодировку PEM. Конвертацию можно выполнить с помощью утилиты *openssl*.

► *Чтобы конвертировать сертификат из кодировки DER в PEM-кодировку, используйте команду:*

```
openssl x509 -in source.cer -inform DER -out cert.pem
```

Полученный файл cert.pem можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера" на стр. 147).

Извлечение цепочки сертификатов из контейнера PKCS#7

После выполнения запроса на выписку сертификата удостоверяющий центр может предоставить цепочку сертификатов в формате PKCS#7 (файл с расширением P7B). Цепочка включает подписанный по вашему запросу сертификат сайта, а также сертификаты промежуточных центров сертификации.

Файл в формате PKCS#7 может быть представлен в двух кодировках:

- DER encoded (DER-кодировка).
- Base64 encoded (PEM-кодировка).

Для дальнейшего использования необходимо извлечь сертификаты из контейнера и получить файл в кодировке PEM. Конвертацию можно выполнить с помощью утилиты *openssl*.

Чтобы конвертировать файл формата PKCS#7 в DER-кодировке, используйте команду:

```
openssl pkcs7 -in source.p7b -inform DER -print_certs -out cert.pem
```

Чтобы конвертировать файл формата PKCS#7 в PEM-кодировке, используйте команду:

```
openssl pkcs7 -in source.p7b -inform PEM -print_certs -out cert.pem
```

Полученный файл cert.pem можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера" на стр. 147).

Извлечение файлов сертификата и приватного ключа из PFX-контейнера

Если удостоверяющий центр предоставил сертификат в форме PFX-контейнера (формат PKCS#12, файл с расширением PFX или P12), необходимо самостоятельно извлечь из него файлы сертификата и приватного ключа в PEM-кодировке.

Извлечение файлов сертификата и приватного ключа можно выполнить с помощью утилиты *openssl.* В процессе извлечения файлов потребуется ввести парольную фразу от PFX-контейнера.

Чтобы извлечь файл приватного ключа, используйте команду:

```
openssl pkcs12 -in source.pfx -nocerts -nodes -out key.pem
```

Чтобы извлечь файл сертификата, используйте команду:

```
openssl pkcs12 -in source.pfx -clcerts -nokeys -out cert.pem
```

В результате вы получите следующие файлы:

- key.pem – файл приватного ключа RSA в PEM-кодировке (без парольной фразы);
- cert.pem – файл сертификата формата X.509 в PEM-кодировке.

Полученные файлы приватного ключа и сертификата можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера" на стр. 147).

Замена SSL-сертификата узла кластера

► *Чтобы заменить SSL-сертификат узла кластера:*

1. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Поместите файлы сертификата (cert.pem) и приватного ключа (key.pem) в директорию `/root`.
3. Перейдите в директорию с конфигурационными файлами веб-сервера с помощью команды:

   ```
   cd /var/opt/kaspersky/klms/certs
   ```

4. Создайте резервные копии файлов действующего сертификата и приватного ключа с помощью команд:

```
cp -p webapi.crt webapi.crt.backup
cp -p webapi.key webapi.key.backup
cp -p webapi-with-dhparam.crt webapi-with-dhparam.crt.backup
```

5. Замените содержимое файлов сертификата и приватного ключа с помощью команд:

   ```
   cat /root/cert.pem > webapi.crt
   cat /root/key.pem > webapi.key
   ```

6. Сгенерируйте параметры DH с помощью команды:

   ```
   openssl dhparam -out dhparam-webapi.pem 4096
   ```

   > Генерация параметров DH может занять 10–20 минут. Дождитесь окончания выполнения операции.

7. Добавьте параметры DH к сертификату с помощью команды:

   ```
   cat webapi.crt dhparam-webapi.pem > webapi-with-dhparam.crt
   ```

8. Укажите владельца сертификата и права доступа к приватному ключу сертификата с помощью команд:

   ```
   chown root:root webapi.crt
   chmod 644 webapi.crt
   chown kluser:root webapi.key
   chmod 600 webapi.key
   chown root:root dhparam-webapi.pem
   chmod 644 dhparam-webapi.pem
   chown root:root webapi-with-dhparam.crt
   chmod 644 webapi-with-dhparam.crt
   ```

9. Перезапустите сервис Apache с помощью команды:

   ```
   systemctl restart apache2
   ```

10. Проверьте статус сервиса Apache с помощью команды:

    ```
    systemctl status apache2
    ```

    Для сервиса должен быть актуален статус `running`.

11. Откройте в браузере веб-интерфейс узла кластера. В случае успешной замены сертификата предупреждение о небезопасном соединении не отображается.

12. Если замена завершилась успешно, удалите исходные файлы сертификата и приватного ключа из директории `/root` с помощью команды:

    ```
    rm -f /root/cert.pem /root/key.pem
    ```

Замена SSL-сертификата узла кластера будет завершена. Если вы хотите заменить сертификат на нескольких узлах кластера, вам требуется выполнить шаги инструкции на каждом узле.

kaspersky

Проверка целостности данных

Проверка целостности модулей приложения запускается автоматически после старта приложения на узле кластера. Это позволяет убедиться, что компоненты приложения установлены корректно, не изменены и не повреждены.

Вы можете в любой момент запустить проверку целостности данных (см. раздел "Запуск проверки целостности вручную" на стр. 150) вручную. Проверка запускается для каждого узла кластера отдельно. При этом проверяются хеши исполняемых файлов приложения по алгоритму ГОСТ Р 34.11-2012.

Вы можете посмотреть результаты запущенных вручную проверок (см. раздел "Просмотр информации о задачах проверки целостности" на стр. 149) в сводной таблице по узлам кластера.

Если в результате проверки не было выявлено нарушений целостности, в окне просмотра результатов отобразится сообщение об этом. Если нарушения целостности обнаружены, вы сможете скачать архив со списком найденных проблем (см. раздел "Скачивание архива с результатом проверки" на стр. 150).

Информация о выполнении проверки целостности записывается в журнал событий (см. раздел "Типы событий приложения" на стр. 215) и в журнал Syslog.

В этом разделе

Просмотр информации о задачах проверки целостности

► *Чтобы просмотреть информацию о последних задачах проверки целостности, выполненных на всех узлах кластера:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.

Отобразится таблица с информацией о последних выполненных задачах проверки целостности на узлах кластера:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу, для которого была запущена проверка целостности.
- **Роль** – роль узла в кластере.
- **Статус последней задачи**:

  Прочерк, если проверка целостности ни разу не была запущена.

  - *В обработке* (с указанием процента выполнения задачи).
  - *Выполняется отмена*.
  - *Выполняется удаление*.

- *Завершено* (с указанием времени завершения задачи).
- *Завершено с ошибкой* (с указанием времени завершения задачи и описания ошибки).
- *Ожидает*.

- **Результат проверки целостности данных**:
  - *Завершено с ошибкой* – задача выполнена, в результате обнаружены нарушения целостности данных.
  - *Успешно* – задача выполнена, в результате нарушения целостности данных не обнаружены.

► *Чтобы просмотреть информацию обо всех задачах проверки целостности, выполненных на одном узле кластера:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. Выберите узел кластера, информацию о задачах которого вы хотите просмотреть.

Откроется окно **Просмотреть результаты**. В окне отображается таблица с информацией о дате запуска и результате всех задач проверки, успешно выполненных на выбранном узле.

Запуск проверки целостности вручную

► *Чтобы запустить проверку целостности вручную:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите запустить проверку целостности.

   Откроется окно **Просмотреть результаты**.
4. В нижней части окна нажмите на кнопку **Запустить**.

Проверка целостности будет запущена.

Статус выполнения задачи отобразится в окне **Просмотреть результаты**, а также в таблице узлов кластера на странице **Проверка целостности данных**. Если будут выявлены нарушения целостности модулей приложения, вы сможете скачать архив со списком найденных проблем (см. раздел "Скачивание архива с результатом проверки" на стр. 150).

Скачивание архива с результатом проверки

Архив с результатом проверки доступен для скачивания, только если были обнаружены нарушения целостности модулей. Если нарушений не обнаружено, отображается только сообщение об успешной проверке.

► *Чтобы скачать архив с результатом проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите скачать архив с результатом проверки.

   Откроется окно **Просмотреть результаты**.
4. В строке с нужным архивом нажмите на значок справа от названия архива.

Архив будет сохранен на вашем компьютере в папке загрузки браузера.

Удаление архива с результатом проверки

► *Чтобы удалить архив с результатом проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите удалить архив с результатом проверки.

   Откроется окно **Просмотреть результаты**.
4. В строке с нужным архивом нажмите на значок справа от названия архива.

Архив будет удален из списка.

Изменение сетевых параметров узла кластера

В этом разделе содержатся инструкции по изменению сетевых параметров узла кластера Kaspersky Security для Linux Mail Server, а также описаны предварительные и заключительные действия, обязательные для корректного выполнения изменений.

В этом разделе справки

Порядок изменения сетевых параметров узла кластера

IP-адрес и номер порта, которые приложение Kaspersky Security для Linux Mail Server использует для межмашинного взаимодействия в кластере, указываются при первоначальной настройке приложения (см.

раздел "Шаг 5. Ввод параметров узла" на стр. 66). Если вам нужно изменить IP-адрес сервера, на котором установлено приложение, после изменения сетевых настроек операционной системы потребуется выполнить процедуру изменения IP-адреса узла кластера. Эту же процедуру потребуется выполнить, если нужно изменить номер порта, используемого для межмашинного взаимодействия в кластере.

Изменение номера порта для веб-интерфейса не влияет на работу остальных узлов и всего кластера и выполняется отдельно от изменения IP-адреса и номера порта для межмашинного взаимодействия (см. раздел "Изменение номера порта для веб-интерфейса" на стр. 156).

Чтобы сохранить целостность и управляемость кластера Kaspersky Security для Linux Mail Server, нужно менять адреса узлов в определенном порядке. Последовательность действий зависит от количества узлов в кластере и от того, скольким из них планируется изменить адреса. Возможны следующие варианты:

- Требуется изменить адреса части узлов в кластере (см. раздел "Сценарий изменения сетевых параметров части узлов" на стр. 152).
- Требуется изменить адреса всех узлов в кластере (см. раздел "Сценарий изменения сетевых параметров всех узлов" на стр. 153). Этот сценарий также используется в случае, если кластер состоит из одного узла.

В этом разделе справки

Сценарий изменения сетевых параметров части узлов

Администратору требуется обеспечить сетевую связность между узлами с новыми и старыми адресами.

Сценарий изменения сетевых параметров части узлов кластера состоит из следующих этапов:

1. **Изменение роли узла с Управляющего на Подчиненный (см. раздел "Изменение роли узла в кластере" на стр. 142)**

   Этот этап нужно выполнить, если в число узлов, адреса которых планируется изменить, входит Управляющий узел. Временно назначьте роль Управляющего тому узлу, адрес которого менять не планируется.

2. **Отключение обработки почтового трафика на выбранных узлах**

   Если используется балансировщик нагрузки для почтового трафика, в параметрах балансировщика отключите нагрузку на узлы, адреса которых планируете менять. Если балансировщика нагрузки нет, отключите прием почтовых сообщения средствами почтового сервера или межсетевого экрана.

   После отключения нагрузки нужно дождаться, когда на выбранных узлах будут отправлены сообщения из всех очередей.

3. **Изменение адресов Подчиненных узлов**

Последовательно измените адреса выбранных Подчиненных узлов. Для этого для каждого узла выполните следующие действия:

a. Измените сетевые настройки средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов.

b. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 155).

   Этот шаг позволяет убедиться, что новые сетевые параметры были применены.

c. Измените A- и PTR-записи на DNS-сервере для Подчиненного узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

   Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 333) и для успешного взаимодействия с другими почтовыми системами.

d. Измените адрес узла для межмашинного взаимодействия (см. раздел "Изменение адреса узла в Kaspersky Security для Linux Mail Server" на стр. 155).

   Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.

4. **Замена Подчиненных узлов со старыми адресами на Подчиненные узлы с новыми адресами в кластере через веб-интерфейс приложения**

   Узлы, на которых был изменен адрес, нужно удалить из кластера (см. раздел "Удаление узла из кластера" на стр. 141), затем эти узлы с новыми адресами нужно добавить в кластер (см. раздел "Добавление узла в кластер" на стр. 140).

5. **Изменение роли узла с Подчиненного на Управляющий (см. раздел "Изменение роли узла в кластере" на стр. 142)**

   Этот шаг нужно выполнить, если роль Управляющего узла была временно назначена другому узлу.

6. **Проверка доступности и работоспособности всех узлов кластера**

   Вы можете просмотреть статусы узлов кластера (см. раздел "Просмотр таблицы узлов кластера" на стр. 137) в веб-интерфейсе Управляющего узла.

7. **Включение обработки почтового трафика на узлах**

   Последовательно введите узлы кластера в обработку почтового трафика под их новыми адресами. Убедитесь, что обработка трафика происходит без ошибок.

Сценарий изменения сетевых параметров всех узлов

Сценарий изменения сетевых параметров всех узлов кластера состоит из следующих этапов:

1. **Отключение обработки почтового трафика на всех узлах кластера**

   Если используется балансировщик нагрузки для почтового трафика, отключите нагрузку на узлы в параметрах балансировщика. Если балансировщика нагрузки нет, отключите прием почтовых сообщений средствами почтового сервера или межсетевого экрана.

   После отключения нагрузки нужно дождаться, когда на узлах будут отправлены сообщения из всех очередей.

2. **Изменение адреса Управляющего узла**

   Для этого на Управляющем узле выполните следующие действия:

a. Измените сетевые настройки средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов.

b. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 155).

   Этот шаг позволяет убедиться, что новые сетевые параметры были применены.

c. Измените A- и PTR-записи на DNS-сервере для Управляющего узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

   Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 333) и для успешного взаимодействия с другими почтовыми системами.

d. Измените адрес узла для межмашинного взаимодействия.

   Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.

3. **Удаление Подчиненных узлов из кластера (см. раздел "Удаление узла из кластера" на стр. 141)**

   Нужно войти в веб-интерфейс по новому адресу Управляющего узла и удалить все Подчиненные узлы из кластера.

   Если узел в кластере один, то пропустите этот этап и перейдите к этапу 6.

4. **Изменение адресов Подчиненных узлов**

   Последовательно измените адреса всех Подчиненных узлов. Для этого для каждого узла выполните следующие действия:

   a. Измените сетевые настройки средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов.

   b. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 155).

      Этот шаг позволяет убедиться, что новые сетевые параметры были применены.

   c. Измените A- и PTR-записи на DNS-сервере для Подчиненного узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

      Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 333) и для успешного взаимодействия с другими почтовыми системами.

   d. Измените адрес узла для межмашинного взаимодействия (см. раздел "Изменение адреса узла в Kaspersky Security для Linux Mail Server" на стр. 155).

      Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.

5. **Добавление Подчиненных узлов в кластер (см. раздел "Добавление узла в кластер" на стр. 140)**

   Нужно войти в веб-интерфейс по новому адресу Управляющего узла и добавить в кластер Подчиненные узлы с новыми адресами.

6. **Проверка доступности и работоспособности всех узлов кластера**

Вы можете просмотреть статусы узлов кластера (см. раздел "Просмотр таблицы узлов кластера" на стр. 137) в веб-интерфейсе Управляющего узла.

7. **Включение обработки почтового трафика на узлах**

   Последовательно включите прием сообщений на узлах кластера под их новыми адресами. Убедитесь, что обработка трафика происходит без ошибок.

Проверка сетевых параметров операционной системы узла

Перед изменением адреса узла в приложении Kaspersky Security для Linux Mail Server рекомендуется проверить, что были применены новые сетевые параметры операционной системы.

► *Чтобы проверить сетевые параметры операционной системы узла кластера:*

1. Выполните следующие команды:
   - Для проверки параметров сетевых адаптеров:

     ```
     ip address
     ```

   - Для проверки маршрута по умолчанию и статического маршрута:

     ```
     ip route
     ```

   - Для проверки параметров DNS-сервера:

     ```
     cat /etc/resolv.conf
     ```

2. Проверьте, что на DNS-сервере существует запись для нового доменного имени узла, с помощью команды:

   ```
   host <доменное имя узла>
   ```

   > Если для доменного имени узла не найдена запись на DNS-сервере, проверьте правильность указанных сетевых параметров. При необходимости измените сетевые параметры операционной системы.

3. При необходимости измените доменное имя узла с помощью команды:

   ```
   hostnamectl set-hostname <новое доменное имя узла>
   ```

4. Убедитесь, что новое доменное имя назначено узлу, с помощью команды:

   ```
   hostnamectl status
   ```

   В ответе отобразится строка `static hostname` с назначенным доменным именем узла кластера.

Сетевые параметры операционной системы узла будут проверены.

Изменение адреса узла в Kaspersky Security для Linux Mail Server

> Перед изменением адреса узла в приложении Kaspersky Security для Linux Mail Server рекомендуется проверить, что были применены новые сетевые параметры операционной системы были применены (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 155).

► *Чтобы изменить IP-адрес или порт узла кластера:*

1. Запустите мастер изменения сетевых параметров узла кластера с помощью команды:

   ```
   /opt/kaspersky/klms/bin/setup.py --update-address
   ```

2. Укажите следующие ответы на вопросы мастера:
   - Для вопроса **Before changing network settings of a cluster node, you must ensure network connectivity between nodes with new and old addresses. Continue?** укажите ответ `yes`.
   - Для вопроса **Specify IP address of the current node** укажите новый IP-адрес, который будет использоваться для межмашинного взаимодействия.

     Если менять IP-адрес не требуется, нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node** укажите новый номер порта, который будет использоваться для межмашинного взаимодействия.

     Если менять IP-адрес не требуется, нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node for web interface** нажмите на клавишу **ENTER**.

     Номер порта для веб-интерфейса следует менять отдельно, см. инструкцию в разделе Изменение номера порта для-интерфейса (см. раздел "Изменение номера порта для веб-интерфейса" на стр. 156).
3. После завершения работы мастера и перезапуска всех служб перезагрузите узел кластера с помощью команды:

   ```
   shutdown -r
   ```

Адрес узла кластера будет изменен. Перейдите к настройке узлов кластера Kaspersky Security для Linux Mail Server в веб-интерфейсе (см. раздел "Порядок изменения сетевых параметров узла кластера" на стр. 151).

Изменение номера порта для веб-интерфейса

Вы можете изменить номер порта для веб-интерфейса Управляющего или Подчиненного узла кластера. Изменение номера порта для веб-интерфейса отдельного узла не влияет на работу других узлов и всего кластера.

► *Чтобы изменить порт для веб-интерфейса узла кластера:*

1. Запустите мастер изменения сетевых параметров узла кластера с помощью команды:

   ```
   /opt/kaspersky/klms/bin/setup.py --update-address
   ```
2. Укажите следующие ответы на вопросы мастера:
   - Для вопроса **Before changing network settings of a cluster node, you must ensure network connectivity between nodes with new and old addresses. Continue?** укажите ответ `yes`.
   - Для вопроса **Specify IP address of the current node** нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node** нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node for web interface** укажите новый номер порта для веб-интерфейса и нажмите на клавишу **ENTER**.

После завершения работы мастера и перезапуска всех служб веб-интерфейс узла кластера будет готов к использованию на новом порте.

Вы можете проверить доступность веб-интерфейса по адресу `https://<IP-адрес или полное доменное имя (FQDN) Управляющего узла>:<новый порт подключения к веб-интерфейсу>`.

kaspersky

Работа с учетными записями и ролями пользователей

Для того чтобы управлять разрешениями пользователей в приложении, вы можете создавать учетные записи пользователей и назначать им роли.

Роль – это заранее определенный набор прав доступа к функциям консоли управления Kaspersky Security для Linux Mail Server. Роль можно назначить пользователю или группе пользователей. Пользователи приложения, для которых создана учетная запись и которым назначена хотя бы одна роль, называются *привилегированными пользователями*. Подробнее см. Режимы просмотра веб-интерфейса приложения.

Список учетных записей привилегированных пользователей и список ролей, доступных в приложении, отображаются в разделе **Учетные записи и роли** веб-интерфейса приложения.

Kaspersky Security для Linux Mail Server поддерживает создание 100 учетных записей и 100 ролей.

Учетные записи

Вы можете создавать учетные записи (см. раздел "Создание учетной записи" на стр. 158) следующих типов:

- SSO.

  Тип доступен для всех пользователей домена Active Directory, для которого настроена аутентификация с помощью технологии единого входа (SSO) (см. раздел "Аутентификация с помощью технологии единого входа" на стр. 330).

- Локальный.

  Тип доступен для любого пользователя приложения.

В приложении есть предопределенная учетная запись Administrator, всегда обладающая максимальным набором прав. Эту учетную запись нельзя изменить или удалить. Вы можете использовать эту учетную запись для изменения конфигурации продукта в аварийных ситуациях.

Роли

Вы можете создавать роли (см. раздел "Создание роли" на стр. 163) для учетных записей пользователей приложения в зависимости от разрешений, которыми они должны обладать. Разрешения роли настраиваются в соответствии с типовыми задачами и служебными обязанностями пользователей.

В приложении доступны предопределенные роли:

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

Удаление и изменение предопределенных ролей недоступно.

Создание учетной записи

► *Чтобы создать учетную запись пользователя Kaspersky Security для Linux Mail Server:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.

2. Нажмите на кнопку **Создать учетную запись**.

   Откроется окно создания учетной записи.

3. В поле **Тип** выберите тип учетной записи:

   - **Локальный пользователь**
   - **SSO-пользователь**

4. Если вы выбрали тип учетной записи **Локальный пользователь**, укажите следующие данные:

   a. В поле **Логин** введите логин учетной записи.

      Логин чувствителен к регистру. Максимальная длина логина – 128 символов.

   b. В поле **Пароль** укажите пароль учетной записи.

      Пароль должен содержать строчные и прописные буквы латинского алфавита (A–z), цифры (0–9) и специальные символы. Длина пароля должна быть не менее 15 символов.

      Чтобы просмотреть введенный пароль, нажмите на значок  и удерживайте его нужное вам время.

   c. В поле **Подтвердите пароль** повторно введите пароль.

      Перед сохранением учетной записи скопируйте пароль, чтобы передать его пользователю. Вам необходимо самостоятельно обеспечить безопасный канал и способ доставки пароля. Пароль локальной учетной записи (в том числе учетной записи Administrator) действует в течение одного года. После истечения срока действия пароля при попытке входа в веб-интерфейс приложения отобразится запрос на смену пароля. Аутентификация локального пользователя будет возможна только после смены пароля.

      После сохранения учетной записи пароль станет недоступен для просмотра. Kaspersky Security для Linux Mail Server хранит только хеш пароля, но не сам пароль.

   d. Если вы хотите, чтобы пользователь сменил пароль после первой авторизации в приложении, установите флажок **Пользователь должен изменить пароль при следующем входе в систему**.

5. Если вы выбрали тип учетной записи **SSO-пользователь**, в поле **Логин** введите логин SSO-пользователя. Формат логина: `домен\имя пользователя` для NTLM-аутентификации или `user@REALM` для Kerberos-аутентификации. Логин чувствителен к регистру.

   При вводе значения отображается подсказка с учетными записями из LDAP-кеша, которые содержат указанные символы.

   Если в LDAP-кеше совпадение не найдено, вы можете ввести произвольное значение.

6. В раскрывающемся списке **Роль** выберите одну или несколько ролей для учетной записи.

   Выбранные роли отобразятся в строке.

   Чтобы удалить роль из списка выбранных, справа от названия роли нажмите на значок  .
   Чтобы очистить список выбранных ролей, нажмите на значок  .

   Если в раскрывающемся списке нет нужной роли, вы можете ее создать (см. раздел "Создание роли" на стр. 163) по ссылке **Создать роль** внизу раскрывающегося списка, а затем назначить пользователю.

7. В поле **Описание** введите любую поясняющую информацию, например обоснование назначенной роли или имя сотрудника, для которого создана учетная запись. Максимальная длина текста 512 символов.
8. Нажмите на кнопку **Создать**.

Учетная запись пользователя будет создана и отобразится в таблице учетных записей на вкладке **Учетные записи**.

Просмотр учетной записи

► *Чтобы просмотреть информацию об учетной записи:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.

   По умолчанию таблица учетных записей отсортирована по дате создания: наверху таблицы отображается последняя созданная запись.

   Вы можете сортировать учетные записи по столбцам **Логин**, **Тип учетной записи**, **Описание**.

   Столбцы сортируются в алфавитном порядке. С помощью значка  в заголовке столбца можно изменять порядок сортировки по возрастанию или по убыванию. Третье нажатие на значок сортировки сбрасывает сортировку столбца.
2. В таблице выберите учетную запись, информацию о которой вы хотите просмотреть.

Откроется окно просмотра учетной записи со следующей информацией:

- Тип
- Логин
- Роль
- Описание

Вы можете фильтровать таблицу учетных записей (см. раздел "Фильтрация учетных записей" на стр. 160).

Фильтрация учетных записей

Для поиска нужных записей вы можете отфильтровать таблицу учетных записей.

► *Чтобы отфильтровать таблицу учетных записей:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. Нажмите на значок  .

   Отобразится окно добавления фильтра.
3. Нажмите на кнопку **Добавить фильтр**.

4. В появившемся поле укажите нужный фильтр:
   - **Тип учетной записи**.
   - **Роли пользователей**.

     Вы можете выбрать несколько ролей. В отфильтрованной таблице отобразятся учетные записи хотя бы с одной из указанных ролей.

   Если вы хотите добавить второй фильтр, нажмите на кнопку **Добавить фильтр**. Фильтры объединяются по правилу "И".

   Чтобы очистить значение фильтра, нажмите на значок  правее поля значения.
5. Нажмите на кнопку **Применить**.
6. Закройте окно добавления фильтра.

Отобразится таблица учетных записей, удовлетворяющих критериям фильтрации.

См. также

Изменение учетной записи

Изменение учетной записи Administrator недоступно.

► *Чтобы изменить учетную запись пользователя:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. В таблице выберите учетную запись, которую вы хотите изменить.

Откроется окно просмотра учетной записи.

3. Нажмите на кнопку **Изменить**.

   Откроется окно изменения учетной записи.

4. Вы можете изменить значения следующих полей:
   - **Роль**.
   - **Описание**.
5. После внесения изменений нажмите на кнопку **Сохранить**.

Учетная запись пользователя будет изменена.

См. также

Удаление учетной записи

Удаление собственной учетной записи и записи Administrator невозможно.

► *Чтобы удалить учетную запись пользователя:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.

2. В таблице выберите учетную запись, которую вы хотите удалить.

   Откроется окно просмотра учетной записи.

3. Нажмите на кнопку **Удалить**.

4. Подтвердите удаление учетной записи с помощью кнопки **Удалить**.

В результате учетная запись будет удалена из приложения и исчезнет из таблицы на вкладке **Учетные записи**. Пользователь удаленной учетной записи потеряет доступ к приложению.

► *Чтобы удалить несколько учетных записей пользователей:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. Установите флажки около учетных записей, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Если среди выбранных записей оказалась ваша учетная запись, удаление выборки будет отменено.
4. Подтвердите удаление учетных записей с помощью кнопки **Удалить**.

В результате учетные записи будут удалены из приложения и исчезнут из таблицы на вкладке **Учетные записи**. Пользователи удаленных учетных записей потеряют доступ к приложению.

См. также

Создание роли

► *Чтобы создать роль:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**, затем выберите вкладку **Роли**.

Откроется таблица ролей.

2. Нажмите на кнопку **Создать роль**.

   Откроется окно создания роли.

3. В поле **Название роли** введите название новой роли.

   Название роли чувствительно к регистру.

4. В блоке параметров **Разрешения** установите флажки рядом с теми разрешениями, которыми должна обладать роль. Список разрешений приведен в таблице ниже.

5. Нажмите на кнопку **Создать**.

Роль будет создана.

Таблица 6. Разрешения пользователей

Функциональная область	Разрешение	Описание
Мониторинг и отчеты	Просматривать разделы Мониторинг и Отчеты	Позволяет просматривать разделы **Мониторинг** и **Отчеты**, но не изменять их параметры.
	Изменять параметры в разделах Мониторинг и Отчеты	Позволяет изменять параметры отчетов, а также просматривать информацию в разделах **Мониторинг** и **Отчеты**.
Параметры	Просматривать параметры	Позволяет просматривать параметры приложения в разделе **Параметры**, но не изменять их.
	Изменять параметры	Позволяет изменять параметры приложения в разделе **Параметры**. Пользователь сможет также просматривать параметры приложения.
Правила	Просматривать правила	Позволяет просматривать таблицу правил обработки сообщений (см. раздел "Просмотр таблицы правил" на стр. 102). Пользователь не сможет добавлять или удалять правила, а также изменять их параметры.
	Создавать/изменять правила	Позволяет добавлять правила обработки сообщений (см. раздел "Создание правила обработки сообщений" на стр. 105), а также изменять их параметры (см. раздел "Изменение параметров правила" на стр. 129).
	Удалять правила	Позволяет удалять правила обработки сообщений (см. раздел "Удаление правил обработки сообщений" на стр. 129).
События	Просматривать события обработки почтового трафика	Позволяет просматривать информацию о событиях обработки трафика (см. раздел "Просмотр журнала событий" на стр. 204).
	Просматривать события приложения	Позволяет просматривать информацию о событиях приложения (см. раздел "Просмотр журнала событий" на стр. 204).

Функциональная область	Разрешение	Описание
Учетные записи и роли	Просматривать учетные записи и роли	Позволяет просматривать учетные записи (см. раздел "Просмотр учетной записи" на стр. 160) и роли (см. раздел "Создание роли" на стр. 163) в разделе **Учетные записи и роли**. Пользователь не сможет добавлять или удалять учетные записи и роли, а также изменять их параметры.
	Создавать/изменять учетные записи и роли	Позволяет создавать и изменять учетные записи (см. раздел "Создание учетной записи" на стр. 158) и роли (см. раздел "Создание роли" на стр. 163), а также назначать (см. раздел "Назначение роли" на стр. 173) и отзывать роли (см. раздел "Отзыв роли" на стр. 174). Пользователь не сможет удалять учетные записи и роли или изменять пароли учетных записей.
	Удалять учетные записи и роли	Позволяет удалять учетные записи (см. раздел "Удаление учетной записи" на стр. 162) и роли (см. раздел "Удаление роли" на стр. 175). Пользователь сможет также просматривать список учетных записей и ролей в разделе **Учетные записи и роли**.
	Изменять пароль пользователя	Позволяет изменить пароль другого пользователя. Пользователь сможет также просматривать список учетных записей и ролей в разделе **Учетные записи и роли**.
Узлы	Просматривать информацию об узлах	Позволяет просматривать информацию об узлах в разделе **Узлы** (см. раздел "**Управление кластером**" на стр. 136). Пользователь не сможет добавлять и удалять узлы, а также изменять их параметры и роли.

Функциональная область	Разрешение	Описание
	Создавать/изменять/удалять узлы	Позволяет добавлять (см. раздел "Добавление узла в кластер" на стр. 140) и удалять (см. раздел "Удаление узла из кластера" на стр. 141) узлы кластеров, а также изменять параметры (см. раздел "Изменение параметров узла" на стр. 141) и роли узлов (см. раздел "Изменение роли узла в кластере" на стр. 142) в кластере. Пользователь сможет также просматривать информацию об узлах кластера.
	Получать диагностическую информацию	Позволяет получать диагностическую информацию (см. раздел "Получение информации для Службы технической поддержки" на стр. 375) об узлах кластера. Пользователь сможет также просматривать информацию об узлах кластера.
	Проверять целостность данных	Позволяет запускать проверку целостности (см. раздел "Проверка целостности данных" на стр. 149) на узлах кластера, а также просматривать результаты выполнения проверки. Пользователь сможет также просматривать информацию об узлах кластера.
Очередь сообщений	Просматривать информацию о сообщениях	Позволяет просматривать информацию об Анти-Спам карантине и KATA карантине (если настроена интеграция с KATA) в разделе **Очередь сообщений**.
	Выполнять принудительную отправку сообщений	Позволяет принудительно отправить сообщение вне очереди (см. раздел "Принудительная отправка сообщений из очереди" на стр. 223). Пользователь сможет также просматривать информацию об Анти-Спам карантине и KATA карантине (если настроена интеграция с KATA) в разделе **Очередь сообщений**.

Функциональная область	Разрешение	Описание
	Удалять сообщения	Позволяет удалять сообщения из очереди (см. раздел "Принудительная отправка сообщений из очереди" на стр. 223). Пользователь сможет также просматривать информацию об Анти-Спам карантине и KATA карантине (если настроена интеграция с KATA) в разделе **Очередь сообщений**.
Хранилище	Просматривать сообщения	Позволяет просматривать информацию об объектах в Хранилище в разделе **Хранилище**.
	Доставлять сообщения	Позволяет доставлять получателям те сообщения из Хранилища (см. раздел "Отправка сообщений из Хранилища" на стр. 190), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. Пользователь сможет также просматривать информацию об объектах в Хранилище.
	Доставлять небезопасные сообщения	Позволяет доставлять получателям любые сообщения из Хранилища (см. раздел "Отправка сообщений из персонального Хранилища" на стр. 191). Пользователь сможет также просматривать информацию об объектах в Хранилище.
	Пересылать сообщения на любые адреса	Позволяет пересылать на любые адреса те сообщения из Хранилища (см. раздел "Отправка сообщений из персонального Хранилища" на стр. 191), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. Пользователь сможет также просматривать информацию об объектах в Хранилище.

Функциональная область	Разрешение	Описание
	Пересылать небезопасные сообщения на любые адреса	Позволяет пересылать на любые адреса любые сообщения из Хранилища (см. раздел "Отправка сообщений из персонального Хранилища" на стр. 191). Пользователь сможет также просматривать информацию об объектах в Хранилище.
	Удалять сообщения	Позволяет удалять сообщения из Хранилища (см. раздел "Удаление сообщения из Хранилища" на стр. 192). Пользователь сможет также просматривать информацию об объектах в Хранилище.
	Сохранять сообщения	Позволяет скачивать сообщения из Хранилища (см. раздел "Скачивание сообщения из Хранилища" на стр. 197), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. Пользователь сможет также просматривать информацию об объектах в Хранилище.
	Сохранять небезопасные сообщения	Позволяет скачивать любые сообщения из Хранилища (см. раздел "Скачивание сообщения из Хранилища" на стр. 197). Пользователь сможет также просматривать информацию об объектах в Хранилище.
Списки запрещенных и разрешенных адресов	Просматривать все списки разрешенных и запрещенных адресов	Позволяет просматривать персональные списки разрешенных и запрещенных адресов (см. раздел "Просмотр персональных списков разрешенных и запрещенных адресов" на стр. 133). Пользователь не сможет изменять состав этих списков.

Функциональная область	Разрешение	Описание
	Управлять всеми списками разрешенных и запрещенных адресов	Позволяет добавлять, удалять и изменять адреса в персональных списках (см. раздел "Формирование персональных списков" на стр. 134) разрешенных и запрещенных адресов. Пользователь сможет также просматривать все персональные списки.

Просмотр информации о роли

► *Чтобы просмотреть информацию о роли:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**, затем выберите вкладку **Роли**.

   Откроется таблица ролей. В ней вы можете просмотреть список ролей и количество учетных записей пользователей, которым назначена каждая роль.

2. Выберите роль, информацию о которой вы хотите просмотреть.

В окне просмотра роли отобразится следующая информация:

- Название роли.
- Разрешения, которые получает пользователь при назначении ему этой роли, отмечены в списке значком .

Вы можете изменить список разрешений (см. раздел "Изменение параметров роли" на стр. 172) для выбранной роли или удалить роль (см. раздел "Удаление роли" на стр. 175).

kaspersky

См. также

Изменение параметров роли

Изменение ролей Superuser и Viewer недоступно.

Вы можете изменить название роли и набор разрешений, которыми она обладает.

► *Чтобы изменить параметры роли:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**, затем выберите вкладку **Роли**.

   Откроется таблица ролей.
2. Выберите роль, для которой хотите изменить параметры.

   Откроется окно изменения роли.
3. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить роль**.
4. Если требуется, измените название роли в поле **Название роли**.
5. Если требуется, измените набор прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Разрешения**.
6. Нажмите на кнопку **Сохранить**.

Параметры роли будут изменены.

Изменение разрешений роли вступает в силу для пользователя, которому назначена эта роль, через 30 секунд после сохранения изменений или после следующий авторизации в веб-интерфейсе.

См. также

Назначение роли

Вы можете назначить роль пользователю следующими способами:

- При создании учетной записи пользователя (см. раздел "Создание учетной записи" на стр. 158).

  Этим способом вы можете назначить одному пользователю одну или несколько ролей.
- При изменении учетной записи пользователя (см. раздел "Изменение учетной записи" на стр. 161).

  Этим способом вы можете назначить одному пользователю одну или несколько ролей.
- При выборе пользователей в таблице учетных записей.

  Этим способом вы можете назначить одну роль одному или нескольким пользователям.

► *Чтобы назначить роль выбранным пользователям в таблице учетных записей:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. Установите флажки около учетных записей, которым вы хотите назначить роль.
3. Нажмите на кнопку **Назначить роль** и в раскрывающемся списке выберите роль, которую хотите назначить выбранным пользователям.

   Если в раскрывающемся списке нет нужной роли, вы можете ее создать (см. раздел "Создание роли" на стр. 163) по ссылке **Создать роль** внизу раскрывающегося списка, а затем назначить пользователям.
4. В окне подтверждения нажмите на кнопку **Назначить роль**.

Роль будет назначена выбранным пользователям.

Изменение в наборе разрешений вступает в силу для пользователя, которому назначена роль, через 30 секунд после сохранения изменений или после следующий авторизации в веб-интерфейсе.

См. также

Отзыв роли

► *Чтобы отозвать роль у пользователя:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. В таблице выберите учетную запись пользователя, у которого вы хотите отозвать роль.

   Откроется окно просмотра учетной записи.
3. Нажмите на кнопку **Изменить**.

   Откроется окно изменения учетной записи.
4. В поле **Роль** удалите роль или роли, которые вы хотите отозвать.
5. Нажмите на кнопку **Сохранить**.

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

Изменение в наборе разрешений вступает в силу для пользователя, которому назначена роль, через 30 секунд после сохранения изменений или после следующий авторизации в веб-интерфейсе.

kaspersky

См. также

Удаление роли

Удаление предопределенных ролей Superuser и Viewer невозможно.

Вы можете удалить роль следующими способами:

- При просмотре информации о роли (см. раздел "Просмотр информации о роли" на стр. 171).

  Этим способом вы можете удалить одну роль.
- При выборе ролей в таблице.

  Этим способом вы можете удалить одну или несколько ролей.

► *Чтобы удалить роли в таблице:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**, затем выберите вкладку **Роли**.

   Откроется таблица ролей.
2. Установите флажки около ролей, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления ролей.
4. В окне подтверждения нажмите на кнопку **Удалить**.

Роли будут удалены и отозваны у всех пользователей, которым они были назначены.

kaspersky

Изменение своего пароля

Изменить свой пароль может любой пользователь, авторизованный под учетной записью локального пользователя.

Kaspersky Security для Linux Mail Server хранит только хеши паролей пользователей, но не сами пароли.

► *Чтобы изменить свой пароль:*

1. Внизу левой панели меню нажмите на имя текущего пользователя.
2. В раскрывшейся справа панели выберите **Изменить пароль**.

   Отобразится окно изменения пароля.
3. В поле **Старый пароль** введите старый пароль.

   Чтобы просмотреть введенный пароль, нажмите на значок  и удерживайте его нужное вам время.

   > Если вы введете пароль неверно пять раз подряд, возможность изменения пароля в приложении с вашего IP-адреса будет заблокирована на пять минут.
4. В поле **Новый пароль** введите новый пароль.

   Пароль должен содержать строчные и прописные буквы латинского алфавита (A–z), цифры (0–9) и специальные символы. Длина пароля должна быть не менее 15 символов.

   > Новый пароль не должен совпадать ни с одним из 24 последних использованных паролей.
5. В поле **Повторите пароль** повторно введите пароль.
6. Нажмите на кнопку **Сохранить**.

Пароль вашей учетной записи будет изменен.

Пароль локальной учетной записи действует в течение одного года. После истечения срока действия пароля при попытке входа в веб-интерфейс приложения отобразится запрос на смену пароля. Аутентификация локального пользователя будет возможна только после смены пароля.

kaspersky

См. также

Изменение пароля другого пользователя

Изменять пароли учетных записей других пользователей может только пользователь с разрешением **Изменять пароль пользователя**.

► *Чтобы изменить пароль учетной записи другого пользователя:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **Учетные записи и роли**.

   Откроется таблица учетных записей на вкладке **Учетные записи**.
2. В таблице выберите учетную запись, пароль которой вы хотите изменить.
3. В окне просмотра учетной записи нажмите на кнопку **Изменить**.
4. В окне изменения учетной записи перейдите по ссылке **Изменить пароль**.

   Откроется окно изменения пароля.
5. В поле **Новый пароль** введите новый пароль.

   Пароль должен содержать строчные и прописные буквы латинского алфавита (A–z), цифры (0–9) и специальные символы. Длина пароля должна быть не менее 15 символов.

   Чтобы просмотреть введенный пароль, нажмите на значок и удерживайте его нужное вам время.
6. В поле **Подтвердите пароль** повторно введите пароль.

Перед сохранением учетной записи скопируйте пароль, чтобы передать его пользователю. Вам необходимо самостоятельно обеспечить безопасный канал и способ доставки пароля.

После сохранения учетной записи пароль станет недоступен для просмотра. Kaspersky Security для Linux Mail Server хранит только хеш пароля, но не сам пароль.

7. Если вы хотите, чтобы пользователь сменил пароль после первой авторизации в приложении, установите флажок **Пользователь должен изменить пароль при следующем входе в систему**.
8. Нажмите на кнопку **Сохранить**.

Пароль учетной записи пользователя будет изменен.

Пароль локальной учетной записи действует в течение одного года. После истечения срока действия пароля при попытке входа в веб-интерфейс приложения отобразится запрос на смену пароля. Аутентификация локального пользователя будет возможна только после смены пароля.

См. также

kaspersky

Хранилище

Хранилище предназначено для сообщений, которые Kaspersky Security для Linux Mail Server сохраняет перед обработкой. Права доступа к сообщениям в Хранилище ограничены в целях обеспечения безопасности сервера Kaspersky Security для Linux Mail Server.

Если к сообщению применяется правило, в параметрах которого установлен флажок **Поместить сообщение в Хранилище**, то независимо от заданного действия перед его выполнением приложение помещает в Хранилище оригинал сообщения. Сообщения помещаются в Хранилище вместе с вложениями.

В режиме привилегированного пользователя отображается информация обо всех сообщениях, помещенных в Хранилище.

Привилегированный пользователь приложения может выполнять следующие действия с сообщениями в Хранилище при наличии соответствующих прав (см. раздел "Создание роли" на стр. 163):

- Фильтровать сообщения в Хранилище (см. раздел "Фильтрация и поиск сообщений в Хранилище" на стр. 184).
- Просматривать информацию о сообщении (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 188) и результатах его обработки.
- Отправлять сообщения из Хранилища (см. раздел "Отправка сообщений из персонального Хранилища" на стр. 191).
- Скачивать сообщения (см. раздел "Скачивание сообщения из Хранилища" на стр. 197) на компьютер.
- Удалять сообщения (см. раздел "Удаление сообщения из Хранилища" на стр. 192) из Хранилища.

По умолчанию максимальный объем Хранилища составляет 7 ГБ. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, приложение начинает удалять из Хранилища самые старые сообщения. Когда объем Хранилища снова становится меньше порогового значения, приложение прекращает удалять сообщения из Хранилища.

Персональное Хранилище

В режиме персонального пользователя отображается персональное Хранилище с информацией о сообщениях только текущего пользователя.

> Просмотр персонального Хранилища, а также действия с сообщениями доступны персональному пользователю, если администратор включил соответствующие опции в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

В персональном Хранилище доступны сообщения, к которым было применены действия **Вылечить**, **Удалить вложение** или **Удалить сообщение**. Если к сообщению было применено действие **Пропустить** или **Отклонить**, это сообщение недоступно в персональном Хранилище пользователя.

Персональный пользователь приложения может выполнять следующие действия с сообщениями в персональном Хранилище:

- Фильтровать сообщения в Хранилище (см. раздел "Фильтрация и поиск сообщений в Хранилище" на стр. 184).

- Просматривать информацию о сообщении (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 188) и результатах его обработки.
- Отправлять себе сообщения из Хранилища (см. раздел "Отправка сообщений из персонального Хранилища" на стр. 191).
- Удалять сообщения из Хранилища (см. раздел "Удаление сообщения из Хранилища" на стр. 192).

> При удалении из персонального Хранилища сообщение не удаляется из общего Хранилища. Все операции с этим сообщением остаются доступны в общем Хранилище.

Сообщения не помещаются в персональное Хранилище, если имя или адрес электронной почты пользователя совпадает с именем или адресом электронной почты другого пользователя или группы в домене LDAP-сервера. Адреса электронной почты и имена пользователей проверяются на наличие дубликатов после каждой успешной синхронизации с контроллером домена Active Directory.

В этом разделе

Настройка параметров Хранилища

Приведенные параметры доставки сообщений из Хранилища используются как значения по умолчанию. Вы можете изменить эти значения индивидуально для каждого сообщения.

► *Чтобы настроить параметры Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Хранилище** → **Параметры**.
2. В поле **Максимальный размер Хранилища (МБ)** укажите суммарный размер всех сообщений в Хранилище, при достижении которого более старые сообщения будут удаляться.

   Минимальное возможное значение – 1024 МБ. Значение по умолчанию – 7168 МБ (7 ГБ). Значение параметра должно быть не более половины минимального размера свободного места на дисках узлов кластера в разделе, на котором находится директория /var/opt/kaspersky/klms/postgresql.

3. В поле **Срок хранения (дней)** укажите количество дней, по истечении которого более старые сообщения будут удаляться.

   Возможные значения – целые числа от 1 до 1100 (~3 года). Значение по умолчанию – 30 дней.

   > Старые сообщения удаляются при достижении любого из этих ограничений.

4. В раскрывающемся списке ниже выберите, в каком виде следует доставлять сообщения из Хранилища:

   - **Во вложении**.
   - **В исходном виде**.

5. Некоторые почтовые системы, например Microsoft Exchange Server, могут отклонить повторную доставку сообщения с тем же заголовком SMTP message ID. Чтобы доставить сообщения в исходном виде из Хранилища в такие системы, следует удалить заголовок SMTP message ID. Для этого переведите переключатель **Удалять SMTP message ID** в положение **Включено**.

   > Доступно только для формата доставки сообщений **В исходном виде**.

   > Если в сообщении есть DKIM-подпись, удаление заголовка SMTP message ID может повредить ее.

6. Выберите действие для сообщений, которые требуется поместить в Хранилище, если Хранилище недоступно:

   - **Продолжать обработку**.

     Сообщение будет обработано независимо от доступности Хранилища. Если задано действие **Удалить вложение** или **Вылечить**, то измененное сообщение будет отправлено получателям после лечения или удаления вложения. Если задано действие **Удалить сообщение**, то сообщение будет удалено без уведомления отправителя. Если задано действие **Отклонить**, то сообщение будет отклонено.

   - **Сообщать о временной ошибке сервера**.

     Если при помещении сообщения в Хранилище произойдет ошибка, приложение вернет SMTP-ошибку 451.

   - **Отклонять сообщения**.

     Если при помещении сообщения в Хранилище произойдет ошибка, сообщение будет отклонено.

7. Нажмите на кнопку **Сохранить**.

Параметры Хранилища будут настроены.

kaspersky

Настройка параметров персонального Хранилища

Персональное Хранилище отображается в режиме персонального пользователя.

► *Чтобы настроить параметры персонального Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Персональные учетные записи** → **Хранилище**.
2. Если вы хотите, чтобы в режиме персонального пользователя отображался раздел персонального Хранилища с информацией о помещенных в него сообщениях, переведите переключатель **Персональное Хранилище** в положение **Включено**.
3. Если вы хотите, чтобы в режиме персонального пользователя было доступно удаление сообщений из персонального Хранилища, переведите переключатель **Удалять сообщения** в положение **Включено**.

   Доступно только при включенной опции **Персональное Хранилище**.

4. Если вы хотите, чтобы в режиме персонального пользователя была доступна доставка сообщений из персонального Хранилища, переведите переключатель **Доставлять сообщения** в положение **Включено**.

   Доступно только при включенной опции **Персональное Хранилище**.

5. В раскрывающемся списке ниже выберите, в каком формате следует доставлять сообщения из персонального Хранилища:
   - **Во вложении**.
   - **В исходном виде**.
6. Некоторые почтовые системы, например Microsoft Exchange Server, могут отклонить повторную доставку сообщения с тем же заголовком SMTP message ID. Чтобы доставить сообщения в исходном виде из персонального Хранилища в такие системы, следует удалить заголовок SMTP message ID. Для этого переведите переключатель **Удалять SMTP message ID** в положение **Включено**.

   Доступно только для формата доставки сообщений **В исходном виде**.

   Если в сообщении есть DKIM-подпись, удаление заголовка SMTP message ID может повредить ее.

7. Нажмите на кнопку **Сохранить**.

Параметры персонального Хранилища будут настроены.

kaspersky

Просмотр таблицы объектов в Хранилище

Сообщения, к которым были применены действия **Пропустить** или **Отклонить**, не помещаются в персональное Хранилище. Информация о таких сообщениях доступна только в Хранилище в режиме привилегированного пользователя.

► *Чтобы просмотреть таблицу объектов в Хранилище,*

в окне веб-интерфейса приложения выберите раздел **Хранилище**.

В таблице отображается следующая информация об объектах в Хранилище:

- **Email отправителя** – адрес электронной почты отправителя сообщения.
- **IP отправителя** – IP-адрес хоста, с которого было отправлено сообщение.
- **Email получателя** – адреса электронной почты получателей сообщения.

  В персональном Хранилище информация о получателях из поля `BCC` не отображается.

- **Тема** – тема сообщения.
- **Технология обнаружения** – название модуля приложения, который обнаружил угрозу в сообщении.
- **Причина помещения** – название модуля приложения, по результату проверки которого сообщение было помещено в Хранилище.
- **Размер сообщения** – размер сообщения.
- **Время получения** – дата и время получения сообщения.
- **App ID сообщения** – уникальный идентификатор, присваиваемый сообщению приложением.
- **SMTP message ID** – идентификатор, присваиваемый сообщению на почтовом сервере.
- **Узел** – IP-адрес узла кластера, на котором было обработано сообщение.

По умолчанию в таблице отображаются не все столбцы. Вы можете настроить отображение таблицы (см. раздел "Настройка отображения таблицы объектов в Хранилище" на стр. 183).

Настройка отображения таблицы объектов в Хранилище

► *Чтобы настроить отображение таблицы объектов в Хранилище:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.

   Откроется таблица объектов Хранилища.

2. Нажмите на кнопку  .

Откроется окно **Настроить таблицу**.

3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы объектов Хранилища будет настроено.

Фильтрация и поиск сообщений в Хранилище

► *Чтобы найти сообщения в Хранилище:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Нажмите на кнопку  .

   Откроется окно **Фильтры**.
3. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска сообщений.
4. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите значение:
Технология обнаружения	Для этого критерия логические операторы не предусмотрены	Установите флажки рядом с названиями модулей приложения, по результатам проверки которыми в сообщении были обнаружены угрозы. Вы можете выбрать один или несколько модулей проверки: • **Антивирус**. • **Анти-Спам**. • **Анти-Фишинг**. • **Контентная фильтрация**. • **Персональный список запрещенных адресов**. • **Проверка ссылок**. • **Проверка подлинности отправителей**. • **KATA** (отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277)).
Email отправителя	• **включает**	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). Если вы настроили интеграцию с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 270), приложение будет искать записи в LDAP-кеше, совпадающие с введенной строкой поиска, и отображать подсказку с именами учетных записей.
IP отправителя	• **=**	Текст поиска IP-адреса, с которого было отправлено сообщение. Вы можете ввести адрес в формате IPv4 или IPv6.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите значение:
Email получателя	• **включает**	Текст поиска адресов электронной почты получателей 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). Если вы настроили интеграцию с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 270), приложение будет искать записи в LDAP-кеше, совпадающие с введенной строкой поиска, и отображать подсказку с именами учетных записей. При фильтрации сообщений в персональном Хранилище адреса получателей из поля BCC не учитываются.
Тема	• **включает**	Текст поиска темы сообщений
App ID сообщения	• **=**	Уникальный идентификатор, присвоенный сообщению приложением.
SMTP message ID	• **включает**	Идентификатор сообщения на почтовом сервере. Этот идентификатор может быть использован для поиска сообщения в Хранилище при обращении пользователей, если вы настроили добавление идентификатора в уведомления об отклоненных сообщениях (см. раздел "Добавление в уведомление уникального идентификатора сообщения" на стр. 328).
Дата и время	• **после** • **до**	Интервал обработки и помещения сообщений в Хранилище.
Размер сообщения	• **⩾** • **⩽**	Ограничение поиска по размеру сообщений.
Узел	• **=** • **≠**	Узел кластера, на котором было обработано сообщение. Критерий недоступен в персональном Хранилище.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку **Добавить фильтр**.

5. Нажмите на кнопку **Применить**.

Сообщения, удовлетворяющие параметрам поиска, отобразятся в списке сообщений в разделе **Хранилище**.

В таблице отображается информация о последних 5000 сообщений. Если согласно заданным критериям фильтрации найдено более 5000 сообщений, рекомендуется уточнить критерии поиска.

Просмотр информации о сообщении в Хранилище

► *Чтобы просмотреть информацию о сообщении в Хранилище:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. В таблице объектов Хранилища выберите сообщение, информацию о котором вы хотите посмотреть.

   Откроется окно **Просмотреть информацию о сообщении**.

В окне содержится следующая информация о сообщении:

- **Причина**.

  Название модуля приложения, по результатам проверки которого сообщение было помещено в Хранилище.
- **App ID сообщения**.

  Уникальный идентификатор, присваиваемый сообщению приложением в процессе обработки.
- **Тема**.

  Тема сообщения.
- **Email отправителя**.

  Адрес электронной почты отправителя сообщения.
- **IP отправителя**.

  IP-адрес сервера, с которого было отправлено сообщение.
- **Получено**.

  Дата и время получения сообщения приложением.
- **Узел**.

  Узел, на котором было обработано сообщение.

Поле недоступно в персональном Хранилище.

- **SMTP message ID**.

  Идентификатор, присвоенный сообщению почтовым сервером.

- **Вложения**.

  Имена и размеры вложений.

- Раздел **Правила**, содержащий следующую информацию о правилах, согласно которым сообщение было помещено в Хранилище:

  - Название правила.
  - **Email получателя**.

    Адреса электронной почты получателей из поля `To`.

  - **CC**.

    Адреса электронной почты получателей из поля `CC`.

  - **BCC**.

    Адреса электронной почты получателей из поля `BCC`.

    Поле недоступно в персональном Хранилище.

  - **Действие**.

    Действие, которое было выполнено над сообщением по результатам проверки всеми модулями приложения.

  - **Результат проверки**.

    Вы можете развернуть этот блок и просмотреть детальную информацию о результатах проверки по каждому модулю приложения.

    - **Антивирус**.
    - **Анти-Спам**.
    - **Анти-Фишинг**.
    - **Проверка ссылок**.
    - **Контентная фильтрация**.
    - **Персональный список запрещенных адресов**.
    - **Подлинность отправителей**.

      Вы можете развернуть этот блок и просмотреть детальную информацию о результатах проверки по каждой из технологий: SPF, DKIM, DMARC.

    - **KATA**.

      Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

  - **Причина**.

Название модуля приложения, по результатам проверки которого сообщение было помещено в Хранилище.

- Блок параметров **Отправить сообщение**, позволяющих отправить сообщение получателям или переслать его на другие адреса во вложении или в исходном виде (см. раздел "Отправка сообщений из Хранилища" на стр. 190).

  Блок недоступен в персональном Хранилище. В режиме привилегированного пользователя блок отображается только при наличии разрешений на отправку сообщений из Хранилища.

По ссылке в верхней части окна с информацией о сообщении вы можете перейти в раздел **События** и посмотреть информацию о событиях, связанных с обработкой этого сообщения.

Отправка сообщений из Хранилища

В режиме привилегированного пользователя вы можете доставлять сообщения из общего Хранилища получателям или пересылать их на любые адреса. Доступные параметры доставки определяются наличием соответствующих прав (см. раздел "Создание роли" на стр. 163).

Вы можете изменить заданный по умолчанию адрес отправителя (см. раздел "Настройка адреса сообщений от приложения" на стр. 328), который указывается для сообщения, доставленного из Хранилища в виде вложения.

Вы можете отправлять сообщения по одному, группой или сразу все (см. раздел "Отправка группы сообщений из Хранилища" на стр. 193).

► *Чтобы отправить одно сообщение из общего Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Для того чтобы выбрать сообщение и перейти к настройкам отправки, выполните одно из действий:
   - В списке сообщений Хранилища выберите нужное сообщение.

     В открывшемся окне **Просмотреть информацию о сообщении** перейдите к блоку параметров **Отправить сообщение**.
   - В списке сообщений Хранилища установите флажок около сообщения и нажмите на кнопку **Отправить**.

     Откроется окно **Отправить сообщения**.
3. Если вы хотите отправить сообщение исходным получателям, выполните следующие действия:
   a. Включите переключатель **Получателям, чьи сообщения были помещены в Хранилище**.
   b. Если отображается список исходных получателей, установите флажки напротив адресов тех получателей, которым вы хотите доставить сообщение.

      Список исходных получателей отображается только при отправке сообщений из окна **Просмотреть информацию о сообщении**.
4. Если вы хотите переслать сообщение на другие адреса, выполните следующие действия:
   a. Включите переключатель **На следующие адреса**.

b. В поле ввода ниже укажите адреса электронной почты, на которые вы хотите переслать сообщение.

5. Если вы хотите доставить сообщение в виде вложения, установите флажок **Отправить сообщение в виде вложения**.

   Если флажок снят, сообщение будет отправлено в исходном виде.

   По умолчанию состояние флажка соответствует формату доставки сообщений, указанному в параметрах Хранилища.

6. Некоторые почтовые системы, например Microsoft Exchange Server, могут отклонить повторную доставку сообщения с тем же заголовком SMTP message ID. Чтобы доставить сообщение из Хранилища в исходном виде в такую систему, нужно удалить заголовок SMTP message ID. Для этого установите флажок **Удалять SMTP message ID**.

   По умолчанию состояние флажка соответствует значению параметра, указанному в параметрах Хранилища.

   Доступно только для формата доставки сообщений **В исходном виде**.

   Если в сообщении есть DKIM-подпись, удаление заголовка SMTP message ID может повредить ее.

7. Нажмите на кнопку **Отправить**.
8. В окне подтверждения нажмите на кнопку **ОК**.

Сообщение будет помещено в очередь на доставку.

Отправка сообщений из персонального Хранилища

В режиме персонального пользователя вы можете отправлять сообщения из персонального Хранилища на адрес текущего пользователя, если администратор включил эту опцию в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

Доставка небезопасных сообщений из персонального Хранилища недоступна.

Вы можете отправлять сообщения по одному, группой или сразу все (см. раздел "Отправка группы сообщений из персонального Хранилища" на стр. 194).

► *Чтобы отправить одно сообщение из персонального Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Выполните один из вариантов действий:
   - В списке сообщений Хранилища выберите нужное сообщение и в открывшемся окне **Просмотреть информацию о сообщении** нажмите на кнопку **Отправить на мой электронный адрес**.
   - В списке сообщений Хранилища установите флажок около нужного сообщения, нажмите на кнопку **Отправить** и в открывшемся окне **Отправить сообщения** нажмите на кнопку **Отправить на мой электронный адрес**.
3. В окне подтверждения нажмите на кнопку **ОК**.

Сообщение будет помещено в очередь на отправку. Сообщение будет отправлено в формате, заданном администратором в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

Удаление сообщения из Хранилища

При удалении из персонального Хранилища сообщение не удаляется из общего Хранилища. Все операции с сообщением остаются доступны в общем Хранилище.

Вы можете удалять сообщения из Хранилища по одному, группой или сразу все (см. раздел "Удаление группы сообщений из Хранилища" на стр. 195).

В режиме персонального пользователя вы можете удалять сообщения из персонального Хранилища, если администратор включил эту опцию в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

► *Чтобы удалить одно сообщение из общего или персонального Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Выполните один из вариантов действий:
   - В таблице объектов Хранилища выберите сообщение, которое вы хотите удалить. В нижней части окна **Просмотреть информацию о сообщении** нажмите на кнопку **Удалить**.
   - В таблице объектов Хранилища установите флажок слева от нужного сообщения и нажмите на кнопку **Удалить**.
3. В окне подтверждения нажмите на кнопку **ОК**.

Сообщение будет удалено из Хранилища.

Отправка и удаление группы сообщений в Хранилище

Вы можете отправлять (см. раздел "Отправка группы сообщений из Хранилища" на стр. 193) или удалять группу выбранных сообщений (см. раздел "Удаление группы сообщений из Хранилища" на стр. 195) из общего Хранилища.

В персональном Хранилище пользователя доступны отправка группы сообщений на электронный адрес текущего пользователя (см. раздел "Отправка группы сообщений из персонального Хранилища" на стр. 194) и удаление группы сообщений (см. раздел "Удаление группы сообщений из Хранилища" на стр. 195).

Вы можете остановить выполнение групповой операции отправки или удаления сообщений из Хранилища (см. раздел "Остановка отправки или удаления группы сообщений из Хранилища" на стр. 196). В этом случае операция будет остановлена после обработки текущего сообщения и отобразится результат отправки или удаления (см. раздел "Просмотр результата отправки или удаления группы сообщений из Хранилища" на стр. 196) с количеством отправленных и неотправленных сообщений.

kaspersky

В этом разделе

Отправка группы сообщений из Хранилища

► *Чтобы отправить группу сообщений из общего Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Выберите сообщения для отправки:
   - Если вы хотите отправить группу сообщений, в списке сообщений Хранилища установите флажки слева от нужных сообщений и нажмите на кнопку **Отправить**.
   - Если вы хотите отправить все сообщения из Хранилища, установите флажок в заголовке таблицы и нажмите на кнопку **Отправить**.

   Откроется окно **Отправить сообщения**.
3. Если вы хотите отправить сообщение исходным получателям, включите переключатель **Получателям, чьи сообщения были помещены в Хранилище**.
4. Если вы хотите переслать сообщение на другие адреса, выполните следующие действия:
   a. Включите переключатель **На следующие адреса**.
   b. В поле ввода ниже укажите адреса электронной почты, на которые вы хотите переслать сообщение.
5. Если вы хотите доставить сообщение в виде вложения, установите флажок **Отправить сообщение в виде вложения**.

   Если флажок снят, сообщение будет отправлено в исходном виде.

   По умолчанию состояние флажка соответствует формату доставки сообщений, указанному в параметрах Хранилища.
6. Некоторые почтовые системы, например Microsoft Exchange Server, могут отклонить повторную доставку сообщения с тем же заголовком SMTP message ID. Чтобы доставить сообщение из Хранилища в исходном виде в такую систему, следует удалить заголовок SMTP message ID. Для этого установите флажок **Удалять SMTP message ID**.

   По умолчанию состояние флажка соответствует значению параметра, указанному в параметрах Хранилища.

   > Доступно только для формата доставки сообщений **В исходном виде**.

Если в сообщении есть DKIM-подпись, удаление заголовка SMTP message ID может повредить ее.

7. Нажмите на кнопку **Отправить**.
8. В окне подтверждения нажмите на кнопку **ОК**.

Сообщения будут помещены в очередь на отправку. В верхней части окна отобразится индикатор выполнения операции.

Во время отправки сообщений вы можете продолжать работать в веб-интерфейсе Kaspersky Security для Linux Mail Server.

Невозможно запустить отправку новой группы сообщений, если еще не окончена предыдущая операция групповой отправки или удаления сообщений.

По завершении отправки отобразится сообщение с результатом выполнения. Вы можете просмотреть подробности операции (см. раздел "Просмотр результата отправки или удаления группы сообщений из Хранилища" на стр. 196) по ссылке **Подробнее**.

См. также

Отправка группы сообщений из персонального Хранилища

В режиме персонального пользователя вы можете отправлять сообщения из персонального Хранилища на адрес текущего пользователя, если администратор включил эту опцию в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

Доставка небезопасных сообщений из персонального Хранилища недоступна.

- Чтобы отправить группу сообщений из персонального Хранилища:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Выберите сообщения для отправки:
   - Если вы хотите отправить группу сообщений, в списке сообщений Хранилища установите флажки слева от нужных сообщений и нажмите на кнопку **Отправить**.
   - Если вы хотите отправить все сообщения из Хранилища, установите флажок в заголовке таблицы и нажмите на кнопку **Отправить**.
3. В окне **Отправить сообщения** нажмите на кнопку **Отправить на мой электронный адрес**.

Сообщения будут помещены в очередь на отправку. В верхней части окна отобразится индикатор выполнения операции.

Во время отправки сообщений вы можете продолжать работать в веб-интерфейсе Kaspersky Security для Linux Mail Server. Сообщения будут отправлены в формате, заданном администратором в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

Невозможно запустить отправку новой группы сообщений, если еще не окончена предыдущая операция групповой отправки или удаления сообщений.

По завершении отправки отображается сообщение с результатом выполнения. Вы можете просмотреть подробности операции (см. раздел "Просмотр результата отправки или удаления группы сообщений из Хранилища" на стр. 196) по ссылке **Подробнее**.

См. также

Удаление группы сообщений из Хранилища

При удалении из персонального Хранилища сообщение не удаляется из общего Хранилища. Все операции с сообщением остаются доступны в общем Хранилище.

В режиме персонального пользователя вы можете удалять сообщения из персонального Хранилища, если администратор включил эту опцию в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 182).

► *Чтобы удалить группу сообщений из общего или персонального Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. Выберите сообщения для удаления:
   - Если вы хотите удалить группу сообщений, в списке сообщений Хранилища установите флажки слева от нужных сообщений и нажмите на кнопку **Удалить**.
   - Если вы хотите удалить все сообщения из Хранилища, установите флажок в заголовке таблицы и нажмите на кнопку **Удалить**.
3. В окне **Удалить сообщения** нажмите на кнопку **Удалить**.

Сообщения будут помещены в очередь на удаление. В верхней части окна отобразится индикатор выполнения операции.

Во время удаления сообщений вы можете продолжать работать в веб-интерфейсе Kaspersky Security для Linux Mail Server.

Невозможно запустить отправку новой группы сообщений, если еще не окончена предыдущая операция групповой отправки или удаления сообщений.

По завершении удаления отобразится сообщение с результатом выполнения. Вы можете просмотреть подробности операции (см. раздел "Просмотр результата отправки или удаления группы сообщений из Хранилища" на стр. 196) по ссылке **Подробнее**.

Остановка отправки или удаления группы сообщений из Хранилища

► *Чтобы остановить отправку или удаление группы сообщений:*

1. В верхней части окна правее индикатора отправки или удаления нажмите на кнопку **Остановить**.
2. В окне подтверждения нажмите на кнопку **Остановить отправку**.

В результате групповая операция отправки или удаления сообщений будет остановлена. В верхней части окна отобразится сообщение об остановке операции пользователем. По ссылке **Подробнее** из этого сообщения вы можете просмотреть подробности операции (см. раздел "Просмотр результата отправки или удаления группы сообщений из Хранилища" на стр. 196).

Просмотр результата отправки или удаления группы сообщений из Хранилища

► *Чтобы просмотреть подробную информацию об отправленных или удаленных сообщениях и ошибках,*

в верхней части окна в сообщении о результате отправки или удаления группы сообщений перейдите по ссылке **Подробнее**.

В открывшемся окне отобразится информация о количестве успешно и неуспешно отправленных или удаленных сообщений, а также следующие поля:

- **Результат** – значок, отображающий статус отправки или удаления сообщения. Возможные значения:

  – *Успешно*.

  – *Ошибка*.

  – *Отменено*.

  При наведении указателя мыши на значок отображается текстовая подсказка для статуса.
- **Email отправителя** – адрес электронной почты отправителя сообщения.
- **Email получателя** – адреса электронной почты получателей сообщения.

- **Тема** – тема сообщения.
- **SMTP Message ID** – идентификатор, присваиваемый сообщению на почтовом сервере.
- **Время получения** – дата и время получения сообщения.
- **Узел** – IP-адрес узла кластера, на котором было обработано сообщение.

По умолчанию в таблице отображаются не все столбцы. Вы можете настроить отображение таблицы по нажатию на значок шестеренки . Настройка выполняется аналогично процедуре настройке отображения таблицы объектов в Хранилище (см. раздел "Настройка отображения таблицы объектов в Хранилище" на стр. 183).

Вы можете сохранить результат отправки или удаления сообщений из Хранилища в файл формата CSV. Для этого в окне **Результат отправки** или **Результат удаления** под списком сообщений нажмите на кнопку **Экспорт**.

Скачивание сообщения из Хранилища

Скачивание сообщений из персонального Хранилища недоступно.

► *Чтобы скачать сообщение из Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**.
2. В таблице объектов Хранилища выберите сообщение, которое вы хотите сохранить на жесткий диск.

   Откроется окно **Просмотреть информацию о сообщении**.
3. В нижней части окна нажмите на кнопку **Скачать**.

Сообщение будет сохранено в папке загрузки браузера.

kaspersky

Дайджест Хранилища

Дайджест Хранилища – это почтовая рассылка с информацией о последних полученных письмах, помещенных в персональное Хранилище пользователя (см. раздел "Хранилище" на стр. 179).

Дайджест Хранилища содержит информацию о новых сообщениях, которые появились в Хранилище с момента предыдущей рассылки дайджеста и доступны персональному пользователю. Дайджест рассылается по расписанию, установленному администратором. По умолчанию дайджест рассылается ежедневно в 01:00 по локальному времени Управляющего узла. Если узел кластера недоступен, отправка дайджеста с него откладывается до следующей по расписанию рассылки.

Пользователь получает дайджест Хранилища, если с момента прошлой рассылки в персональном Хранилище этого пользователя появились новые сообщения. В качестве адреса отправителя дайджеста Хранилища используется заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от приложения" на стр. 328).

Если в персональном Хранилище пользователя нет сообщений, дайджест этому пользователю не отправляется.

Персональный пользователь может включить или отключить получение дайджеста персонального Хранилища в разделе веб-интерфейса **Хранилище** с помощью переключателя **Получать дайджест**. Если получение дайджеста включено, пользователь может отписаться от него по ссылке в сообщении дайджеста без перехода в веб-интерфейс Kaspersky Security для Linux Mail Server.

Привилегированный пользователь приложения может выполнять следующие действия при наличии соответствующих прав (см. раздел "Создание роли" на стр. 163):

- Включать или отключать рассылку дайджеста Хранилища всем персональным пользователям (см. раздел "Включение и отключение рассылки дайджеста Хранилища" на стр. 199).
- Настраивать расписание рассылки дайджеста Хранилища (см. раздел "Настройка расписания рассылки дайджеста Хранилища" на стр. 199).
- Исключать адреса пользователей из рассылки дайджеста Хранилища (см. раздел "Исключение адресов из рассылки дайджеста Хранилища" на стр. 200).
- Настраивать шаблон дайджеста Хранилища (см. раздел "Настройка шаблона дайджеста Хранилища" на стр. 201).

В этом разделе

kaspersky

Включение и отключение рассылки дайджеста Хранилища

Функциональность доступна только при наличии прав **Изменять параметры**.

► *Чтобы включить или отключить рассылку дайджеста Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Хранилище** и откройте закладку **Дайджест**.
2. Если вы хотите включить отправку дайджеста Хранилища всем персональным пользователям Kaspersky Security для Linux Mail Server, переведите переключатель **Отправлять дайджест** в положение **Включено**.
3. Если вы хотите отключить отправку дайджеста Хранилища всем персональным пользователям Kaspersky Security для Linux Mail Server, переведите переключатель **Отправлять дайджест** в положение **Отключено**.

Рассылка дайджеста будет включена или отключена.

По умолчанию приложение будет рассылать дайджест ежедневно в 01:00 по локальному времени Управляющего узла. Вы можете настроить расписание рассылки дайджеста Хранилища (см. раздел "Настройка расписания рассылки дайджеста Хранилища" на стр. 199).

Настройка расписания рассылки дайджеста Хранилища

Функциональность доступна только при наличии прав **Изменять параметры** и включенной рассылке дайджеста (см. раздел "Включение и отключение рассылки дайджеста Хранилища" на стр. 199).

► *Чтобы настроить расписание рассылки дайджеста Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Хранилище**.
2. Выберите закладку **Дайджест**.
3. В раскрывающемся списке **Расписание** выберите один из вариантов и выполните следующие действия для настройки расписания:
   - **По часам**.
     a. В появившемся поле **Каждые** укажите периодичность отправки дайджеста в часах. Возможные значения: 1–23.

     Если отправка дайджеста не успела завершиться до следующей рассылки из-за большого количества пользователей, следующая рассылка будет пропущена.

     b. В поле **Начиная с** укажите дату начала рассылки дайджеста.
   - **Ежедневно**.

- **Еженедельно**.

  В появившемся поле **День недели** укажите день недели для рассылки дайджеста. Значение по умолчанию: **Пн**.

- **Ежемесячно**.

  В появившемся поле **День месяца** укажите день месяца для рассылки дайджеста. Возможные значения: 1–31. Значение по умолчанию: 1.

  Если указанное значение превышает количество дней в месяце, в такие месяцы дайджест Хранилища не будет создан. Например, если указано значение **31**, в месяцы с 30 днями рассылки дайджеста не будет.

  По умолчанию дайджест рассылается ежедневно.

4. В поле **В** выберите время запуска рассылки. Возможные значения: 00:00–23:59. Значение по умолчанию 01:00.

   Рассылка выполняется по локальному времени Управляющего узла.

   Например, если установлены значения **Еженедельно**, **Пн** и **15:00**, дайджест Хранилища будет рассылаться каждый понедельник в 15 часов.

5. Нажмите на кнопку **Сохранить**.

Расписание рассылки дайджеста будет настроено. Первая рассылка дайджеста Хранилища произойдет в настроенное время.

Исключение адресов из рассылки дайджеста Хранилища

Функциональность доступна только при наличии прав **Изменять параметры** и включенной рассылке дайджеста (см. раздел "Включение и отключение рассылки дайджеста Хранилища" на стр. 199).

► *Чтобы исключить адреса из рассылки дайджеста Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Хранилище** и откройте закладку **Дайджест**.
2. В список **Не отправлять на эти адреса** добавьте адреса электронной почты, на которые не будет отправляться дайджест Хранилища:

   - Чтобы указать адрес вручную, нажмите на кнопку **Добавить**, введите адрес электронной почты и нажмите на значок ✓. Кнопка доступна, если формат введенного текста соответствует формату адреса электронной почты.

     При необходимости повторите действия для остальных адресов.

   - Чтобы вставить адреса из буфера обмена, нажмите на кнопку **Импорт**, введите или вставьте из буфера обмена адреса электронной почты, разделенные точкой с запятой или новой строкой, затем нажмите на кнопку **Импортировать**.

     Поддерживается добавление до 1000 адресов.

3. Если вы хотите изменить ранее добавленный адрес, нажмите на него в поле ввода, внесите необходимые изменения в режиме редактирования и нажмите на значок ✓. При необходимости воспользуйтесь строкой поиска.
4. Если вы хотите удалить адрес из списка исключений, нажмите на значок 🗑 справа от адреса.
5. Нажмите на кнопку **Сохранить**.

> Если хотя бы один из адресов указан в недопустимом формате, сохранение списков недоступно. Исправьте все адреса, выделенные красным фоном, и повторите операцию сохранения еще раз.

Адреса электронной почты будут добавлены в список исключенных из рассылки дайджеста.

Настройка шаблона дайджеста Хранилища

> Функциональность доступна только при наличии прав **Изменять параметры** и включенной рассылке дайджеста (см. раздел "Включение и отключение рассылки дайджеста Хранилища" на стр. 199).

По умолчанию текст шаблона написан на английском языке. Автоматическое переключение языков для шаблона недоступно. Если требуется, вы можете переписать текст на нужном языке. Если вам нужно отправлять уведомления на разных языках в рамках одной группы получателей, вы можете написать один и тот же текст на нескольких языках и расположить их друг за другом в одном шаблоне.

► *Чтобы настроить шаблон дайджеста Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Хранилище** и откройте закладку **Дайджест**.
2. По ссылке **Изменить** откройте окно изменения шаблона.
3. Если требуется, в поле **Тема** измените тему дайджеста.
4. Если требуется, в текстовой области **Шаблон оформления дайджеста** измените оформление и расположение элементов дайджеста.

   Вы можете использовать макрос `%TEXT%` в шаблоне дайджеста. Для этого нажмите на кнопку **Добавить макрос** и выберите макрос из раскрывающегося списка.
5. Если требуется, в текстовой области **Шаблон текста дайджеста (макрос %TEXT%)** измените текст сообщения дайджеста, отображаемый в шаблоне вместо макроса `%TEXT%`. Текст сообщения дайджеста может содержать макрос `%BACKUP_PREVEW_LINES%`, вместо которого будут подставляться строки информации о сообщении Хранилища.

   Вы можете использовать макросы (см. раздел "Использование макросов в шаблоне дайджеста Хранилища" на стр. 202) в тексте сообщения дайджеста. Для этого нажмите на кнопку **Добавить макрос** и выберите нужный макрос из раскрывающегося списка.
6. В раскрывающемся списке **Формат даты и времени** выберите формат даты и времени в дайджесте. Указанный формат даты и времени используется при отображении даты с помощью макроса `%DATE%`. Значение по умолчанию: `ДД/ММ/ГГГГ ЧЧ:ММ`.

7. В поле **Максимальное количество строк информации о сообщениях Хранилища** укажите максимальное количество сообщений Хранилища, информация о которых попадет в дайджест Хранилища. Возможные значения: от 0 до 500. Значение по умолчанию: 10.
8. Если требуется, в текстовой области **Шаблон строки информации о сообщении Хранилища (макрос %BACKUP_PREVIEW_LINES%)** измените строку информации о сообщении Хранилища.

   Вы можете использовать макросы в строке информации о сообщении Хранилища. Для этого нажмите на кнопку **Добавить макрос** и в раскрывающемся списке выберите нужный макрос.
9. Нажмите на кнопку **Сохранить**.

Шаблон дайджеста будет настроен. Вы можете просмотреть его по ссылке **Предпросмотр**.

Использование макросов в шаблоне дайджеста Хранилища

Макрос – это элемент подстановки, используемый в шаблоне дайджеста Хранилища. В формируемом на основе шаблона тексте дайджеста макрос заменяется на некоторое значение.

Синтаксис макроса: `%ИМЯ_МАКРОСА%`

В тексте дайджеста Хранилища можно использовать следующие макросы (см. таблицу ниже).

Таблица 7. Макросы для текста дайджеста Хранилища

Макрос	Описание
%PRODUCT_NAME%	Название приложения – Kaspersky Security для Linux Mail Server.
%DATE%	Дата и время отправки дайджеста Хранилища по часовому поясу Управляющего узла. Формат даты и времени настраивает администратор в параметрах шаблона дайджеста Хранилища (см. раздел "Настройка шаблона дайджеста Хранилища" на стр. 201).
%TOTAL_MESSAGES_COUNT%	Количество сообщений в персональном Хранилище пользователя.
%NEW_MESSAGES_COUNT%	Количество новых сообщений в персональном Хранилище пользователя по сравнению с предыдущим дайджестом.
%WEB_CONSOLE_LINK%	Ссылка на персональное Хранилище пользователя (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 188).
%BACKUP_PREVIEW_SIZE%	Максимальное количество строк информации о сообщениях Хранилища в дайджесте.
%BACKUP_PREVIEW_LINE%	Строка информации о сообщении Хранилища.
%UNSUBSCRIBE_LINK%	Ссылка на страницу отписки от дайджеста Хранилища. Язык страницы соответствует языку, сохраненному в файлах cookie. Если в файлах cookie язык не сохранен, то страница отображается на английском языке.

В строке информации о сообщении Хранилища можно использовать следующие макросы (см. таблицу ниже).

Таблица 8. Макросы для строки информации о сообщении Хранилища

Макрос	Описание
%SENDER%	Адрес отправителя исходного сообщения.
%RECIPIENTS%	Адреса всех получателей исходного сообщения.
%SUBJECT%	Тема исходного сообщения.
%DATE%	Дата и время помещения письма в Хранилище.

kaspersky

Журнал событий

Во время работы Kaspersky Security для Linux Mail Server возникают различного рода события. Они отражают изменение состояния приложения, а также результаты работы правил обработки сообщений. Для того, чтобы администратор мог самостоятельно проанализировать ошибки, допущенные при настройке параметров приложения, отследить работу правил обработки сообщений, а также для того, чтобы специалисты "Лаборатории Касперского" могли оказать эффективную техническую поддержку, Kaspersky Security для Linux Mail Server записывает информацию обо всех этих событиях в *журнал событий*.

Журнал событий хранится на узлах приложения. Записи в журнале событий автоматически ротируются по достижении максимально разрешенного размера файлов или по истечении максимального срока их хранения.

В этом разделе

Просмотр журнала событий

► *Чтобы просмотреть журнал событий Kaspersky Security для Linux Mail Server:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**
   - **Приложение**.

   Информация о событиях отобразится в виде таблицы.

   В таблице событий обработки почтового трафика отображается следующая информация:
   - **Дата и время** – дата и время выполнения события.
   - **Email отправителя** – адрес электронной почты отправителя сообщения.
   - **IP отправителя** – IP-адрес хоста, с которого было отправлено сообщение.
   - **Email получателя** – адрес электронной почты получателя сообщения.

- **Тема** – тема сообщения.
- **Название правила** – название правила, в соответствии с которым было обработано сообщение.

  Вы можете просмотреть подробную информацию о правиле, нажав на ссылку с названием правила.
- **Действие** – действие, выполненное над сообщением.
- **App ID сообщения** – уникальный идентификатор, присваиваемый сообщению приложением.
- **SMTP message ID** – идентификатор, присваиваемый сообщению на почтовом сервере.
- **Узел** – IP-адрес и порт узла, на котором было обработано сообщение.

В таблице событий приложения отображается следующая информация:

- **Дата и время** – дата и время выполнения события.
- **Узел** – IP-адрес и порт узла, на котором было обработано событие.
- **Тип события** – тип события (см. раздел "Типы событий приложения" на стр. 215).
- **Событие** – название события.
- **Имя пользователя** – имя пользователя, с правами которого создано событие.
- **Результат** – результат обработки события.

3. Вы можете сортировать события в столбцах. Для этого нажмите на название столбца в таблице:
   - События в столбцах **Email отправителя**, **Email получателя**, **Тема**, **Название правила**, **Действие**, **Тип события**, **Имя пользователя**, **Результат**, **Событие** сортируются по алфавиту в порядке A–Z и Z–A.

     По умолчанию записи о событиях отображаются по алфавиту в порядке A–Z.
   - События в столбцах **Дата и время** и **Узел** сортируются в порядке возрастания и убывания.

     По умолчанию записи о событиях отображаются в порядке возрастания.

Отобразится таблица событий, удовлетворяющих условиям сортировки.

По умолчанию в таблице отображаются не все столбцы. Вы можете настроить отображение таблицы, открыв окно **Настроить таблицу** по кнопке .

Настройка отображения таблицы событий

► *Чтобы настроить отображение таблицы событий:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**

- **Приложение**.

Информация о событиях отобразится в виде таблицы.

3. Нажмите на кнопку  .

   Отобразится окно **Настроить таблицу**.

4. Если вы хотите включить или отключить отображение столбца в таблице:
   - Если вы хотите включить отображение столбца в таблице, установите флажок рядом с тем параметром, который должен отображаться в таблице. Вы можете выбрать сразу несколько параметров.
   - Если вы хотите отключить отображение столбца в таблице, снимите флажок рядом с тем параметром, который не должен отображаться в таблице. Вы можете выбрать сразу несколько параметров.

   > Должен быть установлен хотя бы один флажок.

5. Если вы хотите изменить порядок отображения столбцов в таблице:
   a. Выберите строку с нужным параметром.
   b. В правой части строки зажмите кнопку  и перетащите строку выше или ниже.
   b. В нижней части окна нажмите на кнопку **ОК**.
6. Закройте окно настройки вида таблицы.

Отображение таблицы событий будет настроено.

Фильтрация событий обработки почтового трафика

Вы можете отфильтровать события в журнале событий по одному или нескольким критериям.

► *Чтобы отфильтровать события обработки почтового трафика в журнале событий:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Почтовый трафик**.

   Информация о событиях отобразится в виде таблицы.

3. Нажмите на кнопку  .

   Отобразится окно добавления фильтра.

4. Нажмите на кнопку **Добавить фильтр**.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите значение:
Дата и время	• **после**. • **до**.	Интервал обработки сообщений.
Email отправителя	• **включает**. • **не включает**. • **=**. • **≠**.	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).
Email получателя	• **включает**. • **не включает**. • **=**. • **≠**.	Текст поиска адресов электронной почты получателей сообщений.
Тема	• **включает**. • **не включает**.	Текст поиска заголовков сообщений
Название правила	• **включает**. • **не включает**. • **=**. • **≠**.	Название правила, которое было применено при обработке сообщения.
Действие	• **=**. • **≠**.	Действие, выполненное над сообщением.
IP отправителя	• **=**. • **≠**.	Текст поиска IP-адреса, с которого было отправлено сообщение. Вы можете ввести адрес в формате IPv4 или IPv6.
App ID сообщения	• **=**. • **≠**.	Уникальный идентификатор, присвоенный сообщению приложением.
SMTP message ID	• **включает**. • **не включает**. • **=**. • **≠**.	Идентификатор сообщения на почтовом сервере. Этот идентификатор может быть использован для поиска события при обращении пользователей, если вы настроили добавление идентификатора в уведомления об отклоненных сообщениях (см. раздел "Добавление в уведомление уникального идентификатора сообщения" на стр. 328).
Узел	• **=**. • **≠**.	Узел кластера, на котором было обработано сообщение.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите значение:
Статус проверки В раскрывающемся списке справа выберите одну из следующих технологий обнаружения: • **Анти-Фишинг**. • **Анти-Спам**. • **Антивирус**. • **Контентная фильтрация**. • **Проверка подлинности отправителей**. • **Проверка ссылок**. • **KATA** (отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277)).	• **включает**. • **не включает**.	Нажмите на поле **Выбрать статусы** и в раскрывшемся списке установите флажки напротив статусов, по которым вы хотите отфильтровать события. Набор отображаемых статусов зависит от выбранной технологии.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку **Добавить фильтр**.

6. Нажмите на кнопку **Найти**.
7. Закройте окно добавления фильтра.

Отобразится таблица событий, удовлетворяющих критериям фильтрации.

В таблице отображается информация о последних 5000 событий. Если согласно заданным критериям фильтрации найдено более 5000 событий, рекомендуется уточнить критерии поиска.

Фильтрация событий приложения

Информация о событиях приложения записывается в журнал событий узла, на котором произошли события. При удалении узла из кластера или потери доступа к узлу журнал событий будет недоступен.

Вы можете отфильтровать события в журнале событий по одному или нескольким критериям.

► *Чтобы отфильтровать события приложения в журнале событий:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Приложение**.

   Информация о событиях отобразится в виде таблицы.

3. Нажмите на кнопку  .

   Отобразится окно добавления фильтра.

4. В выпадающем списке выберите максимальное количество отображаемых событий, соответствующих условию фильтра.
5. Нажмите на кнопку **Добавить фильтр**.
6. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите значение:
Дата и время	• **после**; • **до**.	Интервал времени, в который произошло событие.
Узел	• **=**; • **≠**.	IP-адрес и порт узла, на котором произошло событие.
Тип события	• **=**; • **≠**.	Выберите тип события: • **Аудит.** • **Хранилище.** • **Обновление баз.** • **Проверка целостности.** • **Синхронизация LDAP.** • **Экспорт параметров.** • **Импорт параметров.**
Событие	• **=;** • **≠.**	Выберите событие: • **Антивирусные базы актуальны** • **Антивирусные базы применены** • **Аудит запущен** • **Аудит остановлен** • **Базы Анти-Спама актуальны** • **Базы Анти-Спама применены** • **Базы Анти-Фишинга актуальны** • **Базы Анти-Фишинга применены** • **Дайджест Хранилища отправлен** • **Задача запущена** • **Импорт параметров** • **Ошибка загрузки антивирусных баз** • **Ошибка загрузки баз Анти-Спама** • **Ошибка загрузки баз Анти-Фишинга** • **Ошибка обновления баз** • **Проверка целостности** • **Приложение запущено. Проверка в режиме реального времени запущена** • **Экспорт параметров**
Имя пользователя	• **=;** • **≠;** • **включает**; • **не включает.**	Имя пользователя в LDAP, под учетной записью которого произошло событие. Действия, выполненные приложением автоматически, записываются в журнал событий под учетной записью пользователя kluser.
Результат	• **=**; • **≠**.	Выберите результат: • **Успешно**; • **Ошибка**.

Вы можете указать несколько критериев фильтрации. Чтобы добавить еще один критерий, нажмите на кнопку **Добавить фильтр**. Критерии фильтрации объединяются логическим оператором "И".

7. Нажмите на кнопку **Применить**.
8. Закройте окно добавления фильтра.

Отобразится таблица событий, удовлетворяющих критериям фильтрации.

Просмотр информации о событии обработки почтового трафика

По ссылке в верхней части окна вы можете перейти в раздел **Хранилище** и посмотреть информацию о сообщениях в Хранилище, связанных с этим событием.

► *Чтобы просмотреть информацию о событии обработки почтового трафика:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Почтовый трафик**.

   Информация о событиях обработки почтового трафика отобразится в виде таблицы.
3. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии.

В окне с информацией о событии обработки почтового трафика отображаются следующие поля:

- **Дата и время** – дата и время выполнения события.
- **Узел** – IP-адрес и порт узла, на котором было обработано сообщение.
- **Email отправителя** – имя отправителя сообщения.
- **Кому** – имя получателя сообщения.
- **CC** – имя получателя копии сообщения.
- **BCC** – имя получателя скрытой копии сообщения.
- **Тема** – тема сообщения.
- **Название правила** – название правила, в соответствии с которым было обработано сообщение.

  Вы можете просмотреть подробную информацию о правиле, нажав на ссылку с названием правила.
- **Действие** – действие, выполненное над сообщением.
- Блок параметров **Результат проверки**, в котором отображаются статусы, присвоенные сообщению каждым модулем проверки.
  - **Антивирус**:
    - *Не проверено*.
    - *Не обнаружено*.
    - *Зашифровано*.
    - *Ошибка*.
    - *Вылечено*.
    - *Заражено*.
  - **Анти-Спам**:

- *Не проверено*.
- *Не обнаружено*.
- *Доверенный источник*.
- *Формальное сообщение*.
- *Ошибка*.
- *Предполагаемый спам*.
- *В списке запрещенных адресов*.
- *Спам*.
- *Массовая рассылка*.

- **Анти-Фишинг**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Ошибка*.
  - *Фишинг*.
- **Проверка ссылок**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Ошибка*.
  - *Обнаружено*.
  - *Ошибка баз*.
- **Контентная фильтрация**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Превышен допустимый размер*.
  - *Запрещенное имя вложения*.
  - *Запрещенный формат вложения*.
  - *Ошибка*.
- **KATA**:
  - *Обнаружено*.
  - *Ошибка*.
  - *Не обнаружено*.
  - *Не проверено*.
  - *Пропущено*.

  Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

- Информация о вложении:
  - **Имя файла**.
  - **Размер файла (в байтах)**.
  - **Формат файла**.

    Информация о формате файла отображается, если формат вложенного файла был указан в правиле обработки контентной фильтрации (см. раздел "Настройка контентной фильтрации" на стр. 116).
- Результат проверки вложения.

Просмотр информации о событии приложения

► *Чтобы просмотреть информацию о событии приложения:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Приложение**.

   Информация о событиях приложения отобразится в виде таблицы.
3. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии.

В окне с информацией о событии приложения отображаются следующие поля:

- **Дата и время** – дата и время события.
- **Узел** – IP-адрес и порт узла, на котором произошло событие.
- **Тип события** – тип события приложения (см. раздел "Типы событий приложения" на стр. 215):
  - **Аудит**.
  - **Хранилище**.
  - **Обновление баз**.
  - **Экспорт параметров**.
  - **Импорт параметров**.
  - **Проверка целостности**.
  - **Синхронизация LDAP**.
- **Событие** – название события.
- **Имя пользователя** – имя пользователя узла, на котором произошло событие.
- **Результат** – результат обработки события:
  - **Ошибка**.
  - **Успешно**.
- **Сведения** – информация о событии приложения.

kaspersky

См. также

Типы событий приложения

Описание событий приложения, информация о которых записывается в журнал событий (раздел **События** → **Приложение**), представлено в таблице ниже.

Таблица 9. Описание событий приложения разных типов

Тип события	Событие	Результат обработки события	Сведения
Обновление баз	Антивирусные базы применены	Успешно	Время обновления: "<Дата и время обновления>"
	Ошибка загрузки антивирусных баз	Ошибка	Ошибка загрузки: <Название ошибки>
	Антивирусные базы актуальны	Успешно	
	Базы Анти-Спама применены	Успешно	Время обновления: "<Дата и время обновления>"
	Ошибка загрузки баз Анти-Спама	Ошибка	Ошибка загрузки: <Название ошибки>
	Базы Анти-Спама актуальны	Успешно	
	Базы Анти-Фишинга применены	Успешно	Время обновления: "<Дата и время обновления>"
	Ошибка загрузки баз Анти-Фишинга	Ошибка	Ошибка загрузки: <Название ошибки>
	Базы Анти-Фишинга актуальны	Успешно	
	Задача запущена	Успешно	Обновление запущено
	Ошибка обновления баз	Ошибка	Ошибка: <Название ошибки>
Аудит	Аудит запущен	Успешно	
	Приложение запущено. Проверка в режиме реального времени запущена	Успешно	
	Аудит остановлен	Успешно	
Синхронизация LDAP	Задача запущена	Успешно	Запущена синхронизация LDAP
Проверка целостности	Проверка целостности	Успешно	Нарушения не найдены
		Ошибка	Найдены нарушения
Хранилище	Дайджест Хранилища отправлен	Успешно	Дайджест Хранилища отправлен <количество пользователей> пользователям
		Ошибка	Не удалось отправить дайджест Хранилища <количество пользователей> пользователям

Тип события	Событие	Результат обработки события	Сведения
Экспорт параметров	Экспорт параметров	Успешно	Параметры экспортированы
		Ошибка	Экспорт завершился с ошибкой
Импорт параметров	Импорт параметров	Успешно	Параметры импортированы
		Ошибка	Импорт завершился с ошибкой

Экспорт журнала событий

Вы можете экспортировать таблицу событий в файл формата CSV.

► *Чтобы экспортировать таблицу событий:*

1. В окне веб-интерфейса приложения в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**
   - **Приложение**.

   Информация о событиях отобразится в виде таблицы.
3. Нажмите на кнопку **Экспорт**.
4. Если в параметрах браузера включена возможность выбирать путь для сохранения при скачивании файлов, то откроется окно выбора. Укажите путь, по которому должен быть сохранен файл, и нажмите на кнопку **Save**.

Начнется загрузка файла. Таблица событий будет экспортирована в файл формата CSV.

Если вы предварительно отфильтровали события в таблице (см. раздел "Фильтрация событий обработки почтового трафика" на стр. 206), настроили сортировку событий в столбцах (см. раздел "Просмотр журнала событий" на стр. 204) и отображение столбцов в таблице (см. раздел "Настройка отображения таблицы событий" на стр. 205), все заданные настройки сохранятся при экспорте таблицы в файл.

kaspersky

Настройка параметров журнала событий

При настройке длительности хранения событий и выборе типов событий для записи нужно учитывать доступное дисковое пространство на обрабатывающих серверах.

Параметры записи событий в журнал событий не влияют на параметры записи событий по протоколу Syslog.

► *Чтобы настроить параметры записи в журнал событий:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Журналы и события** → **События**.
2. В блоке параметров **Почтовый трафик** выполните следующие действия:
   a. В раскрывающемся списке **Записывать события обработки трафика** выберите, какие события обработки трафика должны быть записаны в журнал событий. Вы можете выбрать один из следующих вариантов:
      - **Все**.
      - **Применено действие Удалить сообщение/Удалить вложение/Отклонить**.
      - **Не записывать**.

      По умолчанию выбран параметр **Все**.

      Выбранное значение параметра применяется только к событиям, записанным в журнал событий после применения изменений. К событиям, которые были записаны в журнал ранее, новое значение параметра не применяется.
      Выбранное значение параметра применяется на всех узлах кластера.

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

      Значение по умолчанию: 1024 МБ. Допустимые значения – целые числа от 100 до 2147483647.

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

      Значение по умолчанию: 3 дня. Допустимые значения – целые числа от 1 до 8589934592.
3. В блоке параметров **Приложение** выполните следующие действия:
   a. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

      Значение по умолчанию: 1024 МБ. Допустимые значения – целые числа от 100 до 2147483647.

   b. В поле **Срок хранения событий в журнале (дней)** укажите, сколько дней приложение должно хранить события приложения на сервере.

Параметры записи событий в журнал событий будут настроены.

kaspersky

Очередь сообщений

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 таблицы сообщений в очереди

► *Чтобы просмотреть таблицу сообщений в очереди,*

в окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.

В таблице отображается следующая информация о сообщениях в очереди:

- **Очередь**.
- **ID сообщения**.
- **Email отправителя**.
- **Email получателя**.
- **Тема**.
- **Размер сообщения**.
- **Время получения**.
- **Ошибка**.
- **Узел**.

По умолчанию в таблице отображаются не все столбцы. Вы можете настроить отображение таблицы, открыв окно **Настроить таблицу** по кнопке .

kaspersky

Просмотр сводной статистики

Информация о KATA карантине отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

► *Чтобы просмотреть сводную статистику по всем узлам кластера,*

в окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.

Отобразится следующая информация:

- **Анти-Спам карантин, занято**. Размер Анти-Спам карантина и процент использования Анти-Спам карантина по сравнению с максимальным размером, заданным в параметрах модуля Анти-Спам (см. стр. 249).
- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине в настоящий момент.
- **KATA карантин, занято**. Размер KATA карантина и процент использования KATA карантина по сравнению с максимальным размером, заданным в параметрах защиты KATA (см. раздел "Настройка параметров защиты KATA" на стр. 283).
- **KATA карантин, сообщений**. Количество сообщений в KATA карантине в настоящий момент.

Вы также можете просмотреть статистику по каждому узлу кластера отдельно (см. раздел "Просмотр статистики по узлам" на стр. 221).

Просмотр статистики по узлам

Информация о KATA карантине отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).

► *Чтобы просмотреть статистику по узлам кластера:*

1. В веб-интерфейсе приложения выберите раздел **Очередь сообщений**.
2. Нажмите на кнопку **Показать статистику очередей по узлам**.

   Откроется страница **Статистика очередей по узлам**.

На странице отображается таблица со статистикой очередей по узлам кластера. Таблица содержит следующие столбцы:

- **Узел**. IP-адрес и порт подключения к узлу кластера.
- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине в настоящий момент.
- **Анти-Спам карантин, занято**. Размер Анти-Спам карантина.
- **Анти-Спам карантин, занято (%)**. Процент использования Анти-Спам карантина по сравнению с максимальным размером, заданным в параметрах модуля Анти-Спам (см. стр. 249).

- **KATA карантин, сообщений**. Количество сообщений в KATA карантине в настоящий момент.
- **KATA карантин, занято**. Размер KATA карантина.
- **KATA карантин, занято (%)**. Процент использования KATA карантина по сравнению с максимальным размером, заданным в параметрах защиты KATA (см. раздел "Настройка параметров защиты KATA" на стр. 283).

Если в очередях более 5000 сообщений, отображается примерное их количество.

Сортировка сообщений в очереди

► Чтобы отсортировать *сообщения в очереди*:

1. В окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.

   Откроется таблица сообщений в очереди.
2. Нажмите на название того столбца таблицы, по которому вы хотите отсортировать сообщения:
   - **Очередь** – название очереди.
   - **ID сообщения** – ID сообщений в очереди.
   - **Email отправителя** – адрес отправителя сообщений.
   - **Email получателя** – адрес получателя сообщений.
   - **Тема** – тема сообщения.
   - **Размер сообщения** – размер сообщений.
   - **Время получения** – время поступления сообщений в очередь.
   - **Ошибка** – ошибка проверки сообщений.
   - **Узел** – узел кластера, на котором было обработано сообщение.
3. Если вы хотите изменить порядок сортировки, нажмите на название столбца повторно. Слева от названия столбца отобразится новый порядок сортировки в виде кнопки или .

Сообщения в очереди будут отсортированы.

Фильтрация и поиск сообщений в очереди

► Чтобы отфильтровать или найти сообщения в *очереди*:

1. В окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.
2. Нажмите на кнопку **Фильтры**.

   Откроется окно **Фильтры**.
3. В блоке параметров **Очередь** установите флажки рядом с названиями очередей, по которым вы хотите отфильтровать сообщения.

   Вы можете выбрать одну или несколько очередей:

- **KATA-карантин**.
- **Анти-Спам карантин**.

4. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска сообщения.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите критерий:	b. Выберите логический оператор:	c. Укажите следующее значение:
Email отправителя	• **включает**.	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).
Email получателя	• **включает**.	Текст поиска адресов электронной почты получателей сообщений.
Дата сообщения	• **после**; • **до**.	Интервал обработки и помещения сообщений в Хранилище.
Размер сообщения	• **⩽**; • **⩾**.	Ограничение поиска по размеру сообщений в килобайтах.
ID сообщения	• **включает**.	Уникальный идентификатор, присвоенный сообщению приложением.
Узел	• **=**; • **≠**.	Узел кластера, на котором было обработано сообщение.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку .

5. Нажмите на кнопку **Применить**.

Сообщения, удовлетворяющие параметрам поиска, отобразятся в списке сообщений в разделе **Очередь сообщений**.

В таблице отображается информация о последних 5000 сообщений. Если согласно заданным критериям фильтрации найдено более 5000 сообщений, рекомендуется уточнить критерии поиска.

Принудительная отправка сообщений из очереди

Принудительная отправка сообщений из Анти-Спам карантина может привести к снижению уровня обнаружения спама.

Чтобы принудительно отправить сообщения из очереди:

1. В окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.
2. Установите флажки рядом с сообщениями, которые вы хотите отправить, или выделите все сообщения.
3. В панели инструментов в верхней части рабочей области нажмите на кнопку **Отправить**.

   Если вы выделили все сообщения и установили критерии фильтрации, то операция применяется только к сообщениям, удовлетворяющим заданным критериям. При необходимости отправить все сообщения в очереди требуется сбросить фильтр.

4. В окне подтверждения выполните одно из следующих действий:
   - Если количество сообщений менее 5000, нажмите на кнопку **ОК**, чтобы подтвердить принудительную отправку всех сообщений (выбранных или удовлетворяющих заданным критериям фильтрации).
   - Если количество сообщений превышает 5000, выберите, требуется ли отправить только отображаемые сообщения или все сообщения (находящиеся во всех очередях или удовлетворяющие заданным критериям фильтрации).

Сообщения будут отправлены.

См. также

Удаление сообщений из очереди

► *Чтобы удалить сообщения из очереди:*

1. В окне веб-интерфейса приложения выберите раздел **Очередь сообщений**.
2. Установите флажки рядом с сообщениями, которые вы хотите удалить, или выделите все сообщения.
3. В панели инструментов в верхней части рабочей области нажмите на кнопку **Удалить**.

Если вы выделили все сообщения и установили критерии фильтрации, то операция применяется только к сообщениям, удовлетворяющим заданным критериям. При необходимости удалить все сообщения в очереди требуется сбросить фильтр.

4. В окне подтверждения выполните одно из следующих действий:
   - Если количество сообщений менее 5000, нажмите на кнопку **ОК**, чтобы подтвердить удаление всех сообщений (выделенных или удовлетворяющих заданным критериям фильтрации).
   - Если количество сообщений превышает 5000, выберите, требуется ли удалить только отображаемые сообщения или все сообщения (находящиеся во всех очередях или удовлетворяющие заданным критериям фильтрации).

Сообщения будут удалены.

kaspersky

Отчеты

Для отслеживания результатов работы приложения вы можете создавать отчеты.

Kaspersky Security для Linux Mail Server поддерживает создание разовых отчетов по запросу пользователя (см. раздел "Создание отчета по требованию" на стр. 227), а также настройку регулярных отчетов, создаваемых по расписанию (см. раздел "Настройка параметров отчетов по расписанию" на стр. 228).

Информация обо всех созданных отчетах (см. раздел "Просмотр информации об отчете" на стр. 231) отображается в виде таблицы в разделе **Отчеты**. Для удобства поиска вы можете фильтровать и сортировать записи об отчетах (см. раздел "Фильтрация и сортировка отчетов" на стр. 230).

Чтобы ознакомиться с содержанием отчета (см. раздел "Содержание отчетов" на стр. 232), вы можете выполнить следующие действия:

- настроить отправку отчета по электронной почте во время его создания по требованию или при настройке расписания;
- переслать ранее созданный отчет на дополнительные адреса (см. раздел "Отправка отчетов по электронной почте" на стр. 236), а также повторно отправить на исходные адреса;
- скачать отчет на компьютер (см. раздел "Скачивание отчетов" на стр. 236).

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от приложения" на стр. 328), который указывается в качестве отправителя отчетов о работе приложения.

Отчеты хранятся в базе данных на Управляющем узле. Если вы назначите роль Управляющего узла в кластере другому серверу, все ранее созданные отчеты будут потеряны.

В этом разделе

kaspersky

Создание отчета по требованию

► *Чтобы создать отчет по требованию:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите закладку **По требованию**.
3. Нажмите на кнопку **Создать отчет**.

   Откроется окно **Создать отчет вручную**.
4. В раскрывающемся списке **Период** выберите тип временного интервала, за который вы хотите сформировать отчет:
   - **Другой** – любой временной интервал (доступны последние 124 дня).
   - **День** – с 00:00:00 до 23:59:59 выбранного дня (при выборе текущего дня – с 00:00:00 до момента создания отчета).

     Доступны последние 7 дней, включая текущий.
   - **Неделя** – с 00:00:00 понедельника до 23:59:59 воскресенья выбранной недели (при выборе текущей недели – с 00:00:00 понедельника до момента создания отчета).

     Доступны последние 17 недель, включая текущую.
   - **Месяц** – с 00:00:00 1 числа до 23:59:59 последнего дня выбранного месяца (при выборе текущего месяца – с 00:00:00 1 числа до момента создания отчета).

     Доступны последние 4 месяца, включая текущий.
   - **Год** – с 00:00:00 1 января до 23:59:59 31 декабря выбранного года (при выборе текущего года – с 00:00:00 1 января до момента создания отчета).

     Доступны последние 3 года, включая текущий.
5. Нажмите на текстовую область в поле ниже и в раскрывшемся календаре выберите временной интервал, данные за который должны быть представлены в отчете.
6. В раскрывающемся списке **Узлы** выберите адрес узла кластера, данные о котором вы хотите получить в отчете, или **Все узлы**, если вы хотите получить данные обо всех узлах.
7. Если вы хотите отправить созданный отчет по электронной почте, в блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится новый блок параметров доставки отчета.
8. В поле **Адреса электронной почты** введите адреса, на которые вы хотите отправить отчет.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.
9. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправить отчет.
10. В раскрывающемся списке **Язык** выберите язык отчета.
11. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка  справа от блока.
12. Нажмите на кнопку **Создать**.

Отчет будет создан. Информация об отчете (см. раздел "Просмотр информации об отчете" на стр. 231) отобразится в таблице на закладке **По требованию**. Вы можете скачать созданный отчет (см. раздел

"Скачивание отчетов" на стр. 236) или отправить его по электронной почте (см. раздел "Отправка отчетов по электронной почте" на стр. 236).

Настройка параметров отчетов по расписанию

Вы можете настроить любой тип отчета по расписанию (ежедневный, еженедельный или ежемесячный) независимо друг от друга.

Отчеты, создаваемые по расписанию, содержат данные о работе всех узлов кластера. Выбор отдельных узлов недоступен.

► *Чтобы настроить параметры отчетов по расписанию:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите закладку **По расписанию**.
3. Нажмите на кнопку **Настроить расписание**.

   Откроется окно **Настроить расписание**.
4. Выберите одну из следующих закладок в зависимости от типа отчета, который вы хотите настроить:
   - **Ежедневно**. Отчет содержит данные с 00:00 до 23:59 предыдущего дня.
   - **Еженедельно**. Отчет содержит данные с 00:00 понедельника до 23:59 воскресенья предыдущей недели.
   - **Ежемесячно**. Отчет содержит данные с 00:00 первого числа до 23:59 последнего дня предыдущего месяца.
5. Переведите переключатель с названием типа отчета в положение **Включено**.
6. Задайте расписание создания нужного отчета:
   - На закладке **Ежедневно** укажите время создания отчета.
   - На закладке **Еженедельно** укажите день недели и время создания отчета.

     Например, если установлены значения **Пн** и **15:00**, отчет создается каждый понедельник в 15 часов.
   - На закладке **Ежемесячно** укажите день месяца и время создания отчета.

     Например, если установлены значения **20** и **15:00**, отчет создается каждый месяц двадцатого числа в 15 часов.

     Если указанное значение превышает количество дней в месяце, в такие месяцы отчет не будет создан. Например, если указано значение **31**, отчет не будет сформирован в месяцы с 30 днями.
7. Если вы хотите отправлять отчеты по электронной почте, в блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится блок параметров доставки отчета.
8. В поле **Адреса электронной почты** введите адреса, на которые вы хотите отправлять отчеты.

Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.

9. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправлять отчеты. Возможные значения: **Pdf**, **Html**.
10. В раскрывающемся списке **Язык** выберите язык отчетов.
11. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка справа от блока.
12. Нажмите на кнопку **Сохранить**.

Параметры отчетов по расписанию будут настроены. Как только первый отчет будет создан в указанное время, информация о нем (см. раздел "Просмотр информации об отчете" на стр. 231) отобразится в таблице отчетов. Вы сможете скачать отчет (см. раздел "Скачивание отчетов" на стр. 236) или отправить его по электронной почте (см. раздел "Отправка отчетов по электронной почте" на стр. 236).

Настройка отображения таблицы отчетов

По умолчанию в таблице отчетов отображаются все доступные столбцы. Если требуется, вы можете скрыть некоторые из них или изменить их очередность.

► *Чтобы настроить отображение таблицы отчетов:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите настроить таблицу отчетов, созданных разово по запросу пользователя.
   - **По расписанию**, если вы хотите настроить таблицу отчетов, созданных автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Нажмите на кнопку в первой строке таблицы.

   Откроется окно **Настроить таблицу**.
4. Установите флажки напротив тех столбцов, которые должны отображаться в таблице.
5. Если вы хотите изменить расположение столбца в таблице, в правой части строки с названием столбца зажмите кнопку и перетащите столбец на нужное место.
6. Нажмите на кнопку **ОК**.

Отображение таблицы отчетов будет настроено.

kaspersky

Фильтрация и сортировка отчетов

Вы можете отсортировать все записи о созданных ранее отчетах по значению любого столбца в таблице отчетов. С помощью значка  в заголовке столбца можно изменять порядок сортировки по возрастанию или по убыванию.

Вы также можете отфильтровать отчеты по времени создания, временному интервалу содержащихся в них данных, а также по типу (только для отчетов по расписанию).

► *Чтобы отфильтровать отчеты:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите отфильтровать отчеты, созданные разово по запросу пользователя.
   - **По расписанию**, если вы хотите отфильтровать отчеты, созданные автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Нажмите на значок  .

   Откроется окно **Фильтры**.
4. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска отчетов.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Тип	• **=**; • **≠**.	Выберите тип отчета из раскрывающегося списка (применимо только для отчетов, созданных по расписанию): • **Ежедневный**; • **Еженедельный**; • **Ежемесячный**.
Время создания	• **после**; • **до**.	Временной диапазон создания отчета.
Начало периода	• **после**; • **до**.	Временной диапазон начала отчетного периода.
Окончание периода	• **после**; • **до**.	Временной диапазон окончания отчетного периода.

   Вы можете указать несколько критериев фильтрации.
6. Нажмите на кнопку **Применить**.

Отчеты, удовлетворяющие параметрам поиска, отобразятся в таблице отчетов.

kaspersky

Просмотр информации об отчете

► Чтобы просмотреть информацию об отчете:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите просмотреть информацию об отчетах, созданных разово по запросу пользователя.
   - **По расписанию**, если вы хотите просмотреть информацию об отчетах, созданных автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, информацию о котором вы хотите просмотреть.

   Откроется окно **Просмотреть информацию об отчете**.

В окне отображается следующая информация об отчете:

- **Время создания**. Время создания отчета.
- **Период**. Интервал времени, за который получена информация о работе приложения, представленная в отчете.
- **Тип**. Тип отчета, созданного по расписанию:
  - **Ежедневный**.
  - **Ежемесячный**.
  - **Еженедельный**.

  Не отображается для отчетов, созданных по запросу пользователя.
- **Узлы**. IP-адреса и порты подключения тех узлов, информация о работе которых представлена в отчете (или **Все узлы**).
- **Параметры доставки**. Группа параметров доставки отчета по электронной почте, которая включает в себя список адресов, язык и формат отчета.
  - **При создании**. Параметры доставки, указанные во время создания отчета.
  - **При пересылке**. Параметры доставки, указанные для созданного ранее отчета при его пересылке на дополнительные адреса (см. раздел "Отправка отчетов по электронной почте" на стр. 236).

  В блоке **Параметры доставки** отображаются только уникальные группы параметров.
- **Результат**. Возможны следующие значения:
  - *Ошибка*.
  - *Ожидает*.
  - *Успешно*.

kaspersky

Содержание отчетов

Отчеты содержат следующую информацию о работе приложения.

1. Блок **Общая информация**.
   - **Обнаружения**. Количество и объем обработанных сообщений, подсчитанных по каждому модулю приложения в отдельности:
     - **Антивирус**.
     - **Проверка ссылок**.
     - **Защита KATA**.

       Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 277).
     - **Анти-Фишинг**.
     - **Анти-Спам**.
     - **Проверка подлинности**.
     - **Контентная фильтрация**.
   - **Действия над сообщениями**. Количество и объем обработанных сообщений, подсчитанных по каждому типу выполненного приложением действия:
     - **Не обнаружено**.
     - **Вылечено**.
     - **Удалены вложения**.
     - **Пропущено**.
     - **Не проверено**.
     - **Удалено**.
     - **Отклонено**.
     - **Помещено в Карантин**.
   - **Узлы**. Количество и объем обработанных сообщений, подсчитанных по каждому узлу кластера, обрабатывающему почтовый трафик.
2. Блок **Типы объектов**.
   - **Антивирус**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Антивирус:
     - **Не обнаружено**.
     - **Обнаружено**.
     - **Вложения с макросами**.
     - **Непроверенные сообщения**.

       Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

- **Зашифровано**. Не удалось выполнить проверку, т.к. сообщение зашифровано.
- **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
- **Параметры программы**. Отключена антивирусная проверка в общих параметрах защиты.
- **Ограничения лицензирования**. Возникли проблемы с лицензией.
- **Ошибка баз**. Отсутствуют антивирусные базы.

- **Проверка ссылок**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки ссылок:
  - **Не обнаружено**.
  - **Обнаружено**.
  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:
    - **Ошибка проверки**. Возникла ошибка во время проверки ссылок.
    - **Параметры программы**. Отключена проверка ссылок в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы приложения.
- **Анти-Фишинг**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Анти-Фишинг:
  - **Не обнаружено**.
  - **Обнаружено**.
  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:
    - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
    - **Параметры программы**. Отключена проверка модулем Анти-Фишинг в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы приложения.
- **Анти-Спам**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Анти-Спам:
  - **Не обнаружено**.
  - **Обнаружено**.

    Обнаруженные объекты сгруппированы по следующим типам:
    - **Спам**.
    - **Предполагаемый спам**.
    - **Массовые рассылки**.

- **На карантине**.
- **Непроверенные сообщения**.

  Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

  - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
  - **Параметры программы**. Отключена проверка модулем Анти-Спам в общих параметрах защиты.
  - **Ограничения лицензирования**. Возникли проблемы с лицензией.
  - **Ошибка баз**. Отсутствуют базы приложения.

- **Проверка подлинности отправителей**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки подлинности отправителя:
  - **Не обнаружено**.
  - **Обнаружено**.
  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

    - **Параметры программы**. Отключена проверка подлинности отправителя в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы приложения.

- **Контентная фильтрация**.
  - **Не обнаружено**.
  - **Обнаружено**.

    Обнаруженные объекты сгруппированы по следующим типам:

    - **Размер сообщения**. Превышен максимальный допустимый размер сообщения.
    - **Имя вложения**. Имя вложения соответствует критериям, заданным в правиле обработки сообщений.
    - **Тип вложения**. Формат вложения соответствует критериям, заданным в правиле обработки сообщений.

  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

    - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
    - **Параметры программы**. Отключена контентная фильтрация в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы приложения.

- **Примененные правила обработки сообщений**. Количество и объем сообщений, обработанных по каждому сработавшему правилу.

3. Блок **Статистика Антивируса**.
   - **Топ 10 полученных вредоносных объектов**. Имена самых частых вредоносных объектов в полученных сообщениях и количество срабатываний модуля Антивирус по каждому объекту.
   - **Топ 10 отправителей вредоносных объектов**. Адреса электронной почты самых частых отправителей вредоносных объектов, а также количество срабатываний модуля Антивирус по каждому отправителю.
   - **Топ 10 получателей вредоносных объектов**. Адреса электронной почты самых частых получателей вредоносных объектов, а также количество срабатываний модуля Антивирус по каждому получателю.
4. Блок **Статистика проверки ссылок**.
   - **Топ 10 источников вредоносных|рекламных|легальных ссылок**. IP-адреса серверов, с которых чаще всего отправлялись вредоносные/рекламные/легальные ссылки, а также количество срабатываний по каждому источнику.
   - **Топ 10 получателей вредоносных|рекламных|легальных ссылок**. Адреса электронной почты самых частых получателей вредоносных/рекламных/легальных ссылок, а также количество срабатываний по каждому получателю.
5. Блок **Статистика Анти-Фишинга**.
   - **Топ 10 источников фишинга**. IP-адреса серверов, с которых чаще всего отправлялись фишинговые сообщения, а также количество срабатываний по каждому источнику.
   - **Топ 10 получателей фишинга**. Адреса электронной почты самых частых получателей фишинговых сообщений, а также количество срабатываний по каждому получателю.
6. Блок **Статистика Анти-Спама**.
   - **Топ 10 источников спама**. IP-адреса серверов, с которых чаще всего отправлялся спам или массовые рассылки, а также количество срабатываний по каждому источнику.
   - **Топ 10 получателей спама**. Адреса электронной почты самых частых получателей спама или массовых рассылок, а также количество срабатываний по каждому получателю.

Удаление отчетов

► Чтобы удалить отчет:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите удалить отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите удалить отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите удалить.

   Откроется окно **Просмотреть информацию об отчете**.
4. В нижней части окна нажмите на кнопку **Удалить**.
5. В окне подтверждения нажмите на кнопку **ОК**.

Отчет будет удален.

kaspersky

Скачивание отчетов

► *Чтобы скачать отчет:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите скачать отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите скачать отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите скачать.

   Откроется окно **Просмотреть информацию об отчете**.
4. В нижней части окна нажмите на кнопку **Скачать**.

   Откроется окно **Скачать отчет**.
5. В раскрывающемся списке **Язык** выберите язык отчета.
6. В раскрывающемся списке **Формат** выберите один из следующих форматов файла отчета:
   - **Html**.
   - **Pdf**.
7. Нажмите на кнопку **Скачать**.

Файл отчета будет сохранен на вашем компьютере в папке загрузки браузера.

Отправка отчетов по электронной почте

Вы можете указать адреса электронной почты, на которые требуется отправить отчет при его создании по требованию (см. раздел "Создание отчета по требованию" на стр. 227) или при настройке отчетов по расписанию (см. раздел "Настройка параметров отчетов по расписанию" на стр. 228).

Если требуется, вы можете переслать созданный ранее отчет на дополнительные адреса или отправить повторно на исходные адреса, указанные при создании отчета.

► *Чтобы отправить созданный ранее отчет по электронной почте:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите отправить отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите отправить отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите отправить.

   Откроется окно **Просмотреть информацию об отчете**.
4. В нижней части окна нажмите на кнопку **Доставить отчет**.

   Откроется окно **Доставить отчет**.

5. В блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится новый блок параметров доставки отчета на дополнительные адреса.

6. В поле **Адреса электронной почты** введите адреса, на которые вы хотите переслать созданный ранее отчет.

   > Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.

7. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправить отчет.
8. В раскрывающемся списке **Язык** выберите язык отчета.
9. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка справа от блока.
10. Если вы хотите повторно отправить отчет на адреса, указанные при его создании, включите переключатель **Отправить повторно оригинальным получателям**.

    > Переключатель не отображается, если при создании отчета по требованию или при настройке расписания автоматических отчетов вы не указали ни одного адреса в блоке **Параметры доставки**.

11. В нижней части окна нажмите на кнопку **Отправить**.

Отчет будет отправлен на указанные адреса. В нижней части рабочей области отобразится всплывающее окно с информацией о результате отправки.

kaspersky

Общие параметры защиты

Kaspersky Security для Linux Mail Server обеспечивает защиту входящей и исходящей почты организации. Вы можете настроить следующие общие параметры защиты:

- Антивирусная защита.
- Проверка ссылок.
- Защита сообщений от спама.
- Защита сообщений от фишинга.
- Контентная фильтрация сообщений.
- Проверка подлинности отправителей сообщений.

Общие параметры защиты применяются при проверке всех сообщений. Вы можете настроить действия над сообщениями по результатам проверки, а также дополнительные параметры с помощью правил обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 101).

Антивирусная защита

Kaspersky Security 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.

Вы можете настроить следующие параметры модуля Антивирус (см. стр. 247):

- использование эвристического анализа;
- максимальное время проверки сообщений;
- максимальный уровень проверки архивов;
- исключения из проверки некоторых легальных программ, которые могут быть использованы злоумышленниками.

По результатам проверки модуль Антивирус присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не заражено.
- *Заражено* – сообщение заражено, не может быть вылечено или лечение не проводилось.
- *Вылечено* – сообщение вылечено.
- *Зашифровано* – не удалось проверить объект из-за того, что он зашифрован.
- *Ошибка* – при проверке сообщения произошла ошибка.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки применения баз приложения.
- *Угроза вторжения* – объект может быть использован злоумышленниками для вторжения в локальную сеть.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.

- *Возможно зараженный* – объект содержит признаки вредоносного кода.

По умолчанию модуль Антивирус включен. Если требуется, вы можете отключить модуль Антивирус или отключить антивирусную проверку сообщений для любого правила (см. раздел "Настройка антивирусной защиты" на стр. 109).

Проверка ссылок

Kaspersky Security для Linux Mail Server проверяет, являются ли ссылки в тексте сообщения вредоносными, рекламными или относящимися к легальным программам (см. раздел "О защите компьютеров от некоторых легальных программ" на стр. 243), способным причинить вред компьютеру.

Вы можете настроить следующие параметры проверки ссылок (см. раздел "Настройка параметров проверки ссылок" на стр. 248):

- Максимальное время проверки сообщения.
- Исключения из проверки.

  Вы можете отключить обнаружение рекламных ссылок и ссылок, связанных с некоторыми легальными программами.

По результатам проверки ссылок приложение присваивает сообщению один из следующих статусов:

- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз приложения.
- *Не обнаружено* – сообщение не содержит ссылок, обнаружение которых включено согласно параметрам приложения.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Обнаружено* – в сообщении содержатся вредоносные, рекламные или относящиеся к легальным программам ссылки.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.

Защита сообщений от спама

Kaspersky Security для Linux Mail Server фильтрует сообщения, проходящие через почтовый сервер, от нежелательной почты (спама).

Проверку сообщений на спам выполняет модуль Анти-Спам. Модуль Анти-Спам проверяет каждое сообщение на присутствие в нем признаков спама. Для этого модуль Анти-Спам, во-первых, проверяет атрибуты сообщения, такие, как: адреса отправителя и получателя, размер сообщения, заголовки (включая заголовки От и Кому). Во-вторых, модуль Анти-Спам анализирует содержание сообщения (включая заголовок Тема) и вложенных файлов.

Приложение присваивает сообщению, в котором обнаружен спам или вероятный спам, определенный статус в соответствии со спам-рейтингом. *Спам-рейтинг сообщения* – это целое число от 0 до 100, которое складывается из баллов, начисленных сообщению приложением за каждое срабатывание модуля Анти-Спам. При определении спам-рейтинга учитываются также результаты SPF-проверки и репутационной фильтрации сообщений.

При включении модуля Анти-Спам автоматически включается защита от BEC-атак. Это позволяет распознавать поддельные письма злоумышленников, направленные на компрометацию деловой переписки.

Вы можете настроить следующие параметры модуля Анти-Спам (см. стр. 249):

- Использование службы Moebius.

  Служба Moebius определяет разницу между текущей базой Анти-Спама, используемой в приложении, и базой на сервере Moebius. После этого недостающие записи передаются на

Управляющий узел по протоколу HTTPS. Чтобы объем передаваемых данных не становился большим и служба Moebius работала стабильно, в приложении должны регулярно обновляться базы Анти-Спама.

- Защиту от спуфинга Active Directory.

  Модуль Анти-Спам позволяет предотвращать спуфинговые атаки, в которых злоумышленники используют поддельное имя (Display Name) в заголовке сообщений From. При этом домен, с которого было отправлено сообщение, не совпадает с доменом организации. Вы можете указать в приложении одну группу Active Directory численностью не более 10 000, к пользователям которой будет применяться защита от спуфинга.

- Проверку репутации IP-адресов и доменов.

  Эта опция позволяет проверять данные SMTP-сессии на основе записей о запрещенных IP-адресах и доменах в базах модуля Анти-Спам.

- Использование Анти-Спам карантина.

  Использование Анти-Спам карантина доступно только при участии в KSN (см. раздел "Участие в Kaspersky Security Network и использование Kaspersky Private Security Network" на стр. 266).

  После помещения сообщения в Анти-Спам карантин приложение обращается к серверам KSN для дальнейшей проверки сообщения. Использование облачной службы KSN повышает точность обнаружения признаков спама, так как базы KSN содержат более актуальную информацию, чем базы Анти-Спама, используемые в приложении.

- Максимальное время проверки сообщений.
- Максимальное время хранения сообщения в Анти-Спам карантине
- Максимальное количество сообщений в Анти-Спам карантине.
- Максимальный размер Анти-Спам карантина.

По результатам проверки модуль Анти-Спам присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не содержит спам.
- *Спам* – приложение однозначно расценивает сообщение как спам.
- *Предполагаемый спам* – возможно, сообщение является спамом.
- *Массовая рассылка* – сообщение относится к массовой рассылке.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз приложения.
- *Формальное сообщение* – приложение расценивает сообщение как формальное автоматически сгенерированное уведомление (например, автоответы пользователей или уведомления о превышении размера почтового ящика).
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.
- *Доверенный источник* – сообщение получено от отправителя, домен которого находится в списке разрешенных в базах модуля Анти-Спам, и прошло DMARC-проверку подлинности отправителей.

По результатам проверки приложение добавляет в сообщение X-заголовок `X-MS-Exchange-Organization-SCL`, который содержит SCL-оценку.

По умолчанию модуль Анти-Спам включен. Если требуется, вы можете отключить модуль Анти-Спам или отключить проверку сообщений на спам для любого правила (см. раздел "Настройка защиты от спама" на стр. 113).

Защита сообщений от фишинга

Kaspersky Security для Linux Mail Server фильтрует сообщения, проходящие через почтовый сервер, от фишинга.

Проверку сообщений на наличие фишинга выполняет модуль Анти-Фишинг. Модуль Анти-Фишинг анализирует содержание сообщения (включая заголовок Тема) и вложенных файлов.

Вы можете настроить (см. раздел "Настройка параметров модуля Анти-Фишинг" на стр. 251) максимальное время проверки сообщений модулем Анти-Фишинг.

По результатам проверки модуль Анти-Фишинг присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не содержит ссылок на фишинговые веб-адреса, изображений или текста, побуждающих пользователя предоставить конфиденциальные данные злоумышленникам, и не содержит ссылок на веб-ресурсы, содержащие вредоносные программы.
- *Фишинг* – приложение обнаружило в сообщении изображение или текст, побуждающие пользователя предоставить конфиденциальные данные злоумышленникам.
- *Фишинговая ссылка* – приложение обнаружило в сообщении ссылку на веб-ресурс, содержащий вредоносные программы.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз приложения.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.

По умолчанию модуль Анти-Фишинг включен. Если нужно, вы можете отключить модуль Анти-Фишинг или отключить проверку сообщений на фишинг для любого правила (см. раздел "Настройка защиты от фишинга" на стр. 115).

Контентная фильтрация сообщений

Kaspersky Security для Linux Mail Server выполняет контентную фильтрацию сообщений, проходящих через почтовый сервер. Вы можете ограничить пересылку почтовым сервером сообщений с определенными параметрами.

Вы можете настроить следующие параметры контентной фильтрации (см. раздел "Настройка параметров контентной фильтрации" на стр. 251):

- максимальное время проверки сообщений;
- максимальный уровень проверки архивов.

В результате контентной фильтрации модуль управления проверкой сообщений Scan Logic присваивает сообщению один из следующих статусов контентной фильтрации:

- *Не обнаружено* – в сообщении не обнаружены нарушения ограничений, заданных в параметрах контентной фильтрации.
- *Запрещенное имя вложения* – сообщение содержит вложение с запрещенным именем.
- *Запрещенный формат вложения* – сообщение содержит вложение запрещенного формата.
- *Превышен допустимый размер* – превышен максимально разрешенный размер сообщения.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз приложения.

- *Ошибка* – проверка сообщения завершилась с ошибкой.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.

По умолчанию контентная фильтрация сообщений включена. Если нужно, вы можете отключить контентную фильтрацию в общих параметрах защиты или для любого правила (см. раздел "Настройка контентной фильтрации" на стр. 116).

Проверка подлинности отправителей сообщений

Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры вашей организации от спама и фишинга.

Kaspersky Security 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 для Linux Mail Server получает списки возможных источников сообщений с DNS-сервера.

Включайте SPF-проверку, если Kaspersky Security для Linux Mail Server принимает сообщения напрямую из интернета. Отключайте SPF-проверку, если Kaspersky Security 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 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.

Для выполнения DMARC-проверки требуется включить SPF- и DKIM-проверки. Если SPF- или DKIM-проверки отключены, то DMARC-проверка также будет отключена.

После того, как сообщение прошло SPF- и DKIM-проверки, выполняется проверка того, что домен, содержащий адрес отправителя в поле **От** заголовка сообщения, соответствует идентификаторам SPF и DKIM.

Для выполнения SPF-, DKIM- и DMARC-проверок подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Security для Linux Mail Server к DNS-серверу. Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

По результатам проверки подлинности отправителей приложение присваивает сообщению один из следующих статусов:

- *Не обнаружено* – в сообщении не обнаружены нарушения проверки подлинности.
- *Ошибка* – во время проверки подлинности произошла ошибка.
- *Аутентификация не пройдена* – не удалось выполнить проверку подлинности.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам приложения.
- *Обнаружено нарушение* – обнаружено нарушение хотя бы одной проверки подлинности.
- *Нарушение не обнаружено* – не обнаружено ни одного нарушения проверки подлинности.

По умолчанию все проверки подлинности отправителей включены. Если нужно, вы можете отключить любую проверку в общих параметрах защиты (см. раздел "Настройка параметров внешних служб" на стр. 252) или для любого правила (см. раздел "Проверка подлинности отправителей сообщений" на стр. 120).

Для того чтобы удаленный почтовый сервер мог проверить подлинность отправителя исходящих сообщений (если отправителем является Kaspersky Security для Linux Mail Server), вам нужно предварительно добавить SPF- и DMARC-записи в параметры вашего DNS-сервера (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 254).

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.

Таблица 10. Легальные программы

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на том компьютере, на котором они установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры для наблюдения за компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу HTTP.

Тип	Название	Описание
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

Настройка параметров модуля Антивирус

► *Чтобы настроить параметры модуля Антивирус:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Антивирус**.
3. Включите или отключите модуль Антивирус с помощью переключателя **Использовать Антивирус**.

   По умолчанию модуль Антивирус включен.
4. Если на предыдущем шаге вы включили модуль Антивирус, настройте следующие параметры антивирусной проверки:

   a. Если вы хотите использовать технологию обнаружения угроз, не определяемых с помощью антивирусных баз, включите функцию эвристического анализа с помощью переключателя **Использовать эвристический анализ**.

      По умолчанию эвристический анализ включен.

   b. Если вы включили использование эвристического анализа, в раскрывающемся списке **Уровень эвристического анализа** выберите один из следующих уровней:

      - **Поверхностный**.
      - **Средний**.
      - **Глубокий**.

      По умолчанию выбран уровень **Средний**.

c. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время антивирусной проверки сообщений в секундах.

Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 180.

Если антивирусная проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Security для Linux Mail Server выполняет следующие действия:

- Прерывает проверку сообщения.
- Выполняет действие над сообщением, которое вы настроили.
- Присваивает сообщению статус *Ошибка.*
- Добавляет запись в журнал событий.

d. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности сообщений, проверяемых модулем Антивирус.

Возможные значения – целые числа от 1 до 20000. Значение по умолчанию – 32.

5. Если требуется, настройте исключения из антивирусной проверки. Для этого в блоке параметров **Исключения из проверки** включите или отключите антивирусную проверку легальных программ[1], которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, с помощью переключателя **Некоторые легальные программы**.

> По умолчанию сообщения, в которых обнаружены легальные программы, исключаются из проверки. При отключении этого параметра к таким сообщениям будет применяться действие, указанное в правилах для зараженных объектов.

6. Нажмите на кнопку **Сохранить**.

Параметры модуля Антивирус будут настроены.

Настройка параметров проверки ссылок

Вы можете включить проверку ссылок, чтобы отслеживать ссылки, ведущие на вредоносные веб-ресурсы, а также рекламные ссылки и ссылки, относящиеся к легальному ПО, которое при использовании злоумышленниками может нанести вред компьютерной сети вашей организации.

► *Чтобы настроить параметры проверки ссылок:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Проверка ссылок**.
3. Включите или отключите проверку ссылок с помощью переключателя **Проверять ссылки**.

   По умолчанию проверка ссылок включена.
4. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений в секундах.

[1] К легальным программам, которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями.

Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Security для Linux Mail Server выполняет следующие действия:

- Прерывает проверку сообщения.
- Выполняет действие над сообщением, которое вы настроили.
- Присваивает сообщению статус *Ошибка*.
- Добавляет запись в журнал событий Syslog.

5. Если требуется, настройте исключения из проверки. Для этого в блоке параметров **Исключения из проверки** выполните следующие действия:
   - Включите или отключите проверку рекламных программ с помощью переключателя **Рекламные ссылки**.

     По умолчанию этот параметр включен, то есть проверка рекламных программ не выполняется.
   - Включите или отключите проверку ссылок на некоторые легальные программы, которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, с помощью переключателя **Ссылки, связанные с некоторыми легальными программами**.

     По умолчанию этот параметр включен, то есть проверка ссылок на некоторые легальные программы не выполняется.
6. Нажмите на кнопку **Сохранить**.

Параметры проверки ссылок будут настроены.

Настройка параметров модуля Анти-Спам

Модуль Анти-Спам проверяет только первые 50 МБ сообщения. При превышении этого размера сообщение не будет проверено полностью, а статус будет присвоен на основе проверки первых 50 МБ.

► *Чтобы настроить параметры модуля Анти-Спам:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Спам**.
3. Включите или отключите модуль Анти-Спам с помощью переключателя **Использовать Анти-Спам**.

   По умолчанию модуль Анти-Спам включен.
4. Если на предыдущем шаге вы включили модуль Анти-Спам, настройте следующие параметры:
   a. Включите или отключите службу Moebius с помощью переключателя **Использовать службу Moebius**.

      По умолчанию служба Moebius включена.
   b. Включите или отключите защиту от спуфинговых атак с помощью переключателя **Защита от спуфинга Active Directory**.

      По умолчанию защита от спуфинговых атак отключена.

c. Если на предыдущем шаге вы включили защиту от спуфинговых атак, в поле **Группа LDAP: distinguishedName** укажите группу Active Directory, к пользователям и контактам которой будет применяться защита.

> Защита применяется к контактам группы, если включено получение почтовых адресов контактов в параметрах соединения с LDAP-сервером и прошла успешная синхронизация с LDAP-сервером.
> Вы можете добавить только одну группу. Количество записей в группе, содержащих адрес электронной почты, не должно превышать 10 000. При превышении этого количества защита от спуфинговых атак будет применена к случайным 10 000 пользователей и контактов из этой группы.

d. Включите или отключите проверку репутации IP-адресов и доменов, с которых были отправлены сообщения, по базам модуля Анти-Спам с помощью переключателя **Репутация IP-адресов и доменов**.

По умолчанию проверка репутации IP-адресов и доменов включена.

e. Включите или отключите использование Анти-Спам карантина с помощью переключателя **Использовать Анти-Спам карантин**.

Если использование Анти-Спам карантина включено, сообщения электронной почты размером не более 200 МБ, для которых результат проверки модулем Анти-Спам не окончателен, временно помещаются в Анти-Спам карантин.

> Изменение значений для параметров Анти-Спам карантина, установленных по умолчанию, может привести к снижению уровня обнаружения спама.

f. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений на спам в секундах.

Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

Если проверка сообщения на спам не успевает завершиться за указанное вами время, Kaspersky Security для Linux Mail Server выполняет следующие действия:

- Прерывает проверку сообщения (действие **Пропустить**).
- Присваивает сообщению статус *Ошибка.*
- Доставляет сообщение получателю.
- Добавляет запись в журнал событий Syslog.

5. В поле **Максимальное время хранения сообщения (сек.)** укажите время нахождения сообщения в Анти-Спам карантине, по истечении которого сообщение будет доставлено получателю.

Возможные значения – целые числа от 1 до 86400. Значение по умолчанию – 3000.

6. В поле **Максимальное количество сообщений** укажите количество сообщений, при превышении которого сообщения не будут помещаться в карантин.

Укажите 0, если ограничения не требуются.

Возможные значения – целые числа от 0 до 9007199254740993. Значение по умолчанию – 0.

7. В поле **Максимальный размер карантина (МБ)** укажите размер Анти-Спам карантина, при превышении которого сообщения не будут помещаться в карантин.

Минимальное значение – 1 МБ. Значение по умолчанию – 1024 МБ (1 ГБ).

> Если для сообщения результат проверки модулем Анти-Спам не окончателен, но оно не может быть помещено в Анти-Спам карантин из-за сработавшего ограничения, такому сообщению будет присвоен статус *Не обнаружено*.

8. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Спам будут настроены.

Настройка параметров модуля Анти-Фишинг

► *Чтобы настроить параметры модуля Анти-Фишинг:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Фишинг**.
3. Включите или отключите модуль Анти-Фишинг с помощью переключателя **Использовать Анти-Фишинг**.

   По умолчанию модуль Анти-Фишинг включен.
4. Если на предыдущем шаге вы включили модуль Анти-Фишинг, в поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений на фишинг в секундах.

   Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

   Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Security для Linux Mail Server выполняет следующие действия:

   - Прерывает проверку сообщения.
   - Выполняет действие над сообщением, которое вы настроили.
   - Присваивает сообщению статус *Ошибка*.
   - Добавляет запись в журнал событий Syslog.
5. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Фишинг будут настроены.

Настройка параметров контентной фильтрации

► *Чтобы настроить параметры контентной фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Контентная фильтрация**.
3. Включите или отключите контентную фильтрацию с помощью переключателя **Использовать Контентную фильтрацию**.

По умолчанию контентная фильтрация включена.

4. Если на предыдущем шаге вы включили контентную фильтрацию, настройте следующие параметры:

   a. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время контентной проверки сообщений в секундах.

      Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

      Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Security для Linux Mail Server выполняет следующие действия:

      - Прерывает проверку сообщения (действие **Пропустить**).
      - Присваивает сообщению статус *Ошибка*.
      - Доставляет сообщение получателю.
      - Добавляет запись в журнал событий /var/log/messages.

   b. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности сообщений, до которого выполняется контентная фильтрация.

      Возможные значения – целые числа от 1 до 20000. Значение по умолчанию – 32.

      Если задать для этого поля значение, отличное от 0, то приложение будет проверять архивы только до заданной глубины, даже если их уровень вложенности превышает заданное значение. Если в архиве до заданной глубины не было найдено нарушений ограничений, заданных в параметрах контентной фильтрации, приложение будет отображать результат проверки *Не обнаружено*.

5. Нажмите на кнопку **Сохранить**.

Параметры контентной фильтрации будут настроены.

Настройка параметров внешних служб

► *Чтобы настроить параметры внешних служб:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Внешние службы**.
3. Разрешите или запретите подключение к DNS-серверу с помощью переключателя **Разрешить подключение к DNS-серверу**.

   По умолчанию подключение разрешено.

   Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

4. В поле **Время ожидания DNS-сервера (сек.)** укажите максимальное время ожидания ответа DNS-сервера в секундах.

Значение по умолчанию – 10 сек. По истечении этого времени DNS-сервер будет считаться недоступным, и сообщение будет обработано приложением без проверки подлинности отправителей.

5. В поле **Время ожидания сервера KSN (сек.)** укажите максимальное время ожидания ответа сервера KSN в секундах.

   Значение по умолчанию – 10 сек. По истечении этого времени сервер KSN будет считаться недоступным, и сообщение будет обработано приложением без проверки с помощью репутационной базы KSN.

   > Опция используется, только если вы согласились участвовать в программе Kaspersky Security Network или Kaspersky Private Security Network.

6. Включите или отключите SPF-проверку подлинности отправителей с помощью переключателя **Использовать SPF-проверку**.

   Если вы включили SPF-проверку подлинности отправителей, приложение будет сопоставлять IP-адреса отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

   > Перед включением SPF-проверки требуется выполнить предварительную настройку (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 254) на DNS-сервере.

   По умолчанию проверка включена.

7. Включите или отключите DKIM-проверку подлинности отправителей с помощью переключателя **Использовать DKIM-проверку**.

   Если вы включили DKIM-проверку подлинности отправителей, приложение будет проверять цифровую подпись к сообщениям.

   По умолчанию проверка включена.

8. Включите или отключите DMARC-проверку подлинности отправителей с помощью переключателя **Использовать DMARC-проверку**.

   Если вы включили DMARC-проверку подлинности отправителей, приложение будет проверять, соответствует ли идентификаторам SPF и DKIM домен, содержащий адрес отправителя в поле "От" заголовка сообщения электронной почты.

   > Перед включением DMARC-проверки требуется выполнить предварительную настройку (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 254) на DNS-сервере.

   По умолчанию проверка включена.

   > Если SPF- или DKIM- проверки отключены, то DMARC-проверка будет также отключена.

9. Нажмите на кнопку **Сохранить**.

Параметры внешних служб будут настроены.

kaspersky

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 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:*

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 7208.
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.

kaspersky

Настройка параметров соединения с прокси-сервером

Заданные параметры прокси-сервера будут использованы для обновления баз, активации приложения, а также работы служб KSN/KPSN и службы Moebius.

► *Чтобы настроить параметры соединения с прокси-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с прокси-сервером**.
2. Включите или отключите использование прокси-сервера с помощью переключателя **Использовать прокси-сервер**.
3. Если на предыдущем шаге вы включили использование прокси-сервера, то в полях **Адрес прокси-сервера** введите адрес и номер порта прокси-сервера.

   По умолчанию используется порт 8080.
4. Установите флажок **Не использовать прокси-сервер для локальных и частных адресов**, если вы не хотите использовать прокси-сервер для внутренних и частных адресов электронной почты.
5. В полях **Имя пользователя (необязательно)** и **Пароль (необязательно)** введите имя пользователя и пароль, если вы хотите использовать аутентификацию при подключении к прокси-серверу.
6. Нажмите на кнопку **Сохранить**.

Параметры соединения с прокси-сервером будут настроены.

kaspersky

Обновление баз

Базы модулей Антивирус, Анти-Спам и Анти-Фишинг (далее также "базы") представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Эти записи содержат информацию о контрольных участках вредоносного кода и алгоритмы лечения объектов, в которых содержатся угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, прошедшее 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 (см. раздел "Настройка расписания и параметров обновления баз" на стр. 258) или устанавливать пакеты обновлений вручную (см. раздел "Запуск обновления баз вручную" на стр. 260), загружая их с веб-сайта "Лаборатории Касперского".

Об источниках обновлений

Во время установки Kaspersky Security для Linux Mail Server получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". После установки доступно несколько источников обновлений.

Основным источником обновлений служат серверы обновлений "Лаборатории Касперского". Это специальные интернет-сайты, на которые выкладываются обновления баз и программных модулей для всех приложений "Лаборатории Касперского". Если для доступа в интернет вы используете прокси-сервер, вам нужно настроить параметры подключения к прокси-серверу (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 256).

Чтобы уменьшить интернет-трафик, вы можете настроить обновление баз из *пользовательского источника обновлений.* Пользовательским источником обновлений могут служить указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

Если в инфраструктуре вашей организации отсутствует подключение к интернету, вы можете настроить получение обновления баз Kaspersky Security для Linux Mail Server через серверы Kaspersky Security Center (см. раздел "Обновление баз приложения через Kaspersky Security Center" на стр. 262).

Мониторинг состояния баз

Kaspersky Security для Linux Mail Server периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского". Статусы баз приложения в зависимости от времени последнего обновления описаны в таблице ниже.

Таблица 11. Статусы баз приложения

Модуль проверки	Актуальны	Устарели	Сильно устарели
Антивирус	менее 24 часов	от 24 часов до 7 суток	более 7 суток
Анти-Спам	менее 5 часов	от 5 до 24 часов	более 24 часов
Анти-Фишинг	менее 48 часов	от 48 до 72 часов	более 72 часов

Актуальное состояние баз приложения (см. раздел "Мониторинг состояния баз приложения" на стр. 260) отображается на информационной панели **Лицензирование**, а также в таблице с информацией о базах на каждом узле кластера в разделе **Параметры → Внешние службы → Обновление баз → Статус обновления**.

В этом разделе

Настройка расписания и параметров обновления баз

► *Чтобы настроить расписание и параметры обновления баз:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Внешние службы → Обновление баз**.
2. Выберите закладку **Параметры обновления**.
3. В раскрывающемся списке **Источник** выберите один из следующих источников обновлений:
   - **Серверы "Лаборатории Касперского" (безопасное соединение)**.
   - **Серверы "Лаборатории Касперского" (небезопасное соединение)**.
   - **Kaspersky Security Center** (см. раздел "**Обновление баз приложения через Kaspersky Security Center**" на стр. 262).
   - **Пользовательский**.

   По умолчанию установлено значение **Серверы "Лаборатории Касперского" (безопасное соединение)**.
4. Если на предыдущем шаге вы выбрали **Пользовательский**, в поле **Пользовательский источник** укажите адрес пользовательского источника, из которого вы хотите получать пакеты обновлений. Вы можете указать следующие источники:
   - URL-адрес сервера обновления.

     Для серверов, использующих протокол HTTPS, обновление будет выполняться, только если указан сервер "Лаборатории Касперского".

   - Локальную папку.

     Требуется указать полный путь к папке обновления, расположенной на всех узлах кластера. Если папка по указанному пути отсутствует на Управляющем узле, то отображается уведомление. Если указанной папки нет на Подчиненном узле, то для этого узла обновление баз будет выполняться со старыми параметрами.
   - Сетевую папку, то есть папку на удаленном компьютере, смонтированную по протоколам SMB или NFS.

Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории Касперского"**, если вы хотите получать пакеты обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен. По умолчанию флажок снят.

5. В раскрывающемся списке **Расписание** выберите один из вариантов и выполните следующие действия для настройки расписания:

   - **Вручную**.
   - **Один раз**. В появившемся поле укажите дату и время запуска обновления баз.
   - **Ежедневно**. В появившемся поле укажите время ежедневного запуска обновления баз.
   - **Еженедельно**. В появившихся полях укажите день недели и время запуска обновления баз.

     Например, если установлены значения **Пн** и **15:00**, обновление баз запускается каждый понедельник в 15 часов.
   - **Ежемесячно**. В появившихся полях укажите день месяца и время запуска обновления баз.

     Например, если установлены значения **20** и **15:00**, обновление баз запускается каждый месяц двадцатого числа в 15 часов.

     Если указанное значение превышает количество дней в месяце, в такие месяцы обновление баз будет выполняться в последний день месяца. Например, если указано значение **31**, в месяцы с 30 днями обновление баз будет выполнено 30 числа.
   - **Запускать каждые**. В появившихся полях укажите периодичность запуска обновления баз в минутах, часах или днях.

     Например, если для периодичности установлено значение **30** и выбрана периодичность **Минуты**, то обновление баз запускается каждые полчаса.

     Первое обновление баз запустится сразу после сохранения внесенных изменений.

   По умолчанию обновление баз запускается каждые 15 минут.

6. В поле **Максимальная длительность (мин)** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.

   Если задача обновления баз не завершена за указанное время, она запустится в следующий раз, указанный в расписании.

   По умолчанию установлено значение 180.

7. Переведите переключатель **Запускать пропущенные задачи** в положение **Включено**, если вы хотите запускать пропущенные задачи обновления баз при последующем запуске приложения.

   Обновление могло не выполняться в заданное расписанием время, например, если компьютер был выключен или если приложение не было запущено.

   > Если запуск пропущенных задач выключен, то пропущенные задачи обновления баз не будут запущены при последующем запуске приложения. Следующий запуск обновления баз будет выполнен согласно расписанию.

   По умолчанию запуск пропущенных задач включен.

8. Нажмите на кнопку **Сохранить**.

Расписание и параметры обновления баз будут настроены.

kaspersky

Запуск обновления баз вручную

Функциональность доступна только при наличии права **Изменять параметры**.

► *Чтобы запустить обновление баз вручную:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. Выберите закладку **Статус обновления**.
3. Нажмите на кнопку **Обновить базы**.

Обновление баз будет запущено. В нижней части окна отобразится сообщение о статусе задачи обновления.

Мониторинг состояния баз приложения

Чтобы отслеживать проблемы, связанные с обновлением баз приложения, вы можете просматривать сводную информацию о состоянии баз на всех узлах кластера на информационной панели **Обновление баз** в разделе **Узлы**.

Возможны следующие статусы:

- *Без ошибок* – все базы приложения обновлены, в процессе обновления не возникло ошибок.
- *Базы устарели* – обработка трафика не остановлена, и возникло хотя бы одно из следующих событий:
  - базы Антивируса не обновлялись от 24 часов до 7 суток;
  - базы Анти-Спама не обновлялись от 5 до 24 часов;
  - базы Анти-Фишинга не обновлялись от 48 до 72 часов.
- *Базы сильно устарели* – обработка трафика не остановлена, и возникло хотя бы одно из следующих событий:
  - базы Антивируса не обновлялись более 7 суток;
  - базы Анти-Спама не обновлялись более 24 часов;
  - базы Анти-Фишинга не обновлялись более 72 часов.
- *Ошибки* – возникло одно из следующих событий:
  - отсутствуют базы для одного или более модулей проверки;
  - на одном или нескольких узлах кластера остановлена обработка трафика;
  - один или несколько узлов кластера недоступен, нет возможности получить информацию о состоянии баз приложения.

Под чертой в поле *Ошибки последнего обновления* отображается количество узлов кластера, на которых последняя задача обновления завершилась с ошибкой.

► *Чтобы просмотреть детальную информацию о состоянии баз приложения на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Обновление баз** перейдите в раздел **Параметры** → **Внешние службы** → **Обновление баз** → **Статус обновления**.

В рабочей области отображается таблица узлов кластера с информацией о базах приложения по каждому модулю проверки:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Антивирус** – состояние антивирусных баз.
- **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
- **Анти-Спам** – состояние баз модуля Анти-Спам.
- **Статус обновления** – статус последней задачи обновления:
  - если задача завершилась успешно, отображается время завершения этой задачи;
  - если задача завершилась с ошибкой, отображается время запуска текущей задачи и время последнего успешного обновления баз (при наличии);
  - если задача еще ни разу не была запущена после установки приложения или если узел кластера недоступен, отображается прочерк;
  - если задача находится в процессе, отображается процент ее выполнения.

Таблица отображается при наличии у пользователя прав **Просматривать информацию об узлах** и/или **Создавать/изменять/удалять узлы**, а также **Просматривать параметры** и/или **Изменять параметры**.

Вы также можете просмотреть сведения о состоянии баз приложения в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).

kaspersky

Обновление баз приложения через Kaspersky Security Center

Организации, сетевая инфраструктура которых не предполагает подключение к интернету, могут получать обновления баз Kaspersky Security для Linux Mail Server через Kaspersky Security Center. Обновления баз загружаются в Kaspersky Security Center, развернутый в инфраструктуре организации, и передаются в Kaspersky Security для Linux Mail Server.

В этом разделе содержатся инструкции по настройке получения обновлений баз Kaspersky Security для Linux Mail Server с помощью следующих приложений:

- Kaspersky Security Center Web Console версии 13 или 14.
- Kaspersky Security Center версии 13 или 14.

Настройка получения обновлений баз Kaspersky Security для Linux Mail Server через Kaspersky Security Center состоит из следующих этапов:

1. **Подготовка к запуску Агента администрирования Kaspersky Security Center в режиме замкнутой программной среды**

   Этот этап нужно выполнить, если вы будете использовать Агент администрирования в операционной системе с включенным режимом замкнутой программной среды.

   Подробную информацию см. в *справке Kaspersky Security Center 14 Linux* или в *справке Kaspersky Security Center 14*.

2. **Установка Агента администрирования через Kaspersky Security Center Web Console на сервер с установленным Kaspersky Security для Linux Mail Server**

   Агент администрирования обеспечивает взаимодействие между Сервером администрирования Kaspersky Security Center и узлом Kaspersky Security для Linux Mail Server. Агент администрирования нужно установить на все узлы, где требуется обновление баз Kaspersky Security для Linux Mail Server.

   Подробную информацию об Агенте администрирования см. в *справке Kaspersky Security Center 14 Linux* или в *справке Kaspersky Security Center 13*.

3. **Создание задачи загрузки обновлений в хранилище на сервере Kaspersky Security Center**

   Подробную информацию см. в *справке Kaspersky Security Center 14 Linux или в справке Kaspersky Security Center 13*.

4. **Выполнение задачи загрузки обновлений в хранилище на сервере Kaspersky Security Center**

   Kaspersky Security Center запускает задачу загрузки обновлений баз Kaspersky Security для Linux Mail Server в соответствии с расписанием, заданным в свойствах задачи. Вы можете запустить задачу вручную в любое время.

   Подробную информацию см. в *справке Kaspersky Security Center 14 Linux или в справке Kaspersky Security Center 13*.

5. **Определение источника обновлений в Kaspersky Security для Linux Mail Server**

   Для этого в веб-интерфейсе Kaspersky Security для Linux Mail Server перейдите в раздел **Параметры → Внешние службы → Обновление баз**, выберите закладку **Параметры обновления** и в раскрывающемся списке **Источник** выберите значение **Kaspersky Security Center**.

В результате будет настроено автоматическое получение обновлений баз Kaspersky Security для Linux Mail Server через Kaspersky Security Center.

kaspersky

Экспорт и импорт параметров

Функциональность доступна при наличии у пользователя права **Изменять параметры**.

Экспорт и импорт параметров Kaspersky Security для Linux Mail Server может быть использован для следующих целей:

- Резервное копирование параметров приложения.

  Если вам потребуется развернуть приложение на новом сервере, вы сможете импортировать ранее экспортированные параметры правил, а также персональные списки разрешенных и запрещенных адресов. Это позволит сократить время на конфигурацию нового узла.

- Миграция приложения на новую версию (см. раздел "Миграция параметров из более старой версии" на стр. 265).

  Перед обновлением приложения вы можете экспортировать параметры из старой версии и импортировать их в новую версию.

  Миграция с более новой на более старую версию не поддерживается.

При экспорте параметров (см. раздел "Экспорт параметров" на стр. 263) создается конфигурационный файл, содержащий версию приложения и значения параметров. Созданный конфигурационный файл сохраняется локально на Управляющем узле.

При импорте конфигурационного файла (см. раздел "Импорт параметров" на стр. 264) вы можете выбрать, какие параметры должны быть применены:

- правила обработки сообщений (включая предустановленные правила Allowlist и Denylist);
- персональные списки разрешенных и запрещенных адресов.

Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров

Информацию о способах экспорта параметров из Kaspersky Security для Linux Mail Server версии 8 см. в Экспорт параметров из Kaspersky Security 8 для Linux Mail Server (на стр. 78).

► *Чтобы экспортировать параметры:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Экспорт**.
3. Нажмите на кнопку **Экспортировать**.

   В таблице ниже отобразится текущее состояние операции экспорта. После успешного завершения операции отобразится строка с датой и временем экспорта.
4. Нажмите на значок  в нужной строке.

Конфигурационный файл с экспортированными параметрами будет сохранен в папке загрузки браузера.

Администратор должен самостоятельно обеспечить безопасное хранение файлов с экспортированными параметрами. Меры безопасности, помимо прочего, должны включать:

- Запрет несанкционированных изменений файлов с экспортированными параметрами.
- Проверку подлинности и целостности файлов с экспортированными параметрами.

Ненадлежащее хранение файлов с параметрами влечет следующие риски:

- Утрата файлов с параметрами и невозможность их восстановления на нужном экземпляре Kaspersky Security для Linux Mail Server.
- Подмена файла злоумышленником. В результате параметры Kaspersky Security для Linux Mail Server могут быть изменены, и может деградировать безопасность.

Импорт параметров

Если в экспортированных персональных списках разрешенных и запрещенных адресов содержится более 500 записей, при импорте список сокращается до 500 адресов.

► *Чтобы импортировать параметры:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Импорт**.
3. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
4. Выберите файл с ранее экспортированными параметрами.

   Под областью загрузки отобразится блок параметров **Импортировать параметры**.
5. Установите флажки напротив тех параметров, которые вы хотите импортировать.
6. Нажмите на кнопку **Импортировать**.

Отобразится сообщение о результате выполнения операции импорта.

kaspersky

Миграция параметров из более старой версии

Доступна миграция параметров из следующих версий:

- Kaspersky Security 8 для Linux Mail Server (см. раздел "Экспорт параметров из Kaspersky Security 8 для Linux Mail Server" на стр. 78) (версия 8.0.3.30);
- Kaspersky Secure Mail Gateway 1.1;
- Kaspersky Secure Mail Gateway 2.0;
- Kaspersky Secure Mail Gateway 2.0 MR1.

Миграция из более ранних версий приложения не поддерживается.

Настройка хранения экспортированных файлов

Вы можете ограничить количество экспортированных конфигурационных файлов, которые хранятся на сервере. В случае превышения установленного ограничения ранее экспортированные файлы будут удалены.

► *Чтобы настроить хранение экспортированных файлов:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Экспорт**.
3. Нажмите на кнопку **Параметры хранения**.

   Откроется окно **Параметры хранения экспортированных файлов**.
4. В поле **Максимальное количество хранимых конфигурационных файлов** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.

   Возможные значения: 1 – 2 147 483 647. По умолчанию установлено значение 50.

Количество экспортированных файлов будет ограничено заданным значением.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Использование Kaspersky Security Network приводит к выходу приложения 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*.

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

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям 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 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 пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний приложения, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky Security для Linux Mail Server отправляет в Kaspersky Security Network запросы о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после создания кластера в веб-интерфейсе приложения (раздел **Параметры** → **Внешние службы** → **KSN/KPSN** → **Параметры KSN/KPSN**). Его можно изменить в любой момент.

Подробнее об участии в Kaspersky Security Network вы можете прочитать в Положении о Kaspersky 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 приложения Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

kaspersky

Настройка участия в KSN производится на Управляющем узле и распространяется на все Подчиненные узлы в кластере.

В этом разделе

Настройка участия в Kaspersky Security Network

Вы можете ознакомиться с составом данных, передаваемых на серверы KSN, в разделе О предоставлении данных (на стр. 33). Все передаваемые данные обрабатываются согласно действующим в данном регионе законам. Если сервер с установленным приложением перемещается в другой регион, то к обрабатываемым данным начинают применяться законы нового региона. Администратору отображается уведомление об этом в разделе **Узлы**.

► *Чтобы настроить участие в KSN:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите закладку **Параметры KSN/KPSN**.
3. В раскрывающемся списке **Использование KSN/KPSN** выберите один из следующих вариантов:
   - **KSN**, если вы хотите участвовать в KSN.
   - **Не использовать**, если вы не хотите участвовать в KSN.

   Если вы выбрали **KSN**, откроется окно **Положение о KSN**.
4. Прочитайте текст Положения о KSN и нажмите на кнопку **Я согласен участвовать в KSN**, чтобы подтвердить свое согласие с условиями участия.

   Откроется окно **Дополнительное Положение о KSN**.
5. Прочитайте текст Дополнительного Положения о KSN и выполните одно из следующих действий:
   - Если вы согласны отправлять статистику вашего использования службы KSN в "Лабораторию Касперского", нажмите на кнопку **Я согласен отправлять KSN-статистику**.
   - Если вы не хотите отправлять статистику, нажмите на кнопку **Отклонить**.
6. Нажмите на кнопку **Сохранить**.

Участие в Kaspersky Security Network будет настроено. После этого требуется задать максимальное время ожидания ответа от сервера KSN (см. раздел "Настройка параметров внешних служб" на стр. 252).

kaspersky

Настройка использования Kaspersky Private Security Network

► *Чтобы настроить использование KPSN:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите закладку **Параметры KSN/KPSN**.
3. В раскрывающемся списке **Использование KSN/KPSN** выберите один из следующих вариантов:
   - **KPSN**, если вы хотите участвовать в KPSN.
   - **Не использовать**, если вы не хотите участвовать в KPSN.

   Если вы выбрали **KPSN**, в рабочей области отобразится блок параметров для добавления конфигурационного файла KPSN.
4. Перед добавлением конфигурационного файла KPSN в формате PKCS7 проверьте его подлинность:
   a. Загрузите файл сертификата kpsn_certs.pem с сервера обновлений "Лаборатории Касперского" по ссылке http://downloads.kaspersky-labs.com/updates/ksn/kpsn_certs.pem.
   b. Выполните команду:

      ```
      openssl smime -verify -CAfile kpsn_certs.pem -in
      <имя_конфигурационного файла_KPSN> -inform DER >/dev/null
      ```

   Результат выполнения команды должен быть "Verification successful".

   Если результат выполнения команды – "Verification failure", проверка подлинности не пройдена, использовать этот файл конфигурации недопустимо.
5. Для добавления файла конфигурации KPSN в окне веб-интерфейса приложения в разделе **Параметры** → **Внешние службы** → **KSN/KPSN** на закладке **Параметры KSN/KPSN** нажмите на кнопку **Обзор**.
6. В окне выбора файлов укажите конфигурационный файл KPSN, который вы хотите добавить.

   Конфигурационный файл KPSN должен быть в формате ZIP или PKCS7.
7. Нажмите на кнопку **Сохранить**.

Использование Kaspersky Private Security Network будет настроено.

Мониторинг работы KSN/KPSN

Чтобы отслеживать проблемы, связанные с использованием KSN/KPSN, вы можете просматривать сводную информацию о работе служб на всех узлах кластера на информационной панели **Состояние соединения с KSN/KPSN** в разделе **Узлы**.

Возможны следующие статусы:

- *Без ошибок* – служба KSN или KPSN используется и работает без ошибок.
- *Отключено* – использование служб KSN/KPSN отключено в параметрах приложения.
- *Запросы отфильтрованы* – количество запросов, отправляемых службам KSN/KPSN для проверки репутации объектов, ограничено.

  Такое ограничение позволяет снизить нагрузку на серверы KSN/KPSN.
- *Ошибки* – в работе служб KSN/KPSN произошли ошибки.

В правой части информационной панели указано количество узлов кластера по каждому статусу.

► *Чтобы просмотреть детальную информацию об использовании служб KSN/KPSN на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Состояние соединения с KSN/KPSN** или из списка разделов в левой панели перейдите в раздел **Параметры** → **Внешние службы** → **KSN/KPSN** → **Состояние соединения с KSN/KPSN**.

В рабочей области отображается таблица узлов кластера с информацией об использовании KSN/KPSN на каждом узле:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Статус** – статус работы службы KSN/KPSN.

  Для статусов *Запросы отфильтрованы* и *Ошибки* отображается также дата и время, когда на этом узле последний раз был статус *Без ошибок*.
- **Роль** – роль узла в кластере.

Таблица отображается при наличии у пользователя прав **Просматривать информацию об узлах** и/или **Создавать/изменять/удалять узлы**, а также **Просматривать параметры** и/или **Изменять параметры**.

Вы также можете просмотреть сведения об использовании KSN/KPSN в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).

kaspersky

Интеграция с внешней службой каталогов

Kaspersky Security для Linux Mail Server позволяет подключаться к серверам внешних служб каталогов, используемых в вашей организации, по протоколу LDAP.

Соединение с внешней службой каталогов по протоколу LDAP предоставляет администратору Kaspersky Security для Linux Mail Server следующие возможности:

- Добавлять отправителей или получателей из внешней службы каталогов в правила обработки сообщений.
- Использовать функцию автодополнения полей **Email отправителя** и **Email получателя** при фильтрации событий обработки почтового трафика и сообщений пользователей локальной сети организации в Хранилище.

Если в организации используется несколько доменов, то для каждого из них должно быть настроено LDAP-соединение.

Для одного домена во внешней службе каталогов может быть настроено несколько LDAP-соединений при условии, что каждое LDAP-соединение будет содержать уникальное значение поля **База поиска** (**Search base**).

Если в одном LDAP-домене используется несколько контроллеров домена для сценария отказоустойчивости, добавлять дополнительное LDAP-соединение не требуется. Приложение автоматически выбирает доступный контроллер домена в рамках ранее настроенного соединения в соответствии с приоритетами SRV-записей на сервере доменных имен (DNS).

После настройки соединения с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272) приложение выполняет автоматическую синхронизацию данных с контроллером домена Active Directory каждые 30 минут. Вы можете настроить запуск синхронизации по расписанию (см. раздел "Настройка расписания синхронизации с контроллером домена Active Directory" на стр. 275). Если требуется обновить данные об учетных записях пользователей немедленно (например, при добавлении нового пользователя), вы можете запустить синхронизацию вручную (см. раздел "Запуск синхронизации с контроллером домена Active Directory вручную" на стр. 275).

Каждый узел кластера выполняет синхронизацию самостоятельно, независимо от других узлов. В результате успешной синхронизации в LDAP-кеше сохраняется следующая информация:

- учетные записи всех пользователей домена;
- контакты Active Directory (если в параметрах соединения с LDAP-сервером настроено получение адресов электронной почты контактов);
- группы, в которых состоят пользователи домена и контакты;
- адреса электронной почты пользователей домена, групп и контактов.

Приложение хранит и использует эти данные до следующего запуска синхронизации. Если контроллер домена недоступен, используются последние полученные данные. После удаления соединения с LDAP-сервером (см. раздел "Удаление соединения с LDAP-сервером" на стр. 274) все данные LDAP-кеша удаляются.

kaspersky

После успешной синхронизации Kaspersky Security для Linux Mail Server проверяет наличие дублирующихся данных в учетных записях LDAP. Следующие данные проверяются на наличие дубликатов:

- Имена всех пользователей домена. Для пользователей с дублирующимися именами отключена защита от спуфинга Active Directory, а также таким пользователям недоступны персональное Хранилище и персональные списки разрешенных и запрещенных адресов отправителей.
- Группы, в которых состоят пользователи домена. Для групп с дублирующимися именами отключена защита от спуфинга Active Directory.
- Контакты Active Directory. Для контактов с дублирующимися именами отключена защита от спуфинга Active Directory.
- Учетные записи пользователей Kerberos. Пользователям с дублирующимися именами Kerberos недоступны персональное Хранилище и персональные списки разрешенных и запрещенных адресов отправителей.
- Учетные записи пользователей NTLM. Пользователям с дублирующимися именами NTLM недоступны персональное Хранилище и персональные списки разрешенных и запрещенных адресов отправителей.
- Адреса электронной почты пользователей домена. Сообщения, предназначенные для дублирующихся адресов, не будут помещаться в персональное Хранилище пользователей, и к таким адресам не будут применяться персональные списки разрешенных и запрещенных адресов отправителей.

Если в учетных записях обнаружены дублирующиеся данные, в таблице узлов кластера (см. раздел "Просмотр таблицы узлов кластера" на стр. 137) отображается предупреждение.

В этом разделе

Создание keytab-файла

Keytab-файл создается на сервере контроллера домена или на компьютере под управлением Windows Server®, входящем в домен, под учетной записью с правами доменного администратора.

► *Чтобы создать keytab-файл:*

1. В оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя, которая будет использоваться для подключения приложения к LDAP-серверу (например, с именем `klms-ldap`).

При создании пользователя выберите опцию **Password never expires**.

2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** в свойствах созданной учетной записи на закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `klms-ldap` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<FQDN Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser klms-ldap@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя klms-ldap> -out <путь к файлу>\<имя файла>.keytab
```

Вы можете использовать символ * в качестве значения параметра -pass, чтобы не указывать пароль в тексте команды. В этом случае утилита запросит пароль в процессе выполнения команды.

Пример:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.company.com@COMPANY.COM -mapuser klms-ldap@<COMPANY.COM> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\Keytabs\klms-ldap.keytab
```

Keytab-файл будет создан. В случае изменения пароля учетной записи потребуется сгенерировать новый keytab-файл.

Добавление соединения с LDAP-сервером

Функциональность доступна только при наличии права **Изменять параметры**.

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

► *Чтобы добавить соединение с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить соединение**.
3. В поле **Название** введите имя, которое будет отображаться в веб-интерфейсе приложения.

   Это имя не используется приложением при взаимодействии с LDAP-сервером.

4. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 271).

   Откроется окно выбора файла.

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

   Keytab-файл должен содержать только одну запись с учетными данными пользователя, имеющего доступ к добавляемому домену.

6. В поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Security для Linux Mail Server осуществляет поиск записей.

   Вводите суффикс каталога в формате `ou=<название подразделения>`(если требуется),`dc=<имя домена>,dc=<имя родительского домена>`.

   Например, вы можете ввести `ou=people,dc=example,dc=com`.

   Здесь `people` – уровень в схеме каталога, начиная с которого Kaspersky Security 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 для Linux Mail Server осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

7. В блоке параметров **Пользователи и группы LDAP** в поле **Атрибуты, содержащие адреса email** укажите атрибуты, из которых приложение будет получать адреса электронной почты пользователей и групп:

   - **Атрибут mail**.
   - **Атрибут proxyAddresses**.
   - **Атрибуты mail и proxyAddresses**.

     Если вы настраиваете соединение LDAP для интеграции с почтовым сервером Microsoft Exchange, то рекомендуется использовать **Атрибут proxyAddresses**, так как Microsoft Exchange хранит почтовые адреса пользователей и групп в атрибуте `proxyAddresses`.

8. Если вы хотите, чтобы приложение получало адреса электронной почты контактов LDAP, переведите переключатель **Контактная информация LDAP** в положение **Включено.**

9. Если на предыдущем шаге вы включили получение контактной информации LDAP, в поле **Атрибуты, содержащие адреса email** укажите атрибуты, из которых приложение будет получать адрес электронной почты контактов LDAP:

   - **Атрибут mail**.
   - **Атрибут proxyAddresses**.
   - **Атрибуты mail и proxyAddresses**.

10. Нажмите на кнопку **Добавить**.

Соединение с LDAP-сервером будет добавлено.

kaspersky

Удаление соединения с LDAP-сервером

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

► *Чтобы удалить соединение с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Выберите LDAP-сервер, который вы хотите удалить.

   Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.
4. Нажмите на кнопку **ОК**.

Соединение с LDAP-сервером будет удалено. Синхронизация данных с контроллером домена будет прекращена. Из LDAP-кеша будут удалены данные об учетных записях пользователей, контактов и групп, принадлежащих к этому домену.

Изменение параметров соединения с LDAP-сервером

► *Чтобы изменить параметры соединения с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.

   Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Изменить**.
4. Если требуется, измените следующие параметры:
   - Имя LDAP-сервера, которое отображается в веб-интерфейсе приложения, в поле **Название**.
   - Keytab-файл, нажав на кнопку **Обзор**.
   - Каталог, начиная с которого приложение ищет записи, в поле **База поиска**.
   - Атрибуты, из которых приложение будет получать адреса электронной почты пользователей и групп, в раскрывающемся списке **Атрибуты, содержащие адреса email**.
   - Включите или отключите получение адресов электронной почты контактов LDAP с помощью переключателя **Контактная информация LDAP**.
   - Если вы включили получение адресов электронной почты контактов LDAP, в поле **Атрибуты, содержащие адреса email** укажите атрибуты, из которых приложение будет получать адреса электронной почты контактов LDAP.
5. Нажмите на кнопку **Сохранить**.

Параметры соединения с LDAP-сервером будут изменены.

kaspersky

Настройка расписания синхронизации с контроллером домена Active Directory

► *Чтобы настроить расписание синхронизации с контроллером домена Active Directory:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Выберите закладку **Параметры синхронизации**.
3. В раскрывающемся списке **Расписание** выберите один из вариантов и выполните следующие действия для настройки синхронизации:
   - **Вручную**.
   - **Один раз**. В появившемся поле укажите дату и время запуска синхронизации.
   - **Ежедневно**. В появившемся поле укажите время ежедневного запуска синхронизации.
   - **Еженедельно**. В появившихся полях укажите день недели и время запуска синхронизации.

     Например, если установлены значения **Пн** и **15:00**, синхронизация запускается каждый понедельник в 15 часов.
   - **Ежемесячно**. В появившихся полях укажите день месяца и время запуска синхронизации.

     Например, если установлены значения **20** и **15:00**, синхронизация запускается каждый месяц двадцатого числа в 15 часов.

     Если указанное значение превышает количество дней в месяце, в такие месяцы синхронизация будет выполняться в последний день месяца. Например, если указано значение **31**, в месяцы с 30 днями синхронизация будет выполнена 30 числа.
   - **Запускать каждые**. В появившихся полях укажите периодичность запуска синхронизации в минутах, часах или днях.

     Например, если для периодичности установлено значение **30** и выбрана периодичность **Минуты**, то синхронизация запускается каждые полчаса.

     Первая синхронизация запустится сразу после сохранения внесенных изменений.

   По умолчанию синхронизация запускается каждые 30 минут.
4. Нажмите на кнопку **Сохранить**.

Расписание синхронизации данных с контроллером домена будет настроено.

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).

Запуск синхронизации с контроллером домена Active Directory вручную

► *Чтобы запустить синхронизацию с контроллером домена Active Directory вручную:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Нажмите на кнопку **Синхронизировать**.

Синхронизация данных с контроллером домена будет запущена. В результате будут обновлены данные учетных записей пользователей и групп, используемые при подборе правил и при автозаполнении имен пользователей и групп в веб-интерфейсе приложения. Данные о контактах будут обновлены, если в приложении настроено получение адресов электронной почты контактов LDAP (см. раздел "Добавление соединения с LDAP-сервером" на стр. 272).

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).

kaspersky

Защита KATA

Вы можете настроить интеграцию Kaspersky Security для Linux Mail Server с Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform (KATA) – приложение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки (англ. advanced persistent threats, далее также APT).

В результате интеграции Kaspersky Security для Linux Mail Server сможет отправлять сообщения электронной почты на проверку KATA и получать результат проверки. KATA проверяет сообщения на наличие признаков целевых атак и вторжений в IT-инфраструктуру организации.

По результатам проверки KATA приложение Kaspersky Security для Linux Mail Server может блокировать отдельные сообщения.

Возможны следующие варианты интеграции с приложением KATA:

- С одним сервером KATA (см. раздел "Интеграция с одним сервером KATA" на стр. 278).

  Для интеграции достаточно указать IP-адрес сервера KATA с компонентом Central Node. Если компонент Central Node развернут в виде кластера (доступно для версии KATA 5.0 и выше), вы можете указать IP-адрес любого обрабатывающего сервера кластера.

  Адрес указывается в параметрах интеграции с приложением KATA через веб-интерфейс управляющего узла Kaspersky Security для Linux Mail Server.

- С несколькими серверами KATA и с локальным балансировщиком (см. раздел "Интеграция с несколькими серверами KATA" на стр. 278) (доступно для версии KATA 5.0 и выше).

  Несколько обрабатывающих серверов KATA из кластера Central Node обеспечивают отказоустойчивость: в случае потери связи с одним из серверов клиенты автоматически переключатся на другой доступный сервер.

  Администратор самостоятельно устанавливает локальный балансировщик на узлах кластера Kaspersky Security для Linux Mail Server. Локальный балансировщик контролирует доступность серверов KATA для каждого узла и обеспечивает автоматическое переключение между серверами KATA.

В этом разделе

kaspersky

Интеграция с одним сервером KATA

Настройка интеграции Kaspersky Security для Linux Mail Server с одним сервером KATA состоит из следующих этапов.

1. **Добавление сервера KATA (на стр. 282)**

   При добавлении сервера KATA требуется сверить отпечатки сертификата, отображаемые в веб-интерфейсах Kaspersky Security для Linux Mail Server и KATA. Если отпечатки совпадают, администратор подтверждает добавление сервера KATA. После этого Управляющий узел отправляет адрес и сертификат сервера KATA на все узлы кластера, не дожидаясь подтверждения авторизации.

2. **Настройка параметров защиты KATA (на стр. 283)**

   Вы можете настроить следующие параметры:

   - отправка на проверку в KATA всех сообщений или только сообщений, в которых по результатам проверки всеми модулями Kaspersky Security для Linux Mail Server ничего не обнаружено;
   - время ожидания ответа от сервера KATA;
   - параметры KATA карантина.

3. **Авторизация Kaspersky Security для Linux Mail Server в веб-интерфейсе приложения KATA**

   Во время добавления сервера KATA отправляется запрос на авторизацию внешней системы. Администратору KATA требуется подтвердить в веб-интерфейсе KATA запрос на авторизацию от каждого узла кластера. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

4. **Проверка соединения с сервером KATA (см. раздел "Мониторинг интеграции с KATA" на стр. 284)**

Интеграция с несколькими серверами KATA

Применимо только при интеграции с KATA версии 5.0 и выше.

Настройка интеграции Kaspersky Security для Linux Mail Server с несколькими серверами KATA состоит из следующих этапов.

1. **Установка локального балансировщика**

   Установите пакет балансировщика haproxy из репозитория операционной системы на каждом узле кластера Kaspersky Security для Linux Mail Server.

   Версия haproxy должна быть не ниже 1.8. Для операционных систем Astra Linux Special Edition 1.6 и 1.7 пакет необходимо устанавливать из репозитория с последним доступным обновлением.

2. **Подготовка конфигурационного файла для локального балансировщика (см. раздел "Создание конфигурационного файла для локального балансировщика" на стр. 279)**

3. **Настройка и запуск локального балансировщика на каждом узле кластера Kaspersky Security для Linux Mail Server (см. раздел "Настройка и запуск локального балансировщика на узле кластера" на стр. 281)**

4. **Добавление сервера KATA (на стр. 282)**

   В качестве адреса сервера KATA нужно указать значение 127.0.0.1:8000.

   При добавлении сервера KATA требуется сверить отпечатки сертификата, отображаемые в веб-интерфейсах Kaspersky Security для Linux Mail Server и KATA. Если отпечатки совпадают, администратор подтверждает добавление сервера KATA. После этого Управляющий узел отправляет адрес и сертификат сервера KATA на все узлы кластера, не дожидаясь подтверждения авторизации.

5. **Настройка параметров защиты KATA (на стр. 283)**

   Вы можете настроить следующие параметры:

   - отправка на проверку в KATA всех сообщений или только сообщений, в которых по результатам проверки всеми модулями приложения ничего не обнаружено;
   - время ожидания ответа от сервера KATA;
   - параметры KATA карантина.

6. **Авторизация Kaspersky Security для Linux Mail Server в веб-интерфейсе приложения KATA**

   Во время добавления сервера KATA отправляется запрос на авторизацию внешней системы. Администратору KATA требуется подтвердить в веб-интерфейсе KATA запрос на авторизацию от каждого узла кластера. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

7. **Проверка соединения с сервером KATA (см. раздел "Мониторинг интеграции с KATA" на стр. 284)**

Создание конфигурационного файла для локального балансировщика

Применимо только при интеграции с несколькими серверами (см. раздел "Интеграция с несколькими серверами KATA" на стр. 278) KATA версии 5.0 и выше.

► *Чтобы создать конфигурационный файл для локального балансировщика:*

1. Создайте текстовый файл в формате Unix (символ LF для перевода строки) и назовите его haproxy.cfg.
2. Добавьте в файл следующие строки:

```
global
    log 127.0.0.1 local6
    chroot /var/lib/haproxy
    pidfile /var/run/haproxy.pid
    stats socket /var/lib/haproxy/stats user root group adm mode 660
level user
    maxconn 1000
```

```
    user haproxy
    group haproxy
    daemon

defaults
    mode tcp
    log global
    retries 3
    timeout queue 1m
    timeout connect 10s
    timeout client 1m
    timeout server 1m
    timeout check 10s
    maxconn 1000

frontend kata_balancer
    bind 127.0.0.1:8000
    default_backend kata_servers
```

3. Выберите подходящий способ указания адресов серверов KATA и добавьте соответствующую запись в файл.

   - Если вы хотите указать IP-адреса всех серверов KATA в конфигурационном файле, добавьте в файл следующие строки:

     ```
     backend kata_servers
         balance roundrobin
         default-server check
         server kata_node1 <IP-адрес1:порт1>
         server kata_node2 <IP-адрес2:порт2>
         server kata_node3 <IP-адрес3:порт3>
         server kata_node4 <IP-адрес4:порт4>
     ```

   - Если вы хотите получать актуальный список адресов с помощью доменного имени (DNS-запись), добавьте в файл следующие строки:

     ```
     resolvers dns_servers
         parse-resolv-conf
         accepted_payload_size 8192
         timeout resolve 10s
         timeout retry 10s
     ```

```
    hold valid 60s

backend kata_servers
    balance roundrobin
    default-server check resolvers dns_servers init-addr none
    server-template kata_node 8 <доменное_имя>:<порт>
```

Чтобы получать список адресов с помощью доменного имени, создайте на DNS-сервере отдельное доменное имя (например, kata.example.com) с несколькими A-записями, указывающими на IP-адреса серверов KATA.

4. Сохраните конфигурационный файл.

Конфигурационный файл для локального балансировщика будет создан.

Настройка и запуск локального балансировщика на узле кластера

Применимо только при интеграции с несколькими серверами KATA версии 5.0 и выше (см. раздел "Интеграция с несколькими серверами KATA" на стр. 278).

► *Чтобы настроить локальный балансировщик на узле кластера:*

1. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Переименуйте базовый конфигурационный файл балансировщика с помощью команды:

   ```
   mv /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.orig
   ```

3. Поместите ранее подготовленный конфигурационный файл haproxy.cfg (см. раздел "Создание конфигурационного файла для локального балансировщика" на стр. 279) в директорию /etc/haproxy и укажите права доступа к нему с помощью команд:

   ```
   chown root:root /etc/haproxy/haproxy.cfg
   chmod 640 /etc/haproxy/haproxy.cfg
   ```

4. Создайте файл /etc/rsyslog.d/haproxy.conf следующего содержания:

   ```
   $ModLoad imudp
   $UDPServerRun 514
   $UDPServerAddress 127.0.0.1
   if $syslogfacility-text == 'local6' then /var/log/haproxy.log
   if $syslogfacility-text == 'local6' then stop
   ```

5. Создайте лог-файл /var/log/haproxy.log и укажите права доступа к нему с помощью команд:

```
touch /var/log/haproxy.log
chown root:adm /var/log/haproxy.log
chmod 640 /var/log/haproxy.log
```

6. При необходимости отредактируйте файл параметров ротации журнала локального балансировщика /etc/logrotate.d/haproxy.

   По умолчанию записи ротируются ежедневно. Срок хранения записей – 10 дней.

7. Перезапустите службу системного журнала с помощью команды:

   ```
   systemctl restart rsyslog
   ```

8. Запустите службу локального балансировщика с помощью команды:

   ```
   systemctl start haproxy
   ```

9. Разрешите автоматический старт службы локального балансировщика с помощью команды:

   ```
   systemctl enable haproxy
   ```

10. Проверьте статус службы локального балансировщика с помощью команды:

    ```
    systemctl status haproxy
    ```

    Статус должен быть *running*.

11. Проверьте наличие записей в журнале локального балансировщика:

    ```
    tail /var/log/haproxy.log
    ```

Локальный балансировщик будет настроен и запущен на узле кластера Kaspersky Security для Linux Mail Server.

Добавление сервера KATA

Если вы используете приложение KATA версии ниже 5.0, вы можете настроить интеграцию только с одним сервером KATA (см. раздел "Интеграция с одним сервером KATA" на стр. 278).

► *Чтобы добавить сервер KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры**.
3. В блоке параметров **Сервер KATA** нажмите на кнопку **Добавление сервера KATA**.

   Откроется окно **Добавление сервера KATA**.

4. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4-адрес сервера KATA, на котором установлен компонент Central Node.

   При интеграции с несколькими серверами KATA 5.0 и выше (см. раздел "Интеграция с несколькими серверами KATA" на стр. 278) укажите значение `127.0.0.1`.

IPv6-адреса не поддерживаются.

5. В поле **Порт** введите порт подключения к серверу KATA.

   По умолчанию указано значение 443.

   При интеграции с несколькими серверами KATA 5.0 и выше укажите значение `8000`.

6. Нажмите на кнопку **Далее**.

   В поле **Отпечаток SHA256** отобразится отпечаток сертификата сервера KATA.

7. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет добавлен. Информация о сервере отобразится в разделе **Защита KATA**, на закладке **Параметры** в блоке параметров **Сервер KATA**.

Настройка параметров защиты KATA

► *Чтобы настроить параметры защиты KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры**.
3. Переведите переключатель **Отправлять на сервер KATA сообщения без обнаружений** в положение **Включено**.

   Это требуется для авторизации Kaspersky Security для Linux Mail Server в веб-интерфейсе приложения KATA.

4. Если вы хотите отправлять на проверку в KATA все сообщения, переведите переключатель **Отправлять на сервер KATA сообщения с обнаружениями** в положение **Включено**.

   Доступно только при включенном переключателе **Отправлять на сервер KATA сообщения без обнаружений**.

5. В поле **Максимальное время ожидания ответа от KATA (сек.)** введите максимальное время ожидания результата проверки сообщения от сервера KATA.

   При превышении указанного времени ожидания приложение прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

   Возможные значения: 60 - 86400 (24 часа). Значение по умолчанию: 600

6. В поле **Максимальный размер KATA-карантина (МБ)** введите максимальный допустимый размер, занимаемый на диске KATA карантином, при превышении которого копии сообщений не будут помещаться в карантин.

   При превышении указанного размера приложение прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

Минимальное возможное значение – 1 МБ. Значение по умолчанию – 1024 МБ (1 ГБ).

7. В поле **Максимальное количество сообщений в KATA-карантине** введите количество сообщений в KATA карантине, при превышении которого копии сообщений не будут помещаться в карантин.

   При превышении указанного количества приложение прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

   Возможные значения: 1 - 4294967296. Значение по умолчанию: 5000

   > В KATA карантин помещаются сообщения размером не более 200 МБ. Если размер сообщения превышает 200 МБ, такое сообщение не проверяется, ему присваивается статус *Пропущено* для модуля **KATA**.

8. Нажмите на кнопку **Сохранить**.

Параметры защиты KATA будут настроены.

Мониторинг интеграции с KATA

Вы можете использовать следующие способы отслеживания статуса интеграции с KATA:

- Просматривать сводную информацию о состоянии подключения к серверу KATA на всех узлах кластера на информационной панели **Защита KATA** в разделе **Узлы**.

  Возможны следующие статусы:

  - *Подключено* – все узлы кластера успешно подключились и авторизованы на сервере KATA.
  - *Ошибки* – минимум на одном узле кластера возникла хотя бы одна из следующих ошибок в течение последнего часа:
    - *Неавторизованное соединение*.
    - *Проблемы соединения*.
    - *Слишком много запросов авторизации*.
  - *Отключено* – интеграция с KATA отключена в параметрах приложения.

- Просматривать детальную информацию о состоянии подключения к серверу KATA на каждом узле кластера.

  Для этого в информационной панели **Защита KATA** по ссылке **Подробнее** перейдите в раздел **Параметры → Внешние службы → Защита KATA → Статус**.

  В рабочей области отображается таблица узлов кластера с информацией о подключении к серверу KATA:

  - **IP-адрес:порт** – IP-адрес и порт узла кластера.
  - **Роль** – роль узла в кластере.
  - **Отпечаток SHA256** – отпечаток сертификата сервера.
  - **Статус** – состояние подключения к серверу KATA:
    - **Подключено** – узел кластера успешно подключен и авторизован на сервере KATA.
    - **Неавторизованное соединение** – подключение с сервером KATA установлено, но администратор KATA еще не подтвердил запрос на интеграцию.

- **Проблемы соединения** – ошибка подключения к серверу KATA.
- **Отключено** – интеграция с KATA отключена в параметрах приложения.
- **Слишком много запросов авторизации** – превышено максимальное количество запросов на интеграцию, установленное на сервере KATA.

  По умолчанию установлено значение 50.

Если есть подключение хотя бы к одному серверу KATA, в таблице отображается успешный статус подключения. Если нет связи ни с одним сервером KATA, в таблице отображается ошибка.

- Просматривать сведения о подключении к серверу KATA в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 138).
- Использовать скрипт для контроля статуса подключения к отдельным серверам KATA (при интеграции с несколькими серверами KATA версии 5.0 и выше).

► *Чтобы просмотреть статусы подключения к отдельным серверам KATA:*

1. Создайте файл /opt/kaspersky/klms/bin/hastat и добавьте в него следующие строки:

```
#!/bin/env python3

import socket

columns = [ 'pxname', 'svname', 'status' ]
out_form = '{:<20} | {:<20} | {}'
out_line = '-' * 68

s = socket.socket(socket.AF_UNIX, socket.SOCK_STREAM)
s.connect('/var/lib/haproxy/stats')
s.sendall('show stat\n'.encode())
response = s.recv(65000)
s.close()

rows = response.decode().split('\n')
headers = rows.pop(0)[2:].strip().split(',')
indexes = [ headers.index(c) for c in columns ]

print(out_line)
print(out_form.format(*columns))
print(out_line)
```

```
    for row in rows:
        vals = row.split(',')
        if len(vals) >= len(headers):
            data = [ vals[p] for p in indexes ]
            print(out_form.format(*data))

    print(out_line)
```

2. Сохраните файл.
3. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
4. Выполните команду:

   ```
   python3 /opt/kaspersky/klms/bin/hastat
   ```

   На экране отобразится таблица подключений и их статусов.

Пример результата выполнения команды показан на рисунке ниже:

```
------------------------------------------------------------------
pxname              | svname              | status
------------------------------------------------------------------
kata_balancer       | FRONTEND            | OPEN
kata_servers        | kata_node1          | UP
kata_servers        | kata_node2          | DOWN
kata_servers        | kata_node3          | DOWN
kata_servers        | kata_node4          | DOWN
kata_servers        | BACKEND             | UP
------------------------------------------------------------------
```

Рисунок 1. Пример результата выполнения команды

В последнем столбце таблицы отображается статус подключения к отдельным серверам KATA (например, строки kata_node1, kata_node2) и общий статус подключения (строка BACKEND).

Возможные статусы подключения:

- *UP* – подключение есть.
- *DOWN* – подключения нет.

Если есть подключение хотя бы к одному из серверов KATA, общий статус подключения будет *UP*.

Скрипт запрашивает у локального балансировщика статус подключения и выводит его в консоль.

Добавление, изменение и удаление IP-адресов серверов KATA

Порядок добавления, изменения и удаления IP-адресов зависит от количества серверов KATA.

Интеграция с одним сервером KATA

► *Чтобы изменить IP-адрес сервера:*

1. В веб-интерфейсе Kaspersky Security для Linux Mail Server выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры** и в блоке параметров **Сервер KATA** нажмите на кнопку **Заменить**.

► *Чтобы удалить IP-адрес сервера:*

1. В веб-интерфейсе Kaspersky Security для Linux Mail Server выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры** и в блоке параметров **Сервер KATA** нажмите на кнопку **Удалить**.

Интеграция с несколькими серверами KATA

Применимо только при интеграции с KATA версии 5.0 и выше.

Порядок действий для добавления, изменения и удаления адресов серверов KATA зависит от способа указания адресов, выбранного на этапе подготовки конфигурационного файла локального балансировщика (см. раздел "Создание конфигурационного файла для локального балансировщика" на стр. 279):

- Для получения адресов серверов KATA используется доменное имя.

  ► *Чтобы изменить или удалить адреса серверов KATA,*

  опубликуйте необходимые изменения на DNS-сервере.

  Локальный балансировщик в течение 5 минут автоматически обнаружит и применит опубликованные изменения. Ручной перезапуск службы не требуется.

  После внесения изменений рекомендуется проверить статус подключения к серверам KATA в командной оболочке операционной системы на каждом узле кластера с помощью скрипта для мониторинга интеграции с KATA.

- IP-адреса серверов KATA были указаны в конфигурационном файле.

  ► *Чтобы изменить или удалить адреса серверов KATA, на каждом узле кластера выполните следующие действия:*

  1. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
  2. Сделайте резервную копию конфигурационного файла локального балансировщика:

     ```
     cp -p /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.backup
     ```

     В случае возникновения проблем можно будет восстановить конфигурационный файл из резервной копии с помощью команды:

     ```
     cp -p /etc/haproxy/haproxy.cfg.backup /etc/haproxy/haproxy.cfg
     ```

3. Откройте конфигурационный файл локального балансировщика /etc/haproxy/haproxy.cfg в текстовом редакторе и внесите необходимые изменения в секцию backend или замените файл заранее подготовленной исправленной версией.
4. Перезапустите службу локального балансировщика с помощью команды:

   ```
   systemctl restart haproxy
   ```

5. Проверьте статус службы локального балансировщика с помощью команды:

   ```
   systemctl status haproxy
   ```

   Статус должен быть *running*.
6. Проверьте статус подключения к серверам KATA с помощью скрипта для мониторинга интеграции с KATA.

Отключение интеграции с KATA

► *Чтобы отключить интеграцию с KATA:*

1. В веб-интерфейсе управляющего узла Kaspersky Security для Linux Mail Server выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**, выберите вкладку **Параметры** и в блоке параметров **Сервер KATA** нажмите на кнопку **Удалить**.
2. При интеграции с несколькими серверами KATA версии 5.0 и выше на каждом узле кластера выполните следующие действия:
   a. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
   b. Остановите службу локального балансировщика с помощью команды:

      ```
      systemctl stop haproxy
      ```

   b. Отключите автоматический запуск службы локального балансировщика с помощью команды:

      ```
      systemctl disable haproxy
      ```

   c. Проверьте статус службы локального балансировщика с помощью команды:

      ```
      systemctl status haproxy
      ```

      Статус должен быть *stopped*.

Интеграция с приложением KATA будет отключена.

kaspersky

Работа с приложением по протоколу SNMP

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

В Kaspersky Security для Linux Mail Server для работы по протоколу SNMP используется *SNMP-агент*, который отслеживает информацию о работе приложения. Kaspersky Security для Linux Mail Server может отправлять эту информацию в виде статистики, а также *SNMP-ловушек* – уведомлений о событиях работы приложения.

По протоколу SNMP вы можете получить доступ к следующей информации о приложении:

- общим сведениям;
- статистике работы Kaspersky Security для Linux Mail Server с момента установки приложения;
- данным о событиях, возникающих в ходе работы Kaspersky Security для Linux Mail Server.

Доступ предоставляется только на чтение информации.

Информация об SNMP-ловушках и статистике, отправляемой по протоколу SNMP, хранится в базе данных MIB. В качестве SNMP-сервера, принимающего статистику, используется локальная служба snmpd на каждом узле кластера. Взаимодействие с внешним SNMP-сервером по протоколу AgentX не поддерживается. SNMP-ловушки можно принимать с помощью службы snmptrapd локально на каждом узле кластера или перенаправлять на внешний сервер.

Для работы по протоколу SNMP требуется предварительно настроить службу snmpd в операционной системе (см. раздел «Настройка службы snmpd в операционной системе» на стр. 290) на каждом узле кластера.

В этом разделе

kaspersky

Настройка службы snmpd в операционной системе

Для работы по протоколу SNMP с Kaspersky Security для Linux Mail Server используется служба snmpd из состава операционной системы. Служба snmpd выступает в роли мастер-агента, принимая и обрабатывая запросы от систем мониторинга и других внешних потребителей по протоколу SNMP. Kaspersky Security для Linux Mail Server подключается к службе snmpd в качестве субагента по протоколу AgentX через UNIX™-сокет.

Установка службы snmpd

Проверьте, что в вашей операционной системе установлена служба snmpd. Если службы нет, установите соответствующие пакеты.

► *Чтобы установить службу snmpd и вспомогательные утилиты в операционной системе Astra Linux Special Edition, используйте команду:*

```
apt install snmp snmpd
```

Создание учетной записи пользователя для доступа к данным

Перед созданием учетной записи остановите службу snmpd.

Для безопасного доступа к данным по протоколу SNMPv3 с аутентификацией и шифрованием нужно создать учетную запись на стороне службы snmpd со следующими данными:

- Имя пользователя (чувствительно к регистру).
- Алгоритм аутентификации (MD5 или SHA, рекомендуется SHA).
- Пароль для аутентификации.
- Алгоритм шифрования (DES или AES, рекомендуется AES).
- Пароль для шифрования.

В целях безопасности рекомендуется использовать отдельные учетные записи на разных узлах кластера Kaspersky Security для Linux Mail Server.

Создать учетную запись можно следующими способами:

- С помощью утилиты net-snmp-create-v3-user, если она есть в операционной системе.
- Вручную, добавив соответствующую директиву в конфигурационный файл службы snmpd.

► *Чтобы создать учетную запись пользователя с помощью утилиты net-snmp-create-v3-user, используйте команду*

```
net-snmp-create-v3-user -ro -a <snmp_auth_algo> -x <snmp_priv_algo>
<snmp_username>
```

Пароли для аутентификации и шифрования будут запрошены интерактивно.

Пример:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

► *Чтобы создать учетную запись пользователя без утилиты:*

1. Создайте конфигурационный файл /var/lib/snmp/snmpd.conf с помощью команды:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Добавьте в конфигурационный файл строку вида:

   ```
   createUser <snmp_username> <snmp_auth_algo> "<snmp_auth_pass>"
   <snmp_priv_algo> "<snmp_priv_pass>"
   ```

Пример:

```
createUser MonitoringUser SHA "MonitoringAuthSecret" AES
"MonitoringPrivSecret"
```

Создание учетной записи пользователя для приема SNMP-ловушек

Для приема SNMP-ловушек по протоколу SNMPv3 с аутентификацией и шифрованием нужно на стороне системы мониторинга создать учетную запись в контексте соответствующей службы (обычно это служба snmptrapd).

Учетная запись должна содержать следующие данные:

- Имя пользователя.
- Алгоритм аутентификации.
- Пароль для аутентификации.
- Алгоритм шифрования.
- Пароль для шифрования.

В целях безопасности нужно использовать разные учетные записи для доступа к данным и для приема SNMP-ловушек.
Рекомендуется создавать отдельные учетные записи для приема SNMP-ловушек с разных узлов кластера Kaspersky Security для Linux Mail Server.

Инструкцию по созданию учетной записи пользователя для приема SNMP-ловушек см. в документации вашей системы мониторинга.

Настройка службы snmpd

Конфигурация службы snmpd хранится в файле /etc/snmp/snmpd.conf. Вы можете добавить нужные данные в существующий конфигурационный файл или создать новый конфигурационный файл и последовательно добавить в него строки, приведенные ниже.

► *Чтобы настроить службу snmpd:*

1. Если вы создали новый конфигурационный файл, убедитесь, что доступ к нему имеет только суперпользователь. При необходимости установите разрешения с помощью команд:

   ```
   chown root:root /etc/snmp/snmpd.conf
   chmod 600 /etc/snmp/snmpd.conf
   ```

2. Укажите протокол, адрес сетевого интерфейса и номер порта, на котором служба snmpd будет принимать входящие запросы.

   - Если вы хотите принимать запросы на всех сетевых интерфейсах, добавьте в конфигурационный файл следующие строки:

     ```
     # Listen for incoming SNMP requests via UDP
     agentAddress udp:161
     ```

   - Если вы хотите принимать запросы только на локальном сетевом интерфейсе, например если система мониторинга установлена на этой же машине, добавьте строки:

     ```
     # Listen for incoming SNMP requests via UDP
     agentAddress udp:127.0.0.1:161
     ```

3. Укажите путь и разрешения для UNIX-сокета, на котором служба snmpd будет принимать подключения от субагента по протоколу AgentX. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Listen for subagent connections via UNIX socket
   master agentx
   agentXSocket unix:/var/run/agentx-master.socket
   agentXPerms 770 770 kluser klusers
   ```

4. При необходимости вы можете указать описание системы, расположение системы, контактный адрес администратора. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Basic system information
   sysDescr    <system_description>
   sysLocation <system_location>
   sysContact  <contact_address>
   sysServices 72
   ```

5. Укажите область OID-дерева, которая будет доступна вашей системе мониторинга по протоколу SNMP. Для доступа к данным приложения Kaspersky Security для Linux Mail Server добавьте в конфигурационный файл следующие строки:

   ```
   # Kaspersky Security для Linux Mail Server SNMP statistics
   view monitoring included .1.3.6.1.4.1.23668.1463
   ```

6. Вы можете дополнительно указать область OID-дерева с информацией об операционной системе, которую хранит служба snmpd. Эта область будет доступна вашей системе мониторинга.

   Информация об операционной системе включает, например, данные об использовании процессора и оперативной памяти, данные о свободном месте на дисковых разделах, загрузке сетевых интерфейсов, список установленного программного обеспечения, список открытых сетевых

соединений, список запущенных процессов. Эта информация может содержать конфиденциальные данные.

- Если вы хотите разрешить доступ только к общей информации о системе и данным об использовании памяти, процессора, сетевых и дисковых устройств, добавьте в конфигурационный файл следующие строки:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Если вы хотите разрешить доступ ко всей системной информации, добавьте в конфигурационный файл следующие строки:

```
# Allow access to the whole OID tree
view monitoring included .1
```

7. Укажите режим доступа и область данных для созданной учетной записи. Для этого добавьте в конфигурационный файл следующие строки:

```
# Access control for SNMPv3 monitoring system user
rouser <snmp_username> priv -V monitoring
```

8. Для отправки SNMP-ловушек укажите IP-адрес системы мониторинга и учетные данные пользователя для приема ловушек. Для этого добавьте в конфигурационный файл следующие строки:

```
# Send SNMPv3 traps to the monitoring system
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <trap_username> -a
<trap_auth_algo> -A "<trap_auth_pass>" -x <trap_priv_algo> -X
"<trap_priv_pass>" udp:<IP-address>:162
```

Служба snmpd будет настроена.

Для интеграции с несколькими системами мониторинга создайте отдельную учетную запись для каждой системы, укажите для учетных записей область доступных данных (директивы view и rouser) и настройте отправку SNMP-ловушек (директива trapsess).

Пример конфигурационного файла службы snmpd:

```
# Listen for incoming SNMP requests via UDP
agentAddress udp:161

# Listen for subagent connections via UNIX socket
master agentx
agentXSocket unix:/var/run/agentx-master.socket
agentXPerms 770 770 kluser klusers

# Basic system information
sysDescr    Example Mail Gateway Server, Node 05
sysLocation Example Datacenter, Ground floor, B23-U45
sysContact  Mail system administrator <admin@example.com>
sysServices 72

# Kaspersky Security для Linux Mail Server SNMP statistics
view monitoring included .1.3.6.1.4.1.23668.1463

# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31

# Access control for SNMPv3 monitoring system user
rouser MonitoringUser priv -V monitoring

# Send SNMPv3 traps to the monitoring system
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u TrapUser -a SHA -A
"TrapAuthSecret" -x AES -X "TrapPrivSecret" udp:10.16.32.64:162
```

Запуск новой конфигурации службы snmpd

► *Чтобы применить новую конфигурацию:*

1. Перезапустите службу snmpd с помощью команды:

   ```
   systemctl restart snmpd
   ```

2. Проверьте статус службы snmpd с помощью команды:

   ```
   systemctl status snmpd
   ```

   Статус должен быть `running`.

3. Разрешите автоматический запуск службы при старте операционной системы с помощью команды:

   ```
   systemctl enable snmpd
   ```

4. Если у вас используется сетевой экран в операционной системе или на сетевом оборудовании, добавьте соответствующие правила для пропуска пакетов протокола SNMP.

Служба snmpd будет запущена.

Проверка работоспособности службы snmpd

Для проверки работоспособности службы snmpd настройте использование SNMP в веб-интерфейсе Kaspersky Security для Linux Mail Server (см. раздел "Настройка параметров подключения к SNMP-серверу" на стр. 296) и выполните запрос SNMP-данных с помощью утилиты snmpwalk.

► *Чтобы получить области SNMP-данных, предоставляемых приложением Kaspersky Security для Linux Mail Server, выполните команду:*

```
snmpwalk -v3 -l authPriv -u <snmp_username> -a <snmp_auth_algo> -A
"<snmp_auth_pass>" -x <snmp_priv_algo> -X "<snmp_priv_pass>" <IP-адрес>
.1.3.6.1.4.1.23668.1463
```

Пример:

snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret" 127.0.0.1 .1.3.6.1.4.1.23668.1463

Включение и отключение использования SNMP в Kaspersky Security для Linux Mail Server

Перед включением использования протокола SNMP требуется настроить службу snmpd в операционной системе (см. раздел "Настройка службы snmpd в операционной системе" на стр. 290).

► *Чтобы включить или отключить использование SNMP в работе приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите или отключите переключатель **Использовать SNMP**.
3. Нажмите на кнопку **Сохранить**.

Использование SNMP будет включено или отключено.

kaspersky

Настройка параметров подключения к SNMP-серверу

► *Чтобы настроить параметры подключения к SNMP-серверу:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите переключатель **Использовать SNMP**, если он отключен.
3. В поле **Путь к сокету** укажите путь к файлу сокета.

   По умолчанию указан путь `/var/run/agentx-master.socket`.

   > Для подключения к SNMP-серверу используется UNIX-сокет. Использование TCP- и UDP-сокетов не поддерживается.

4. В поле **Время ожидания ответа сервера (сек.)** укажите максимальное время ожидания ответа от SNMP-сервера в секундах. Вы можете указать значение в интервале от 1 до 255 секунд.

   Значение по умолчанию: 15 секунд.
5. Нажмите на кнопку **Сохранить**.

Параметры подключения к SNMP-серверу будут настроены.

Включение и отключение отправки SNMP-ловушек

► *Чтобы включить или отключить отправку SNMP-ловушек событий, возникающих в ходе работы приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите или отключите переключатель **Отправлять SNMP-ловушки**.

   Опция доступна только при включенном переключателе **Использовать SNMP**.

Отправка SNMP-ловушек будет включена или отключена. Приложение будет отправлять SNMP-ловушки при наступлении событий, соответствующих объектам MIB (см. раздел "Описание объектов MIB Kaspersky Security для Linux Mail Server" на стр. 299).

Настройка внешней системы мониторинга

Kaspersky Security для Linux Mail Server предоставляет данные по протоколу SNMP отдельно для каждого узла кластера. Для хранения, агрегации и анализа этих данных используется *внешняя система мониторинга* (далее также *система мониторинга*).

Настройка внешней системы мониторинга для работы по протоколу SNMP

► *Чтобы настроить внешнюю систему мониторинга:*

1. Если система мониторинга поддерживает импорт MIB-файлов, импортируйте информацию об объектах MIB приложения Kaspersky Security для Linux Mail Server (см. раздел "Экспорт объектов MIB" на стр. 320).

2. Добавьте в систему мониторинга все узлы кластера Kaspersky Security для Linux Mail Server в качестве наблюдаемых устройств (узлов сети).
3. Для каждого наблюдаемого устройства укажите параметры подключения по протоколу SNMPv3:
   - адрес подключения;
   - порт;
   - протокол;
   - учетные данные пользователя: имя пользователя, алгоритм аутентификации, пароль для аутентификации, алгоритм шифрования, пароль для шифрования.

     Используйте данные учетной записи, которая была создана при настройке службы snmpd на узле кластера Kaspersky Security для Linux Mail Server (см. раздел "Настройка службы snmpd в операционной системе" на стр. 290).
4. Для каждого наблюдаемого устройства укажите список данных, передаваемых по протоколу SNMP. Используйте символьные имена объектов MIB или их числовые идентификаторы. Для каждого элемента данных задайте его тип (целое число или строка), периодичность опроса, срок хранения.
5. Настройте графики, триггеры и оповещения, используя в качестве основы данные, передаваемые по протоколу SNMP.
6. Для каждого узла кластера Kaspersky Security для Linux Mail Server создайте учетную запись пользователя для получения ловушек по протоколу SNMPv3.

   Учетные данные пользователей укажите в настройках службы snmpd на узлах кластера (директива trapsess).
7. Для каждого наблюдаемого устройства укажите список событий, получаемых в виде SNMPv3-ловушек. Используйте символьные имена объектов MIB или их числовые идентификаторы. Для событий, которые вы считаете важными, создайте соответствующие триггеры.

Настройка службы snmptrapd для приема SNMP-ловушек

Некоторые системы мониторинга (например, Zabbix, LibreNMS) используют службу snmptrapd из состава операционной системы в качестве агента для приема SNMP-ловушек. Служба snmptrapd сохраняет информацию о полученных событиях в файл журнала, который в дальнейшем считывается системой мониторинга.

Настройка службы snmptrapd выполняется на компьютере, на котором установлена служба мониторинга.

► *Чтобы настроить службу snmptrapd:*

1. Проверьте, что в операционной системе установлены служба snmptrapd и базовые MIB-файлы (см. раздел "Экспорт объектов MIB" на стр. 320).

   Если служба snmptrapd отсутствует, установите соответствующие пакеты:
   - В операционных системах Red Hat® Enterprise Linux®, CentOS, Rocky Linux выполните команду:

     ```
     yum install net-snmp net-snmp-utils
     ```
   - В операционных системах Debian, Ubuntu, Astra Linux Special Edition выполните команду:

     apt install snmp snmptrapd

Чтобы установить базовые MIB-файлы:

- В операционных системах Red Hat Enterprise Linux, CentOS, Rocky Linux выполните команду:

  ```
  yum install net-snmp-libs
  ```

- В операционных системах Debian, Ubuntu выполните команду:

  ```
  apt install snmp-mibs-downloader
  ```

- В операционной системе Astra Linux Special Edition следуйте инструкциям в документации Astra Linux.

2. Скопируйте MIB-файлы Kaspersky Security для Linux Mail Server (см. раздел "Экспорт объектов MIB" на стр. 320) в каталог с MIB-файлами, например в папку /usr/share/snmp/mibs/klms.
3. Для подключения MIB-файлов приложения добавьте в конфигурационный файл /etc/snmp/snmp.conf следующие строки:

   ```
   mibdirs +/usr/share/snmp/mibs/klms
   mibs all
   ```

4. Конфигурация службы snmptrapd хранится в файле /etc/snmp/snmptrapd.conf. Вы можете добавить нужные данные в существующий конфигурационный файл или создать новый конфигурационный файл и последовательно добавить в него строки параметров.

   Если вы создали новый конфигурационный файл, убедитесь, что доступ к нему имеет только суперпользователь. При необходимости задайте нужные разрешения при помощи команд:

   ```
   chown root:root /etc/snmp/snmptrapd.conf
   chmod 600 /etc/snmp/snmptrapd.conf
   ```

5. Укажите протокол, адрес сетевого интерфейса и номер порта, на котором служба snmptrapd будет принимать SNMP-ловушки. Чтобы принимать запросы на всех сетевых интерфейсах, добавьте в конфигурационный файл следующую строку:

   ```
   snmpTrapdAddr udp:162
   ```

6. Для приема SNMP-ловушек по протоколу SNMPv3 с аутентификацией и шифрованием необходимо на стороне службы snmptrapd добавить учетные записи пользователей со следующими данными:

   - имя пользователя (чувствительно к регистру);
   - алгоритм аутентификации (MD5 или SHA, рекомендуется SHA);
   - пароль для аутентификации;
   - алгоритм шифрования (DES или AES, рекомендуется AES);
   - пароль для шифрования.

   > В целях безопасности рекомендуется создавать разные учетные записи пользователей для приема SNMP-ловушек с разных узлов кластера Kaspersky Security для Linux Mail Server.

7. Для каждой созданной учетной записи пользователя добавьте в конфигурационный файл следующие строки:

   ```
   createUser <trap_username> <trap_auth_algo> "<trap_auth_pass>"
   <trap_priv_algo> "<trap_priv_pass>"
   authUser log <trap_username> priv
   ```

Пример конфигурационного файла:

```
snmpTrapdAddr udp:162
createUser TrapUser SHA "TrapAuthSecret" AES "TrapPrivSecret"
authUser log TrapUser priv
createUser TrapUser2 SHA "TrapAuthSecret2" AES "TrapPrivSecret2"
authUser log TrapUser2 priv
```

8. Для проверки работоспособности службы snmptrapd выполните следующие действия:

   a. Настройте службу snmpd на узле кластера Kaspersky Security для Linux Mail Server (см. раздел "Настройка службы snmpd в операционной системе" на стр. 290) на отправку SNMP-ловушек на адрес системы мониторинга.

   b. Настройте отправку SNMP-ловушек в веб-интерфейсе Kaspersky Security для Linux Mail Server (см. раздел "Включение и отключение отправки SNMP-ловушек" на стр. 296).

   c. Запустите службу snmptrapd в отладочном режиме и ожидайте получения SNMP-ловушек.

      Для запуска службы snmptrapd в отладочном режиме выполните команду:

      ```
      snmptrapd -f -Lo
      ```

      Чтобы сгенерировать SNMP-ловушку, можно перезапустить службу klms на узле кластера Kaspersky Security для Linux Mail Server с помощью команды:

      ```
      systemctl restart klms
      ```

   Если все настроено правильно, вы получите SNMP-ловушку с событием о перезапуске приложения:

   ```
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (56062) 0:09:20.62
   SNMPv2-MIB::snmpTrapOID.0 = OID: KLMS-EVENTS-MIB::productStartEvent
   KLMS-EVENTS-MIB::sourceNode = STRING: mailgw01.example.com
   ```

9. Настройте интеграцию службы snmptrapd с системой мониторинга.

   Для этого следуйте инструкциям документации вашей системы мониторинга.

Служба snmptrapd будет настроена.

Описание объектов MIB Kaspersky Security для Linux Mail Server

В таблице ниже приведена информация об объектах MIB Kaspersky Security для Linux Mail Server.

kaspersky

События в работе приложения

Таблица 12. События в работе приложения

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.10	updateErrorEvent	Обновление баз приложения завершилось ошибкой.	• FQDN узла, на котором произошло событие. • Причина ошибки.
.1.3.6.1.4.1.23668.1463.1.30	aspBasesCompilationFailedEvent	Компиляция баз модуля Анти-Спам завершилась ошибкой.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.100	avBasesOutdatedEvent	Базы модуля Антивирус устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.120	avBasesObsoletedEvent	Базы модуля Антивирус сильно устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.130	aspBasesOutdatedEvent	Базы модуля Анти-Спам устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.140	aspBasesObsoletedEvent	Базы модуля Анти-Спам сильно устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.150	apBasesOutdatedEvent	Базы модуля Анти-Фишинг устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.160	apBasesObsoletedEvent	Базы модуля Анти-Фишинг сильно устарели.	• FQDN узла, на котором произошло событие.
.1.3.6.1.4.1.23668.1463.1.200	backupAddErrorEvent	Ошибка добавления сообщения в Хранилище.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения. • Причина ошибки.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.210	backupRotateErrorEvent	Ошибка удаления сообщений из Хранилища.	• FQDN узла, на котором произошло событие. • Причина ошибки.
.1.3.6.1.4.1.23668.1463.1.220	backupLimitReachedEvent	Достигнут максимально допустимый объем Хранилища.	• FQDN узла, на котором произошло событие. • Количество сообщений. • Суммарный размер сообщений. • Максимально допустимый объем Хранилища.
.1.3.6.1.4.1.23668.1463.1.300	licenseInstalledEvent	Код активации или файл ключа добавлен.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа.
.1.3.6.1.4.1.23668.1463.1.360	licenseUpdatedEvent	Статус лицензионного ключа изменен.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа. • Тип лицензии. • Тип функциональности. • Дата окончания срока действия лицензии.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.380	gracePeriodEvent	Начался льготный период действия лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа. • Количество дней до завершения льготного периода.
.1.3.6.1.4.1.23668.1463.1.310	licenseRevokedEvent	Код активации или файл ключа удален.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа.
.1.3.6.1.4.1.23668.1463.1.320	licenseExpiresSoonEvent	Срок действия лицензии скоро истечет.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа. • Количество дней до окончания срока действия лицензии.
.1.3.6.1.4.1.23668.1463.1.330	licenseExpiredEvent	Истек срок действия лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа. • Дата окончания срока действия лицензии.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.340	licenseTrialPeriodIsOverEvent	Истек срок действия пробной лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа. • Дата окончания срока действия лицензии.
.1.3.6.1.4.1.23668.1463.1.350	licenseBlacklistedEvent	Код активации или файл ключа помещен в список запрещенных.	• FQDN узла, на котором произошло событие. • Серийный номер лицензионного ключа.
.1.3.6.1.4.1.23668.1463.1.400	taskCrashEvent	Процесс приложения завершился аварийно.	• FQDN узла, на котором произошло событие. • Полный путь к бинарному файлу.
.1.3.6.1.4.1.23668.1463.1.410	taskRestartEvent	Процесс приложения перезапущен.	• FQDN узла, на котором произошло событие. • Полный путь к бинарному файлу.
.1.3.6.1.4.1.23668.1463.1.420	productStartEvent	Приложение запущено. Это событие возникает после того, как запускаются все службы, необходимые для работы Kaspersky Security для Linux Mail Server.	• FQDN узла, на котором произошло событие.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.510	threatDetectedEvent	Обнаружена угроза.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Статус модуля Антивирус. • Список обнаруженных объектов.
.1.3.6.1.4.1.23668.1463.1.520	antiVirusErrorEvent	Ошибка модуля Антивирус.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Причина ошибки.
.1.3.6.1.4.1.23668.1463.1.530	antiSpamErrorEvent	Ошибка модуля Анти-Спам.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Причина ошибки.
.1.3.6.1.4.1.23668.1463.1.700	ksnConnectionStatusEvent	Изменилось состояние соединения с сервером KSN.	• FQDN узла, на котором произошло событие. • Новое состояние соединения с сервером KSN.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.1463.1.1600	clusterConsistencyErrorEvent	Ошибка состояния серверов. Например, нет ни одного сервера с ролью Управляющий узел.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.
.1.3.6.1.4.1.23668.1463.1.1610	clusterEmergencyStateEvent	Приложение перешло в аварийный режим.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.
.1.3.6.1.4.1.23668.1463.1.1620	settingsSynchronizationErrorEvent	Ошибка синхронизации параметров между Управляющим и Подчиненными узлами.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.
.1.3.6.1.4.1.23668.1463.1.910	ldapCacheUpdateEvent	Синхронизация данных с Active Directory завершена.	• FQDN узла, на котором произошло событие. • Статус синхронизации LDAP-кеша. • Статус синхронизации данных для автозаполнения учетных записей.

Статистика модуля Антивирус

Таблица 13. Статистика модуля Антивирус

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.2.1.0	antivirusStatistics.notDetectedMessages	Counter64	Количество проверенных сообщений, в которых не обнаружены угрозы.
.1.3.6.1.4.1.23668.1463.2.2.2.0	antivirusStatistics.infectedMessages	Counter64	Количество сообщений, в которых обнаружены угрозы.
.1.3.6.1.4.1.23668.1463.2.2.4.0	antivirusStatistics.encryptedMessages	Counter64	Количество сообщений, для которых не удалось проверить зашифрованные (защищенные паролем) вложения.
.1.3.6.1.4.1.23668.1463.2.2.5.0	antivirusStatistics.docWithMacroMessages	Counter64	Количество сообщений, содержащих вложения с макросами.
.1.3.6.1.4.1.23668.1463.2.2.6.0	antivirusStatistics.scanErrors	Counter64	Количество сообщений, при обработке которых произошли ошибки.
.1.3.6.1.4.1.23668.1463.2.2.7.0	antivirusStatistics.notScannedSettingsMessages	Counter64	Количество сообщений, которые не были проверены на наличие угроз согласно заданным значениям параметров для модуля Антивирус.

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.2.8.0	antivirusStatistics.notScannedViolationsMessages	Counter64	Количество сообщений, которые не были проверены на наличие угроз из-за проблем, связанных с лицензией или базами приложения.

Статистика антивирусных баз

Таблица 14. Статистика антивирусных баз

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.6.1.0	antivirusbasesStatistics.basesDate	String	Дата и время последнего обновления антивирусных баз.
.1.3.6.1.4.1.23668.1463.2.6.2.0	antivirusbasesStatistics.basesRecordCount	Counter64	Количество записей в антивирусных базах.
.1.3.6.1.4.1.23668.1463.2.6.3.0	antivirusbasesStatistics.basesStatus	String	Текущее состояние антивирусных баз. Возможные значения: *UpToDate*, *Outdated*, *Obsoleted*.

Статистика Проверки ссылок

Таблица 15. Статистика Проверки ссылок

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.12.1.0	linksScanning.notDetectedMessages	Counter64	Количество проверенных сообщений, в которых не обнаружены ссылки.
.1.3.6.1.4.1.23668.1463.2.12.3.0	linksScanning.linksScanningMessages	Counter64	Количество сообщений, в которых обнаружены вредоносные, рекламные ссылки или ссылки, связанные с легальными программами, которые могут быть использованы злоумышленниками.
.1.3.6.1.4.1.23668.1463.2.12.4.0	linksScanning.scanErrors	Counter64	Количество сообщений, при обработке которых произошли ошибки.
.1.3.6.1.4.1.23668.1463.2.12.5.0	linksScanning.notScannedSettingsMessages	Counter64	Количество сообщений, которые не были проверены на наличие ссылок согласно заданным значениям параметров для Проверки ссылок.
.1.3.6.1.4.1.23668.1463.2.12.6.0	linksScanning.notScannedViolationsMessages	Counter64	Количество сообщений, которые не были проверены на наличие ссылок из-за проблем, связанных с лицензией или базами приложения.

kaspersky

Статистика модуля Анти-Спам

Таблица 16. Статистика модуля Анти-Спам

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.3.1.0	antispamStatistics.notDetectedMessages	Counter64	Количество проверенных сообщений, в которых не обнаружен спам.
.1.3.6.1.4.1.23668.1463.2.3.2.0	antispamStatistics.spamMessages	Counter64	Количество сообщений, в которых обнаружен спам.
.1.3.6.1.4.1.23668.1463.2.3.3.0	antispamStatistics.probableSpamMessages	Counter64	Количество сообщений, в которых обнаружен предполагаемый спам.
.1.3.6.1.4.1.23668.1463.2.3.5.0	antispamStatistics.antiSpamQuarantinedMessages	Counter64	Количество сообщений, помещенных в Анти-Спам карантин.
.1.3.6.1.4.1.23668.1463.2.3.6.0	antispamStatistics.scanErrors	Counter64	Количество сообщений, при обработке которых произошли ошибки.
.1.3.6.1.4.1.23668.1463.2.3.7.0	antispamStatistics.notScannedSettingsMessages	Counter64	Количество сообщений, которые не были проверены на наличие спама согласно заданным значениям параметров для модуля Анти-Спам.
.1.3.6.1.4.1.23668.1463.2.3.8.0	antispamStatistics.notScannedViolationsMessages	Counter64	Количество сообщений, которые не были проверены на наличие спама из-за проблем, связанных с лицензией или базами приложения.

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.3.9.0	antispamStatistics.massMail	Counter64	Количество сообщений, признанных массовой рассылкой.

Статистика баз модуля Анти-Спам

Таблица 17. Статистика баз модуля Анти-Спам

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.7.1.0	antispambasesStatistics.basesDate	String	Дата и время последнего обновления баз модуля Анти-Спам.
.1.3.6.1.4.1.23668.1463.2.7.2.0	antispambasesStatistics.basesStatus	String	Текущее состояние баз модуля Анти-Спам. Возможные значения: *UpToDate*, *Outdated*, *Obsoleted*.

Статистика модуля Анти-Фишинг

Таблица 18. Статистика модуля Анти-Фишинг

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.10.1.0	antiphishingStatistics.notDetectedMessages	Counter64	Количество проверенных сообщений, в которых не обнаружен фишинг.
.1.3.6.1.4.1.23668.1463.2.10.2.0	antiphishingStatistics.phishingMessages	Counter64	Количество сообщений, в которых обнаружен фишинг.
.1.3.6.1.4.1.23668.1463.2.10.4.0	antiphishingStatistics.scanErrors	Counter64	Количество сообщений, при обработке которых произошли ошибки.
.1.3.6.1.4.1.23668.1463.2.10.5.0	antiphishingStatistics.notScannedSettingsMessages	Counter64	Количество сообщений, которые не были проверены на наличие фишинга согласно заданным значениям параметров для модуля Анти-Фишинг.
.1.3.6.1.4.1.23668.1463.2.10.6.0	antiphishingStatistics.notScannedViolationsMessages	Counter64	Количество сообщений, которые не были проверены на наличие фишинга из-за проблем, связанных с лицензией или базами приложения.

Статистика баз модуля Анти-Фишинг

Таблица 19. Статистика баз модуля Анти-Фишинг

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.11.1.0	antiphishingbasesStatistics.basesDate	String	Дата и время последнего обновления баз модуля Анти-Фишинг.
.1.3.6.1.4.1.23668.1463.2.11.2.0	antiphishingbasesStatistics.basesStatus	String	Текущее состояние баз модуля Анти-Фишинг. Возможные значения: *UpToDate*, *Outdated*, *Obsoleted*.

Статистика контентной фильтрации

Таблица 20. Статистика контентной фильтрации

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.4.1.0	cfStatistics.notDetectedMessages	Counter64	Количество проверенных объектов, к которым не были применены никакие действия.
.1.3.6.1.4.1.23668.1463.2.4.2.0	cfStatistics.sizeExcededMessages	Counter64	Количество объектов, размер которых превышает максимальный допустимый размер, заданный в параметрах контентной фильтрации.
.1.3.6.1.4.1.23668.1463.2.4.3.0	cfStatistics.prohibitedTypeMessages	Counter64	Количество сообщений, содержащих вложения запрещенного формата.
.1.3.6.1.4.1.23668.1463.2.4.4.0	cfStatistics.prohibitedNameMessages	Counter64	Количество сообщений, содержащих вложения с запрещенными именами.
.1.3.6.1.4.1.23668.1463.2.4.5.0	cfStatistics.notScannedSettingsMessages	Counter64	Количество сообщений, для которых не осуществлялась контентная фильтрация согласно заданным значениям параметров.

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.4.6.0	cfStatistics.notScannedViolationsMessages	Counter64	Количество сообщений, для которых не осуществлялась контентная фильтрация из-за проблем, связанных с лицензией или базами приложения.

Статистика примененных действий

Таблица 21. Статистика примененных действий

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.5.1.0	actionStatistics.notDetectedMessages	Counter64	Количество сообщений, к которым не были применены никакие действия по результатам проверки всех включенных модулей приложения.
.1.3.6.1.4.1.23668.1463.2.5.2.0	actionStatistics.disinfectedMessages	Counter64	Количество вылеченных сообщений.
.1.3.6.1.4.1.23668.1463.2.5.3.0	actionStatistics.attachmentDeletedMessages	Counter64	Количество сообщений, в которых были удалены зараженные вложения.
.1.3.6.1.4.1.23668.1463.2.5.4.0	actionStatistics.deletedMessages	Counter64	Количество удаленных сообщений.
.1.3.6.1.4.1.23668.1463.2.5.5.0	actionStatistics.rejectedMessages	Counter64	Количество отклоненных сообщений.
.1.3.6.1.4.1.23668.1463.2.5.6.0	actionStatistics.quarantinedMessages	Counter64	Количество сообщений, помещенных на карантин, так как их обработка была отложена.
.1.3.6.1.4.1.23668.1463.2.5.7.0	actionStatistics.skippedMessages	Counter64	Количество сообщений, в которых хотя бы один модуль проверки обнаружил угрозу или выдал ошибку проверки и было выполнено действие **Пропустить**.

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.5.8.0	actionStatistics.unprocessedMessages	Counter64	Количество сообщений, не проверенных ни одним модулем из-за недоступности баз приложения.

Статистика приложения

Таблица 22. Статистика приложения

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.8.1.0	productinfoStatistics.applicationName	String	Название приложения.
.1.3.6.1.4.1.23668.1463.2.8.2.0	productinfoStatistics.applicationVersion	String	Версия приложения.
.1.3.6.1.4.1.23668.1463.2.8.3.0	productinfoStatistics.installDate	String	Дата и время установки приложения.
.1.3.6.1.4.1.23668.1463.2.8.4.0	productinfoStatistics.licenseExpireDate	String	Дата и время истечения срока действия лицензии.
.1.3.6.1.4.1.23668.1463.2.8.5.0	productinfoStatistics.licenseStatus	String	Текущее состояние лицензионного ключа.

Сводная статистика

Таблица 23. Сводная статистика

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.9.1.0	reportsummaryStatistics.threatNumber	Counter64	Количество сообщений, в которых обнаружены угрозы.
.1.3.6.1.4.1.23668.1463.2.9.2.0	reportsummaryStatistics.threatSize	Counter64	Общий размер сообщений, в которых обнаружены угрозы.
.1.3.6.1.4.1.23668.1463.2.9.3.0	reportsummaryStatistics.spamNumber	Counter64	Количество сообщений, в которых обнаружен спам.
.1.3.6.1.4.1.23668.1463.2.9.4.0	reportsummaryStatistics.spamSize	Counter64	Общий размер сообщений, в которых обнаружен спам.
.1.3.6.1.4.1.23668.1463.2.9.5.0	reportsummaryStatistics.contentFilteringDetectsNumber	Counter64	Количество сообщений, отклоненных согласно параметрам контентной фильтрации.
.1.3.6.1.4.1.23668.1463.2.9.6.0	reportsummaryStatistics.contentFilteringDetectsSize	Counter64	Общий размер сообщений, отклоненных согласно параметрам контентной фильтрации.
.1.3.6.1.4.1.23668.1463.2.9.7.0	reportsummaryStatistics.notScannedNumber	Counter64	Количество непроверенных сообщений.
.1.3.6.1.4.1.23668.1463.2.9.8.0	reportsummaryStatistics.notScannedSize	Counter64	Общий размер непроверенных сообщений.
.1.3.6.1.4.1.23668.1463.2.9.9.0	reportsummaryStatistics.notDetectedNumber	Counter64	Количество проверенных сообщений, в которых ничего не обнаружено.

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.9.10.0	reportsummaryStatistics.notDetectedSize	Counter64	Общий размер проверенных сообщений, в которых ничего не обнаружено.
.1.3.6.1.4.1.23668.1463.2.9.11.0	reportsummaryStatistics.totalNumber	Counter64	Количество всех обработанных сообщений.
.1.3.6.1.4.1.23668.1463.2.9.12.0	reportsummaryStatistics.totalSize	Counter64	Общий размер всех обработанных сообщений.
.1.3.6.1.4.1.23668.1463.2.9.13.0	reportsummaryStatistics.phishingNumber	Counter64	Количество сообщений, содержащих фишинг.
.1.3.6.1.4.1.23668.1463.2.9.14.0	reportsummaryStatistics.phishingSize	Counter64	Общий размер сообщений, содержащих фишинг.

Статистика Хранилища

Таблица 24. Статистика Хранилища

Идентификатор (OID)	Символьное имя	Тип данных	Описание
.1.3.6.1.4.1.23668.1463.2.1.1.0	backupStatistics.messageCount	Counter64	Количество объектов, находящихся в Хранилище в данный момент.
.1.3.6.1.4.1.23668.1463.2.1.2.0	backupStatistics.usedSpace	Counter64	Объем дискового пространства, занимаемый Хранилищем.

Экспорт объектов MIB

Файлы, содержащие информацию об объектах MIB Kaspersky Security для Linux Mail Server, расположены в директории /opt/kaspersky/klms/share/snmp-mibs. Вы можете скопировать эти файлы с любого узла кластера и импортировать их в свою систему мониторинга.

Директория /opt/kaspersky/klms/share/snmp-mibs содержит следующие файлы:

- KASPERSKY-MIB.txt
- KLMS-ACTION-STATISTICS.txt

- KLMS-ANTIPHISHINGBASES-STATISTICS.txt
- KLMS-ANTIPHISHING-STATISTICS.txt
- KLMS-ANTISPAMBASES-STATISTICS.txt
- KLMS-ANTISPAM-STATISTICS.txt
- KLMS-ANTIVIRUSBASES-STATISTICS.txt
- KLMS-ANTIVIRUS-STATISTICS.txt
- KLMS-BACKUP-STATISTICS.txt
- KLMS-CF-STATISTICS.txt
- KLMS-EVENTS-MIB.txt
- KLMS-MIB.txt
- KLMS-PRODUCTINFO-STATISTICS.txt
- KLMS-REPORTSUMMARY-STATISTICS.txt
- KLMS-STATISTICS-MIB.txt

Перед использованием MIB-файлов Kaspersky Security для Linux Mail Server убедитесь, что в вашей системе установлены следующие базовые объекты MIB:

- SNMPv2-SMI
- SNMPv2-CONF
- SNMPv2-TC
- SNMP-FRAMEWORK-MIB

kaspersky

Почтовые уведомления приложения

Вы можете настроить следующие виды почтовых уведомлений:

- уведомления о событиях в работе приложения (см. раздел "Настройка уведомлений о событиях в работе приложения" на стр. 323);
- уведомления о срабатывании правил обработки сообщений (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 123).

Уведомления о событиях в работе приложения

Уведомления о событиях в работе приложения (далее также "уведомления приложения") содержат информацию о параметрах приложения, ошибках, возникающих во время работы приложения, а также о восстановлении приложения после сбоев.

Вы можете настроить отправку уведомлений (см. раздел "Настройка уведомлений о событиях в работе приложения" на стр. 323) администратору о следующих событиях в работе приложения:

- Защита:
  - Антивирусные базы устарели.
  - Базы Анти-Спама устарели.
  - Базы Анти-Фишинга устарели.
  - Проблемы с обновлением баз.
  - Проблемы со службой KSN/KPSN.
  - Запросы KSN отфильтрованы.
- Синхронизация:
  - Узел недоступен.
  - Не удалось синхронизировать данные.
  - Не удалось применить значения параметров.
  - Время не совпадает со временем на Управляющем узле.
  - Проблемы конфигурации кластера.
- Интеграция LDAP:
  - Проблемы подключения к LDAP.
  - Не удалось сохранить данные LDAP для сопоставления правил.
  - Не удалось сохранить данные LDAP для автозаполнения учетных записей.

Текст уведомления содержит следующую информацию:

- Название группы и список ошибок, возникших на момент отправки уведомления.
- Дата и время последнего возникновения каждой ошибки.

  Для ошибок из групп **Синхронизация** и **Интеграция LDAP** также указывается дата и время последней успешной синхронизации.

- IP-адрес и порт подключения к узлу кластера, на котором возникли указанные ошибки.
- Комментарий к узлу кластера.

Приложение отправляет уведомления о событиях в работе один раз в сутки в 00:00 по локальному времени Управляющего узла, если на этот момент есть хотя бы одна из перечисленных выше ошибок. Если возникают новые ошибки или исправлены уже известные ошибки, уведомления приложения отправляются не чаще чем один раз в 15 минут.

Уведомления о срабатывании правил обработки сообщений

Уведомления о срабатывании правил обработки сообщений содержат информацию об объектах, обнаруженных одним или несколькими модулями приложения в результате проверки сообщения.

Вы можете настроить отправку уведомлений (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 324) отправителю и получателям сообщения, адресатам из дополнительного списка, заданного в сработавшем правиле, а также получателям из общего списка для всех правил. Для каждой из перечисленных групп получателей вы можете настроить разные шаблоны уведомлений (см. раздел "Настройка шаблонов уведомлений" на стр. 325).

В этом разделе

Настройка уведомлений о событиях в работе приложения

Доступно только при наличии права **Изменять параметры**.

► *Чтобы настроить отправку уведомлений о событиях в работе приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Мониторинг → Уведомления приложения**.
2. Включите или отключите отправку уведомлений о событиях в работе приложения с помощью переключателя **Отправлять уведомления**.
3. Если на предыдущем шаге вы включили отправку уведомлений, в блоке параметров **Параметры уведомлений** нажмите на кнопку **Добавить**.
4. В появившемся поле **Адреса** введите адрес электронной почты и нажмите клавишу **ENTER**.

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.

5. В раскрывающемся списке **Язык** выберите, на каком языке будет отображаться текст уведомления.
6. Если требуется, повторите шаги 5-6, чтобы добавить адресатов уведомлений на другом языке.
7. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о событиях в работе приложения будет настроена.

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от приложения" на стр. 328), который указывается в качестве отправителя уведомлений о событиях в работе приложения.

Настройка уведомлений о срабатывании правил обработки сообщений

Доступно только при наличии права **Изменять параметры**.

Убедитесь, что отправка уведомлений включена в правиле (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 123), о срабатывании которого вы хотите получать уведомления.

► *Чтобы настроить отправку уведомлений о срабатывании правил обработки сообщений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Перейдите по ссылке **Уведомления об обнаружениях**.

   Откроется окно **Уведомления об обнаружениях**.
3. Включите или отключите отправку уведомлений о событиях в работе приложения с помощью переключателя **Отправлять уведомления об обнаружениях**.
4. Если на предыдущем шаге вы включили отправку уведомлений, в поле **Общий список получателей** введите адрес электронной почты и нажмите клавишу **ENTER**.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.

   Вы можете использовать символы "*" и "?" для создания масок адресов.
5. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о срабатывании правил обработки сообщений будет настроена. Приложение будет отправлять уведомления на указанные адреса в зависимости от параметров, заданных в сработавшем правиле:

- адресатам из общего списка, если в правиле установлен флажок **Уведомить получателей из общего списка**;
- отправителю сообщения, если в правиле установлен флажок **Уведомить отправителя**;
- получателям сообщения, если в правиле установлен флажок **Уведомить получателя**;
- на дополнительные адреса, если в правиле установлен флажок **Дополнительные адреса**.

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от приложения" на стр. 328), который указывается в качестве отправителя уведомлений о срабатывании правил обработки сообщений.

Настройка шаблонов уведомлений

Изменение шаблонов доступно для уведомлений о срабатывании правила. Вы не можете изменить текст уведомлений приложения.

Вы можете настроить разные шаблоны уведомлений для адресатов из общего списка, отправителя сообщения, получателей сообщения и адресатов из списка дополнительных адресов, заданных в правиле.

По умолчанию тексты шаблонов написаны на английском языке. Автоматическое переключение языков для шаблонов недоступно. Если требуется, вы можете переписать текст на нужном языке. Если вам нужно отправлять уведомления на разных языках в рамках одной группы получателей, вы можете написать один и тот же текст на нескольких языках и расположить их друг за другом в одном шаблоне.

► *Чтобы настроить шаблоны уведомлений:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. Перейдите по ссылке **Уведомления об обнаружениях**.

   Откроется окно **Уведомления об обнаружениях**.
3. По ссылке **Изменить шаблон** напротив нужного получателя откройте окно изменения шаблона.
4. Если требуется, в поле **Тема** измените тему уведомления.
5. Если требуется, в текстовой области **Тело сообщения** измените текст уведомления.

   Вы можете использовать макросы в теме и тексте сообщения. Для этого нажмите на кнопку **Добавить макрос** и выберите нужный макрос из раскрывающегося списка.

   > Значения макросов автоматически подставляются на английском языке. Переключение языков для макросов недоступно.
6. Нажмите на кнопку **Сохранить**.
7. Повторите шаги 3-6 для каждого шаблона.

Шаблоны уведомлений будут настроены.

kaspersky

Использование макросов в шаблонах уведомлений

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 срабатывании правила можно использовать следующие макросы (см. таблицу ниже).

Таблица 25. Макросы для шаблонов уведомлений

Макрос	Описание
%NODE_IP%	IP-адрес узла кластера, на котором было обработано сообщение.
%NODE_PORT%	Порт подключения к узлу кластера, на котором было обработано сообщение.
%PRODUCT_NAME%	Название приложения – Kaspersky Security для Linux Mail Server.
%SMTP_MESSAGE_ID%	Заголовок сообщения `Message-Id`.
%SENDER%	Адрес отправителя сообщения.
%SENDER_IP%	IP-адрес отправителя сообщения.
%ALL_RECIPIENTS%	Адреса всех получателей исходного сообщения.
%AFFECTED_RECIPIENTS%	Адреса получателей исходного сообщения, имеющие отношение к событию, описанному в уведомлении.
%AFFECTED_RULES%	Список идентификаторов сработавших правил.
%MESSAGE_ID%	Идентификатор, присвоенный сообщению приложением Kaspersky Security для Linux Mail Server.
%SUBJECT%	Тема исходного сообщения.
%DATE%	Дата получения сообщения.
%MESSAGE_ACTION%	Действие приложения над сообщением. Возможные значения: • `Skipped`. • `Disinfected`. • `AttachmentDeleted`. • `Deleted`. • `Rejected`. Если сообщение помещено в Хранилище, то через запятую после действия указывается `backed up`.

Макрос	Описание
%DATA_BEGIN%	Служебный макрос для обозначения начала списка вложений.
%DATA_END%	Служебный макрос для обозначения конца списка вложений.
%OBJECT_NAME%	Имя обнаруженного объекта. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляется имя вложения сообщения; • вне макросов %DATA_BEGIN% и %DATA_END% подставляется значение `Message`. В теме уведомления на место макроса всегда подставляется значение `Message`.
%OBJECT_SIZE%	Размер сообщения целиком или отдельных его вложений. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляется размер вложения сообщения; • вне макросов %DATA_BEGIN% и %DATA_END% подставляется размер сообщения целиком. В теме уведомления на место макроса всегда подставляется размер сообщения целиком.
%STATUS%	Результат проверки сообщения или вложения. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляются статусы проверки вложений модулями Антивирус и Контентная фильтрация; • вне макросов %DATA_BEGIN% и %DATA_END% подставляются статусы, присвоенные по результатам проверки сообщению целиком (если для этих статусов включена отправка уведомлений в правиле). В теме уведомления на место макроса всегда подставляются статусы, присвоенные по результатам проверки сообщению целиком (если для этих статусов включена отправка уведомлений в правиле). Если статусов несколько, они перечисляются через запятую.
%OBJECT_ACTION%	Действие приложения над сообщением или вложением. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляются действия над вложениями, выполненные модулями Антивирус или Контентная фильтрация (`Blocked`, `Not blocked`, `Disinfected`), или действие над сообщением целиком, выполненное модулем Анти-Фишинг. • вне макросов %DATA_BEGIN% и %DATA_END% подставляется действие, выполненное над сообщением целиком. В теме уведомления на место макроса всегда подставляется действие, выполненное над сообщением целиком.

kaspersky

Добавление в уведомление уникального идентификатора сообщения

Если пользователь получил уведомление об отклоненном сообщении, он может обратиться к администратору за более подробной информацией. В этом случае потребуется найти исходное письмо в Хранилище. Чтобы оптимизировать поиск, вы можете добавить уникальный идентификатор сообщения (далее также "ID сообщения") в шаблон уведомления.

► *Чтобы добавить ID сообщения в текст уведомления:*

1. В окне веб-интерфейса приложения выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить уведомления о событиях проверки.

   Откроется окно **Просмотреть правило**.
3. В левой панели выберите раздел **Уведомления**.
4. Убедитесь, что флажки напротив нужных получателей уведомлений установлены. При необходимости внесите изменения и нажмите на кнопку **Сохранить**.
5. Перейдите по ссылке **Настроить шаблоны уведомлений** в правом верхнем углу окна.

   Откроется окно **Уведомления об обнаружениях**.
6. По ссылке **Изменить шаблон** напротив нужного получателя откройте окно настройки шаблона уведомления.
7. Добавьте в шаблон следующую строку:

   ```
   Message ID: %SMTP_MESSAGE_ID%
   ```
8. Нажмите на кнопку **Сохранить**.

Макрос для ID сообщения будет добавлен в шаблон уведомления. В тексте последующих уведомлений будет указан уникальный идентификатор сообщения.

Настройка адреса сообщений от приложения

Вы можете указать адрес электронной почты, который будет указан в качестве отправителя следующих сообщений от приложения:

- уведомлений о срабатывании правил (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 324);
- уведомлений о событиях в работе приложения (см. раздел "Настройка уведомлений о событиях в работе приложения" на стр. 323);
- сообщений из Хранилища, отправленных в виде вложения (см. раздел "Отправка сообщений из Хранилища" на стр. 190);
- дайджеста Хранилища (см. раздел "Дайджест Хранилища" на стр. 198);
- отчетов (см. стр. 226);
- уведомлений о недоставке сообщений в случае применения приложением действия **Отклонить**.

► *Чтобы настроить адрес сообщений от приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Мониторинг** → **Обратный адрес**.
2. В поле **Обратный адрес** укажите адрес, который будет отображаться в поле *От кого* в сообщениях от приложения.

   Можно указать только один адрес.

   По умолчанию установлено значение `klms@<FQDN Управляющего узла кластера>`.
3. Нажмите на кнопку **Сохранить**.

Адрес сообщений от приложения будет настроен.

kaspersky

Аутентификация с помощью технологии единого входа

При включении технологии единого входа пользователям не требуется вводить данные учетной записи приложения для подключения к веб-интерфейсу. Аутентификация осуществляется с помощью доменной учетной записи пользователя.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является более надежным. При NTLM-аутентификации злоумышленники могут получить доступ к хешам паролей пользователей, перехватив сетевой трафик.

В этом разделе

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих узлов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого узла кластера, для которого вы хотите настроить Kerberos-аутентификацию.

Keytab-файл создается на сервере контроллера домена или на компьютере под управлением Windows Server, входящем в домен, под учетной записью с правами доменного администратора.

► *Чтобы создать keytab-файл, используя одну учетную запись:*

1. В оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).
2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

   В созданный keytab-файл будет добавлено SPN Управляющего узла. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`
4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

► *Чтобы создать keytab-файл, используя отдельную учетную запись для каждого узла:*

1. В оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого узла кластера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).
2. Чтобы использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <путь к файлу>\<имя файла>.keytab
   ```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS в зонах обратного просмотра присутствует PTR-запись для полного доменного имени (FQDN) и URL (если URL отличается от FQDN) каждого узла кластера.

► *Чтобы настроить Kerberos-аутентификацию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Доступ к приложению** → **Единый вход (SSO)**.
2. Выберите закладку **Kerberos**.
3. Переведите переключатель **Использовать Kerberos** в положение **Включено**.
4. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 330).

   Функциональность доступна только при наличии права **Изменять параметры**.

   Keytab-файл должен содержать SPN Управляющего узла и Подчиненных узлов.

   Откроется окно выбора файла.
5. Выберите keytab-файл и нажмите на кнопку **Open**.
6. Нажмите на кнопку **Сохранить**.

   Если в keytab-файле не найдено SPN Управляющего узла или SPN какого-либо из Подчиненных узлов, то для этого узла в разделе **Узлы** отображается статус *Отсутствует SPN-идентификатор для службы единого входа Kerberos*. Если в keytab-файле не найдено SPN ни одного из узлов, кнопка **Сохранить** недоступна.

Kerberos-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу приложения с помощью технологии единого входа. Доступ к функциональности приложения будет определяться правами учетной записи приложения.

При отключении Kerberos-аутентификации ранее загруженный keytab-файл удаляется.

Настройка NTLM-аутентификации

Рекомендуется использовать Kerberos-аутентификацию (см. раздел "Настройка Kerberos-аутентификации" на стр. 333), так как данный механизм является самым надежным. При NTLM-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

► *Чтобы настроить NTLM-аутентификацию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Доступ к приложению** → **Единый вход (SSO)**.
2. Выберите закладку **NTLM**.
3. Переведите переключатель **Использовать NTLM** в положение **Включено**.

4. В поле **IP-адрес/доменное имя контроллера домена** укажите IP-адрес или доменное имя доменного контроллера, с помощью которого будет осуществляться аутентификация.

   Вы можете указать два доменных контроллера. Для добавления второго контроллера необходимо нажать на кнопку .

5. В поле **Порт** укажите порт для подключения к доменному контроллеру.

   По умолчанию используется порт 445.

6. Нажмите на кнопку **Сохранить**.

NTLM-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу приложения с помощью технологии единого входа. Доступ к функциональности приложения будет определяться правами учетной записи приложения.

При подключении с компьютеров, не входящих в домен, пользователю потребуется указать данные своей доменной учетной записи.

Дополнительная настройка в операционной системе и браузере

Данная инструкция применима к компьютерам с операционной системой Windows®.

В зависимости от используемого протокола аутентификации и типа браузера для корректной авторизации пользователей с компьютеров, входящих в домен Active Directory, для которого настроена аутентификация SSO, может потребоваться дополнительная настройка. Авторизация с компьютеров, не входящих в домен Active Directory, для которого настроена аутентификация SSO, не требует дополнительной настройки и осуществляется согласно алгоритму используемого протокола аутентификации (см. раздел "Подключение к веб-интерфейсу приложения" на стр. 89).

Kerberos-аутентификация

Для корректной работы Kerberos-аутентификации независимо от типа используемого браузера требуется выполнить предварительную настройку в операционной системе:

- Настроить синхронизацию времени на серверах контроллеров домена Active Directory, на узлах кластера Kaspersky Security для Linux Mail Server, а также на компьютере, с которого осуществляется подключение к веб-интерфейсу.
- Добавить A- и PTR-записи на DNS-сервере для узлов кластера Kaspersky Security для Linux Mail Server и убедиться, что они корректно распознаются на узлах кластера и на компьютере, с которого осуществляется подключение к веб-интерфейсу.

Подробнее о настройке этих параметров *см. сопроводительную документацию к операционной системе*.

► *Чтобы выполнить дополнительную настройку в браузерах Google Chrome и Microsoft Edge:*

1. На компьютере, с которого осуществляется подключение к веб-интерфейсу, в панели управления выберите раздел **Internet options**.
2. На закладке **Security** выберите зону **Local intranet** и нажмите на кнопку **Sites**.

   Откроется окно **Local intranet**.

3. Нажмите на кнопку **Advanced**.
4. В открывшемся окне в поле ввода укажите полный URL-адрес узла кластера в формате FQDN и нажмите на кнопку **Add**. Повторите это действие для каждого узла кластера.

   Вы также можете ввести имя домена, чтобы добавить сразу все входящие в него адреса (например, `.example.com`).
5. Убедитесь, что адреса добавлены, и нажмите на кнопку **Close**.
6. Закройте все открытые ранее окна с помощью кнопок **OK**.

Дополнительная настройка будет выполнена. Пользователь, в профиле которого была выполнена настройка, сможет подключаться к веб-интерфейсу приложения с этого компьютера с помощью браузеров Google Chrome и Microsoft Edge, не вводя свои учетные данные.

► *Чтобы выполнить дополнительную настройку в браузере Mozilla Firefox:*

1. В адресной строке браузера введите `about:config` и на открывшейся странице нажмите на кнопку **Accept the Risk and Continue**.
2. В строке поиска параметров введите `negotiate`.
3. В открывшемся списке параметров в полях **network.negotiate-auth.delegation-uris** и **network.negotiate-auth.trusted-uris** введите полные URL-адреса всех узлов кластера в формате FQDN через запятую.

   Нажмите на значок  справа от поля, чтобы сохранить введенные адреса.

   Вы также можете ввести имя домена, чтобы добавить сразу все входящие в него адреса (например, `.example.com`).

Дополнительная настройка будет выполнена. Пользователь, в профиле которого была выполнена настройка, сможет подключаться к веб-интерфейсу приложения с этого компьютера с помощью браузера Mozilla Firefox, не вводя свои учетные данные.

NTLM-аутентификация

Для корректной работы NTLM-аутентификации в браузерах Google Chrome и Microsoft Edge дополнительная настройка не требуется.

► *Чтобы выполнить дополнительную настройку в браузере Mozilla Firefox:*

1. В адресной строке браузера введите `about:config` и на открывшейся странице нажмите на кнопку **Accept the Risk and Continue**.
2. В строке поиска параметров введите `ntlm`.
3. В открывшемся списке параметров в поле **network.automatic-ntlm-auth.trusted-uris** введите полные URL-адреса всех узлов кластера через запятую в формате FQDN или IP-адреса.

   Нажмите на значок  справа от поля, чтобы сохранить введенные адреса.

   Вы также можете ввести имя домена, чтобы добавить сразу все входящие в него адреса (например, `.example.com`).

При подключении к веб-интерфейсу нужно будет вводить адрес узла в том же формате, в котором он указан в этом поле.

Дополнительная настройка будет выполнена. Пользователь, в профиле которого была выполнена настройка, сможет подключаться к веб-интерфейсу приложения с этого компьютера с помощью браузера Mozilla Firefox, не вводя свои учетные данные.

kaspersky

Установка приложения на один сервер с Kaspersky Endpoint Security for Linux

Вы можете установить Kaspersky Security для Linux Mail Server на одном сервере с приложением Kaspersky Endpoint Security для Linux версии 11.3 и выше.

Если вы используете Kaspersky Security Center для централизованного управления приложением Kaspersky Endpoint Security для Linux, для настройки параметров приложения Kaspersky Endpoint Security для Linux вам нужно изменить параметры групповой политики. При отсутствии централизованного управления вы можете настроить параметры приложения локально на каждом сервере с помощью командной строки.

► *Чтобы установить и настроить Kaspersky Security для Linux Mail Server и Kaspersky Endpoint Security for Linux для использования на одном сервере:*

1. Если операционная система работает в режиме замкнутой программной среды, добавьте соответствующие ключи (см. раздел "Подготовка к установке в Astra Linux Special Edition в режиме замкнутой программной среды" на стр. 62) для обоих приложений.
2. Если используется централизованное управление через Kaspersky Security Center, установите Агент администрирования.
3. Установите приложение Kaspersky Endpoint Security for Linux, выполните его первоначальную настройку, активируйте и настройте необходимые компоненты защиты.

   Информацию об установке и настройке Kaspersky Endpoint Security for Linux см. в *справке Kaspersky Endpoint Security for Linux*.
4. В параметрах компонента защиты от файловых угроз Kaspersky Endpoint Security for Linux добавьте в исключения следующие директории:
   - /var/spool/exim4 – очередь сообщений почтового сервера.
   - /var/opt/kaspersky/klms – база данных, журналы событий, Хранилище сообщений приложения Kaspersky Security для Linux Mail Server.
   - /tmp/klmstmp и /tmp/klms_filter – временные рабочие директории приложения <PRODUC_NAME_GEN>.

   Подробнее см. раздел Настройка исключений для компонента файловой защиты Kaspersky Endpoint Security для Linux (на стр. 339).
5. Если вы включили компонент управления сетевым экраном Kaspersky Endpoint Security for Linux, разрешите входящие соединения на следующие TCP-порты:
   - 25 – порт для входящих соединений по протоколу SMTP для приема почтовых сообщений.
   - 443 – значение по умолчанию для порта веб-интерфейса управления узлом кластера приложения Kaspersky Security для Linux Mail Server.

     Номер порта может быть другим, значение указывается при первоначальной настройке Kaspersky Security для Linux Mail Server (см. раздел "Шаг 5. Ввод параметров узла" на стр. 66).

- 9045 – порт для взаимодействия между узлами кластера приложения Kaspersky Security для Linux Mail Server.

Подробнее см. раздел Настройка сетевого экрана Kaspersky Endpoint Security для Linux (на стр. 341).

6. Если вы используете компоненты защиты от сетевых угроз или защиты от веб-угроз Kaspersky Endpoint Security for Linux, временно отключите их (см. раздел "Отключение компонентов защиты от сетевых и веб-угроз в Kaspersky Endpoint Security for Linux" на стр. 343).
7. Установите (см. стр. 59) приложение Kaspersky Security для Linux Mail Server, выполните его первоначальную настройку (см. раздел "Подготовка приложения к работе" на стр. 64).
8. Включите компоненты защиты от сетевых угроз и защиты от веб-угроз Kaspersky Endpoint Security for Linux (см. раздел "Включение компонентов защиты от сетевых и веб-угроз в Kaspersky Endpoint Security for Linux" на стр. 343).

В этом разделе

Настройка исключений для компонента файловой защиты Kaspersky Endpoint Security для Linux

► *Чтобы настроить исключения для компонента файловой защиты через Kaspersky Security Center:*

1. Откройте групповую политику на редактирование.
2. Перейдите на вкладку **Базовая защита** → **Области исключения**.
3. В списке исключений нажмите на кнопку **Добавить** и укажите параметры новой области исключения:
   - **Название**: `exim-spool`
   - **Файловая система**: `Локальная`
   - **Путь**: `/var/spool/exim4`

   Для завершения добавления новой области исключения нажмите на кнопку **ОК**.
4. В списке исключений нажмите на кнопку **Добавить** и укажите параметры новой области исключения:
   - **Название**: `klms-var`
   - **Файловая система**: `Локальная`
   - **Путь**: `/var/opt/kaspersky/klms`

   Для завершения добавления новой области исключения нажмите на кнопку **ОК**.

5. В списке исключений нажмите на кнопку **Добавить** и укажите параметры для новой области исключения:
   - **Название**: `klms-tmp`
   - **Файловая система**: `Локальная`
   - **Путь**: `/tmp/klmstmp`

   Для завершения добавления новой области исключения нажмите на кнопку **ОК**.
6. В списке исключений нажмите кнопку **Добавить** и укажите параметры для новой области исключения:
   - **Название**: `klms-filter`
   - **Файловая система**: `Локальная`
   - **Путь**: `/tmp/klms_filter`

   Для завершения добавления новой области исключения нажмите на кнопку **ОК**.
7. Сохраните список исключений.
8. Сохраните изменения групповой политики.

► *Чтобы настроить исключения для компонента файловой защиты с помощью командной строки:*

1. Сохраните параметры задачи **Защита от файловых угроз** в конфигурационный файл с помощью следующей команды:

   ```
   kesl-control --get-settings 1 --file <полный путь к файлу>
   ```
2. Откройте созданный конфигурационный файл на редактирование.
3. Добавьте в созданный файл следующие строки:

   ```
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/var/spool/exim4
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/var/opt/kaspersky/klms
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/tmp/klmstmp
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/tmp/klms_filter
   ```

   `<номер элемента>` – порядковый номер секции ExcludedFromScanScope, нумерация начинается с нуля.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры из конфигурационного файла в задачу **Защита от файловых угроз** с помощью команды:

   ```
   kesl-control --set-settings 1 --file <полный путь к файлу>
   ```

kaspersky

Настройка сетевого экрана Kaspersky Endpoint Security для Linux

► *Чтобы настроить сетевой экран через Kaspersky Security Center:*

1. Откройте групповую политику на редактирование.
2. Перейдите на вкладку **Базовая защита** → **Управление сетевым экраном**.
3. В разделе **Сетевые пакетные правила** нажмите на кнопку **Настроить**.
4. В списке сетевых пакетных правил нажмите на кнопку **Добавить** и укажите параметры нового правила:
   - **Протокол**: `TCP`
   - **Направление**: `Входящие`
   - **Удаленные порты**: `Любой`
   - **Локальные порты**: `25`
   - **Удаленные адреса**: `Любой адрес`
   - **Локальные адреса**: `Любой адрес`
   - **Действие**: `Разрешать`
   - **Запись в отчет**: `Не записывать`
   - **Название правила**: `TCP:25`

   Завершите создание нового правила.
5. В списке сетевых пакетных правил нажмите на кнопку **Добавить** и укажите параметры нового правила:
   - **Протокол**: `TCP`
   - **Направление**: `Входящие`
   - **Удаленные порты**: `Любой`
   - **Локальные порты**: `443`
   - **Удаленные адреса**: `Любой адрес`
   - **Локальные адреса**: `Любой адрес`
   - **Действие**: `Разрешать`
   - **Запись в отчет**: `Не записывать`
   - **Название правила**: `TCP:443`

   > Номер локального порта может быть другим, значение указывается при первоначальной настройке Kaspersky Security для Linux Mail Server (см. раздел "Шаг 5. Ввод параметров узла" на стр. 66).

   Завершите создание нового правила.

6. В списке сетевых пакетных правил нажмите на кнопку **Добавить** и укажите параметры нового правила:
   - **Протокол**: TCP
   - **Направление**: Входящие
   - **Удаленные порты**: Любой
   - **Локальные порты**: 9045
   - **Удаленный адреса**: Любой адрес
   - **Локальные адреса**: Любой адрес
   - **Действие**: Разрешать
   - **Запись в отчет**: Не записывать
   - **Название правила**: TCP:9045

   Завершите создание нового правила.
7. Сохраните изменения в списке правил.
8. Сохраните изменения групповой политики.

► *Чтобы настроить сетевой экран с помощью командной строки:*

1. Сохраните параметры задачи **Управление сетевым экраном** в конфигурационный файл с помощью следующей команды:

   ```
   kesl-control --get-settings 12 --file <полный путь к файлу>
   ```
2. Откройте созданный конфигурационный файл на редактирование.
3. Добавьте в созданный файл следующие строки:

   ```
   [PacketRules.item_<номер элемента>]
   FirewallAction=Allow
   Direction=Incoming
   Protocol=TCP
   LocalPorts=25
   [PacketRules.item_<номер элемента>]
   FirewallAction=Allow
   Direction=Incoming
   Protocol=TCP
   LocalPorts=443
   [PacketRules.item_<номер элемента>]
   FirewallAction=Allow
   Direction=Incoming Protocol=TCP
   LocalPorts=9045
   ```

`<номер элемента>` – порядковый номер секции PacketRules, нумерация начинается с нуля.

4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры из конфигурационного файла в задачу **Управление сетевым экраном** с помощью команды:

   ```
   kesl-control --set-settings 12 --file <полный путь к файлу>
   ```

Отключение компонентов защиты от сетевых и веб-угроз в Kaspersky Endpoint Security for Linux

Отключение компонентов защиты требуется на время выполнения установки и первоначальной настройки приложения Kaspersky Security для Linux Mail Server.

► *Чтобы отключить компоненты защиты от сетевых угроз и защиты от веб-угроз через Kaspersky Security Center:*

1. Откройте групповую политику на редактирование.
2. Перейдите на вкладку **Базовая защита** → **Защита от веб-угроз**.
3. Снимите флажок **Включить защиту от веб-угроз**.
4. Перейдите на вкладку **Базовая защита** → **Защита от сетевых угроз**.
5. Снимите флажок **Включить защиту от сетевых угроз**.
6. Сохраните изменения групповой политики.

► *Чтобы временно отключить компоненты защиты от сетевых угроз и защиты от веб-угроз с помощью командной строки, выполните следующие команды:*

```
kesl-control --stop-task Network_Threat_Protection
kesl-control --stop-task Web_Threat_Protection
```

Включение компонентов защиты от сетевых и веб-угроз в Kaspersky Endpoint Security for Linux

► *Чтобы включить компоненты защиты от сетевых угроз и защиты от веб-угроз через Kaspersky Security Center:*

1. Откройте групповую политику на редактирование.
2. Перейдите на вкладку **Базовая защита** → **Защита от веб-угроз**.
3. Установите флажок **Включить защиту от веб-угроз**.
4. Перейдите на вкладку **Базовая защита** → **Защита от сетевых угроз**.
5. Установите флажок **Включить защиту от сетевых угроз**.
6. Сохраните изменения групповой политики.

► *Чтобы включить компоненты защиты от сетевых угроз и защиты от веб-угроз с помощью командной строки, выполните следующие команды:*

```
kesl-control --start-task Network_Threat_Protection
kesl-control --start-task Web_Threat_Protection
```

kaspersky

Публикация событий приложения в SIEM-систему

Kaspersky Security для Linux Mail Server может публиковать события, происходящие во время работы приложения, в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Информация о каждом событии приложения передается как отдельное syslog-сообщение формата CEF (см. раздел "Содержание и свойства syslog-сообщений в формате CEF" на стр. 348) (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 приложении отключен. Вы можете настроить публикацию событий в SIEM-систему (см. раздел "Настройка публикации событий приложения в SIEM-систему" на стр. 345) и включить экспорт событий (см. раздел "Настройка экспорта событий в формате CEF" на стр. 347).

В этом разделе

Настройка публикации событий приложения в SIEM-систему

Вы можете настроить публикацию событий в формате CEF во внешнюю SIEM-систему, а также сохранять их локально в файлы журналов на сервере. Если сохранять события локально не требуется, пропустите шаги 3, 5, 6 инструкции этого раздела.

Выполните шаги по настройке публикации событий на каждом узле кластера, события с которого вы хотите публиковать в SIEM-систему. Только после настройки публикации событий следует включать экспорт событий в формате CEF (см. раздел "Настройка экспорта событий в формате CEF" на стр. 347).

► *Чтобы настроить публикацию событий приложения в SIEM-систему:*

1. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Создайте файл /etc/rsyslog.d/klms-cef-messages.conf и добавьте в него следующие строки:

```
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
```

```
$ActionResumeRetryCount -1
<категория (facility)>.* @@<IP-адрес SIEM-системы>:<порт, на котором SIEM-система принимает сообщения от Syslog по протоколу TCP>
```

3. Если вы хотите сохранять события локально, добавьте в тот же файл строку:

```
<категория (facility) для формата CEF>.* -/var/log/klms-cef-messages
```

4. В конец файла добавьте строку:

```
<категория (facility) для формата CEF>.* stop
```

Пример файла:

```
# Publish CEF messages to the SIEM system
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local2.* @@10.16.32.64:514

# Also store CEF messages locally
local2.* -/var/log/klms-cef-messages

# Prevent logging to the system log files
local2.* stop
```

5. Если вы хотите сохранять события локально, создайте файл журнала /var/log/klms-cef-messages и настройте права доступа к нему. Для этого выполните команды:

```
touch /var/log/klms-cef-messages
chown root:klusers /var/log/klms-cef-messages
chmod 640 /var/log/klms-cef-messages
```

6. При необходимости настройте правила ротации файлов журналов с экспортированными событиями. Для этого создайте файл /etc/logrotate.d/klms-cef-messages и добавьте в него следующие строки:

```
/var/log/klms-cef-messages
{
  size 500M
  rotate 10
  compress
  missingok
```

```
    notifempty
    sharedscripts
    postrotate
    /usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1 ||
true
    endscript
}
```

7. Перезапустите службу rsyslog. Для этого выполните команду:

   ```
   service rsyslog restart
   ```

Публикация событий приложения в SIEM-систему будет настроена.

Настройка экспорта событий в формате CEF

Включать экспорт сообщений в формате CEF можно только после того, как была настроена служба системного журнала для локального сохранения CEF-сообщений или их публикации в SIEM-систему (см. раздел "Настройка публикации событий приложения в SIEM-систему" на стр. 345).

► *Чтобы настроить экспорт событий в формате CEF:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Журналы и события** → **Syslog**.
2. На вкладке **Формат CEF** включите переключатель **Включить логирование событий в формате CEF**.
3. Если вы хотите выбрать категорию (facility) для syslog, в которую будут экспортироваться события, в раскрывающемся списке **Категория Syslog (facility)** выберите одно из следующих значений:
   - **Auth**.
   - **Authpriv**.
   - **Cron**.
   - **Daemon**.
   - **Ftp**.
   - **Lpr**.
   - **Mail**.
   - **News**.
   - **Syslog**.
   - **User**.
   - **Uucp**.
   - **Local0**.

- **Local1**.
- **Local2**.
- **Local3**.
- **Local4**.
- **Local5**.
- **Local6**.
- **Local7**.

> Рекомендуется указать такую категорию для syslog, которая не используется другими программами на сервере.

По умолчанию установлено значение **Local2**.

4. В поле **Уровень событий** установите уровень детализации экспорта:
   - **Error** – экспорт событий, связанных с возникновением ошибок.
   - **Info** – экспорт всех событий.

Экспорт событий в формате CEF будет настроен.

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 каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название приложения (всегда имеет значение `KLMS`).

Поля syslog-сообщения о событии, определяемые параметрами приложения, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Ключи, а также их значения, содержащиеся в сообщении, зависят от класса события.

Пример:

```
July 16 10:34:23 host.domain.com

KLMS: CEF:0|AO Kaspersky Lab|Kaspersky Security для Linux Mail
Server|10.0.0.1234|LMS_EV_SETTINGS_CHANGED|task settings
changed|severity|cn1=taskId cn1Label=TaskId cs1=taskName csLabel=TaskName
act=created/changed/deleted
```

Максимальный размер syslog-сообщения об обнаруженном событии зависит от значений параметров syslog на сервере, на котором установлен Kaspersky Security для Linux Mail Server.

Классы событий группы Settings

В теле CEF-сообщений классов событий группы Settings допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 26. Допустимые значения полей классов событий группы Settings

Ключ	Значение
cn1	Номер задачи.
cn1Label	Всегда имеет значение `TaskId`.
cs1	Имя задачи.
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 27. 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

Классы событий группы Tasks

В теле CEF-сообщений классов событий группы Tasks допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 28. Допустимые значения полей классов событий группы Tasks

Ключ	Значение
deviceProcessName	Имя задачи.

Ключ	Значение
cs1	Режим работы приложения (`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 29. Релевантные ключи для классов событий группы Tasks

Класс событий	Релевантные ключи
LMS_EV_PROCESS_CRASHED	deviceProcessName
LMS_EV_RESTARTED	deviceProcessName
LMS_EV_PRODUCT_STARTED	cs1, cs1Label

Классы событий группы Backup

В теле CEF-сообщений классов событий группы Backup допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 30. 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.
KLMSMessageSubject	Тема письма
cs2	Статус антивирусной проверки.
cs2Label	Всегда имеет значение `AvStatus`.
cs3	Статус проверки ссылок.
cs3Label	Всегда имеет значение `MlfStatus`.
cs4	Статус проверки на спам.
cs4Label	Всегда имеет значение `AsStatus`.
cs5	Статус проверки на фишинг.
cs5Label	Всегда имеет значение `ApStatus`.
cs6	Имя вредоносного объекта.
cs6Label	Всегда имеет значение `Threat`.
cs7	Статус контентной фильтрации.
cs7Label	Всегда имеет значение `CfStatus`.
duser	Список получателей сообщения.
reason	Описание ошибки.

Ключ	Значение
outcome	Результат события дайджеста Хранилища: `No messages`, `Success`, `Failed`.

В каждом классе событий группы Backup допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 31. 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_MESSAGE_RESTORE	cs1, cs1Label, act, suser, cs2, cs2Label, cs3, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, cs7, cs7Label, duser, KLMSMessageSubject

Классы событий группы Backup digest

В теле CEF-сообщений классов событий группы Backup digest допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 32. Допустимые значения полей для классов событий группы Backup digest

Ключ	Значение
cnt	Количество пользователей.
outcome	Результат. Допустимые значения: `Success, Fail`.

В каждом классе событий группы Backup digest допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 33. Релевантные ключи для классов событий группы Backup digest

Класс событий	Релевантные ключи
LMS_EV_BACKUPDIGEST	cnt, outcome

Классы событий группы License

В теле CEF-сообщений классов событий группы License допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 34. Допустимые значения полей классов событий группы License

Ключ	Значение
cs1	Серийный номер лицензионного ключа.
cs1Label	Всегда имеет значение `LicenseID`.
cs2	Режим работы Kaspersky Security для Linux Mail Server в соответствии с лицензией.
cs2Label	Всегда имеет значение `FunctionalityLevel`.
cs3	Тип лицензии.
cs3Label	Всегда имеет значение `KeyType`.
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 35. 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

Классы событий группы Rules

В каждом классе событий группы Rules допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 36. Релевантные ключи для классов событий группы Rules

Класс событий	Релевантные ключи
LMS_EV_ALL_RULES_IMPORTED	Нет значения

Классы событий группы Quarantine

В теле CEF-сообщений классов событий группы Quarantine допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 37. 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.
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`).
KLMSMessageSubject	Тема письма

В каждом классе событий группы Quarantine допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 38. Релевантные ключи для классов событий группы Quarantine

Класс событий	Релевантные ключи
LMS_EV_ASP_QUARANTINE	cs1, cs1Label, src, suser, cs3, cs3Label, act, KLMSMessageSubject
LMS_EV_KATA_QUARANTINE	cs1, cs1Label, cs2, cs2Label, suser, duser, act, cs3, cs3Label, KLMSMessageSubject

Классы событий группы Update

В теле CEF-сообщений классов событий группы Update допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 39. Допустимые значения полей классов событий группы Update

Ключ	Значение
reason	Причина возникновения события.
cn1	Количество дней.
cn1Label	Всегда имеет значение `Days`.
cn2	Количество часов.

Ключ	Значение
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 40. Релевантные ключи для классов событий группы Update

Класс событий	Релевантные ключи
LMS_EV_ANTIVIRUS_BASES_UPDATED	Нет значения
LMS_EV_ANTISPAM_BASES_UPDATED	Нет значения
LMS_EV_ANTIPHISHING_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_UPDATE_ERROR	reason
LMS_EV_ANTISPAM_BASES_UPDATE_ERROR	reason
LMS_EV_ANTIPHISHING_BASES_UPDATE_ERROR	reason

kaspersky

Классы событий группы ScanLogic

В теле CEF-сообщений классов событий группы ScanLogic допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 41. 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.
	cs2Label	Всегда имеет значение `Rules`.
	outcome	Статус проверки.
	cs3	Список получателей сообщения с вредоносными объектами или другими объектами, которые могут быть использованы злоумышленниками (с действием Skip).
	cs3Label	Всегда имеет значение `UnsafeRecipients`.
	fname	Имя файла.
	KLMSMessageSubject	Тема письма
LMS_EV_SCAN_LOGIC_AS_STATUS LMS_EV_SCAN_LOGIC_AP_STATUS LMS_EV_SCAN_LOGIC_MLF_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`.

Класс событий	Ключ	Значение
LMS_EV_SCAN_LOGIC_KT_STATUS	suser	Отправитель сообщения.
	cs4	Причина пропуска сканирования.
	cs4Label	Всегда имеет значение `SkipReason`.
	cs5	Имя учетной записи пользователя, который извлек сообщение из KATA-карантина.
	cs5Label	Всегда имеет значение `Account`.
LMS_EV_SCAN_LOGIC_CF_STATUS	cs4	`DetectedFileFormat`; `DetectedFileName`; `DetectedFileSize`.
	cs4Label	Всегда имеет значение `DetectedEntity`.
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.
	cs5Label	Всегда имеет значение `DetectedFileName`.
	cs6	Формат заблокированного файла.
	cs6Label	Всегда имеет значение `DetectedFileFormat`.
	cn2	Размер заблокированного файла
	cn2Label	Всегда имеет значение `DetectedFileSize`

В каждом классе событий группы ScanLogic допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 42. 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, KLMSMessageSubject reason
LMS_EV_SCAN_LOGIC_AS_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, KLMSMessageSubject, cs2, cs2Label, cs4, cs4Label, reason, outcome
LMS_EV_SCAN_LOGIC_AV_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, KLMSMessageSubject, cs2, cs2Label, cs3, cs3Label, reason, outcome
LMS_EV_SCAN_LOGIC_MLF_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, KLMSMessageSubject, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, 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, cs4, cs4Label, cs5, cs5Label, reason, suser, outcome, KLMSMessageSubject
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, KLMSMessageSubject
LMS_EV_SCAN_LOGIC_CF_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, outcome, KLMSMessageSubject
LMS_EV_SCAN_LOGIC_PART_RESULT	cs1, cs1Label, cn1, cn1Label, fname, act, reason, cs2, cs2Label, cs3, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, cn2, cn2Label, outcome
LMS_EV_SCAN_LOGIC_MESSAGE_BACKUP	cs1, cs1Label, src, act, fsize, suser, duser, reason, cs2, cs2Label, KLMSMessageSubject

Если в событии LMS_EV_SCAN_LOGIC_PART_RESULT в поле mime part указан статус `avStatus=Infected` или `avStatus=Disinfected`, то в качестве значения ключа `cn1` указывается список `disinfectedObjects` или `deletedObjects` при наличии одного из них. Если оба списка непустые, то ключи `cn1` и `cn1Label` будут добавлены дважды.

kaspersky

Антивирусная проверка модулем kavscanner

В состав Kaspersky Security для Linux Mail Server входит модуль kavscanner, выполняющий антивирусную проверку файлов.

В этом разделе

kaspersky

Конфигурационный файл

В поставку Kaspersky Security для Linux Mail Server входит конфигурационный файл модуля kavscanner **kavscanner_defaults.conf**, содержащий параметры работы модуля kavscanner. Конфигурационный файл находится в директории `/etc/opt/kaspersky/klms/kavscanner_defaults.conf`.

В этом разделе

Секция [locale]

Секция [locale] содержит параметры, определяющие форматы даты и времени:

- **DateFormat=%d-%m-%y**. Формат представления даты согласно strftime.

  Вы можете изменить формат представления даты, например, на: **%y/%m/%d или %m/%d/%y**.

- **TimeFormat=%H:%M:%S**. Формат представления времени согласно strftime.

  Вы можете изменить формат представления времени на двенадцатичасовой (am, pm): **%I:%M:%S %P**.

Секция [scanner.options]

Секция [scanner.options] содержит параметры проверки файловых систем сервера:

- **SelfExtArchives=yes**. Режим проверки самораспаковывающихся архивов.

  Для отключения режима присвойте параметру значение **no**.

  Если включен режим проверки архивов (**Archives=yes**), самораспаковывающиеся архивы будут проверены, даже если параметру **SelfExtArchives** присвоено значение **no**.

- **ExcludeDirs=маска1:маска2:...:маскаN**. Маски каталогов, которые исключаются из проверки.

  По умолчанию проверяются все каталоги.

  Маски задаются в виде стандартных shell-масок.

- **MailBases=yes**. Режим проверки почтовых баз.

  Для отключения режима присвойте параметру значение **no**.

- **Archives=yes**. Режим проверки архивов.

  Для отключения режима присвойте параметру значение **no**.

- **Packed=yes**. Режим проверки запакованных файлов.

  Для отключения режима присвойте параметру значение **no**.

- **ExcludeMask=маска1:маска2:...:маскаN**. Маски файлов, которые исключаются из проверки.

  По умолчанию проверяются все файлы.

  Маски задаются в виде стандартных shell-масок.

- **MaxLoadAvg**. Максимальная загрузка процессора. В случае превышения данного значения компонент kavscanner прекращает работу.

- **LocalFS=false**. Режим проверки только локальной файловой системы.

  Для включения режима присвойте параметру значение **true**.

- **Cure=no**. Режим лечения инфицированных объектов.

  Для включения режима присвойте параметру значение **yes**.

- **MailPlain=yes**. Режим проверки почтовых сообщений в виде plain text.

  Для отключения режима присвойте параметру значение **no**.

- **Heuristic=yes**. Режим использования во время проверки эвристического анализатора кода.

  Для отключения режима присвойте параметру значение **no**.

- **Recursion=true**. Режим рекурсивного прохода каталогов при проверке на наличие вирусов.

  Для отключения режима присвойте параметру значение **false**.

- **FollowSymlinks**. Режим работы с символьными ссылками.

  Если параметру присвоено значение **true**, при проверке будут раскрываться ссылки, указывающие на директорию.

Секция [scanner.options.other]

Секция [scanner.options.other] содержит параметры проверки легальных программ, которые могут быть использованы злоумышленниками:

- **EnableOtherProgramsDetectiom=false**. Режим проверки легальных программ.

  Для включения режима присвойте параметру значение **true**.

- **OtherProgramsAreThreats=false**. Результат проверки легальных программ.

  По умолчанию легальные программы не признаются угрозами. Чтобы утилита классифицировала легальные программы как угрозы, присвойте параметру значение **true**.

Секция [scanner.report]

Секция [scanner.report] содержит параметры формирования отчета о результатах работы компонента kavscanner:

- **Append=true**. Режим добавления новых сообщений в файл отчета.

Для отключения режима присвойте параметру значение **false**.

- **ShowContainerResultOnly=false**. Режим отображения в отчете результатов проверки архива в кратком формате.

  Для отображения краткого отчета присвойте параметру значение **true**.

- **ShowOK=false**. Режим вывода в отчет сообщений о незараженных файлах.

  Для включения режима присвойте параметру значение **true**.

- **ReportLevel=4**. Уровень детализации отчета.

- **ShowObjectResultOnly=false**. Режим отображения в отчете результатов проверки простого объекта в кратком формате.

  Для отображения результатов проверки в кратком формате присвойте параметру значение **true**.

- **ReportFileName**. Имя файла отчета, в котором фиксируются результаты работы компонента.

  Если параметру задано значение **syslog**, информация будет записана в системный журнал под категорией daemon.

Секция [scanner.container]

Секция [scanner.container] включает параметры, определяющие действия над архивами при антивирусной защите файловых систем сервера:

- **OnCorrupted=действие**. Действия в случае обнаружения поврежденного контейнера.
- **OnInfected=действие**. Действия в случае обнаружения зараженного объекта в контейнере. Если включен режим лечения зараженных файлов, то данное действие применяется к контейнерам, вылечить которые не удалось, и выполняется после всех действий с объектами контейнера.
- **OnWarning=действие**. Действия в случае обнаружения внутри контейнера объекта, код которого сходен с кодом известного вируса.
- **OnCured=действие**. Действия в случае обнаружения внутри контейнера зараженного объекта, который был успешно вылечен.
- **OnProtected=действие**. Действия в случае обнаружения внутри контейнера объекта, зашифрованного паролем. Такие объекты проверить невозможно.
- **OnError=действие**. Действия в случае возникновения ошибки при проверке контейнера.

Секция [scanner.object]

Секция [scanner.object] содержит параметры, определяющие действия над простыми объектами того или иного типа при антивирусной защите файловых серверов:

- **OnCorrupted=действие**. Действия в случае обнаружения поврежденного файла.
- **OnInfected=действие**. Действия в случае обнаружения зараженного файла.

  Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, которые не удалось вылечить.

- **OnWarning=действие**. Действия в случае обнаружения файла, код которого сходен с кодом известного вируса.
- **OnCured=действие**. Действия в случае обнаружения и успешного лечения зараженного объекта.
- **OnProtected=действие**. Действия в случае обнаружения объекта, зашифрованного паролем. Такие объекты проверить невозможно.
- **OnError=действие**. Действия в случае возникновения ошибки при проверке объекта.

Секция [scanner.display]

Секция [scanner.display] содержит параметры вывода отчета на консоль управления:

- **ShowContainerResultOnly=false**. Режим отображения на консоли управления результатов проверки архива в кратком формате.

  Для отображения результатов проверки в кратком формате присвойте параметру значение **true**.
- **ShowObjectResultOnly=false**. Режим отображения на консоли управления результатов проверки простого объекта в кратком формате.

  Для отображения краткого отчета присвойте параметру значение **true**.
- **ShowOK=true**. Режим вывода на консоль управления сообщений о незараженных файлах.

  Для отключения режима присвойте параметру значение **false**.
- **ShowProgress=true**. Режим отражения на консоли управления текущей работы компонента (процесс загрузки антивирусных баз, информация о проверке текущего файла).

  Для отключения режима присвойте параметру значение **false**.

Секция [scanner.path]

Секция [scanner.path] содержит параметр, определяющий путь к файлам, без которых модуль kavscanner не будет функционировать:

BackupPath= путь. Полный путь к каталогу хранения резервных копий объектов, проверяемых компонентом.

kaspersky

Ключи командной строки

Параметры конфигурационного файла можно переопределить из командной строки при запуске программы с помощью ключей командной строки.

Опции помощи:

- **–h**. Вывести на консоль справочную информацию о компоненте kavscanner;
- **–v**. Показать версию программы.

Опции конфигурации:

- **–c (–C) <путь_к_файлу>**. Использовать альтернативный конфигурационный файл <путь_к_файлу>.
- **–f**. Игнорировать испорченную подпись компонента kavscanner и пытаться вылечить компонент.

Опции проверки:

- **–e <опция>**. Изменить опцию проверки, используемую по умолчанию. В качестве <опция> могут быть использованы следующие режимы:
  - **P/p**. Включить/выключить проверку упакованных файлов.
  - **A/a**. Включить/выключить проверку архивов.
  - **S/s**. Включить/выключить проверку самораспаковывающихся архивов.
  - **B/b**. Включить/выключить проверку почтовых баз.
  - **M/m**. Включить/выключить проверку сообщений в виде plain text.
  - **E/e**. Включить/выключить эвристический анализатор кода.
- **–R/r**. Включить/выключить рекурсивную проверку.
- **-S/s**. Включить/выключить режим раскрытия символьных ссылок.
- **–l**. Проверять только локальные файловые системы.

Опции формирования отчета:

- **–q**. Не выводить на консоль сообщения.
- **–o <имя>**. Задать имя файла, в который будет выводиться отчет о работе компонента. Если имя файла не задано, то отчет формироваться не будет. Помимо файла, информация о работе компонента будет выведена на консоль управления. Для вывода информации в системный журнал задайте syslog в качестве значения параметра <имя>.
- **–j<число>**. Задать уровень детализации отчета по объему содержащейся в нем информации. В качестве <опция> можно использовать следующие уровни детализации:
  - **1**. Сообщения об ошибках.
  - **2**. Информационные сообщения.
  - **3**. Сообщения о проверке.
  - **10**. Уровень отладки.
- **–x<опция>**. Задать уровень детализации отчета о проверке, выводимого на консоль управления. В качестве <опция> можно использовать следующие уровни детализации:
  - **O/o**. Краткий/расширенный формат сообщений о проверке простого объекта.

- **C/c**. Краткий/расширенный формат сообщений о проверке архива.
- **N/n**. Включить/выключить вывод на экран сообщений о незараженных файлах.
- **P/p**. Включить/выключить вывод на консоль управления информации о текущей работе компонента.

- **–m<опция>**. Задать уровень детализации отчета о проверке, выводимого в файл отчета. В качестве <опция> могут быть использованы:
  - **O/o**. Краткий/расширенный формат сообщений о проверке простого объекта.
  - **C/c**. Краткий/расширенный формат сообщений о проверке архива.
  - **N/n**. Включить/выключить вывод в файл отчета сообщений о незараженных файлах.

Опции файлов:

- **–p<опция> <имя_файла>**. Сохранить список объектов в заданный файл, сохранять каждый объект с полным путем с новой строки. В качестве <опция> могут быть использованы:
  - **i**. Сохранить в файл <имя_файла> список инфицированных объектов.
  - **c**. Сохранить в файл <имя_файла> список поврежденных объектов.
  - **w**. Сохранить в файл <имя_файла> список объектов, код которых похож на код известных вирусов.
- **–@ <filelist.lst>**. Проверить объекты, путь к которым приведен в файле <filelist.lst>.

Опции обработки файлов (определение данных ключей в командной строке отменяет выполнение действий, заданных в конфигурационном файле):

- **–i0**. Только проверять на присутствие вирусов.
- **–i1**. Лечить зараженные объекты. Если лечение невозможно – пропустить.
- **–i2**. Лечить зараженные объекты. Если лечение невозможно, и объект является простым – удалить; зараженный объект из контейнера не удалять.
- **–i3**. Лечить зараженные объекты. Если лечение невозможно, и объект является простым – удалить; если зараженный объект находится в контейнере – удалить контейнер целиком.
- **–i4**. Удалить зараженные объекты и контейнеры.

kaspersky

Коды возврата

В процессе работы компонент kavscanner может возвращать следующие коды:

- **0**. Вирусы не найдены.
- **5**. Все зараженные объекты были вылечены.
- **10**. Обнаружены архивы, защищенные паролем.
- **15**. Обнаружены поврежденные файлы.
- **20**. Обнаружены возможно зараженные файлы.
- **21**. Обнаружены файлы, код которых похож на код известных вирусов.
- **25**. Обнаружены зараженные файлы.
- **30**. При проверке файлов возникла системная ошибка.
- **50**. Невозможно загрузить антивирусные базы (путь, указанный в конфигурационном файле, не найден).
- **55**. Антивирусные базы повреждены.
- **60**. Дата антивирусных баз выходит за пределы срока действия ключа.
- **64**. Лицензионная информация отсутствует, либо не найдено ни одного ключа по пути, указанному в конфигурационном файле.
- **65**. Невозможно загрузить конфигурационный файл.
- **66**. Неверная опция конфигурационного файла.
- **70**. Компонент kavscanner поврежден.
- **75**. Компонент kavscanner поврежден и не может быть вылечен.

kaspersky

Запуск и проверка работы модуля

► *Чтобы запустить модуль kavscanner и проверить его работу:*

1. Запустите командную оболочку от имени суперпользователя (root) на сервере с установленным приложением.
2. Отключите проверку доступа на чтение файлов для процесса scan-сервера. Введите команду:

   ```
   # setcap cap_dac_read_search+ep /opt/kaspersky/klms/libexec/scan_server
   ```

3. Перезагрузите службу klms. Введите команду:

   ```
   # service klms restart
   ```

4. Проверьте права доступа к директории. Введите команду:

   ```
   # ls -lahd /root/
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   dr-xr-x--- 5 root root 4.0K Oct  6 20:10 /root/
   ```

5. Проверьте наличие файла `eicar.com` в текущей директории. Введите команду:

   ```
   # ls -lah /root/eicar.com
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   -rw-r--r-- 1 root root 69 Dec 22 09:22 /root/eicar.com
   ```

6. Запустите модуль kavscanner, убедитесь, что модуль kavscanner проверил файл `eicar.com`, обнаружил, что файл заражен и удалил его из директории. Введите команду:

   ```
   # /opt/kaspersky/klms/bin/kavscanner -i4 eicar.com
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   Kaspersky Anti-Virus On-Demand Scanner.
   The latest bases update 26-12-2021
   Config file: /etc/opt/kaspersky/klms/kavscanner_defaults.conf
   /root/eicar.com INFECTED EICAR-Test-File
   ```

7. Убедитесь, что зараженный файл `eicar.com` действительно удален. Введите команду:

   ```
   # ls -lah /root/eicar.com
   ```

   Результатом выполнения команды будет, например:

   ```
   ls: cannot access /root/eicar.com: No such file or directory
   ```

kaspersky

Проверка сохраненных сообщений модулем EML-scanner

В состав Kaspersky Security для Linux Mail Server входит модуль EML-scanner, выполняющий проверку сохранённых сообщений электронной почты с расширением .eml.

Администратор имеет возможность указать следующие технологии проверки сообщения:

- Анти-Фишинг (`ap`);
- Антивирус (`av`);
- Анти-Спам (`as`);
- Проверка ссылок (`mlf`).

Проверка возможна только при наличии действующего лицензионного ключа, определяющего набор доступных технологий проверки.

По завершении модуль выводит на консоль результат проверки сообщения технологиями, указанными при запуске. Модуль не производит никаких действий с проверяемыми сообщениями.

В этом разделе

Ключи командной строки

При работе с модулем из командной строки доступны следующие ключи:

- **--help**. Вывести на консоль справочную информацию о компоненте eml_scanner.
- **--av**. Выполнить антивирусную проверку сообщения.
- **--as**. Выполнить проверку сообщения на спам.
- **--ap**. Выполнить проверку сообщения на фишинг.
- **--mlf**. Выполнить проверку сообщения на наличие вредоносных и рекламных ссылок, а также ссылок, связанных с легальными программами.
- **-f [--file] arg**. Путь к файлу сохраненного сообщения, который требуется проверить.
- **--envelope-from arg**. Адрес отправителя сообщения.
- **--envelope-to arg**. Список получателей сообщения.
- **--helo arg**. HELO-имя сервера.
- **--client arg**. Имя SMTP-клиента.
- **--ip arg (=127.0.0.1)**. IP-адрес хоста.

kaspersky

Коды возврата

В процессе работы модуль EML-scanner отображает в консоли код возврата. Если обнаружение выполнено несколькими технологиями, соблюдается следующий приоритет кодов возврата:

- **0**. Угрозы не найдены.
- **1**. Обнаружены зараженные или возможно зараженные файлы.
- **2**. Обнаружены вредоносные, рекламные или связанные с легальными программами ссылки.
- **3**. Обнаружен фишинг.
- **4**. Обнаружен спам, возможный спам или массовая рассылка.
- **10**. Ошибка инициализации модуля (неверный синтаксис команды, не найден файл по указанному пути и т.д.).
- **11**. Ошибка лицензирования хотя бы одной из технологий проверки.
- **12**. Ошибка во время проверки файла.

Запуск и проверка работы модуля

► *Чтобы запустить модуль EML-scanner и проверить его работу:*

1. Запустите командную оболочку от имени суперпользователя (root) на сервере с установленным приложением.
2. Отключите проверку доступа на чтение файлов для процесса scan-сервера. Введите команду:

   ```
   # setcap cap_dac_read_search+ep /opt/kaspersky/klms/libexec/scan_server
   ```

3. Перезагрузите службу klms. Введите команду:

   ```
   # service klms restart
   ```

4. Проверьте права доступа к директории. Введите команду:

   ```
   # ls -lahd /root/
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   dr-xr-x--- 5 root root 4.0K Oct  6 20:10 /root/
   ```

5. Сохраните сообщение с расширением .eml, содержащее файл `eicar.com`, в текущей директории.
6. Запустите модуль EML-scanner и убедитесь, что модуль проверил сообщение с файлом `eicar.com` и обнаружил, что файл заражен. Для этого выполните команду:

   ```
   # /opt/kaspersky/klms/libexec/klms_eml_scanner --av -f /root/<имя файла>.eml
   ```

kaspersky

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Security для Linux Mail Server (см. раздел "Источники информации о приложении" на стр. 12), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security для Linux Mail Server.

Kaspersky предоставляет поддержку Kaspersky Security для Linux Mail Server в течение жизненного цикла (см. страницу жизненного цикла приложений (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться 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:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2c);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас предоставить отладочную информацию, которая содержит в себе файлы трассировки и дополнительную информацию об операционной системе, запущенных процессах на сервере и другую диагностическую информацию. Файлы трассировки позволяют отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка. Вы можете выбрать, какие события будут записаны в файлы трассировки: ошибки или информационные сообщения. Все файлы трассировки и дополнительная отладочная информация помещаются в архив, который вы сможете передать в Службу технической поддержки.

Файлы трассировки могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Необходимо согласовать состав отправляемого архива (см. раздел "О предоставлении данных" на стр. 33) со Службой безопасности вашей организации. Перед отправкой журнала трассировки удалите из него все данные, которые вы считаете конфиденциальными.

Все операции с диагностической информацией доступны при наличии права **Получать диагностическую информацию**.

Получение информации для Службы технической поддержки состоит из следующих этапов:

1. **Изменение уровня трассировки (на стр. 376) на значение Отладка**
2. **Воспроизведение действий пользователя, которые предшествовали возникновению неполадки**
3. **Создание файла трассировки (на стр. 376)**
4. **Скачивание файла трассировки (на стр. 377)**

Уровень трассировки **Отладка** значительно повышает требования к подсистеме хранения данных и снижает производительность приложения. После получения файла трассировки рекомендуется изменить уровень трассировки на значение **Ошибки.**

В этом разделе

Создание файла трассировки

При возникновении неполадок специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать архив с диагностической информацией о работе Kaspersky Secure Mail Gateway.

Файл трассировки следует создавать после воспроизведения действий пользователя, которые привели к возникновению неполадки.

► *Чтобы создать файл трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

   В рабочей области отобразится таблица узлов кластера с информацией о времени последнего создания файла трассировки для каждого узла.
3. В таблице выберите узел, для которого вы хотите получить диагностическую информацию.

   Откроется окно **Просмотреть результаты**.
4. В нижней части окна нажмите на кнопку **Запустить**.

Архив с диагностической информацией будет создан. Вы можете скачать (см. раздел "Скачивание файла трассировки" на стр. 377) или удалить (см. раздел "Удаление файла трассировки" на стр. 377) полученный архив.

Изменение уровня трассировки

Изменение уровня трассировки сохраняется в конфигурации приложения и не влияет на уже созданные файлы трассировки.

► *Чтобы изменить уровень трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.
3. По ссылке Уровень диагностики в верхней части рабочей области откройте окно **Уровень диагностики**.
4. Выберите один из следующих вариантов:
   - **Ошибки**.
   - **Отладка**.

     Этот уровень трассировки значительно повышает требования к подсистеме хранения данных и снижает производительность приложения. Используйте уровень отладки, только если Служба технической поддержки "Лаборатории Касперского" просит предоставить файлы трассировки такого типа.

   По умолчанию установлено значение **Ошибки**.
5. Нажмите на кнопку **Сохранить**.

Уровень трассировки будет изменен. Новые файлы трассировки будут создаваться в соответствии с выбранным уровнем.

Скачивание файла трассировки

► *Чтобы получить файл трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

   В рабочей области отобразится таблица узлов кластера с информацией о времени последнего создания файла трассировки для каждого узла.
3. В таблице выберите узел, для которого вы хотите скачать файл трассировки.

   Откроется окно **Просмотреть результаты**.
4. В строке с нужным файлом нажмите на значок  справа от названия файла.

Архив с файлом будет сохранен на вашем компьютере в папке загрузки браузера.

Удаление файла трассировки

► *Чтобы удалить файл трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

В рабочей области отобразится таблица узлов кластера с информацией о предыдущих запусках трассировки.

3. В таблице выберите узел, для которого вы хотите удалить файл трассировки.

   Откроется окно **Просмотреть результаты**.

4. В строке с нужным файлом нажмите на значок справа от названия файла.
5. В окне подтверждения нажмите на кнопку **ОК**.

Архив с файлом будет удален из списка.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления приложения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Действия после сбоя или неустранимой ошибки в работе приложения

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.

kaspersky

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.

B

BEC-атака

Business Email Compromise – компрометация деловой переписки в целях финансового мошенничества, добычи конфиденциальной информации или подрыва репутации компании. Под BEC-атакой обычно понимают целый комплекс действий, в результате которых злоумышленники начинают переписку с сотрудником компании, завоевывают его доверие с помощью методов социальной инженерии и убеждают выполнить действия, идущие во вред интересам компании или ее клиентов.

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.

K

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных приложений "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Center

Решение, предназначенное для централизованного выполнения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к

детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского".

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 приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля пользователя. Keytab-файлы используются в системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

M

MTA

Mail Transfer Agent – агент, осуществляющий пересылку сообщений между почтовыми серверами.

N

NTLM-аутентификация

Механизм аутентификации, который работает посредством вопросов/ответов между сервером и клиентом без передачи пароля пользователя через сеть в открытом виде. Для шифрования запроса и ответа используются хеши пароля пользователя, которые передаются по сети. При захвате сетевого трафика злоумышленники могут получить доступ к хешам пароля, что делает этот механизм менее надежным, чем Kerberos-аутентификация.

kaspersky

P

PTR-запись

DNS-запись, связывающая IP-адрес компьютера с его доменным именем.

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 приложением Kaspersky Security для Linux Mail Server в соответствии с результатами проверки сообщения.

SIEM-система

SIEM-система (Security Information and Event Management) – решение для управления информацией и событиями в системе безопасности организации.

SMTP-проверка

SMTP-проверка адресов электронной почты – проверка существования адресов электронной почты получателей сообщений.

SNMP-агент

Программный модуль сетевого управления Kaspersky Security для Linux Mail Server, отслеживает информацию о работе приложения.

SNMP-ловушка

Уведомление о событиях работы приложения, отправляемое SNMP-агентом.

SPF-проверка подлинности отправителей сообщений

Сопоставление IP-адресов отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

A

Антивирус

Компонент Kaspersky Security для Linux Mail Server, предназначенный для обнаружения вирусов в сообщениях электронной почты и вложениях в сообщения электронной почты.

kaspersky

Анти-Спам

Компонент Kaspersky Security для Linux Mail Server, предназначенный для обнаружения сообщений, которые классифицируются как спам.

Анти-Спам карантин

Хранилище, в которое временно помещаются сообщения электронной почты, если модулю Анти-Спам не удалось присвоить им окончательный статус по результатам проверки.

Анти-Фишинг

Компонент Kaspersky Security для Linux Mail Server, предназначенный для обнаружения сообщений, которые классифицируются как фишинг.

В

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

Д

Дайджест Хранилища

Почтовая сводка, которая рассылается по расписанию и содержит информацию о последних полученных письмах, помещенных в персональное Хранилище пользователя.

З

Замкнутая программная среда

Механизм контроля целостности (неизменности) файлов для повышения безопасности в Astra Linux Special Edition. Применение замкнутой программной среды позволяет определить перечень программного обеспечения, разрешенного для использования.

И

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

Источник обновлений

Ресурс, содержащий обновления антивирусных баз приложения Kaspersky Security для Linux Mail Server. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

kaspersky

К

Кластер

Группа серверов с установленным приложением Kaspersky Security для Linux Mail Server, объединенных для централизованного управления через веб-интерфейс приложения.

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.

М

Мандатное управление доступом

Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

О

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Персональный пользователь

Пользователь домена Active Directory, для которого настроена аутентификация в приложении с помощью технологии единого входа (SSO) и которому не назначена ни одна роль.

Подчиненный узел

Компонент приложения, который проверяет почтовый трафик согласно правилам обработки сообщений. Подчиненный узел получает заданные администратором параметры от Управляющего узла.

Почтовое уведомление

Сообщение электронной почты с описанием события приложения или события проверки сообщений, которое Kaspersky Security для Linux Mail Server отправляет на заданные адреса электронной почты.

Привилегированный пользователь

Пользователь, которому доступна функциональность консоли управления приложением. Доступные элементы в меню консоли управления зависят от назначенной пользователю роли.

kaspersky

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 Moebius

Служба быстрых обновлений баз Анти-Спама, позволяющая в режиме реального времени установить критические обновления.

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

Тип атаки, основанной на фальсификации передаваемых данных. Спуфинг может быть нацелен на получение расширенных привилегий и основан на обходе механизма верификации при помощи формирования запроса, аналогичного настоящему. Одним из вариантов такой подмены является подделка HTTP-заголовка для получения доступа к скрытому контенту.

Целью спуфинга может также быть обман пользователя — классическим примером подобной атаки может служить подмена адреса отправителя в письмах электронной почты.

У

Управляющий узел

Компонент приложения, который позволяет администратору управлять параметрами приложения через веб-интерфейс. Управляющий узел следит за состоянием Подчиненных узлов, передает им заданные параметры и добавленные лицензионные ключи.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать приложение "Лаборатории Касперского" по пробной или коммерческой лицензии.

kaspersky

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Х

Хранилище

Специальное хранилище для оригиналов почтовых сообщений, обработанных приложением.

Если к сообщению применяется правило обработки, в параметрах которого выбрано Поместить сообщение в Хранилище, приложение помещает оригинал сообщения в Хранилище независимо от заданного действия.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке /opt/kaspersky/klms/share/doc.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации Крипто-Си версии 2.0, (C) ООО "КриптоЭкс" http://www.cryptoex.ru http://www.cryptoex.ru.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Google Chrome – товарный знак Google LLC.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Microsoft Edge, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

Red Hat, Red Hat Enterprise Linux и CentOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

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

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

Zabbix – зарегистрированный товарный знак Zabbix SIA.

kaspersky

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 43. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
приложение	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы приложения	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение. Значения параметров программы в сертифицированном режиме

Этот раздел содержит перечень параметров программы, влияющих на сертифицированный режим работы программы. В таблице ниже приведены значения этих параметров в сертифицированном режиме работы программы.

Если вы меняете какие-либо из перечисленных значений параметров с их значений в сертифицированном режиме работы программы на другие значения, вы выводите программу из сертифицированного режима работы.

Таблица 44. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Параметры → Общие → Защита	**Антивирус**	**Использовать Антивирус**	**Включено**
		Использовать эвристический анализ	**Включено**
	Анти-Спам	**Использовать Анти-Спам**	**Включено**
		Использовать Анти-Спам карантин	**Включено**
Параметры → Внешние службы	**KSN/KPSN → Параметры KSN/KPSN**	**Использование KSN/KPSN**	Допускается использование только KPSN (Kaspersky Private Security Network – KPSN)

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Параметры правила **Default** в разделе **Правила**	**Общие**	**Режим**	Одно из следующих значений: • **Использовать параметры модулей проверки** • **Отклонять без проверки** • **Удалять без уведомления отправителя**
	Анти-Спам		**Включено**
	Антивирус	**Антивирус**	**Включено**
		Если обнаружен зараженный объект	Одно из следующих значений: • **Вылечить** • **Удалить вложение** • **Удалить сообщение** • **Отклонить**
		Если обнаружены ошибки проверки модулем Антивирус	Одно из следующих значений: • **Удалить вложение** • **Удалить сообщение** • **Отклонить**
		Если обнаружен зашифрованный объект	Одно из следующих значений: • **Удалить вложение** • **Удалить сообщение** • **Отклонить**
		Если обнаружен макрос	**Обрабатывать вложения с макросами**
		Если обнаружен макрос → Действие	Одно из следующих значений: • **Удалить вложение** • **Удалить сообщение** • **Отклонить**
	Защита KATA		Включено, если настроена интеграция с Kaspersky Anti Targeted Attack Platform
	Уведомления	Все параметры раздела	Включено, если настроено оповещение администратора безопасности по электронной почте об обнаруженных КВ