kaspersky

Kaspersky Security 9.0 для Microsoft Exchange Servers

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 9.7.364.0

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: 05.03.2024

Обозначение документа: 643.46856491.00078-06 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 9.0 для Microsoft Exchange Servers " (далее также "Kaspersky Security", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

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

kaspersky

О программе

Kaspersky Security представляет собой средство антивирусной защиты типа "Б" второго класса защиты и предназначено для применения на серверах информационных систем.

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

В программе реализованы следующие функции безопасности:

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

В этом разделе

Что нового

В Kaspersky Security появились следующие возможности и доработки:

- Добавлена проверка вложения к письмам на наличие фишинга, даже если установлен только компонент АВ-защиты для почтовых ящиков.
- Добавлена поддержка взаимодействия с новой версией KSC 14.2.
- Добавлена возможность использования протокола SMTP в качестве альтернативы отправки уведомлений с помощью EWS.
- Доработана защита от класса атак AD-спуфинг (при отправке спама от адресантов, похожих на настоящие).
- Поддержана работа по безопасной версии протокола LDAPS вместо устаревшего LDAP.
- Добавлена поддержка NTLM 2.0 и Kerberos.
- Добавлена возможность блокировки b2b-рассылок.
- Добавлена подержка новых ОС и СУБД.

Kaspersky Security 9.0 для Microsoft Exchange Servers Maintenance Release 7 соответствует Общему регламенту по защите данных (General Data Protection Regulation, GDPR) и применимым законам Европейского союза о конфиденциальной информации, персональных данных и защите данных.

О предоставлении данных

Для работы программы используются данные, на обработку которых требуется согласие администратора Kaspersky Security.

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

- В Лицензионном соглашении и Политике конфиденциальности (см. раздел "Шаг 2. Просмотр информации о начале установки. Ознакомление с Лицензионным соглашением и Политикой конфиденциальности" на стр. 27).

  Согласно условиям принятого Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении в пункте Предоставление информации. Эта информация требуется для повышения уровня оперативной защиты.

- В Положении о Kaspersky Security Network (см. раздел "О Kaspersky Security Network" на стр. 98).

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

  Вы можете ознакомиться с условиями Положения о Kaspersky Security Network следующими способами:

  - По ссылке **Положение о KSN** в узле **Настройка**.
  - Прочитав документ ksn_agreement.rtf, расположенный в папке установки программы.

  Участие в Kaspersky Security Network добровольное. Вы можете в любой момент отказаться от участия в Kaspersky Security Network.

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

- В разделе Работа с персональными данными пользователей (на стр. 62).

  Администратору Kaspersky Security необходимо ознакомиться с перечнем этих данных и обеспечить их безопасность.

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

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

Для работы Kaspersky Security компьютер должен удовлетворять аппаратным и программным требованиям, приведенным ниже.

Аппаратные требования

Аппаратные требования для установки Сервера безопасности соответствуют аппаратным требованиям защищаемого сервера Microsoft Exchange, за исключением объема оперативной памяти. Совместно с Сервером безопасности устанавливается Консоль управления.

Аппаратные требования для установки Сервера безопасности:

- процессор – в соответствии с аппаратными требованиями защищаемого сервера Microsoft Exchange;
- минимум 2 ГБ свободной оперативной памяти;
- 6 ГБ свободного дискового пространства.

> В зависимости от значений параметров программы и режима ее эксплуатации может потребоваться дополнительное дисковое пространство.

Консоль управления также может быть установлена отдельно от Сервера безопасности.

Аппаратные требования для установки Консоли управления:

- процессор Intel® Pentium® 400 МГц или выше (рекомендуется 1000 МГц);
- 256 МБ свободной оперативной памяти;
- 500 МБ свободного дискового пространства для установки программы.

Программные требования

Для установки Сервера безопасности требуется одна из следующих операционных систем:

- Microsoft Windows Server 2022 Standard или Datacenter;
- Microsoft Windows Server 2019 Standard или Datacenter;
- Microsoft Windows Server 2016 Standard или Datacenter.

Программа поддерживает операционные системы Microsoft Windows Server также в режиме Core.

Для установки Сервера безопасности требуется следующее программное обеспечение:

- Один из следующих почтовых серверов:
  - Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт;
  - Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт;
  - Microsoft Exchange Server 2013, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).
- Одна из следующих программных платформ:
  - Microsoft .NET Framework 4.5;
  - Microsoft .NET Framework 4.6;
  - Microsoft .NET Framework 4.7;
  - Microsoft .NET Framework 4.8.
- Одна из следующих систем управления базами данных (СУБД):
  - Microsoft SQL Server 2022 Express, Standard или Enterprise;
  - Microsoft SQL Server 2019 Express, Standard или Enterprise;
  - Microsoft SQL Server 2017 Express, Standard или Enterprise;
  - Microsoft SQL Server 2016 Express, Standard или Enterprise;

Для установки Консоли управления требуется одна из следующих операционных систем:

- Microsoft Windows Server 2022 Standard или Datacente;
- Microsoft Windows Server 2019 Standard или Datacenter;
- Microsoft Windows Server 2016 Standard или Datacenter;
- Microsoft Windows 10 (x64)
- Microsoft Windows 11 (x64).

Программа поддерживает операционные системы Microsoft Windows Server также в режиме Core.

Для установки Консоли управления требуется следующее программное обеспечение:

- Microsoft Management Console 3.0;
- Одна из следующих программных платформ:
  - Microsoft .NET Framework 4.5;
  - Microsoft .NET Framework 4.6;
  - Microsoft .NET Framework 4.7;
  - Microsoft .NET Framework 4.8.

Для установки любого компонента программы (Сервера безопасности или Консоли управления) требуется пакет обновлений Microsoft Windows KB2999226.

Для установки плагина управления требуется следующая версия Kaspersky Security Center:

- Kaspersky Security Center 14.2

kaspersky

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. Должна быть обеспечена возможность периодического контроля целостности ПО программы и БД ПКВ.
17. 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.
18. Среда функционирования должна быть настроена таким образом, чтобы исключить возможность инициирования сетевых соединений процессами, не обладающими административными привилегиями, или процессами, не относящимися к Kaspersky Security.

kaspersky

Архитектура программы

В этом разделе

Компоненты программы и их предназначение

В состав Kaspersky Security входят три основных компонента:

- **Сервер безопасности** устанавливается на сервере Microsoft Exchange и отвечает за защиту от вирусов и фильтрацию почтового трафика от спама и фишинга. Сервер безопасности перехватывает сообщения, поступающие на сервер Microsoft Exchange, и проверяет их на вирусы, спам и фишинг с помощью встроенных модулей Антивирус и Анти-Спам соответственно. В случае заражения поступившего сообщения вирусом или наличия в сообщении признаков спама или фишинговых ссылок, программа выполняет над ним действия, заданные в параметрах соответствующего модуля.
- **Консоль управления** представляет собой специализированную изолированную оснастку, интегрированную в Microsoft Management Console 3.0. С помощью Консоли управления вы можете формировать список защищаемых серверов Microsoft Exchange и управлять Серверами безопасности. Консоль управления может быть установлена как на самом сервере Microsoft Exchange вместе с Сервером безопасности, так и на удаленном компьютере (см. раздел "Особенности установки программы на одиночном сервере Microsoft Exchange" на стр. 19).
- **Плагин управления Kaspersky Security для Microsoft Exchange Servers –** библиотеки, позволяющие управлять объектом охраны через Kaspersky Security Center.

Модули Сервера безопасности

Сервер безопасности состоит из следующих модулей:

- Перехватчик сообщений электронной почты. Перехватывает сообщения, поступающие на сервер Microsoft Exchange, и направляет их Антивирусу и Анти-Спаму. Этот модуль участвует в процессах Microsoft Exchange с помощью технологии транспортных агентов (Transport Agents).

  При установке Kaspersky Security транспортный агент "Kaspersky Antispam filter agent" регистрируются на сервере Microsoft Exchange с наивысшим приоритетом. Не изменяйте приоритет этого транспортного агента, в противном случае эффективность защиты может снизиться.

- Антивирус. Выполняет проверку сообщений на наличие вирусов и других вредоносных объектов. Этот модуль включает в себя антивирусное ядро и хранилище временных объектов для проверки в оперативной памяти. Хранилище представляет собой служебную папку store.

Папка store создается в папке хранения данных программы (по умолчанию – <папка установки программы>/data). Вам необходимо исключить ее из проверки антивирусными программами, установленными в сети организации. В противном случае Kaspersky Security может работать неправильно.

- Анти-Спам. Фильтрует нежелательную почту. Копии удаленных сообщений могут быть сохранены в резервном хранилище.
- Модуль внутреннего управления программы и контроля целостности. Представляет собой службу Microsoft Windows под именем Kaspersky Security 9.0 для Microsoft Exchange Servers.

  Модуль запускается автоматически при прохождении первого сообщения через сервер Microsoft Exchange;

  Служба не зависит от состояния сервера Microsoft Exchange (включен, остановлен), что позволяет настраивать программу, когда сервер Microsoft Exchange остановлен.

  Необходимо, чтобы модуль внутреннего управления программы и контроля целостности был всегда запущен. Не останавливайте службу Kaspersky Security 9.0 для Microsoft Exchange Servers вручную, так как это приведет к выключению Сервера безопасности и прекращению проверки.

База данных резервного хранилища и статистики

Программа хранит данные резервного хранилища и статистические сведения о работе программы в специальной базе данных, работающей под управлением Microsoft SQL Server, так называемой *базе данных резервного хранилища и статистики* (далее также *база данных*).

При установке программа может создавать новую или использовать ранее созданную базу данных. При удалении программы вы можете сохранить базу данных на SQL-сервере для дальнейшего использования.

База данных резервного хранилища и статистики может размещаться локально на одном компьютере вместе с Сервером безопасности или на удаленном компьютере, установленном в сети организации.

Kaspersky Security не обеспечивает шифрование данных между Сервером безопасности и базой данных. При размещении базы данных на удаленном компьютере вам необходимо самостоятельно выполнять шифрование данных при передаче по каналам связи, если это предусмотрено требованиями информационной безопасности вашей организации.
Часть конфигурационных данных программы хранится в базе данных. Программа не выполняет контроль за несанкционированным изменением этих данных и контроль целостности этих данных. Вам необходимо предпринять собственные меры по защите этих данных от несанкционированного доступа и контролю их целостности.
При создании базы данных SQL сервер использует локальные правила сопоставления. Учитывайте параметр Collation при установке программы для избежания регистрозависимого поведения и ошибок при подключении к базе данных.

kaspersky

Параметры базы данных

Параметры базы данных резервного хранилища и статистики хранятся в следующем конфигурационном файле:
`<папка установки программы>\Configuration\BackendDatabaseConfiguration2.config`

Это доступный для изменения файл формата XML. В нем указаны следующие параметры:

- **AdditionalConnectionParameters** – дополнительные параметры соединения с SQL-сервером. Значение этого параметра указывается программой автоматически на основании информации, указанной администратором при установке программы.
- **SqlServerName** – имя SQL-сервера. Указывается программой автоматически в формате `<имя SQL-сервера>\<экземпляр>` на основании информации, указанной администратором при установке программы.
- **DatabaseName** – имя основной базы данных. Указывается программой автоматически на основании информации, указанной администратором при установке программы.
- **FailoverPartner** – параметры (SQL-сервер и экземпляр) зеркала базы данных. Указываются программой автоматически в формате `<имя SQL-сервера>\<экземпляр>`.

Не рекомендуется указывать в поле Дополнительные параметры соединения параметры SqlServerName и DatabaseName, так как они определяются в полях Имя SQL-сервера и Имя базы данных.

Резервирование базы данных

Программа поддерживает технологию зеркального отображения баз данных (Database Mirroring). Если эта технология используется в конфигурации вашего SQL-сервера, она будет задействована в программе автоматически, то есть при отключении или отказе основной базы данных резервного хранилища и статистики программа автоматически переходит на использование зеркала базы данных. При восстановлении основной базы данных программа автоматически возвращается к ее использованию.

При установке или работе программы с использованием базы SQL с настроенной технологией AlwaysOn необходимо синхронизировать права между всеми серверами, входящими в группу зеркального отображения баз данных.

kaspersky

Типовые схемы и сценарии развертывания программы

Этот раздел содержит информацию о конфигурациях почтовой инфраструктуры Microsoft Exchange, в которых может быть развернута программа Kaspersky Security.

В этом разделе

Основные схемы установки программы

Вы можете выбрать один из двух вариантов развертывания программы в зависимости от почтовой инфраструктуры Microsoft Exchange в вашей организации:

- Сервер безопасности устанавливаются на компьютер, на котором развернут одиночный сервер Microsoft Exchange (см. раздел "Особенности установки программы на одиночном сервере Microsoft Exchange" на стр. 16). Консоль управления устанавливается на тот же компьютер.
- Сервер безопасности устанавливается в группе доступности баз данных Microsoft Exchange (Database Availability Group, далее также группа DAG) (см. раздел "Особенности установки программы в группе доступности баз данных Microsoft Exchange" на стр. 17). В этом случае Сервер безопасности и Консоль управления устанавливаются вместе на каждом сервере Microsoft Exchange, входящем в группу DAG.

Вы можете дополнительно установить Консоль управления на любой другой компьютер сети вашей организации для удаленного управления Серверами безопасности.

Особенности установки программы на одиночном сервере Microsoft Exchange

Программа может быть установлена на одном или нескольких одиночных серверах Microsoft Exchange. На сервере Microsoft Exchange могут быть одновременно установлены Сервер безопасности и Консоль управления, с помощью которой осуществляется управление Сервером безопасности.

При необходимости вы можете установить Консоль управления отдельно от Сервера безопасности на любой компьютер сети организации для удаленного управления Сервером безопасности. В случае совместной работы нескольких администраторов Консоль управления может быть установлена на компьютер каждого из них.

Подключение Консоли управления к Серверу безопасности осуществляется через порт TCP 13100. Необходимо открыть этот порт в брандмауэре на удаленном сервере Microsoft Exchange или добавить службу Kaspersky Security для Microsoft Exchange Servers в список доверенных программ брандмауэра.

Особенности установки программы в группе доступности баз данных Microsoft Exchange

Программа Kaspersky Security может быть установлена на серверах, входящих в группу доступности баз данных Microsoft Exchange (группу DAG). В этом случае Сервер безопасности и Консоль управления устанавливаются вместе на каждом сервере Microsoft Exchange, входящем в группу DAG. Вы можете дополнительно установить Консоль управления на любой другой компьютер в сети вашей организации для удаленного управления Серверами безопасности.

При установке программа автоматически распознает группу DAG. Последовательность установки программы на узлы, входящие в группу DAG, не имеет значения.

Установка Kaspersky Security в группе доступности баз данных имеет следующие особенности:

- Требуется использовать единую базу данных для всех узлов группы DAG. Для этого вам нужно указать эту базу данных при установке Kaspersky Security на всех узлах группы DAG.
- Учетная запись, от имени которой выполняется установка, должна иметь права на запись в раздел конфигурации Active Directory®.
- Если на серверах, входящих в группу DAG, включен брандмауэр, вам нужно добавить службу *Kaspersky Security для Microsoft Exchange Servers* в список доверенных программ на каждом сервере, входящем в группу DAG. Это необходимо для работы Kaspersky Security с резервным хранилищем.

Во время обновления предыдущей версии программы на серверах, входящих в DAG, не рекомендуется подключаться к этим серверам с помощью Консоли управления и изменять параметры программы. В противном случае обновление может завершиться с ошибкой, что может привести к сбоям в работе программы. Если подключение во время обновления необходимо, перед подключением требуется убедиться, что версии Сервера безопасности и Консоли управления, с помощью которой выполняется подключение, совпадают.

После установки программы на серверах группы DAG большая часть параметров программы хранится в Active Directory, и все серверы, входящие в группу DAG, работают с этими параметрами. Kaspersky Security автоматически определяет активные серверы и распространяет на них конфигурацию из Active Directory. Однако индивидуальные параметры сервера Microsoft Exchange требуется настроить вручную для каждого сервера. Индивидуальными параметрами сервера Microsoft Exchange являются, например, параметры антивирусной защиты для роли Транспортный концентратор, параметры проверки на спам, параметры резервного хранилища, параметры отчетов о работе Анти-Спама и работе Антивируса для роли Транспортный концентратор, параметры обновления баз Анти-Спама.

Использование профилей для настройки параметров серверов, входящих в группу DAG, имеет следующие особенности:

- вы можете добавить в профиль серверы, входящие в группу DAG, только все вместе одновременно;
- при добавлении группы DAG в профиль все серверы и все их роли (включая роль Транспортный концентратор) добавляются в этот профиль;
- вы можете удалить из профиля все серверы группы DAG только одновременно.

После удаления Kaspersky Security с серверов в составе группы DAG конфигурация хранится в Active Directory и может быть использована при повторной установке программы.

Сценарии развертывания программы

Перед развертыванием программы необходимо подготовить следующие учетные записи:

- Учетная запись для установки программы. От имени этой учетной записи запускается мастер установки программы и мастер настройки программы.
- Учетная запись для запуска службы программы. Если SQL-сервер находится на том же компьютере, на котором выполняется установка программы, роль этой учетной записи может выполнять учетная запись Local System. В этом случае создавать специальную учетную запись для запуска службы не нужно.
- Учетная запись для подготовки базы данных. От имени этой учетной записи мастер установки программы выполняет подготовку базы данных программы на SQL-сервере. После завершения установки эта учетная запись не используется.

Для работы программы необходимо, чтобы на всех компьютерах, предназначенных для установки Сервера безопасности и Консоли управления, а также на пути передачи данных между ними был открыт сетевой порт TCP 13100.

Вы можете выполнить развертывание программы по одному из следующих сценариев:

- Сценарий развертывания программы с полным набором прав доступа.
- Сценарий развертывания программы с ограниченным набором прав доступа.

В этом разделе

Сценарий развертывания программы с полным набором прав доступа

Этот сценарий развертывания подходит вам, если вы обладаете достаточными полномочиями, чтобы выполнить все действия по установке самостоятельно, не привлекая других специалистов, а ваша учетная запись обладает соответствующим набором прав доступа.

► *Чтобы выполнить развертывание программы с полным набором прав доступа, выполните следующие действия:*

1. Убедитесь, что учетная запись, предназначенная для установки программы, включена в локальную группу "Администраторы" на сервере Microsoft Exchange, на котором выполняется установка программы.
2. Убедитесь, что учетная запись, предназначенная для установки программы, включена в группы "Администраторы домена" и "Администраторы предприятия". Если не включена, включите учетную запись в эти группы. Это необходимо, чтобы мастер установки программы мог создать конфигурационное хранилище и группы разграничения доступа в Active Directory.

   Если установка программы уже выполнена хотя бы на одном компьютере в сети организации, для установки программы на других компьютерах организации достаточно учетной записи локального администратора. При этом требуется предоставить учетной записи, предназначенной для установки программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов: `CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`
3. Назначьте учетной записи, предназначенной для подготовки базы данных, роль sysadmin на SQL-сервере. Эти права необходимы для создания и настройки базы данных. Учетная запись так же должна обладать правом Allow Logon Locally ("Разрешить локальный вход в систему"), выданным в локальной политике безопасности на сервере Microsoft Exchange, на котором выполняется установка программы.
4. Добавьте учетную запись, предназначенную для запуска службы, в локальную группу "Администраторы" на сервере Microsoft Exchange, на котором выполняется установка программы.

   Если ранее вы удалили право Debug Programs, предоставляемое группе "Администраторы" по умолчанию, назначьте это право учетной записи, предназначенной для запуска службы.
5. Добавьте учетную запись, предназначенную для запуска службы, в группу Organization Management. Это необходимо для получения программой конфигурационных параметров сервера Microsoft Exchange.
6. Запустите и выполните шаги мастера установки программы (см. раздел "Установка программы при помощи мастера установки" на стр. 26) и мастера настройки программы (см. раздел "Первоначальная настройка программы" на стр. 38).
7. Назначьте учетным записям, которые принадлежат пользователям, выполняющим разные обязанности в вашей организации, соответствующие роли пользователя (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58). Для этого включите учетные записи пользователей в следующие группы учетных записей Active Directory:
   - Учетные записи администраторов – в группу Kse Administrators.
   - Учетные записи специалистов по антивирусной безопасности – в группу Kse AV Security Officers.
   - Учетные записи операторов антивирусной безопасности – в группу Kse AV Operators.
8. Выполните репликацию данных Active Directory во всей организации. Это действие необходимо, чтобы параметры программы, сохраненные в Active Directory, стали доступны для последующих установок программы на другие серверы Microsoft Exchange вашей организации.

При создании базы данных SQL сервер использует локальные правила сопоставления. Учитывайте параметр Collation при установке программы для избежания регистрозависимого поведения и ошибок при подключении к базе данных.

При установке или работе программы с использованием базы SQL с настроенной технологией AlwaysOn требуется синхронизировать права между всеми серверами, входящими в группу зеркального отображения баз данных.

Сценарий развертывания программы с ограниченным набором прав доступа

Этот сценарий развертывания подходит вам, если политика безопасности вашей организации не позволяет выполнить все действия по установке программы от имени вашей учетной записи и ограничивает права доступа к SQL-серверу или к Active Directory. Например, если администрирование баз данных в организации осуществляется другим специалистом, имеющим полный доступ к SQL-серверу.

► *Чтобы подготовиться к установке с ограниченным набором прав доступа к SQL-серверу или Active Directory, выполните следующие действия:*

1. Убедитесь, что учетная запись, предназначенная для установки программы, включена в локальную группу "Администраторы" на сервере Microsoft Exchange, на котором выполняется установка программы. Если не включена, включите учетную запись в эту группу.
2. Создайте в Active Directory следующий контейнер:

   `CN=KasperskyLab,CN=Services,CN=Configuration,DC=<root domain>`
3. Настройте полный доступ к этому контейнеру и ко всем его дочерним объектам для учетной записи, предназначенной для установки программы.
4. Создайте группу учетных записей Kse Watchdog Service. Тип группы – «Универсальная». Включите в нее учетную запись, предназначенную для работы службы программы. Если в качестве этой учетной записи используется Local System, включите в группу Kse Watchdog Service также учетную запись компьютера, на котором выполняется установка.
5. Добавьте группу Kse Watchdog Service в локальную группу "Администраторы" на сервере Microsoft Exchange, на котором выполняется установка программы.

   Если ранее вы удалили право Debug Programs, предоставляемое группе "Администраторы" по умолчанию, назначьте это право группе Kse Watchdog Service.
6. Предоставьте группе Kse Watchdog Service и учетной записи, предназначенной для установки программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов:

   `CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`
7. Предоставьте группе Kse Watchdog Services право ms-Exch-Store-Admin. Для этого выполните в консоли Exchange Management Shell следующую команду:

```
Add-ADPermission -Identity "<путь к контейнеру с конфигурацией
Microsoft Exchange>" -User "<имя домена>\Kse Watchdog Service" -
ExtendedRights ms-Exch-Store-Admin
```

Например:

```
Add-ADPermission -Identity "CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=<root domain>" -User
"domain\Kse Watchdog Service" -ExtendedRights ms-Exch-Store-Admin
```

8. Предоставьте группе Kse Watchdog Service право на запуск под другим именем (impersonation). Для этого выполните в консоли Exchange Management Shell следующую команду:

   ```
   New-ManagementRoleAssignment -Name KSE_IMPERSONATION -Role
   applicationImpersonation -SecurityGroup "Kse Watchdog Service"
   ```

9. Создайте следующие группы учетных записей: Kse Administrators, Kse AV Security Officers, Kse AV Operators. Эти группы могут быть созданы в любом домене организации. Тип групп – "Универсальная".
10. Выполните репликацию данных Active Directory во всей организации.
11. Назначьте учетным записям, которые принадлежат пользователям, выполняющим разные обязанности в вашей организации, соответствующие роли пользователя (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58). Для этого включите учетные записи пользователей в следующие группы учетных записей Active Directory:

    - Учетные записи администраторов – в группу Kse Administrators.
    - Учетные записи специалистов по антивирусной безопасности – в группу Kse AV Security Officers.
    - Учетные записи операторов антивирусной безопасности – в группу Kse AV Operators.

    Если вы планируете управлять программой с помощью Kaspersky Security Center (см. раздел "Управление программой с помощью Kaspersky Security Center" на стр. 242), добавьте учетные записи всех компьютеров, на которые вы устанавливаете Kaspersky Security, в группу KSE Administrators в Active Directory.

    > Если вы не добавили учетные записи всех компьютеров, на которых вы устанавливаете Kaspersky Security в группу KSE Administrators в Active Directory, на экране появляется сообщение с информацией о том, как обеспечить возможность управления программой с помощью Kaspersky Security Center (см. раздел "Управление программой с помощью Kaspersky Security Center" на стр. 242).

12. Убедитесь, что учетная запись, предназначенная для установки программы, также входит в группу KSE Administrators в Active Directory.

    > Если установка программы уже выполнена хотя бы на одном компьютере в сети организации, для установки программы на других компьютерах организации достаточно учетной записи локального администратора. При этом требуется предоставить учетной записи, предназначенной для установки программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов: `CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`

13. Обеспечьте создание базы данных программы. Выполните это действие самостоятельно или делегируйте его выполнение уполномоченному специалисту.

14. Создайте на SQL-сервере учетную запись для следующей группы Active Directory: Kse Watchdog Service.
15. Назначьте группе учетных записей Kse Watchdog Service роли db_owner на уровне базы данных программы.
16. Назначьте учетной записи, предназначенной для подготовки базы данных, роли db_owner на уровне базы данных программы и права VIEW ANY DEFINITION на уровне SQL-сервера.

    Если вы не предоставили этой учетной записи право VIEW ANY DEFINITION, при проверке мастером установки ролей и прав пользователей на базу данных программы на экране появляется сообщение с запросом права ALTER ANY LOGIN. Право ALTER ANY LOGIN требуется мастеру установки, чтобы создать пользователей SQL-сервера, присвоить этим пользователям роли и выдать им права на использование базы данных.

17. Предоставьте учетной записи, предназначенной для подготовки базы данных, права Allow Logon Locally ("Разрешить локальный вход в систему").
18. Предоставьте учетной записи, предназначенной для работы службы программы, права Allow Logon Locally ("Разрешить локальный вход в систему").
19. Выполните шаги мастера установки программы (см. раздел "Установка программы при помощи мастера установки" на стр. 26) и мастера настройки программы (см. раздел "Первоначальная настройка программы" на стр. 38) от имени учетной записи, предназначенной для установки программы.
20. Выполните репликацию данных Active Directory во всей организации. Это действие требуется, чтобы параметры программы, сохраненные в Active Directory, стали доступны для последующих установок программы на другие серверы Microsoft Exchange вашей организации.

При создании базы данных SQL сервер использует локальные правила сопоставления. Учитывайте параметр Collation при установке программы для избежания регистрозависимого поведения и ошибок при подключении к базе данных.

При установке или работе программы с использованием базы SQL с настроенной технологией AlwaysOn требуется синхронизировать права между всеми серверами, входящими в группу зеркального отображения баз данных.

kaspersky

Установка, восстановление и удаление программы

Этот раздел содержит информацию об установке, первоначальной настройке, восстановлении и удалении программы.

В этом разделе

Установка программы при помощи мастера установки

Во время установки Kaspersky Security требуется перезапуск служб MSExchangeTransport и MSExchangeIS. Перезапуск служб выполняется автоматически без дополнительного запроса.

Вы можете установить программу, запустив мастер установки программы, который приводит информацию о том, какие действия требуется выполнить на каждом шаге. Кнопки **Назад** и **Далее** служат для перехода между окнами мастера установки. Кнопка **Отмена** служит для выхода из мастера установки.

При установке в режиме командной строки (см. раздел "Параметры работы с командной строкой" на стр. 34) настройки по умолчанию могут отличаться от настроек, предлагаемых по умолчанию при установке с помощью мастера установки программы.

Перед запуском установки программы требуется убедиться, что вы выполнили все необходимые подготовительные действия (см. раздел "Сценарии развертывания программы" на стр. 21).

Во время первой установки Kaspersky Security в организации мастер установки программы автоматически добавляет учетную запись компьютера, на котором выполняется установка, в группу KSE Administrators в Active Directory. Добавление учетной записи компьютера в группу KSE Administrators требуется, если вы планируете управлять работой Kaspersky Security с помощью Kaspersky Security Center.

Если установка уже выполнена хотя бы на одном компьютере в сети организации, для установки идентичной версии программы на другие компьютеры организации достаточно учетной записи локального администратора. При этом требуется предоставить учетной записи, предназначенной для установки программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов:
`CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`

► *Чтобы запустить установку программы при помощи мастера установки, выполните следующие действия:*

запустите установочный файл, входящий в пакет установки программы. Откроется

приветственное окно мастера установки программы.

В этом разделе

Шаг 1. Проверка наличия обязательного программного обеспечения

Приветственное окно мастера установки программы содержит содержит общую информацию об установке и ссылку на онлайн-справку программы.

На этом шаге мастер установки программы проверяет наличие на компьютере программного обеспечения (см. раздел "Аппаратные и программные требования" на стр. 13), необходимого для работы программы – Microsoft .NET Framework 4.5. Если Microsoft .NET Framework 4.5 не установлен, отображается сообщение об ошибке, и мастер установки программы завершает работу.

Шаг 2. Просмотр информации о начале установки. Ознакомление с Лицензионным соглашением и Политикой конфиденциальности

На этом шаге в окне мастера установки просмотрите информацию о начале установки Kaspersky Security на ваш компьютер и по кнопке **Далее** перейдите к окну, содержащему текст Лицензионного соглашения и Политики конфиденциальности. Лицензионное соглашение заключается между пользователем программы и "Лабораторией Касперского". Политика конфиденциальности описывает обработку персональных данных пользователя и сохранение конфиденциальности этих данных.

Подтвердите, что полностью прочитали, поняли и принимаете Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения и Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности», установив соответствующие флажки.

Если вы не примете условия Лицензионного соглашения и Политики конфиденциальности, вы не сможете установить Kaspersky Security.

Шаг 3. Выбор типа установки

На этом шаге выберите тип установки программы:

- **Обычная**. Программа установит все компоненты и модули программы. Файлы программы будут скопированы в папку установки программы и папку хранения данных, заданные по умолчанию. Если вы выбрали этот тип установки, мастер переходит к Шагу 5. Настройка подключения программы к базе данных резервного хранилища и статистики (см. раздел "Шаг 5. Создание базы данных и настройка подключения программы к SQL-серверу" на стр. 30).
- **Выборочная**. В этом случае на следующем шаге мастера установки программы вы сможете выбрать компоненты и модули программы, которые нужно установить, а также папку установки программы и папку хранения данных. Если вы выбрали этот тип установки, мастер переходит к Шагу 4. Выбор компонентов и модулей программы (см. раздел "Шаг 4. Выбор компонентов и модулей программы" на стр. 28).

Шаг 4. Выбор компонентов и модулей программы

На этом шаге вам нужно выбрать компоненты и модули программы, которые вы хотите установить, а также указать пути к папкам установки и хранения данных. Набор доступных для установки компонентов и модулей зависит от наличия на компьютере установленного сервера Microsoft Exchange и ролей, в которых он развернут.

Таблица 1. Компоненты и модули, доступные для установки на сервере Microsoft Exchange 2013

Роль сервера Microsoft Exchange 2013	Консоль управления	Анти-Спам	Антивирус для роли Почтовый ящик	Перехватчик CAS	Антивирус для роли Транспортный концентратор
Сервер клиентского доступа (Client Access Server)	**Да**	**Нет**	**Нет**	**Да**	**Нет**
Почтовый ящик (Mailbox Server)	**Да**	**Да**	**Да**	**Нет**	**Да**
Пограничный транспорт (Edge Transport Server)	**Да**	**Да**	**Нет**	**Нет**	**Да**

Модуль Перехватчик CAS доступен для выбора только в случае, если сервер Microsoft Exchange 2013 развернут в единственной роли Сервер клиентского доступа.
Модуль Перехватчик CAS предназначен для улучшения обнаружения спама. Его рекомендуется устанавливать на всех серверах Microsoft Exchange 2013, развернутых в единственной роли Сервер клиентского доступа. На серверы Microsoft Exchange 2013, развернутые в роли Почтовый ящик, этот модуль устанавливается автоматически вместе с модулем Анти-Спам (если Анти-Спам выбран для установки).

Таблица 2. Компоненты и модули, доступные для установки на сервере Microsoft Exchange 2016

Роль сервера Microsoft Exchange 2016	Консоль управления	Анти-Спам	Антивирус для роли Почтовый ящик	Антивирус для роли Транспортный концентратор
Почтовый ящик (Mailbox Server)	**Да**	**Да**	**Да**	**Да**
Пограничный транспорт (Edge Transport Server)	**Да**	**Да**	**Нет**	**Да**

Таблица 3. Компоненты и модули, доступные для установки на сервере Microsoft Exchange 2019

Роль сервера Microsoft Exchange 2019	Консоль управления	Анти-Спам	Антивирус для роли Почтовый ящик	Антивирус для роли Транспортный концентратор
Почтовый ящик (Mailbox Server)	**Да**	**Да**	**Да**	**Да**
Пограничный транспорт (Edge Transport Server)	**Да**	**Да**	**Нет**	**Да**

Выберите компоненты и модули программы, которые вы хотите установить. Чтобы отменить ваш выбор компонентов и вернуться к выбору по умолчанию, нажмите на кнопку **Сброс**.

Чтобы просмотреть информацию о наличии на локальных дисках свободного места, необходимого для установки выбранных компонентов, нажмите на кнопку **Диски**.

В нижней части окна в поле **Папка назначения** отображается путь к папке установки программы по умолчанию. Если требуется, укажите другую папку назначения. Для этого нажмите на кнопку **Обзор** и укажите папку в открывшемся окне.

Ниже в поле **Папка хранения данных** отображается путь к папке хранения данных программы, установленный по умолчанию (<папка установки программы>\data). Эта папка предназначена для временного хранения проверяемых объектов и вспомогательных файлов. Если требуется, укажите другую папку хранения данных. Для этого нажмите на кнопку **Обзор** и укажите папку в открывшемся окне.

Шаг 5. Создание базы данных и настройка подключения программы к SQL-серверу

Чтобы создать базу данных на SQL-сервере и настроить подключение к ней, выполните следующие действия:

1. В поле **Имя SQL-сервера** укажите имя компьютера (или его IP-адрес), на котором установлен SQL-сервер, и имя SQL-экземпляра, например, MYCOMPUTER\SQLEXPRESS.

   Нажав на кнопку **Обзор**, расположенную напротив поля **Имя SQL-сервера**, вы можете выбрать SQL-сервер в том сегменте сети, в котором расположен компьютер.

   > В случае удаленного подключения к SQL-серверу необходимо убедиться, что на SQL-сервере включена поддержка TCP/IP в качестве клиентского протокола. Нужный вам SQL-сервер может отсутствовать в списке SQL-серверов, если на компьютере, на котором расположен SQL-сервер, не запущена служба браузера SQL-сервера.

2. В поле **Имя базы данных** укажите имя базы данных, которая будет использоваться для хранения данных резервного хранилища, статистической информации и сведений о конфигурации программы.

Предоставьте учетной записи, от имени которой запущен мастер установки, роль db_owner на уровне базы данных программы и право ALTER ANY LOGIN на уровне SQL-сервера. Право ALTER ANY LOGIN требуется мастеру установки, чтобы создать пользователей SQL-сервера, присвоить этим пользователям роли и выдать им права на использование базы данных. Роль db_owner обеспечивает набор прав, разрешающий выполнять все действия по настройке и обслуживанию базы данных, а также удалять базу данных.

Вы можете использовать для работы с программой одну из следующих баз данных:

- базу данных, предварительно созданную администратором SQL-сервера (см. раздел "Сценарий развертывания программы с ограниченным набором прав доступа" на стр. 23);
- базу данных, которая создается автоматически мастером установки программы.

Если вы хотите использовать единую базу данных резервного хранилища и статистики для нескольких Серверов безопасности, имя SQL-сервера и имя базы данных SQL должны быть одинаковыми для всех Серверов безопасности. В этом случае при установке программы на втором и последующих Серверах безопасности укажите одинаковые значения в полях **Имя SQL-сервера**, **Имя базы данных** и **Дополнительные параметры соединения** для соединения с базой данных, созданной при установке программы на первом Сервере безопасности. Если вы не планируете использовать общую базу данных, вы можете указать собственные параметры соединения с базой данных SQL для каждого сервера, входящего в группу DAG.

Вы можете использовать базу данных предыдущей версии программы. Подключение базы данных от предыдущей версии программы осуществляется при обновлении программы (см. раздел "7" на стр. 50). Если вы удалите, а потом установите новую версию программы при помощи мастера установки, то использовать базу данных от предыдущей версии будет невозможно.

3. В поле **Дополнительные параметры соединения** укажите дополнительные параметры соединения с сервером базы данных резервного хранилища и статистики.

   Описание параметров соединения с сервером базы данных вы можете найти на сайте Microsoft по ссылке: параметры строки соединения https://msdn.microsoft.com/en-us/library/system.data.sqlclient.sqlconnectionstringbuilder_properties(v=vs.110).aspx.

   Пример:

   - `Connection Timeout=30;Integrated Security=SSPI;MultiSubnetFailover=true`

   Не рекомендуется указывать в поле **Дополнительные параметры соединения** параметры `Data Source` и `Database`, так как они определяются в полях **Имя SQL-сервера** и **Имя базы данных.**

4. Для завершения настройки базы данных и перехода к следующему шагу мастера установки нажмите на кнопку **Далее**.

Kaspersky Security не обеспечивает канальное шифрование при передаче данных между сервером и базой данных SQL. В целях безопасности данных вам необходимо самостоятельно выполнить шифрование данных для передачи по каналам связи.

Шаг 6. Выбор учетной записи для запуска службы Kaspersky Security

На этом шаге укажите учетную запись, которая будет использоваться при запуске службы программы и при подключении Kaspersky Security к SQL-серверу:

- **Учетная запись Local System**. В этом случае запуск службы программы и соединение с SQL-сервером выполняется от имени учетной записи локальной системы.
- **Другая учетная запись**. В этом случае запуск службы программы и соединение с SQL-сервером выполняется от имени другой учетной записи. Вам нужно указать имя и пароль учетной записи. Вы также можете выбрать учетную запись, нажав на кнопку **Обзор**.

Указанная учетная запись должна обладать достаточными правами доступа. Информация о назначении прав доступа учетной записи, предназначенной для запуска службы программы, приведена в сценариях развертывания программы с полным (см. раздел "Сценарий развертывания программы с полным набором прав доступа" на стр. 21) и ограниченным (см. раздел "Сценарий развертывания программы с ограниченным набором прав доступа" на стр. 23) набором прав доступа.

Шаг 7. Завершение установки

На этом шаге выполняется копирование файлов программы на компьютер, регистрация компонентов в системе и удаление временных файлов из резервного хранилища.

Нажмите на кнопку **Установить** в окне мастера установки программы.

Мастер установки программы начнет копирование файлов программы на компьютер, регистрацию компонентов в системе, создание базы на SQL-сервере (если вы выбрали создание новой базы данных) и перезапуск служб MSExchangeTransport и MSExchangeIS.

Перезапуск служб MSExchangeTransport и MSExchangeIS будет выполнен автоматически без дополнительного запроса.

После окончания копирования файлов и регистрации компонентов в системе, в окне мастера установки программы появится сообщение о том, что установка программы завершена.

Для завершения установки нажмите на кнопку **Далее**.

Автоматически запустится мастер настройки программы (см. стр. 38). Мастер настройки программы позволяет выполнить первоначальную настройку параметров программы.

kaspersky

Установка программы с помощью командной строки

Во время установки Kaspersky Security требуется перезапуск служб MSExchangeTransport и MSExchangeIS. Перезапуск служб выполняется автоматически без дополнительного запроса.

Вы можете установить программу, запустив из командной строки установочный файл, входящий в пакет установки программы, и указав параметры установки (см. раздел "Параметры работы с командной строкой" на стр. 34).

Установка в режиме командной строки выполняется по заданному сценарию, в котором требуется самостоятельно указать перечень устанавливаемых компонентов.

Перехватчик CAS не входит в набор компонентов при установке с помощью командной строки. Консоль управления всегда устанавливается без указания дополнительных параметров при установке других компонентов.

Перед запуском установки программы требуется убедиться, что вы выполнили все необходимые подготовительные действия (см. раздел "Сценарии развертывания программы" на стр. 21).

Во время первой установки Kaspersky Security в организации мастер установки программы автоматически добавляет учетную запись компьютера, на котором выполняется установка, в группу KSE Administrators в Active Directory. Добавление учетной записи компьютера в группу KSE Administrators требуется, если вы планируете управлять работой Kaspersky Security с помощью Kaspersky Security Center.

Если установка уже выполнена хотя бы на одном компьютере в сети организации, для установки идентичной версии программы на другие компьютеры организации достаточно учетной записи локального администратора. При этом требуется предоставить учетной записи, предназначенной для установки программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов:
`CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`

► *Чтобы установить Kaspersky Security с помощью командной строки, выполните следующие действия:*

запустите установочный файл, входящий в пакет установки программы, с помощью командной строки со следующими параметрами:

```
--install-mode=install --accept-eula --accept-privacy-policy
```

kaspersky

В этом разделе

Параметры работы с командной строкой

Для перехода в режим установки, удаления, обновления или восстановления программы требуется запустить установочный файл, входящий в пакет установки программы, с помощью командной строки, указав при этом соответствующие параметры.

Перед каждым параметром требуется вводить символы «`--`». Например: `--param1=value1`. Разные параметры следует разделять пробелом.

Типы параметров следующие:

- Флаг: `--flag`
- Ключ-значение: `--key=value`
- Список компонентов: `--features=feature1,feature2`

Полный список параметров приведен ниже.

`install-mode`

Этот необязательный параметр типа Key используется для выбора режимов установки, удаления, обновления и восстановления программы.

Допустимые значения параметра:

- `install` – установка программы;
- `delete` – удаление программы;
- `upgrade` – обновление программы;
- `repair` – восстановление программы.

Значение по умолчанию: `install`.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка на совпадение с допустимыми значениями.
  Ошибка: Сообщение о недопустимом значении параметра.

`accept-eula`

Этот обязательный параметр типа Flag используется для принятия условий Лицензионного соглашения при установке или обновлении программы.

Параметр используется в следующих режимах:

- `install` – установка программы;
- `upgrade` – обновление программы

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка наличия параметра.
  Ошибка: Сообщение о невозможности установки продукта без принятия условий Лицензионного соглашения.

accept-privacy-policy

Этот обязательный параметр типа Flag используется для принятия Политики конфиденциальности при установке или обновлении программы.

Параметр используется в следующих режимах:

- `install` – установка программы;
- `upgrade` – обновление программы.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка наличия параметра.
  Ошибка: Сообщение о невозможности установки продукта без принятия Политики конфиденциальности.

components

Этот необязательный параметр типа Features используется для выбора компонентов, которые должны быть установлены.

Параметр используется только в режиме `install` (установка программы).

Допустимые значения параметра:

- `Antispam` – Анти-Спам;
- `AntivirusForMailbox` – Антивирус для роли Почтовый ящик;
- `AntivirusForTransport` – Антивирус для ролей Транспортный концентратор и Пограничный транспорт.

Необходимые компоненты указываются через запятую. Компонент Консоль управления устанавливается без указания дополнительных параметров. Перехватчик CAS не входит в набор компонентов при установке с помощью командной строки.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка на совпадение введенного значения с допустимыми.
  Ошибка: Сообщение о недопустимом значении параметра.

install-dir

Этот необязательный параметр типа Key используется для указания папки установки программы. В случае отсутствия указанной папки, она создается автоматически.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: `%Program Files (x86)%\Kaspersky Lab\Kaspersky Security for Microsoft Exchange Servers`.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка на корректность указанного пути.
  Ошибка: Сообщение о недопустимом значении параметра.

data-dir

Этот необязательный параметр типа Key используется для указания папки хранения данных. В случае отсутствия указанной папки, она создается автоматически.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: `<папка установки программы>\data`.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка на корректность указанного пути.
  Ошибка: Сообщение о недопустимом значении параметра.

sql-server-name

Этот необязательный параметр типа Key используется для указания имени SQL-сервера.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: имя текущего компьютера.

Если была установлена версия SQL Server Express, укажите имя компьютера (или его IP-адрес), на котором установлен SQL-сервер, и имя SQL-экземпляра, например, MYCOMPUTER\SQLEXPRESS. В противном случае установка будет прервана.

Проверки: Проверка корректности наименования параметра.
Ошибка: Сообщение о неизвестном параметре.

sql-db-name

Этот необязательный параметр типа Key используется для указания имени базы данных SQL, которая будет использоваться для хранения данных резервного хранилища, статистической информации и сведений о конфигурации программы.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: `SecurityForExchange`.

Проверки: Проверка корректности наименования параметра.
Ошибка: Сообщение о неизвестном параметре.

additional-sql-params

Этот необязательный параметр типа Key используется для указания дополнительных параметров соединения с сервером базы данных резервного хранилища и статистики.

Параметр используется только в режиме `install` (установка программы).

Перечень параметров и их значений вводится одной строкой.

Пример: `Connection Timeout=30;Integrated Security=SSPI;MultiSubnetFailover=true`.

Проверки: Проверка корректности наименования параметра.
Ошибка: Сообщение о неизвестном параметре.

service-account-name

Этот необязательный параметр типа Key используется для указания имени учетной записи для запуска службы KSE 9.0.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: идентификационные данные учетной записи LocalSystem.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- `service-account-pwd` заполнен, `service-account-name` не может иметь пустое значение или отсутствовать в командной строке установки.
  Ошибка: Сообщение "Не указано имя учетной записи для запуска службы KSE 9.0".

service-account-pwd

Этот необязательный параметр типа Key используется для указания пароля учетной записи для запуска службы KSE 9.0.

Параметр используется только в режиме `install` (установка программы).

Значение по умолчанию: идентификационные данные учетной записи LocalSystem.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- `service-account-name` заполнен, `service-account-pwd <>Null`.
  Ошибка: запрос пароля в интерактивном режиме.

installation-log-name

Этот необязательный параметр типа Key используется для указания пути к файлу журнала выполняемой операции.

Указание в параметре несуществующего пути вызывает ошибку, при этом операция не прерывается. После завершения операции, в командной строке отображается путь к файлу журнала.

Параметр используется в следующих режимах:

- `install` – установка программы;
- `delete` – удаление программы;
- `upgrade` – обновление программы;
- `repair` – восстановление программы.

Значение по умолчанию: `%TMP%\kseinstall.log`.

Проверки:

- Проверка корректности наименования параметра.
  Ошибка: Сообщение о неизвестном параметре.
- Проверка на корректность указанного пути.
  Ошибка: Сообщение о недопустимом значении параметра.

read-eula-privacy-policy

Этот необязательный параметр типа Flag используется для вывода на экран текста Лицензионного соглашения и Политики конфиденциальности.

Если данный параметр используется с другими параметрами установки, срабатывает только он, остальные параметры игнорируются.

Проверки: Проверка корректности наименования параметра.
Ошибка: Сообщение о неизвестном параметре.

`help`

Этот необязательный параметр типа Flag используется для вывода на экран текста справки по параметрам работы с командной строкой.

Проверки: Проверка корректности наименования параметра.
Ошибка: Сообщение о неизвестном параметре.

Первоначальная настройка программы

С помощью мастера настройки программы вы можете настроить минимальный набор параметров, необходимых для построения системы централизованного управления защитой сервера Microsoft Exchange.

Мастер настройки программы поможет вам выполнить следующие действия:

- активировать программу, добавив ключ;
- настроить параметры защиты сервера Microsoft Exchange с помощью модулей Антивирус и Анти-Спам;
- включить использование служб Kaspersky Security Network (далее также KSN);

- настроить параметры прокси-сервера;
- настроить параметры отправки уведомлений.

Мастер настройки программы запускается автоматически после завершения установки с помощью мастера установки. Он приводит информацию о том, какие действия требуется выполнить на каждом шаге. Кнопки **Назад** и **Далее** служат для перехода между окнами мастера настройки программы. Вы можете прекратить работу мастера настройки программы на любом этапе установки, закрыв окно мастера настройки программы.

Вы можете пропустить настройку программы и закрыть мастер, нажав на кнопку **Отмена** в приветственном окне мастера. Вы сможете выполнить настройку программы в Консоли управления программы после ее запуска.

В этом разделе

Шаг 1. Активация программы

На этом шаге вы можете добавить ключ для активации программы Kaspersky Security.

Вы также можете пропустить этот шаг и добавить ключ позже, после завершения работы мастера настройки программы и запуска программы.

Если ключ не добавлен, Kaspersky Security работает в режиме "Только управление" и не обеспечивает защиту сервера Microsoft Exchange. Для использования Kaspersky Security в режиме полной функциональности требуется добавить ключ.

Если вы используете следующие способы активации, пропустите этот шаг, вы сможете выполнить активацию программы в Консоли управления программы после завершения работы мастера настройки программы:

- если вы активируете программу по коду активации;
- если вы активируете программу на основании лицензии типа **Коммерческая (по подписке).**

► *Чтобы активировать программу, выполните следующие действия:*

1. Нажмите на кнопку **Добавить**.
2. В открывшемся окне в поле **Имя файла** укажите путь к файлу ключа (файл с расширением key).
3. Нажмите на кнопку **Открыть**.

Ключ будет добавлен в качестве активного. Активный ключ позволяет использовать программу Kaspersky Security в течение срока действия лицензии на условиях, указанных в Лицензионном соглашении.

Активация программы при установке в группе DAG серверов Microsoft Exchange

Если вы разворачиваете Kaspersky Security в группе DAG серверов Microsoft Exchange, достаточно добавить ключ один раз при установке программы на любой из серверов Microsoft Exchange, входящих в эту группу DAG. После этого при установке программы на другие серверы Microsoft Exchange, входящие в эту группу DAG, мастер настройки программы будет автоматически обнаруживать добавленный ключ. В этом случае добавлять ключи на другие серверы Microsoft Exchange в составе группы DAG не нужно.

Особенности активации программы для разных схем развертывания

Активация программы зависит от схемы развертывания программы (см. раздел «Типовые схемы и сценарии развертывания программы» на стр. 19):

- Если программа используется на одиночных серверах Microsoft Exchange, требуется добавить ключ Сервера безопасности на каждом сервере.
- Если программа используется на серверах Microsoft Exchange, входящих в группу DAG, требуется добавить один ключ Сервера безопасности. Действие ключей распространяется на всю группу DAG (см. раздел "Особенности установки программы в группе доступности баз данных Microsoft Exchange" на стр. 20).
- Если вы используете профили для управления несколькими Серверами безопасности, требуется добавить один ключ Сервера безопасности. Действие ключей распространяется на все Серверы безопасности профиля (см. раздел "Особенности активации программы при использовании профилей" на стр. 69).

Шаг 2. Настройка защиты сервера Microsoft Exchange

На этом шаге вы можете настроить параметры защиты сервера Microsoft Exchange от спама, вирусов и других программ, представляющих угрозу. Модули Антивирус и Анти-Спам начинают работать сразу после запуска программы. По умолчанию антивирусная защита и защита от спама включены. Также по умолчанию используется служба быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service и режим автоматического обновления баз программы (антивирусных баз и баз Анти-Спама).

Для работы Enforced Anti-Spam Updates Service требуется постоянное соединение компьютера, на котором установлен Сервер безопасности, с интернетом.

Если вы не хотите, чтобы Антивирус и Анти-Спам начали работать сразу после запуска программы, снимите флажки **Включить антивирусную защиту** и **Включить защиту от спама**. Позднее вы сможете включить защиту через Консоль управления.

Если вы хотите отключить службу быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service, снимите флажок **Включить Enforced Anti-Spam Updates Service**.

Если вы хотите отключить обновление баз Анти-Спама и Антивируса с серверов "Лаборатории Касперского" сразу после запуска программы, снимите флажок **Включить режим автоматического обновления баз**.

Шаг 3. Включение служб KSN

На этом шаге вы можете включить использование служб KSN (Kaspersky Security Network).

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Использование служб KSN разрешается на условиях специального Положения о Kaspersky Security Network. Вы можете ознакомиться с полным текстом Положения о Kaspersky Security Network в отдельном окне, открыв его по кнопке **Положение о KSN**.

Если вы хотите использовать службы KSN для обработки спама, установите флажок **Я принимаю Положение о Kaspersky Security Network и хочу использовать службы KSN для защиты**, тем самым подтверждая, что вы прочитали Положение о Kaspersky Security Network и согласны с его условиями.

См. также

Окно Использование служб Kaspersky Security Network 44

О Kaspersky Security Network 98

Шаг 4. Настройка параметров прокси-сервера

На этом шаге вы можете настроить параметры прокси-сервера. Эти параметры используются для подключения программы к серверам обновлений "Лаборатории Касперского" при выполнении обновления баз программы и подключения к Kaspersky Security Network.

Если вы хотите, чтобы программа подключалась к серверам обновлений "Лаборатории Касперского" через прокси-сервер, установите флажок **Использовать прокси-сервер** и укажите параметры подключения к прокси-серверу в соответствующих полях: адрес прокси-сервера и порт. По умолчанию используется порт 8080.

Если вы хотите использовать аутентификацию на указанном вами прокси-сервере, установите флажок **Использовать аутентификацию** и укажите учетные данные в полях **Учетная запись** и **Пароль**. Для выбора учетной записи из существующих нажмите на кнопку ....

Шаг 5. Настройка параметров отправки уведомлений

На этом шаге вы можете настроить параметры отправки уведомлений, с помощью которых вы и другие заинтересованные лица могут своевременно узнавать обо всех событиях в работе Kaspersky Security. Уведомления отправляются по электронной почте. Для успешной отправки уведомлений необходимо указать следующие параметры: адрес веб-службы и параметры учетной записи.

В поле **Адрес веб-службы** укажите адрес веб-службы отправки уведомлений через сервер Microsoft Exchange (по умолчанию в сервере Microsoft Exchange используется адрес `https://<имя_сервера_клиентского_доступа>/ews/exchange.asmx`).

В поле **Учетная запись** вручную или с помощью кнопки  укажите любую учетную запись из числа почтовых ящиков, зарегистрированных на Microsoft Exchange Server, и в поле **Учетная запись** введите пароль выбранной учетной записи.

В поле **Адрес администратора** укажите адрес электронной почты получателя уведомлений, например, ваш адрес электронной почты.

Нажмите на кнопку **Тест** для отправки тестового сообщения. Если тестовое сообщение пришло на указанный адрес электронной почты, это означает, что отправка уведомлений настроена правильно.

Шаг 6. Завершение настройки

На этом шаге выполняется сохранение настроенных параметров программы и завершение настройки.

По умолчанию после завершения настройки автоматически запускается Консоль управления. Если вы хотите отключить запуск Консоли управления, снимите флажок **Запустить Консоль управления после завершения работы мастера настройки программы**.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера настройки программы.

Окно Активация программы

Добавить / Заменить

Кнопка, по которой вы можете добавить / заменить активный или резервный ключ.

Ключ

Уникальная буквенно-цифровая последовательность.

Тип лицензии

Может принимать следующие значения:

- **Пробная лицензия**. Лицензия для пробного использования программы. Предоставляется на период, который назначает "Лаборатория Касперского". По истечении срока действия пробной лицензии программа прекращает выполнять все свои функции. Вы можете активировать программу с помощью ключа или кода активации.
- **Коммерческая**. Лицензия для коммерческого использования программы. Предоставляется на период, который назначает "Лаборатория Касперского" при приобретении лицензии. По окончании срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Обновление баз программы, получение новых версий программы, а также обращение в Службу технической поддержки становятся недоступными. Вы можете активировать программу с помощью ключа или кода активации.
- **Коммерческая (по подписке)**. Лицензия для коммерческого использования программы, которая распространяется через поставщиков услуг по подписке. Предоставляется на период, который назначает поставщик услуг по подписке. В соответствии с лицензионным ограничением вы можете использовать программу в течение периода, на который вы приобрели подписку у поставщика услуг. Вы можете активировать программу с помощью кода активации, вы не можете активировать программу с помощью ключа.

Представитель

Контактное лицо организации, заключившей Лицензионное соглашение.

Количество почтовых ящиков

Максимальное количество почтовых ящиков, которые может защитить программа по этому ключу.

Дата окончания

Дата окончания срока действия лицензии.

Статус

- Поле **Статус** отображается только для активных ключей. Возможны следующие статусы ключа Сервера безопасности и соответствующие им ограничения программы:
  - **Действующая лицензия**. Функциональность модулей Антивирус и Анти-Спам не ограничена.
  - **Срок действия пробной лицензии истек**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
  - **Срок действия лицензии истек**. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network. Функциональность модулей Антивирус и Анти-Спам доступна.
  - **Базы повреждены**. Базы Антивируса или базы Анти-Спама отсутствуют или повреждены.
  - **Ключ отсутствует**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
  - **Ключ заблокирован**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
  - **Черный список ключей поврежден или не найден**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
  - **Не удается обновить статус лицензии**. Функциональность модулей Антивирус и Анти-Спам не ограничена. Вы можете просмотреть описание ошибки в блоке **Состояние серверов** в поле **Статус лицензии.**

Используйте эти параметры в следующих задачах

Шаг 1. Активация программы 39

Окно Параметры защиты

Включить антивирусную защиту

Включение модуля Антивирус. Если флажок установлен, Антивирус начинает работать сразу после завершения работы мастера настройки программы. Если флажок снят, после завершения работы мастера настройки программы Антивирус не включается автоматически. По умолчанию флажок установлен.

Включить защиту от спама

Включение модуля Анти-Спам. Если флажок установлен, Анти-Спам начинает работать сразу после завершения работы мастера настройки программы. Если флажок снят, после завершения работы мастера настройки программы Анти-Спам не включается автоматически. По умолчанию флажок установлен.

Включить Enforced Anti-Spam Updates Service

Включение службы быстрых обновлений баз Анти-Спама (Enforced Anti-Spam Updates Service). Если флажок установлен, программа начинает использовать службу быстрых обновлений баз Анти-Спама после завершения работы мастера настройки программы. Если флажок снят, после завершения работы мастера настройки программы служба быстрых обновлений баз Анти-Спама не используется. По умолчанию флажок установлен.

Включить режим автоматического обновления баз

Включение автоматического обновления баз Антивируса и Анти-Спама с серверов "Лаборатории Касперского". Если флажок установлен, после завершения работы мастера настройки программы базы автоматически обновляются с серверов "Лаборатории Касперского". Если флажок снят, после завершения работы мастера настройки программы автоматическое обновление баз не выполняется. По умолчанию флажок установлен.

Используйте эти параметры в следующих задачах

Шаг 2. Настройка защиты сервера Microsoft Exchange..... 40

Окно Использование служб Kaspersky Security Network

В этом окне вы можете включить использование служб Kaspersky Security Network (KSN) в программе. Kaspersky Security Network – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network служит для улучшения качества обнаружения вирусов и других угроз, спама и фишинговых ссылок, а также для получения статистических данных, которые используются для выявления угроз. Использование Kaspersky Security Network регулируется специальным соглашением – Положением о Kaspersky Security Network. Чтобы включить использование Kaspersky Security Network в программе, требуется принять его условия.

Я принимаю Положение о Kaspersky Security Network и хочу использовать службы KSN для защиты

Использование служб Kaspersky Security Network в программе.

Если флажок установлен, программа использует службы Kaspersky Security Network. Если флажок снят, службы Kaspersky Security Network не используются.

По умолчанию флажок снят.

Используйте эти параметры в следующих задачах

Шаг 3. Включение служб KSN..... 41

kaspersky

Окно Параметры прокси-сервера

Соединение через прокси-сервер может использоваться при подключении программы к следующим ресурсам:

- источникам обновлений баз программы;
- службам Kaspersky Security Network;
- внешним службам Анти-Спама, таким как Enforced Anti-Spam Updates Service;
- серверам активации "Лаборатории Касперского".

Использовать прокси-сервер

Если флажок установлен, программа соединяется с источниками обновлений, службами Kaspersky Security Network, внешними службами Анти-Спама и серверами активации "Лаборатории Касперского" через прокси-сервер с учетом заданных в программе параметров.

Если флажок снят, программа выполняет соединения в соответствии с параметрами, заданными в операционной системе по умолчанию.

По умолчанию флажок снят.

Адрес прокси-сервера

IP-адрес или доменное имя прокси-сервера.

Порт

Номер порта прокси-сервера.

По умолчанию задано значение 8080.

Использовать аутентификацию

Включение / выключение аутентификации при соединении с прокси-сервером.

По умолчанию флажок снят.

Учетная запись и Пароль

Имя пользователя и пароль для аутентификации при соединении с прокси-сервером.

Кнопка 

Кнопка открывает окно операционной системы, в котором можно выбрать учетную запись из Active Directory.

Используйте эти параметры в следующих задачах

Шаг 4. Настройка параметров прокси-сервера 41

Окно Параметры уведомлений

Адрес веб-службы

Адрес веб-службы сервера Microsoft Exchange, с помощью которой программа отправляет уведомления. По умолчанию на сервере Microsoft Exchange

используется адрес `https://<имя_сервера_клиентского_доступа>/ews/exchange.asmx`.

Учетная запись и Пароль

Учетная запись, от имени которой программа отправляет уведомления, и пароль для этой учетной записи. Учетная запись должна иметь в почтовой инфраструктуре Microsoft Exchange почтовый ящик, доступный через Outlook® Web Access (OWA). Эта учетная запись также используется для отправки отчетов.

Вы можете выбрать учетную запись, нажав на кнопку ....

Адрес администратора

Адрес или список адресов электронной почты администраторов программы. Программа отправляет уведомления на эти адреса электронной почты при наступлении событий, для которых в списке адресатов установлен флажок **Администратор**. Вы можете указать несколько адресов электронной почты, разделяя их точкой с запятой.

Если вы настраиваете параметры уведомлений для нераспределенного Сервера безопасности, вы можете отправить тестовое сообщение на адрес электронной почты администратора, нажав на кнопку **Тест**.

Используйте эти параметры в следующих задачах

Шаг 5. Настройка параметров отправки уведомлений 41

Восстановление программы

Если в работе программы произошел сбой (например, были повреждены исполняемые файлы программы), вы можете восстановить программу с помощью мастера установки программы или командной строки (см. раздел "Параметры работы с командной строкой" на стр. 34).

► *Чтобы восстановить Kaspersky Security с помощью мастера установки программы, выполните следующие действия:*

1. Запустите установочный файл, входящий в пакет установки программы.

   Откроется приветственное окно пакета установки.

2. По ссылке **Kaspersky Security 9.0 для Microsoft Exchange Servers** откройте приветственное окно мастера установки программы и нажмите на кнопку **Далее**.

3. В окне **Изменение, восстановление, или удаление программы** нажмите на кнопку **Восстановить**.

4. В окне **Восстановление** нажмите на кнопку **Исправить**.

   Откроется окно **Восстановление программы**, в котором содержится информация о восстановлении программы.

5. После окончания восстановления программы в окне мастера установки программы появится сообщение о том, что восстановление программы завершено. Для завершения восстановления программы нажмите на кнопку **Завершить**.

► *Чтобы восстановить Kaspersky Security с помощью командной строки, выполните следующие действия:*

запустите установочный файл, входящий в пакет установки программы, с помощью командной строки со следующими параметрами:

```
--install-mode=repair
```

Во время удаления Kaspersky Security требуется перезапуск служб MSExchangeTransport и MSExchangeIS. Перезапуск служб выполняется автоматически без дополнительного запроса. В случае повреждения конфигурационных файлов восстановление программы невозможно. Рекомендуется удалить и установить программу заново.

Удаление программы

Вы можете удалить программу с помощью мастера установки программы, командной строки (см. раздел "Параметры работы с командной строкой" на стр. 34) или стандартных средств установки и удаления программ Microsoft Windows. Если программа установлена на нескольких серверах, нужно выполнить удаление на каждом сервере.

► *Чтобы удалить Kaspersky Security с компьютера с помощью мастера установки программы, выполните следующие действия:*

1. Запустите установочный файл, входящий в пакет установки программы.

   Откроется приветственное окно пакета установки.

2. По ссылке **Kaspersky Security 9.0 для Microsoft Exchange Servers** откройте приветственное окно мастера установки программы и нажмите на кнопку **Далее**.
3. В окне **Изменение, восстановление или удаление программы** нажмите на кнопку **Удалить**.
4. В окне **Удаление** нажмите на кнопку **Удалить**.

   Откроется окно **Удаление программы**, в котором содержится информация об удаления программы.

5. В открывшемся окне предупреждения выполните следующие действия:
   - Если вы хотите, чтобы база данных была сохранена на SQL-сервере при удалении программы, нажмите на кнопку **Да**.

     Из базы данных будут удалены данные резервного хранилища, добавленные программой. Данные статистики, добавленные программой, сохранятся.

   - Если вы хотите, чтобы база данных и данные статистики были удалены с SQL-сервера при удалении программы, нажмите на кнопку **Нет**.
6. После окончания удаления программы в окне мастера установки программы появится сообщение о том, что удаление программы завершено. Для завершения удаления программы нажмите на кнопку **Завершить**.

► *Чтобы удалить Kaspersky Security с помощью командной строки, выполните следующие действия:*

запустите установочный файл, входящий в пакет установки программы, с помощью командной строки со следующим параметром:

```
--install-mode=delete
```

При удалении Kaspersky Security с помощью командной строки база данных и данные статистики не удаляются с SQL-сервера.
Во время удаления Kaspersky Security требуется перезапуск служб MSExchangeTransport и MSExchangeIS. Перезапуск служб выполняется автоматически без дополнительного запроса.

Вы также можете удалить программу с помощью стандартных средств установки и удаления программ Microsoft Windows.

kaspersky

Поддержка протокола Kerberos

Сетевой протокол Kerberos обеспечивает простой и безопасный способ проверки подлинности при передаче данных через незащищённые сети.

Kaspersky Security может использовать протокол Kerberos при взаимодействии с Active Directory и базой данных резервного хранилища и статистики, работающей под управлением Microsoft SQL Server.

Убедитесь, что используемый Microsoft SQL Server работает с протоколом Kerberos.

Поддержка протокола Kerberos осуществляется начиная с версии Kaspersky Security 9.0 для Microsoft Exchange Servers 9.6 Patch 1 и выше. Для получения установочных файлов и инструкций по установке пакета исправлений обратитесь в службу технической поддержки.

В процессе установки пакета исправлений производится автоматическая регистрация имени субъекта-службы (SPN) для учетной записи, выбранной для запуска службы программы. Регистрация SPN является обязательным условием для использования протокола Kerberos. После завершения установки пакета исправлений, проверьте в журнале событий отсутствие ошибок при выполнении автоматической регистрации SPN. Если регистрация SPN завершилась неудачно, зарегистрируйте SPN вручную. Для этого выполните следующую команду в консоли командной строки:

```
setspn.exe -S KSE/<адрес_сервера> <имя_учетной_записи>
```

Устранение уязвимостей и установка критических обновлений в программе

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления программных модулей необходимо получать путем обращения в техническую поддержку АО «Лаборатория Касперского» по телефону (https://support.kaspersky.ru/b2b) или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ при помощи открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (https://support.kaspersky.ru/vulnerability).

Перед использованием программы на компьютере следует установить все доступные обновления операционной системы.

В этом разделе

kaspersky

Обновление программы до версии 9.0 Maintenance Release 7

Вы можете обновить Kaspersky Security для Microsoft Exchange Servers версии 9.5.1 и более поздних версий до текущей версии 9.0 Maintenance Release 7. Обновление более ранних версий программы не поддерживается.

Перед обновлением программы необходимо установить пакет Visual C++ Redistributable for Visual Studio. Требуется установка последних версий библиотек обеих битностей по следующим ссылкам: https://aka.ms/vs/17/release/vc_redist.x64.exe, https://aka.ms/vs/17/release/vc_redist.x86.exe.

Обновление программы выполняется с помощью мастера установки программы или командной строки (см. раздел "Параметры работы с командной строкой" на стр. 34).

Для корректной работы программы после ее обновления необходимо обновить базы Антивируса и Анти-Спама.

Требования к обновлению программы

Обновление программы должно выполняться с учетом следующих требований:

- Учетная запись, под которой планируется выполнять обновление программы, должна быть включена в группу Domain Admins и в группу Kse Administrators в Active Directory.

  Если обновление уже выполнено хотя бы на одном Сервере безопасности или Консоли управления в сети организации, для обновления остальных экземпляров программы на других компьютерах организации достаточно учетной записи локального администратора. При этом требуется предоставить учетной записи, предназначенной для обновления программы, права на чтение данных конфигурации Microsoft Exchange из следующего контейнера Active Directory и всех его дочерних объектов:
  `CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<root domain>`

- Обновление программы рекомендуется выполнять последовательно на всех развернутых в сети организации Серверах безопасности и Консолях управления. Если на каком-либо Сервере безопасности не удалось обновить программу, вы сможете подключиться к этому Серверу безопасности только с помощью Консоли управления предыдущей версии.
- Обновление программы на серверах Microsoft Exchange, работающих в конфигурации с группой DAG, рекомендуется провести в максимально короткий срок.
- SQL-сервер, на котором находится база данных программы, должен быть доступен в процессе обновления. В противном случае обновление завершится с ошибкой.
- Для работы программы необходимо, чтобы на всех компьютерах, на которых будет обновлена программа, а также на пути передачи данных между ними был открыт сетевой порт TCP 13100.
- В процессе обновления мастер установки программы обращается к базе данных программы. Необходимо, чтобы учетная запись, под которой планируется выполнить процедуру обновления, обладала следующими правами доступа:
  - К SQL-серверу: правами ALTER ANY LOGIN, ALTER ANY CREDENTIAL и VIEW ANY DEFINITION.
  - К базе данных: ролью db_owner.
- На всех компьютерах, на которых планируется обновление программы, должен быть установлен пакет обновлений Microsoft Windows KB2999226.

kaspersky

Перенос параметров и данных программы при обновлении до версии 9.0 Maintenance Release 7

После обновления программы до версии 9.0 Maintenance Release 7, настройки, выполненные в предыдущих версиях программы, установленных на других компьютерах в сети организации, могут быть потеряны.
Если в сети организации присутствуют компьютеры, на которых установлена предыдущая версия программы, профильные роли могут работать некорректно.

Если до обновления программы вы использовали прокси-сервер для подключения программы к службам Анти-Спама Kaspersky Security Network, Enforced Anti-Spam Updates Service, источникам обновлений и серверам активации "Лаборатории Касперского", требуется проверить настройки обновления баз программы и настройки параметров прокси-сервера (см. раздел "Настройка параметров прокси-сервера" на стр. 169) и, при необходимости, внести изменения в программе, инфраструктуре или настройках параметров прокси-сервера.

Обновление компонента Консоль управления

На компьютере, на котором установлена только Консоль управления, мастер установки выполняет только обновление Консоли управления. Мастер установки не устанавливает модули Сервера безопасности на этом компьютере.

Параметры программы после обновления Консоли управления не изменяются. Параметры интерфейса Microsoft Management Console принимают значения по умолчанию.

Обновление компонента Сервер безопасности

На компьютере с установленным Сервером безопасности мастер установки выполняет обновление всех модулей Сервера безопасности.

При обновлении мастер установки переносит значения параметров и данные предыдущей версии программы в новую версию программы следующим образом:

- Действие лицензии на предыдущую версию программы распространяется и на новую версию программы. Дата окончания срока действия лицензии сохраняется без изменений.
- База данных резервного хранилища и статистики, подключенная к программе, обновляется до версии 9.0 Maintenance Release 7.

  Если вместо обновления программы выполнить удаление программы с последующей установкой версии программы 9.0 Maintenance Release 7, база данных резервного хранилища и статистики предыдущей версии не будет обновлена до версии 9.0 Maintenance Release 7 и ее использование в программе будет невозможно.

- Программа автоматически переносит белый и черный списки адресов Анти-Спама с первого обновленного сервера группы DAG на все остальные серверы группы DAG.

- Использование Kaspersky Security Network автоматически отключается. Если вы планируете использовать KSN, вам необходимо принять условия Положения о Kaspersky Security Network в блоке **Параметры KSN** узла **Настройка**. Настройки использования KSN в Антивирусе (см. раздел "Включение и выключение использования Kaspersky Private Security Network в Антивирусе" на стр. 103) и в Анти-Спаме (см. раздел "Настройка дополнительных параметров проверки на спам и фишинг" на стр. 125) после обновления программы остаются без изменений.

  Обновление программы не влияет на настройки использования Kaspersky Private Security Network.
- Значения других параметров программы, настроенные в предыдущей версии, без изменений присваиваются соответствующим параметрам в новой версии программы.
- Данные резервного хранилища и статистики сохраняются.

Процедура обновления программы

Убедитесь, что учетная запись, под которой планируется выполнять обновление, входит в группу Domain Admins.

Во время обновления Kaspersky Security требуется перезапуск служб MSExchangeTransport и MSExchangeIS. Перезапуск служб выполняется автоматически без дополнительного запроса.

Перед выполнением обновления завершите работу Консоли управления, если Консоль управления запущена.

► *Чтобы обновить Kaspersky Security с помощью мастера установки программы, выполните следующие действия:*

1. Запустите установочный файл, входящий в пакет установки программы, на компьютере, на котором вы хотите обновить версию программы.

   Откроется окно с текстом Лицензионного соглашения.
2. Прочитайте и примите условия Лицензионного соглашения и Политики конфиденциальности, установив соответствующие флажки. Затем нажмите на кнопку **Далее**.
3. В открывшемся окне нажмите на кнопку **Установить**.

   Дальнейшие шаги по обновлению программы мастер установки программы выполнит автоматически.
4. После обновления программы нажмите на кнопку **Завершить**, чтобы закрыть мастер установки программы.

► *Чтобы обновить Kaspersky Security с помощью командной строки, выполните следующие действия:*

запустите установочный файл, входящий в пакет установки программы, с помощью командной строки со следующими параметрами:

```
--install-mode=upgrade --accept-eula --accept-privacy-policy
```

Все компоненты и модули программы, установленные на компьютере, будут обновлены.

kaspersky

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности и приведение конфигурации программы в соответствие с требованиями сертификации.

В этом разделе

Сертифицированное состояние программы

► *Чтобы убедиться, что установка программы завершилась успешно и программа готова к работе, выполните следующие действия:*

1. Убедитесь, что на компьютере, где установлены Консоль управления и Сервер безопасности, в списке установленных программ операционной системы отображается Kaspersky Security 9.0 для Microsoft Exchange Servers.
2. Убедитесь, что на компьютере, где установлены Консоль управления и Сервер безопасности, в списке служб операционной системы присутствует служба Kaspersky Security 9.0 для Microsoft Exchange Servers и эта служба запущена. Для службы должен быть настроен автоматический тип запуска.
3. Убедитесь, что для доступа к Консоли управления необходимо ввести пароль.
4. Убедитесь, что ведение журнала аудита событий включено (см. раздел "Включение и выключение ведения журнала событий аудита" на стр. 208).
5. Убедитесь, что папка хранения данных программы (см. раздел "Модули Сервера безопасности" на стр. 16) (по умолчанию – <папка установки программы>/data) исключена из проверки антивирусными программами, установленными в сети организации.
6. Убедитесь, что активный ключ (см. раздел "Активация программы с помощью ключа для Сервера безопасности" на стр. 70) добавлен.
7. Убедитесь, что антивирусная защита включена (см. раздел "Узел Защита сервера" на стр. 95).
8. Убедитесь, что базы Антивируса и Анти-Спама обновлены на всех компьютерах, где установлен Сервер безопасности.
9. Убедитесь, что использование служб глобального Kaspersky Security Network (KSN) отключено (см. раздел "Участие в Kaspersky Security Network" на стр. 99).
10. Убедитесь, что на информационной панели в узле <Имя сервера Microsoft Exchange> отсутствуют сообщения об ошибках в работе программы.
11. Отключите обновление модуля `crypto_ssl` в автоматическом режиме. Для этого создайте файл `disable_modules_autoupdate.enabler` в папке установки программы.

Перечень параметров программы, влияющих на ее сертифицированное состояние, и значения данных параметров в сертифицированном состоянии приведены в приложении (см. раздел "Приложение. Сертифицированное состояние программы: параметры и их значения" на стр. 249) к этому документу.

kaspersky

Проверка работы программы с использованием тестового файла EICAR

После установки и настройки Kaspersky Security рекомендуется проверить правильность заданных параметров программы и работоспособность программы с помощью тестового файла EICAR.

Вы может загрузить тестовый файл с официального сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Проверка работы Антивируса

Проверка работы Антивируса состоит из двух шагов:

1. Отправка сообщения с тестовым файлом.
2. Создание и просмотр отчета с информацией об обнаруженном вирусе.

► *Чтобы отправить сообщение с тестовым файлом, выполните следующие действия:*

1. Создайте сообщение электронной почты с вложенным тестовым файлом EICAR.
2. Отправьте сообщение через сервер Microsoft Exchange с установленной программой Kaspersky Security на любой почтовый ящик вашей организации, к которому вы имеете доступ.
3. Убедитесь, что доставленное сообщение не содержит тестовый файл.

   При обнаружении вируса на сервере, развернутом в роли Почтовый ящик, удаленное вложение заменяется текстовым файлом. При обнаружении вируса на сервере, развернутом в роли Транспортный концентратор, к теме сообщения добавляется префикс: `Malicious object deleted.`

► *Чтобы создать и просмотреть отчет с информацией об обнаруженном вирусе, выполните следующие действия:*

1. В дереве Консоли управления, раскройте узел Сервера безопасности, через который было отправлено сообщение с вложенным тестовым файлом EICAR.
2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Формирование и просмотр отчетов** нажмите на кнопку **Новый отчет**.
4. В открывшемся окне **Параметры формирования отчета** в раскрывающемся списке **Модуль** выберите модуль **Антивирус для роли Почтовый ящик** или **Антивирус для роли Транспортный концентратор** (в зависимости от установленной у вас конфигурации).
5. Нажмите на кнопку **OK**.

   Программа создаст отчет о работе выбранного модуля.
6. Просмотрите созданный отчет, выбрав его в списке и нажав на кнопку **Просмотреть**.

Если отчет содержит информацию о сообщении с вирусом EICAR, Антивирус работает правильно.

По умолчанию программа сохраняет копию зараженного объекта в резервном хранилище.

► *Чтобы проверить, сохранилась ли копия зараженного объекта в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли управления, раскройте узел Сервера безопасности, через который было отправлено сообщение с вложенным тестовым файлом EICAR.
2. Выберите узел **Резервное хранилище**.
3. Убедитесь, что зараженный объект (сообщение с вложенным тестовым файлом EICAR) отображается в таблице в рабочей области.

Проверка работы Анти-Спама

► *Чтобы проверить работоспособность Анти-Спама, выполните следующие действия:*

1. В дереве Консоли управления, раскройте узел Сервера безопасности, на котором вы хотите проверить работу Анти-Спама.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Черный список адресов Анти-Спама** и нажмите на кнопку **Добавить отправителя**.
4. В строке ввода укажите адрес электронной почты любого почтового ящика вашей организации, к которому вы имеете доступ, и нажмите OK.

   Указанный адрес будет добавлен в список.
5. Раскройте блок **Параметры проверки на спам**.
6. В таблице **Параметры обработки спама** для статуса **Адрес в черном списке** выберите в раскрывающемся списке действие **Пропускать** и установите флажок **Добавлять метку в тему сообщения**.
7. Отправьте тестовое сообщение с указанного почтового ящика на адрес администратора через защищаемый почтовый сервер.

Если в теме полученного сообщения содержится метка `[!!Blacklisted]`, Анти-Спам работает правильно.

kaspersky

Проверка целостности компонентов программы

Kaspersky Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько модулей или файлов программы модулями или файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов программы, в Kaspersky Security предусмотрена проверка целостности компонентов программы. Программа проверяет модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Целостность компонентов программы проверяется с помощью инструмента integrity_checker.exe, использующего для проверки файлы манифеста integrity_check_product.xml (для программы) и integrity_check_plugin.xml (для плагина KSC), защищенные криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами Администратора.

Инструмент поставляется отдельно от Kaspersky Security на сертифицированном CD-диске.

Инструмент проверки целостности рекомендуется запускать с сертифицированного CD-диска, чтобы гарантировать целостность самого инструмента. При запуске инструмента с CD-диска необходимо указать полный путь к файлу манифеста в директории программы.

► *Чтобы проверить целостность компонентов программы:*

1. Задайте папку установки программы через пользовательскую переменную окружения при помощи команды:

   ```
   set Binaries=<путь к папке установки программы>
   ```

   По умолчанию используется следующая папка установки Kaspersky Security:

   - для программы: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Microsoft Exchange Servers;
   - для плагина KSC: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSE.

2. Запустите проверку целостности компонентов программы при помощи команд:

   ```
   integrity_checker.exe --manifest <путь к файлу integrity_check_product.xml>

   integrity_checker.exe --manifest <путь к файлу integrity_check_plugin.xml>
   ```

   где параметры `--manifest <путь к файлу integrity_check_product.xml>` и `--manifest <путь к файлу integrity_check_plugin.xml>` используются для указания пути к файлам integrity_check_product.xml и integrity_check_plugin.xml, если они расположены не в одной папке с integrity_checker.exe.

Инструмент проверки целостности можно запустить со следующими дополнительными параметрами:

- `--help` – показать справку для параметров инструмента.
- `--verbose` – применить вывод расширенной информации о выполненных действиях и результатах. Если вы не укажите этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <имя файла>`, где `<имя файла>` – имя файла, используемое для записи событий, произошедших во время проверки. По умолчанию события передаются в стандартный поток stdout.

Пример команды:

```
integrity_checker.exe --manifest integrity_check_manifest.xml
--trace=.\integrity_check_trace.log
```

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

kaspersky

Администратору

Этот раздел справки адресован специалистам, которые осуществляют установку и администрирование Kaspersky Security, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security.

В этом разделе

Ролевое разграничение доступа пользователей к функциям и службам программы

Kaspersky Security позволяет разграничивать доступ пользователей к функциям и службам программы с помощью следующих ролей:

- Роли пользователей программы

Kaspersky Security 9.0 для Microsoft Exchange Servers позволяет управлять общим доступом пользователей к программе с помощью *ролей пользователей программы*. За каждой ролью закреплены набор доступных функций программы и набор доступных узлов, отображаемых в дереве Консоли управления.

Роль назначается пользователю путем добавления учетной записи этого пользователя в группу Active Directory. Один пользователь может совмещать несколько ролей. В этом случае учетную запись пользователя требуется добавить в группы Active Directory, соответствующие этим ролям. Пользователю будут предоставлены права доступа в соответствии с назначенными ролями.

Применение изменений, сделанных в группах Active Directory, может занимать до 10 минут.

В таблице ниже приведены роли и их описания, названия групп Active Directory, соответствующих ролям, а также список узлов, отображаемых в Консоли управления для каждой роли.

Для всех ролей пользователей в Консоли управления отображаются все имеющиеся профили (см. раздел "Управление профилями" на стр. 166).

Таблица 4. Роли пользователей программы

Роль	Описание	Группа Active Directory	Узлы, отображаемые в Консоли управления
Администратор	Специалист, выполняющий общие задачи администрирования программы, такие как настройка параметров Антивируса и Анти-Спама, подготовка отчетов о работе Антивируса и Анти-Спама, создание / удаление профилей, добавление в профили / удаление из профилей Серверов безопасности и настройка доступа к профилям. Задачи администратора и инструкции по их выполнению описаны в разделе Администратору (на стр. 57).	Kse Administrators	Профили <Имя Сервера безопасности> Защита сервера Обновления Уведомления Резервное хранилище Отчеты Настройка Лицензирование
Специалист по антивирусной безопасности	Специалист, имеющий права доступа к следующим функциям программы: просмотр сведений о состоянии защиты серверов Microsoft Exchange, получение отчетов о работе Антивируса, Анти-Спама и фильтрации вложений и содержимого; права ограниченного доступа к функциям управления объектами в резервном хранилище (за исключением удаления объектов), а также права доступа ко всем параметрам программы без возможности их изменения.	Kse AV Security Officers	Профили <Имя Сервера безопасности> Защита сервера Обновления Уведомления Резервное хранилище Отчеты Настройка Лицензирование
Оператор антивирусной безопасности	Специалист, имеющий права доступа на просмотр сведений о состоянии защиты серверов Microsoft Exchange и на получение отчетов о работе Антивируса, Анти-Спама и фильтрации вложений и содержимого.	Kse AV Operators	Профили <Имя Сервера безопасности> Отчеты

Группы пользователей в Active Directory создаются автоматически при установке или обновлении программы до Kaspersky Security 9.0 для Microsoft Exchange Servers. Эти группы также могут быть созданы вручную (см. раздел "Сценарий развертывания программы с ограниченным набором прав доступа" на стр. 23) перед установкой программы с помощью стандартных средств управления данными Active Directory. Группы могут быть созданы в любом домене организации. Тип групп – "Универсальная".

При запуске Консоли управления программа проверяет, в какую из этих групп входит учетная запись пользователя, с правами которой запущена Консоль управления, и на основе этой информации определяет роль пользователя в программе.

Имена групп учетных записей должны оставаться уникальными в рамках леса Active Directory.

- Профильные роли

Набор *профильных ролей* позволяет управлять доступом пользователей к отдельным профилям. За каждой ролью закреплены набор доступных функций программы и набор доступных узлов, отображаемых в дереве Консоли управления в рамках профиля.

Роль назначается пользователям при настройке доступа (см. раздел "Управление доступом к профилю" на стр. 172) к определенному профилю. Один пользователь может совмещать несколько ролей, а также иметь доступ к нескольким профилям.

В таблице ниже приведены профильные роли и их описания, а также список узлов, отображаемых в Консоли управления для каждой роли в рамках профиля.

Таблица 5. Профильные роли

Роль	Описание	Узлы профиля, отображаемые в Консоли управления
Администратор профиля	Специалист, выполняющий общие задачи администрирования программы в рамках профиля, такие как настройка параметров Антивируса и Анти-Спама или подготовка отчетов о работе Антивируса и Анти-Спама.	Защита сервера Обновления Уведомления Резервное хранилище Отчеты Настройка Лицензирование Серверы
Специалист антивирусной безопасности профиля	Специалист, имеющий права доступа к следующим функциям программы в рамках профиля: просмотр сведений о состоянии защиты серверов Microsoft Exchange, получение отчетов о работе Антивируса, Анти-Спама и фильтрации вложений и содержимого; права ограниченного доступа к функциям управления объектами в резервном хранилище (за исключением удаления объектов), а также права доступа ко всем параметрам программы без возможности их изменения.	Защита сервера Обновления Уведомления Резервное хранилище Отчеты Настройка Лицензирование Серверы
Оператор антивирусной безопасности профиля	Специалист, имеющий права доступа на просмотр сведений о состоянии защиты серверов Microsoft Exchange и на получение отчетов о работе Антивируса, Анти-Спама и фильтрации вложений и содержимого в рамках профиля.	Отчеты Серверы

При запуске Консоли управления программа проверяет, какая профильная роль назначена учетной записи пользователя, с правами которой запущена Консоль управления, и на основе этой информации определяет права доступа пользователя к профилям.

Для корректной работы ролевого разграничения доступа пользователей к профилям требуется убедиться, что пользователи не добавлены в группы Kse Administrators, Kse AV Security Officers или Kse AV Operators в Active Directory. В противном случае пользователи будут иметь доступ ко всем имеющимся профилям.

- Системная роль

Системной ролью должна обладать учетная запись, от имени которой запускается служба программы Kaspersky Security 9.0 для Microsoft Exchange Servers.

Системная роль назначается выбранной вами учетной записи во время установки программы (см. раздел "Шаг 6. Выбор учетной записи для запуска службы Kaspersky Security" на стр. 32). Если после установки программы вы хотите указать для запуска службы программы другую учетную запись, требуется назначить ей системную роль. Назначение системной роли выполняется путем добавления учетной записи пользователя в группу Kse Watchdog Service в Active Directory.

Применение изменений, сделанных в группах Active Directory, может занимать до 10 минут.

Работа с персональными данными пользователей

Kaspersky Security обрабатывает следующие персональные данные пользователей для выполнения своих основных функций:

- Учетные записи Active Directory.

  Программа проверяет учетные записи Active Directory для реализации ролевого разграничения доступа пользователей к функциям и службам программы.

- Сообщения электронной почты.

  Программа проверяет сообщения электронной почты, включая вложенные объекты, для обеспечения антивирусной защиты, фильтрации вложений и содержимого, а также защиты от спама и фишинга в соответствии с заданными настройками.

  Оригиналы сообщений, вызвавшие срабатывание одного из компонентов защиты, сохраняются в файловой системе Сервера безопасности. Это обеспечивает возможность восстановления удаленных объектов через резервное хранилище.

- Метаданные сообщений электронной почты.

  Метаданные сообщений электронной почты (поля От, Кому, Тема), вызвавшие срабатывание одного из компонентов защиты, сохраняются в базе данных программы. Это обеспечивает возможность восстановления удаленных объектов через резервное хранилище.

  Метаданные сообщений могут передаваться в Kaspersky Security Center как часть информации о событиях в работе программы, если в организации используется данное программное решение.

  Метаданные сообщений также сохраняются в журнале программы, что необходимо для оказания технической поддержки.

- Адреса электронной почты, исключенные из проверки.

  Адреса электронной почты, исключенные администратором из проверки, сохраняются в Active Directory наряду с другими значениями параметров защиты.

- Имена почтовых ящиков.

  Программа сохраняет имена почтовых ящиков, выбранных для фоновой проверки, для обеспечения корректности проверки.

- Изменения настроек программы.

Информация об изменении настроек сохраняется в журналах программы и в журнале событий Windows. В зависимости от сделанных изменений, информация может содержать адреса электронной почты, исключенные из проверки, и имена почтовых ящиков, выбранных для фоновой поверки.

Аналогичная информация может содержаться в файле экспорта конфигурации программы (`*.kseconfig`).

- Тексты сообщений.

  Тексты обрабатываемых сообщений электронной почты могут сохраняться на Сервере безопасности, если администратор включил подробную запись событий в журналы программы. Данная информация может быть использована для оказания технической поддержки.

- Информация о представителе организации.

  Информация о контактном лице организации, заключившей Лицензионное соглашение, используется для подтверждения актуальности лицензии. В зависимости от конфигурации программы, информация хранится либо в Active Directory, либо локально на Сервере безопасности.

Для ознакомления с особенностями хранения перечисленных данных см. таблицу ниже.

Таблица 6. Особенности хранения персональных данных пользователей в Kaspersky Security

Компонент, использующий персональные данные	Место хранения данных	Срок хранения данных	Обеспечение защиты данных
Файлы конфигурации	<Папка установки программы>\Configuration	Бессрочно.	Защита данных при работе с Консолью управления Kaspersky Security достигается путем ролевого разграничения доступа пользователей к функциям и службам программы. Администратору Kaspersky Security необходимо обеспечить безопасность этих данных самостоятельно.
Резервное хранилище	<Папка установки программы>\data\store\persistent	Бессрочно, если администратором Kaspersky Security не установлено ограничение.	
Статистика и метаданные объектов резервного хранилища	База данных SQL, указанная при установке программы.	Бессрочно, если администратором SQL-сервера не установлено ограничение.	
Отчеты	%Temp%	До перезагрузки программы.	
Журнал событий и аудита	<Папка установки программы>\logs	365 дней, если администратором Kaspersky Security не установлено другие значение.	
Временные файлы	%Temp% <Папка установки программы>\data\temp	До перезагрузки программы или окончания операции, которая использует временные файлы.	

Вы можете ограничить работу программы с персональными данными пользователей следующим образом:

- Изменить срок хранения журналов программы.
- Ограничить срок хранения объектов в резервном хранилище (см. раздел "Настройка параметров резервного хранилища" на стр. 198).
- Удалять объекты (см. раздел "Удаление объектов из резервного хранилища" на стр. 196) из резервного хранилища.
- Контролировать список пользователей, добавленных в белый и черный список Анти-Спама.
- Контролировать список пользователей, сообщения для которых исключены из антивирусной проверки (см. раздел "Настройка исключений по адресам получателей" на стр. 114).
- Контролировать список пользователей, к сообщениям от / для которых применяются правила фильтрации вложений и содержимого (см. раздел "Настройка списков пользователей для правила фильтрации вложений и содержимого" на стр. 158).
- Если вам необходимо изменить контактное лицо организации, обратитесь к поставщику лицензии.

kaspersky

Лицензирование программы

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

В этом разделе

Схемы лицензирования. Ограничения лицензий

Все схемы лицензирования программы используют *ограничение по количеству почтовых ящиков* (см. раздел "*Просмотр количества почтовых ящиков*" на стр. 78), защищаемых с помощью программы.

Лицензирование Сервера безопасности:

- **Пробная лицензия**. Лицензия для пробного использования программы. Предоставляется на период, который назначает "Лаборатория Касперского". По истечении срока действия пробной лицензии программа прекращает выполнять все свои функции. Вы можете активировать программу с помощью ключа или кода активации.
- **Коммерческая**. Лицензия для коммерческого использования программы. Предоставляется на период, который назначает "Лаборатория Касперского" при приобретении лицензии. По окончании срока действия коммерческой лицензии программа продолжает работу, но с ограниченной

функциональностью. Обновление баз программы, получение новых версий программы, а также обращение в Службу технической поддержки становятся недоступными. Вы можете активировать программу с помощью ключа или кода активации.

- **Коммерческая (по подписке)**. Лицензия для коммерческого использования программы, которая распространяется через поставщиков услуг по подписке. Предоставляется на период, который назначает поставщик услуг по подписке. В соответствии с лицензионным ограничением вы можете использовать программу в течение периода, на который вы приобрели подписку у поставщика услуг. Вы можете активировать программу с помощью кода активации, вы не можете активировать программу с помощью ключа.

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

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

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

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

kaspersky

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Security.

Лицензия включает в себя следующие права:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки ;
- обновление баз и предоставление новых версий программы.

Чтобы работать с программой в режиме полной функциональности, вам нужно приобрести лицензию на использование программы и активировать программу. Лицензия имеет ограниченный срок действия.

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

Перед приобретением лицензии вы можете бесплатно ознакомиться с пробной версией Kaspersky Security. Пробная версия Kaspersky Security выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Security прекращает выполнять все свои функции. Для продолжения использования программы вам нужно приобрести лицензию.

О ключе

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

Чтобы добавить ключ в программу, нужно применить *файл ключа* (см. раздел "*Активация программы с помощью ключа для Сервера безопасности*" на стр. 70) или добавить ключ по коду активации (см. раздел "Активация программы с помощью кода активации" на стр. 71).

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

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

Лицензионный ключ может быть активным и резервным.

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

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

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве

резервного лицензионного ключа.

Для активации программы используется **Ключ Сервера безопасности**. В зависимости от схемы развертывания программы (см. раздел «Типовые схемы и сценарии развертывания программы» на стр. 19) для активации программы вам нужно добавить (см. раздел «Активация программы с помощью ключа для Сервера безопасности» на стр. 70) следующие ключи:

- Если программа используется на одиночных серверах Microsoft Exchange, требуется добавить ключ Сервера безопасности на каждом сервере.
- Если программа используется на серверах Microsoft Exchange, входящих в группу DAG, требуется добавить один ключ Сервера безопасности. Действие ключей распространяется на всю группу DAG (см. раздел "Особенности установки программы в группе доступности баз данных Microsoft Exchange" на стр. 20).
- Если вы используете профили для управления несколькими Серверами безопасности, требуется добавить один ключ Сервера безопасности. Действие ключей распространяется на все Серверы безопасности профиля (см. раздел "Особенности активации программы при использовании профилей" на стр. 69).

О файле ключа

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

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

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

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

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

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

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. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security или после заказа пробной версии Kaspersky Security.

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

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 251).

kaspersky

О подписке

Подписка на Kaspersky Security - это предоставление услуги пользования программой на основании лицензии *Коммерческая по подписке*. Лицензия ограничена в использовании количеством почтовых ящиков, защищаемых Kaspersky Security. Подписку на Kaspersky Security можно оформить у поставщика услуг (например, у поставщика услуги защиты почты).

Вы можете активировать программу с помощью кода активации.

Если вы используете программу на основании лицензии типа **Коммерческая (по подписке)**, Kaspersky Security обращается к серверам активации "Лаборатории Касперского" через определенные промежутки времени, чтобы обновлять данные о лицензии.

Если вы используете программу на основании лицензии типа **Коммерческая (по подписке)**, вам требуется обеспечить постоянный доступ в интернет Серверу безопасности и серверу, на котором установлена Консоль управления.

Если ваша подписка еще не истекла, но в течение продолжительного периода времени программа не обновляла данные и не получила подтверждение о том, что подписка еще не истекла, от серверов активации "Лаборатории Касперского" (например, если нет доступа в интернет у Сервера безопасности и у сервера, на котором установлена Консоль управления), то программа прекращает попытки связаться с серверами активации "Лаборатории Касперского", прекращает обновлять антивирусные базы, базы Анти-Спама и использовать Kaspersky Security Network. Если программа получает доступ в интернет после того, как прекратила попытки связаться с серверами активации "Лаборатории Касперского", то программа обновляет данные о лицензии, возобновляет обновление баз Антивируса, баз Анти-Спама и восстанавливает использование Kaspersky Security Network, в программе доступна функциональность модулей Антивирус и Анти-Спам.

Вы можете приостанавливать или возобновлять подписку, продлевать ее, а также отказаться от нее. Для управления подпиской вам нужно связаться с поставщиком, который предоставил услугу пользования Kaspersky Security. В зависимости от того, услугами какого поставщика вы пользуетесь, набор возможных действий при управлении подпиской может различаться.

Чтобы вы могли продлить подписку, вам может предоставляться *льготный период* – период действия, в течение которого программа продолжает выполнять все свои функции. Наличие и длительность льготного периода определяет поставщик услуг. По истечении подписки или льготного периода для продления подписки Kaspersky Security продолжает работу, но прекращает обновлять антивирусные базы программы и использовать Kaspersky Security Network.

Особенности активации программы при использовании профилей

Если вы используете профили (см. раздел «Управление профилями» на стр. 157) для управления несколькими Серверами безопасности, требуется учитывать следующие особенности активации программы:

- Срок действия лицензии отсчитывается с момента добавления активного ключа. Автоматическая замена активных ключей на резервные при истечении срока действия лицензии осуществляется на

каждом из Серверов безопасности, включенных в профиль, по времени сервера Microsoft Exchange, на котором установлен Сервер безопасности. Важно учитывать это, например, если Серверы безопасности, включенные в профиль, находятся в разных часовых поясах.

- В Консоли управления в рабочей области узла **Профили \ <Имя профиля> \ Лицензирование** ключи и даты окончания срока действия лицензии, соответствующие каждому из добавленных ключей, отображаются по времени Консоли управления. Например, если по времени Консоли управления истек срок действия лицензии, определяемый активным ключом, и добавлен резервный ключ, то в рабочей области отображается только резервный ключ и его свойства.
- Вы не можете добавить, заменить или удалить ключ отдельно для Сервера безопасности, добавленного в профиль. Вы можете добавить, заменить или удалить ключ только для всех Серверов безопасности, включенных в профиль, при этом лицензия распространяется на все Серверы безопасности профиля.
- После того как вы добавили Сервер безопасности в профиль, активный ключ этого Сервера безопасности заменяется на активный ключ, добавленный для всего профиля.
- После того как вы удалили Сервер безопасности из профиля, для Сервера безопасности остается активным тот ключ, который был добавлен для профиля. Ключ отображается в рабочей области узла **Лицензирование** этого Сервера безопасности.

Активация программы с помощью ключа для Сервера безопасности

Если программа Kaspersky Security установлена в конфигурации с группой DAG, достаточно добавить один ключ Сервера безопасности для всех серверов группы DAG. Вы можете добавить ключи, подключив Консоль управления к любому из серверов, входящих в эту группу DAG.
Если вы создаете группу DAG из серверов, на которых программа уже была установлена и активирована ранее, требуется активировать программу для этой группы. Для этого нужно добавить один ключ Сервера безопасности после добавления первого сервера в группу DAG.

Перед активацией программы подготовьте файл ключа. Если у вас имеется только код активации для пробной или коммерческой лицензии, вы можете сгенерировать файл ключа по коду активации. Чтобы сгенерировать файл ключа по коду активации, вы можете использовать сайт "Лаборатории Касперского" https://activation.kaspersky.com/.

► *Чтобы добавить ключ, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите добавить ключ Сервера безопасности, раскройте узел того Сервера безопасности, для которого вы хотите добавить ключ,
   - Если вы хотите добавить ключ Сервера безопасности для профиля, выполните следующие действия:
     a. Раскройте узел **Профили**.
     b. Раскройте узел того профиля, для которого вы хотите добавить ключ.
2. Выберите узел **Лицензирование**.
3. В рабочей области выполните одно из следующих действий:

- Чтобы добавить активный ключ Сервера безопасности, выполните следующие действия:

  a. Нажмите на кнопку **Добавить** в блоке **Активный ключ**.

     Откроется окно **Добавление лицензии**

  b. В открывшемся окне **Добавление лицензии** в блоке **Выберите файл ключа** нажмите на кнопку **Добавить**.

- Чтобы добавить резервный ключ Сервера безопасности, нажмите на кнопку **Добавить** в блоке **Резервный ключ**.

  Резервный ключ Сервера безопасности может быть добавлен только при наличии активного ключа Сервера безопасности. В качестве резервного ключа может быть добавлен только ключ для коммерческой лицензии. Ключ для пробной лицензии не может быть добавлен в качестве резервного.

4. В открывшемся окне в поле **Имя файла** укажите путь к файлу ключа (файл с расширением key) и нажмите на кнопку **Открыть**.
5. Если вы добавляете активный ключ Сервера безопасности, нажмите кнопку **Далее.**

Ключ будет добавлен, информация о нем появится в блоке, соответствующем типу ключа.

См. также

Просмотр информации о добавленных ключах 73
Активация программы с помощью кода активации..... 71
Замена ключа 73
Удаление ключа 74
Настройка уведомления о скором истечении срока действия лицензии..... 72
Просмотр количества почтовых ящиков..... 78

Активация программы с помощью кода активации

Если вы активируете программу с помощью кода активации, вам требуется учитывать особенности активации программы:

- Если вы активировали программу на Сервере безопасности с помощью кода активации, вы не можете добавить резервный ключ. Вы можете добавить резервный ключ только в случае, если вы использовали файл ключа, чтобы активировать программу для Сервера безопасности.
- Вы можете заменить код активации на файл ключа на сайте "Лаборатории Касперского" https://activation.kaspersky.com/.

► *Чтобы активировать программу с помощью кода активации, выполните следующие действия:*

1. В дереве Консоли управления выполните одно из следующих действий:

- Если вы хотите активировать программу с помощью кода активации для Сервера безопасности, раскройте узел того Сервера безопасности, для которого вы хотите активировать программу.
- Если вы хотите активировать программу с помощью кода активации для Серверов безопасности профиля, выполните следующие действия:
  a. Раскройте узел **Профили**.
  b. Раскройте узел того профиля, для которого вы хотите активировать программу.

2. Выберите узел **Лицензирование**.
3. Чтобы активировать с помощью кода активации Сервер безопасности, нажмите на кнопку **Добавить** в блоке **Активный ключ**.
4. В открывшемся окне выберите вариант **Введите код активации**.
5. Введите код активации в поля для ввода текста и нажмите **Далее**.

   Если вы активируете программу по коду активации, вам требуется обеспечить постоянный доступ в интернет Серверу безопасности и серверу, на котором установлена Консоль управления.

6. Программа отправит запрос на активацию на сервер активации "Лаборатории Касперского". При успешном выполнении запроса на активацию программа уведомит вас об этом.
7. Нажмите на кнопку **Добавить**, чтобы активировать лицензию.

В окне узла **Лицензирование** в блоке **Активный ключ** отобразится информация о добавленном ключе.

См. также

Уведомления 172

Об уведомлениях, связанных с лицензией

Программа позволяет своевременно узнавать о событиях и об ошибках, связанных с лицензией, с помощью уведомлений.

Программа записывает эти уведомления в журнал и отправляет их по электронной почте, если отправка уведомлений о событиях, связанных с лицензией, настроена (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 175).

Настройка уведомления о скором истечении срока действия лицензии

► *Чтобы настроить уведомление о скором истечении срока действия лицензии, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить уведомление о скором истечении срока действия лицензии, действующей на нераспределенном Сервере безопасности, выберите узел этого Сервера безопасности;

- если вы хотите настроить уведомление о скором истечении срока действия лицензии, действующей на профиле, раскройте узел **Профили** и в нем выберите узел соответствующего профиля.

2. Выберите узел **Уведомления**.

   В рабочей области отобразятся блоки **Параметры отправки уведомлений** и **Уведомления о событиях**.

3. Раскройте блок **Уведомления о событиях** и выполните в нем следующие действия:

   a. В левой части блока в списке **Темы уведомлений** выберите событие **События, связанные с лицензией**.

   b. В правой части блока выберите адресатов уведомлений (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 175).

   c. В правой части блока в поле **Уведомить заранее об истечении срока действия лицензии (дни)** укажите, за сколько дней до окончания срока действия лицензии вы хотите получать уведомление.

4. Нажмите на кнопку **Сохранить**.

Просмотр информации о добавленных ключах

► *Чтобы просмотреть информацию о добавленных ключах, выполните следующие действия:*

1. В дереве Консоли управления выполните одно из следующих действий:

   - Если вы хотите просмотреть информацию о ключах, добавленных для Сервера безопасности, раскройте узел Сервера безопасности, информацию о ключах которого вы хотите просмотреть.
   - Если вы хотите просмотреть информацию о ключах профиля, выполните следующие действия:

     a. раскройте узел **Профили;**

     b. раскройте узел того профиля, информацию о ключах которого вы хотите просмотреть.

2. Выберите узел **Лицензирование**.

   В рабочей области отобразится информация о количестве почтовых ящиков и добавленных ключах.

Замена ключа

► *Чтобы заменить ключ, добавленный для Сервера безопасности, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел того Сервера безопасности, для которого хотите добавить ключ.
2. Выберите узел **Лицензирование**.
3. В рабочей области выполните одно из следующих действий:

   - Чтобы заменить активный ключ Сервера безопасности, выполните следующие действия:

     a. Нажмите на кнопку **Заменить** в блоке **Активный ключ**.

        Откроется окно **Добавление лицензии.**

b. В открывшемся окне **Добавление лицензии** в блоке **Выберите файл ключа** нажмите на кнопку **Заменить**.

- Чтобы заменить резервный ключ Сервера безопасности, нажмите на кнопку **Заменить** в блоке **Резервный ключ**.

4. В открывшемся окне в поле **Имя файла** укажите путь к файлу ключа (файл с расширением key) и нажмите на кнопку **Открыть**.
5. Если вы заменяете активный ключ Сервера безопасности, нажмите кнопку **Далее.**

Ключ будет заменен, информация о новом ключе появится в соответствующем блоке.

► *Чтобы заменить ключ, добавленный для профиля, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили**.
2. Раскройте узел профиля, ключ для которого вы хотите заменить.
3. Выберите узел **Лицензирование**.
4. В рабочей области выполните одно из следующих действий:
   - Чтобы заменить активный ключ Сервера безопасности, выполните следующие действия:
     a. Нажмите на кнопку **Заменить** в блоке **Активный ключ**.

        Откроется окно **Добавление лицензии.**

     b. В открывшемся окне **Добавление лицензии** в блоке **Выберите файл ключа** нажмите на кнопку **Заменить**.
   - Чтобы заменить резервный ключ Сервера безопасности, нажмите на кнопку **Заменить** в блоке **Резервный ключ**.
5. В открывшемся окне в поле **Имя файла** укажите путь к файлу ключа (файл с расширением key) и нажмите на кнопку **Открыть**.
6. Если вы заменяете активный ключ Сервера безопасности для профиля, нажмите кнопку **Далее.**

Ключ будет заменен, информация о новом ключе появится в соответствующем блоке.

Удаление ключа

► *Чтобы удалить ключ, добавленный для Сервера безопасности, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел того Сервера безопасности, для которого хотите удалить ключ.
2. Выберите узел **Лицензирование**.
3. В рабочей области выполните одно из следующих действий:
   - Чтобы удалить активный ключ Сервера безопасности, нажмите на кнопку **Удалить** в блоке **Активный ключ**.
   - Чтобы удалить резервный ключ Сервера безопасности, нажмите на кнопку **Удалить** в блоке **Резервный ключ**.

Программа удалит выбранный ключ. При удалении активного ключа резервный ключ (если он добавлен) становится активным.

► *Чтобы удалить ключ, добавленный для профиля, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили**.
2. Раскройте узел профиля, ключ для которого вы хотите удалить.
3. Выберите узел **Лицензирование**.
4. В рабочей области выполните одно из следующих действий:
   - Чтобы удалить активный ключ Сервера безопасности, нажмите на кнопку **Удалить** в блоке **Активный ключ**.
   - Чтобы удалить резервный ключ Сервера безопасности, нажмите на кнопку **Удалить** в блоке **Резервный ключ**.

Программа удалит выбранный ключ. При удалении активного ключа резервный ключ (если он добавлен) становится активным.

Узел Лицензирование

Количество почтовых ящиков на сервере / Количество почтовых ящиков на серверах профиля

Количество почтовых ящиков на сервере, подсчитанное программой, используется программой для сравнения количества почтовых ящиков на сервере и лицензионных ограничений ключа.

При подсчете лицензионных ограничений программа учитывает следующие типы почтовых ящиков:

- UserMailbox;
- LinkedMailbox;
- SharedMailbox;
- RoomMailbox;
- EquipmentMailbox.

Программа не учитывает служебные ящики и общие папки при подсчете лицензионных ограничений.

Учитывайте следующие особенности подсчета количества почтовых ящиков:

- на отдельном Сервере безопасности (например, на сервере в роли Почтовый ящик), программа учитывает почтовые ящики, находящиеся на данном сервере;
- на сервере в роли Транспортный концентратор количество почтовых ящиков всегда 0;
- на сервере в роли Пограничный транспорт количество почтовых ящиков всегда 0;
- на сервере, входящем в группу DAG, программа учитывает почтовые ящики, находящиеся в активном хранении на данном сервере;
- в профиле (см. раздел "Управление профилями" на стр. 157) программа учитывает почтовые ящики, находящиеся на всех серверах, входящих в профиль.

Чтобы подсчитать количество почтовых ящиков, программа использует команду `Get-MailboxDatabase` для PowerShell, которая входит в состав сервера Microsoft Exchange. Вы можете использовать эту команду для просмотра количества почтовых ящиков на защищаемом сервере Microsoft Exchange:

Команда:

```
@(@(Get-MailboxDatabase | ?{$_.Server -eq "$env:computername"}) | %{Get-
Mailbox -Database $_ -ResultSize Unlimited -RecipientTypeDetails
UserMailbox,LinkedMailbox,SharedMailbox,RoomMailbox,EquipmentMailbox}).Count
```

Блоки **Активный ключ** и **Резервный ключ** содержат сведения об активном и резервном ключах Сервера безопасности, добавленных в программу, а также информацию о лицензиях, связанных с этими ключами. Также в этих блоках можно добавлять, обновлять, заменять и удалять ключи.

Блок **Резервный ключ** отсутствует, если не добавлен активный ключ Сервера безопасности.

Обновить

Кнопка, по которой вы можете обновить информацию о ключе.

Статус

- Поле **Статус** отображается только для активных ключей. Возможны следующие статусы ключа Сервера безопасности и соответствующие им ограничения программы:
  - **Действующая лицензия**. Функциональность модулей Антивирус и Анти-Спам не ограничена.
  - **Срок действия пробной лицензии истек**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
  - **Срок действия лицензии истек**. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network. Функциональность модулей Антивирус и Анти-Спам доступна.
  - **Базы повреждены**. Базы Антивируса или базы Анти-Спама отсутствуют или повреждены.
  - **Ключ отсутствует**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
  - **Ключ заблокирован**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
  - **Черный список ключей поврежден или не найден**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
  - **Не удается обновить статус лицензии**. Функциональность модулей Антивирус и Анти-Спам не ограничена. Вы можете просмотреть описание ошибки в блоке **Состояние серверов** в поле **Статус лицензии.**

Ключ

Уникальная буквенно-цифровая последовательность.

Тип лицензии

Может принимать следующие значения:

- **Пробная лицензия**. Лицензия для пробного использования программы. Предоставляется на период, который назначает "Лаборатория Касперского". По истечении срока действия пробной лицензии программа прекращает выполнять все свои функции. Вы можете активировать программу с помощью ключа или кода активации.

- **Коммерческая**. Лицензия для коммерческого использования программы. Предоставляется на период, который назначает "Лаборатория Касперского" при приобретении лицензии. По окончании срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Обновление баз программы, получение новых версий программы, а также обращение в Службу технической поддержки становятся недоступными. Вы можете активировать программу с помощью ключа или кода активации.
- **Коммерческая (по подписке)**. Лицензия для коммерческого использования программы, которая распространяется через поставщиков услуг по подписке. Предоставляется на период, который назначает поставщик услуг по подписке. В соответствии с лицензионным ограничением вы можете использовать программу в течение периода, на который вы приобрели подписку у поставщика услуг. Вы можете активировать программу с помощью кода активации, вы не можете активировать программу с помощью ключа.

Представитель

Контактное лицо организации, заключившей Лицензионное соглашение.

Количество почтовых ящиков

Максимальное количество почтовых ящиков, которые может защитить программа по этому ключу.

Дата окончания

Дата окончания срока действия лицензии.

Добавить / Заменить

Кнопка, по которой вы можете добавить / заменить активный или резервный ключ.

Удалить

Кнопка, по которой вы можете удалить активный или резервный ключ.

Окно Добавление Лицензии

Выберите файл ключа

Кнопка, по которой вы можете добавить файл ключа.

Введите код активации

Поля ввода, в которые вы можете ввести код активации.

Если вы активируете программу с помощью кода активации, вам требуется учитывать особенности активации программы:

- Если вы используете программу на основании лицензии типа Коммерческая (по подписке), вы можете активировать программу с помощью кода активации. Вы не можете активировать программу с помощью ключа.
- Если вы активировали программу на Сервере безопасности с помощью кода активации, вы не можете активировать резервный ключ. Вы можете активировать резервный ключ только в случае, если вы использовали ключ, чтобы активировать программу для Сервера безопасности.
- Вы можете заменить код активации на файл ключа. Чтобы сгенерировать файл ключа по коду активации, вы можете использовать сайт "Лаборатории Касперского" https://activation.kaspersky.com/.

Если вы активируете программу по коду активации, вам требуется обеспечить постоянный доступ в интернет Серверу безопасности и серверу, на котором установлена Консоль управления.

Назад

Кнопка для возврата к выбору ключа или полям ввода для кода активации.

Далее

Для активации, нажмите на кнопку **Далее**.

Просмотр количества почтовых ящиков

Вы можете сравнить количество почтовых ящиков, которые располагаются на вашем Сервере безопасности, и количество почтовых ящиков, на которые распространяется ваша лицензия.

► *Чтобы просмотреть информацию о количестве почтовых ящиков, подсчитанных программой, выполните следующие действия:*

1. В дереве Консоли управления выполните одно из следующих действий:
   - Если вы хотите просмотреть информацию о количестве почтовых ящиков на отдельном Сервере безопасности (например, на сервере в роли Почтовый ящик или на сервере, входящем в группу DAG), раскройте узел Сервера безопасности, для которого вы хотите просмотреть информацию о количестве почтовых ящиков.
   - Если вы хотите просмотреть информацию о количестве почтовых ящиков профиля, выполните следующие действия:
     a. Раскройте узел **Профили.**
     b. Раскройте узел профиля, для которого вы хотите просмотреть информацию о количестве почтовых ящиков.
2. Выберите узел **Лицензирование**.

В рабочей области отобразится информация о количестве почтовых ящиков, подсчитанных программой на вашем сервере, и информация о добавленных ключах.

При подсчете лицензионных ограничений программа учитывает следующие типы почтовых ящиков:

- UserMailbox;
- LinkedMailbox;
- SharedMailbox;
- RoomMailbox;
- EquipmentMailbox.

Программа не учитывает служебные ящики и общие папки при подсчете лицензионных ограничений.

Учитывайте следующие особенности подсчета количества почтовых ящиков:

- на отдельном Сервере безопасности (например, на сервере в роли Почтовый ящик), программа учитывает почтовые ящики, находящиеся на данном сервере;

- на сервере в роли Транспортный концентратор количество почтовых ящиков всегда 0;
- на сервере в роли Пограничный транспорт количество почтовых ящиков всегда 0;
- на сервере, входящем в группу DAG, программа учитывает почтовые ящики, находящиеся в активном хранении на данном сервере;
- в профиле (см. раздел "Управление профилями" на стр. 157) программа учитывает почтовые ящики, находящиеся на всех серверах, входящих в профиль.

Чтобы подсчитать количество почтовых ящиков, программа использует команду `Get-MailboxDatabase` для PowerShell, которая входит в состав сервера Microsoft Exchange. Вы можете использовать эту команду для просмотра количества почтовых ящиков на защищаемом сервере Microsoft Exchange:

Команда:

```
@(@(Get-MailboxDatabase | ?{$_.Server -eq "$env:computername"}) | %{Get-
Mailbox -Database $_ -ResultSize Unlimited -RecipientTypeDetails
UserMailbox,LinkedMailbox,SharedMailbox,RoomMailbox,EquipmentMailbox}).Count
```

См. также

kaspersky

Запуск и остановка программы

Этот раздел содержит информацию о том, как запустить программу и как завершить работу с ней.

В этом разделе

Запуск и остановка Сервера безопасности

Запуск Сервера безопасности выполняется автоматически в следующих случаях:

- после установки программы;
- при запуске операционной системы на компьютере с установленным Сервером безопасности, если в параметрах службы "Kaspersky Security для Microsoft Exchange Servers" установлен типа запуска **Автоматически**.

► *Чтобы остановить Сервер безопасности вручную, выполните следующие действия:*

1. В Консоли управления отключите антивирусную защиту (см. раздел "Включение и выключение антивирусной защиты сервера" на стр. 107) и защиту от спама (см. раздел "Включение и выключение защиты сервера от спама" на стр. 121) на Сервере безопасности.
2. На компьютере, на котором установлен Сервер безопасности, средствами операционной системы остановите службу "Kaspersky Security для Microsoft Exchange Servers" и установите для нее тип запуска **Отключено**.

   Сервер безопасности будет остановлен.

► *Чтобы запустить Сервер безопасности вручную, выполните следующие действия:*

1. На компьютере, на котором установлен Сервер безопасности, средствами операционной системы запустите службу "Kaspersky Security для Microsoft Exchange Servers" и установите для нее тип запуска **Автоматически**.

   Сервер безопасности будет запущен.
2. В Консоли управления включите антивирусную защиту (см. раздел "Включение и выключение антивирусной защиты сервера" на стр. 107) и защиту от спама (см. раздел "Включение и выключение защиты сервера от спама" на стр. 121) на Сервере безопасности.

   Сервер Microsoft Exchange будет защищен.

kaspersky

Запуск Консоли управления

Запуск Консоли управления возможен только от имени учетной записи, которой назначена роль "Администратор" (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58).

► *Чтобы запустить Консоль управления,*

выберите **Пуск → Программы → Kaspersky Security 9.0 для Microsoft Exchange Servers → Kaspersky Security 9.0 для Microsoft Exchange Servers**.

При запуске Консоли управления оснастка Kaspersky Security подключается к Microsoft Management Console, и в дереве Консоли управления отображаются значок программы и корневой узел **Kaspersky Security 9.0 для Microsoft Exchange Servers**.

После запуска Консоли управления вы можете добавить серверы Microsoft Exchange с установленным Сервером безопасности (далее *защищаемые серверы*) к Консоли управления.

Программа записывает информацию о запуске или остановке Консоли управления в журнал событий Windows. Запись содержит информацию о времени запуска / остановки Консоли управления, а также пользователе, выполнившем эти действия.

Добавление Серверов безопасности к Консоли управления

Для управления работой программы нужно добавить защищаемые серверы к Консоли управления.

Если Серверы безопасности установлены на серверах Microsoft Exchange, входящих в группу доступности баз данных Microsoft Exchange (группу DAG), вы можете подключить Консоль управления к любому из таких Серверов безопасности для настройки параметров, общих для всей группы DAG, или подключить Консоль управления отдельно к Серверу безопасности для настройки его индивидуальных параметров.

Общими параметрами для группы DAG являются, например, параметры антивирусной защиты для роли Почтовый ящик, параметры отчетов о работе Антивируса для роли Почтовый ящик, параметры уведомлений, параметров обновления баз Антивируса. Общими для группы DAG также являются содержимое резервного хранилища и ключ.

Индивидуальными параметрами сервера Microsoft Exchange являются, например, параметры антивирусной защиты для роли Транспортный концентратор, параметры проверки на спам, параметры резервного хранилища, параметры отчетов о работе Анти-Спама и работе Антивируса для роли Транспортный концентратор, параметры обновления баз Анти-Спама.

► *Чтобы добавить Сервер безопасности к Консоли управления, выполните следующие действия:*

1. В дереве Консоли управления выберите узел **Kaspersky Security 9.0 для Microsoft Exchange Servers**.
2. Откройте окно **Добавление сервера** одним из следующих способов:

- выбрав пункт **Добавить сервер** в меню **Действие**;
- выбрав пункт **Добавить сервер** в контекстном меню узла **Kaspersky Security 9.0 для Microsoft Exchange Servers**;
- нажав на кнопку **Добавить сервер** в рабочей области узла;
- по ссылке **Добавить сервер** в панели быстрого доступа.

3. В окне **Добавление сервера** выберите Сервер безопасности, установленный на сервере Microsoft Exchange, к которому вы хотите подключить Консоль управления:
   - Если вы хотите подключить Консоль управления к Серверу безопасности, развернутому на локальном компьютере, выберите вариант **Локальный**.
   - Если вы хотите подключить Консоль управления к Серверу безопасности, развернутому на удаленном сервере Microsoft Exchange, выберите вариант **Удаленный**.

     Подключение Консоли управления к Серверу безопасности осуществляется через порт TCP 13100. Необходимо открыть этот порт в брандмауэре на удаленном сервере Microsoft Exchange или добавить службу *Kaspersky Security 9.0 для Microsoft Exchange Servers* в список доверенных программ брандмауэра.
4. Если вы выбрали вариант **Удаленный**, в поле ввода укажите удаленный сервер Microsoft Exchange, на котором установлен Сервер безопасности. Вы можете выбрать удаленный сервер Microsoft Exchange из списка с помощью кнопки **Обзор** или вручную ввести одно из следующих значений для удаленного сервера Microsoft Exchange:
   - IP-адрес;
   - полное доменное имя (в формате <Имя компьютера>.<DNS-имя домена>);
   - имя компьютера в сети Microsoft Windows (NetBIOS-имя).
5. Нажмите на кнопку **OK**.

Добавленный Сервер безопасности появится в дереве Консоли управления.

Добавленные Серверы безопасности отображаются в дереве Консоли управления в виде отдельных узлов. Чтобы перейти к управлению Сервером безопасности, нужно раскрыть соответствующий ему узел.

Вы также можете управлять группой Серверов безопасности с помощью профилей.

Узел Kaspersky Security 9.0 для Microsoft Exchange Servers

Блок **Защищенные серверы** позволяет подключить сервер, на котором установлен Kaspersky Security, к Консоли управления и перейти к настройке его параметров.

Добавить сервер

Кнопка, по которой вы можете подключить сервер Microsoft Exchange, на котором установлен Kaspersky Security, к Консоли управления.

Блок **Добавленные серверы** содержит кнопки с именами подключенных к Консоли управления серверов.

<Имя сервера>

Кнопка, по которой вы можете перейти к настройке параметров выбранного сервера Microsoft Exchange.

По этой кнопке открывается узел **<Имя сервера>**.

Используйте эти параметры в следующих задачах

Добавление Серверов безопасности к Консоли управления 81

Окно Добавление сервера

Локальный

Консоль управления подключается к Серверу безопасности, установленному на том же компьютере, на котором установлена Консоль управления.

Удаленный

Консоль управления подключается к Серверу безопасности, установленному на удаленном сервере Microsoft Exchange. В поле ввода вам нужно указать имя компьютера, на котором установлен Сервер безопасности. Вы можете выбрать компьютер из списка с помощью кнопки **Обзор** или ввести имя вручную. В качестве имени удаленного сервера Microsoft Exchange может быть указано одно из следующих значений:

- IP-адрес;
- полное доменное имя (FQDN в формате <Имя компьютера>.<DNS-имя домена>);
- имя компьютера в сети Microsoft Windows (NetBIOS-имя).

Подключение Консоли управления к Серверу безопасности осуществляется через порт TCP 13100. Необходимо открыть этот порт в брандмауэре на удаленном сервере Microsoft Exchange или добавить службу "Kaspersky Security для Microsoft Exchange Servers" в список доверенных программ брандмауэра.

Используйте эти параметры в следующих задачах

Добавление Серверов безопасности к Консоли управления 81

kaspersky

Защита сервера Microsoft Exchange по умолчанию

Защита сервера Microsoft Exchange от вредоносных программ и спама начинает работать сразу после установки компонента Сервер безопасности, если она не была отключена в мастере настройки программы (см. раздел "Шаг 2. Настройка защиты сервера Microsoft Exchange" на стр. 40).

По умолчанию реализуется следующий режим работы программы:

- Программа проверяет сообщения на наличие всех имеющихся в базах Антивируса вредоносных программ со следующими параметрами:
  - Программа проверяет содержимое сообщения и вложенные в него объекты любых форматов, за исключением объектов-контейнеров выше 32-го уровня вложенности.
  - Программа проверяет все хранилища почтовых ящиков.
  - Выбор действия при обнаружении зараженного объекта зависит от того, в какой роли развернут сервер Microsoft Exchange, на котором обнаружен объект:
    - При обнаружении зараженного объекта на сервере Microsoft Exchange в роли Пограничный транспорт или Транспортный концентратор объект автоматически удаляется, при этом программа сохраняет исходную копию сообщения в резервном хранилище, а к теме сообщения добавляет метку `[Обнаружен зараженный объект]`.
    - При обнаружении зараженного объекта на сервере Microsoft Exchange в роли Почтовый ящик программа сохраняет исходную копию объекта (вложение или содержимое сообщения) в резервном хранилище и выполняет попытку лечения. Если лечение невозможно, программа удаляет объект и заменяет его текстовым файлом со следующим информационным сообщением:

      ```
      Обнаружен вредоносный объект <имя_вируса>. Файл (<имя_объекта>)
      удален программой Kaspersky Security 9.0 для Microsoft Exchange
      Servers. Имя сервера: <имя_сервера>
      ```
  - При обнаружении защищенного паролем объекта программа пропускает такой объект.
- Программа проверяет сообщения на наличие спама со следующими параметрами:
  - Программа использует низкий уровень чувствительности проверки на спам. Этот уровень обеспечивает оптимальное сочетание скорости и качества проверки.
  - Программа пропускает все сообщения, при этом сообщения, которым присвоены статусы *Спам*, *Возможный спам*, *Массовые рассылки* и *Внесен в черный список*, отмечаются специальными метками в теме сообщения: `[!!SPAM]`, `[!!Probable Spam]`, `[!!Mass Mail]` и `[!!Blacklisted]` соответственно.
  - Максимальное время проверки сообщения – 60 секунд.
  - Максимальный размер проверяемого сообщения вместе с вложениями – 2096128 КБ (2047 МБ).
  - Используются внешние службы проверки IP-адресов и URL-ссылок: DNSBL и SURBL (см. раздел "О дополнительных службах, функциях и технологиях защиты от спама" на стр. 128). Эти службы позволяют выполнять фильтрацию спама с помощью общедоступных черных списков IP-адресов и URL-ссылок.
  - Если вы включили использование KSN в мастере настройки программы (см. раздел "Шаг 3. Включение служб KSN" на стр. 41), то использование служб KSN и Reputation Filtering включено. В противном случае использование служб KSN и Reputation Filtering выключено.

- Если вы включили использование службы Enforced Anti-Spam Updates Service в мастере настройки программы (см. раздел "Шаг 2. Настройка защиты сервера Microsoft Exchange" на стр. 40), то использование Enforced Anti-Spam Updates Service включено. В противном случае использование Enforced Anti-Spam Updates Service выключено.

В этом разделе

Просмотр сведений о состоянии защиты сервера Microsoft Exchange

► *Чтобы просмотреть сведения о состоянии защиты сервера Microsoft Exchange, выполните следующие действия:*

1. Запустите Консоль управления, выбрав в меню **Пуск** пункт **Программы → Kaspersky Security 9.0 для Microsoft Exchange Servers → Kaspersky Security 9.0 для Microsoft Exchange Servers**.
2. В дереве Консоли управления выберите узел Сервера безопасности, установленного на том сервере Microsoft Exchange, сведения о состоянии которого вы хотите просмотреть.

В рабочей области выбранного узла Сервера безопасности отображаются следующие сведения о состоянии защиты сервера:

- В блоке **Профиль** отображается информация о настройке параметров Сервера безопасности с помощью профилей.
- В блоке параметров **Информация о программе** отображается информация о сервере Microsoft Exchange и модулях программы:
  - **Имя сервера**

    Имя сервера может принимать следующие значения:

    - Имя физического сервера, если Консоль управления подключена к Серверу безопасности, установленному на отдельном сервере Microsoft Exchange, на пассивном узле кластера или сервере, входящем в DAG.
    - Имя виртуального сервера, если Консоль управления подключена к виртуальному серверу или его активному узлу.
  - **Информация о схеме развертывания программы**

    Поле содержит одно из следующих значений:

    - **Виртуальный сервер**, если Консоль управления подключена к виртуальному серверу Microsoft Exchange или его активному узлу.
    - **<Имя DAG>**, если Консоль управления подключена к Серверу безопасности, установленному на сервере Microsoft Exchange, входящем в DAG.
  - **Версия**

    Информация о версии установленной программы.

- **Модуль Анти-Спам**

  Состояние модуля Анти-Спам. Отображается, если Сервер безопасности установлен на сервере Microsoft Exchange, который развернут в роли Транспортный концентратор или Пограничный транспорт. Может принимать следующие значения:

  - **Выключен** – модуль Анти-Спам установлен, проверка сообщений на спам отключена.
  - **Не работает или работает с ошибками** – модуль Анти-Спам установлен, проверка сообщений на спам включена, но модуль Анти-Спам не проверяет сообщения на спам из-за ошибок, связанных с лицензией, ошибок баз Анти-Спама или ошибок проверки.
  - **Не установлен** – модуль Анти-Спам не установлен.
  - **Включен** – модуль Анти-Спам установлен, проверка сообщений на спам включена.

- **Модуль Антивирус для роли Транспортный концентратор**

  Состояние модуля Антивирус для роли Транспортный концентратор. Отображается, если Сервер безопасности установлен на сервере Microsoft Exchange, который развернут в роли Транспортный концентратор или Пограничный транспорт. Может принимать следующие значения:

  - **Выключен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт установлен, антивирусная защита для роли Транспортный концентратор отключена.
  - **Не работает или работает с ошибками** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт установлен, антивирусная защита для роли Транспортный концентратор включена, но модуль Антивирус не проверяет сообщения на вирусы и другие угрозы из-за ошибок, связанных с лицензией, ошибок баз Антивируса или ошибок проверки.
  - **Не установлен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт не установлен.
  - **Включен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт установлен, антивирусная защита для роли Транспортный концентратор включена, модуль Антивирус проверяет сообщения на вирусы и другие угрозы.

- **Модуль Антивирус для роли Почтовый ящик**

  Состояние модуля Антивирус для роли Почтовый ящик. Отображается, если Сервер безопасности установлен на сервере Microsoft Exchange, который развернут в роли Почтовый ящик. Может принимать следующие значения:

  - **Выключен** – модуль Антивирус для роли Почтовый ящик установлен, антивирусная защита для роли Почтовый ящик отключена.
  - **Не работает или работает с ошибками** – антивирусная защита для роли Почтовый ящик включена, но модуль Антивирус не проверяет сообщения на вирусы и другие угрозы из-за ошибок, связанных с лицензией, ошибок баз Антивируса или ошибок проверки.
  - **Не установлен** – модуль Антивирус для роли Почтовый ящик не установлен.
  - **Включен** – антивирусная защита для роли Почтовый ящик включена, модуль Антивирус проверяет сообщения на вирусы и другие угрозы.

- **Фильтрация вложений и содержимого**

  Состояние модуля Фильтрация вложений и содержимого. Может принимать следующие значения:

- **Выключен** – Модуль Фильтрация вложений и содержимого установлен, но находится в неактивном состоянии.
- **Не работает или работает с ошибками** – Модуль Фильтрация вложений и содержимого установлен и находится в активном состоянии, но не выполняет фильтрацию в сообщениях из-за ошибок, связанных с лицензией или ошибок проверки.
- **Не установлен** – Модуль Фильтрация вложений и содержимого не установлен.
- **Включен** – Модуль Фильтрация вложений и содержимого установлен и активен.

Набор полей, отображающих состояние модулей Сервера безопасности, может быть сокращен в зависимости от конфигурации сервера Microsoft Exchange. Если поле, соответствующее модулю, не отображается, этот модуль не может быть установлен в этой конфигурации сервера Microsoft Exchange.

Если SQL-сервер недоступен, в блоке параметров **Информация о программе** отображается информация об ошибке подключения к SQL-серверу.

По ссылке **Перейти к настройке защиты сервера** открывается рабочая область узла **Защита сервера**.

- В блоке параметров **Лицензирование** отображается информация о лицензии:
  - **Функциональность**

    Функциональность программы, определяемая действующей лицензией. Может принимать следующие значения:

    - **Полная функциональность**.
    - **Срок действия лицензии истек. Обновление баз и техническая поддержка недоступны**. Срок действия лицензии истек. Обновление баз программы и техническая поддержка недоступны.
    - **Только управление**.
    - **Только обновление**. Только обновление баз программы.
  - **Статус**
  - Поле **Статус** отображается только для активных ключей. Возможны следующие статусы ключа Сервера безопасности и соответствующие им ограничения программы:
    - **Действующая лицензия**. Функциональность модулей Антивирус и Анти-Спам не ограничена.
    - **Срок действия пробной лицензии истек**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
    - **Срок действия лицензии истек**. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network. Функциональность модулей Антивирус и Анти-Спам доступна.
    - **Базы повреждены**. Базы Антивируса или базы Анти-Спама отсутствуют или повреждены.
    - **Ключ отсутствует**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.

- **Ключ заблокирован**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
- **Черный список ключей поврежден или не найден**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
- **Не удается обновить статус лицензии**. Функциональность модулей Антивирус и Анти-Спам не ограничена. Вы можете просмотреть описание ошибки в блоке **Состояние серверов** в поле **Статус лицензии.**

Если в поле **Статус** блока **Лицензирование** отображается значение, отличное от *Действующая лицензия*, соответствующий блок выделяется красным цветом. В этом случае требуется добавить соответствующий активный ключ (см. раздел "Активация программы с помощью ключа для Сервера безопасности" на стр. 70), перейдя к узлу **Лицензирование** по ссылке **Перейти к управлению ключами**.

- **Дата окончания**

  Дата окончания срока действия лицензии.

Если поле **Дата окончания** выделено красным цветом, вам требуется продлить срок действия лицензии, например, добавив соответствующий резервный ключ (см. раздел "Активация программы с помощью ключа для Сервера безопасности" на стр. 70), перейдя к узлу **Лицензирование** по ссылке **Перейти к управлению ключами**.

Период времени до окончания срока действия лицензии, в течение которого поле выделяется красным цветом, задается в параметре **Уведомить заранее об истечении срока действия лицензии (дни)** (см. раздел "**Настройка уведомления о скором истечении срока действия лицензии**" на стр. 72), расположенном в рабочей области узла **Уведомления**. По умолчанию – 15 дней.

- **Количество почтовых ящиков**

  Максимальное количество почтовых ящиков, которые может защитить программа по этому ключу.

- **Резервный ключ**

  Информация о наличии резервного ключа: **Добавлен** или **Отсутствует**.

По ссылке **Перейти к управлению ключами** открывается рабочая область узла **Лицензирование**, в которой вы можете добавлять и удалять ключи.

- В блоке параметров **Базы Анти-Спама** отображается информация о состоянии баз Анти-Спама:
  - **Последнее обновление**

    Дата последнего обновления баз Анти-Спама.

  - **Статус**

    Статус последнего обновления баз Анти-Спама. Может принимать следующие значения:

- **Базы обновлены** – базы успешно обновлены.
- **Завершено с ошибкой** – при обновлении баз произошла ошибка.
- **Не выполнено** – обновление баз не выполнялось.

- **Дата и время выпуска**

  Дата и время выпуска баз Анти-Спама. Отображаются в формате, установленном в параметрах операционной системы.

  Если базы Анти-Спама устарели более чем на час, текст в этом поле выделяется красным цветом.

Если блок **Базы Анти-Спама** и поле **Дата и время выпуска** в этом блоке выделены красным цветом, требуется обновить базы Анти-Спама (см. раздел "Запуск обновления баз вручную" на стр. 167). При необходимости вы можете настроить параметры обновления баз Анти-Спама (см. раздел "Настройка обновления баз программы по расписанию" на стр. 167).
Если последнее обновление баз Анти-Спама завершилось с ошибкой, блок **Базы Анти-Спама** выделяется красным цветом, а в поле **Статус** отображается сообщение об ошибке.

По ссылке **Перейти к настройке параметров обновления** открывается рабочая область узла **Обновления**.

- В блоке параметров **Антивирусные базы** отображается информация о состоянии баз Антивируса:

  - **Последнее обновление**

    Дата последнего обновления антивирусных баз

  - **Статус**

    Статус последнего обновления антивирусных баз. Может принимать следующие значения:

    - **Базы обновлены** – базы успешно обновлены.
    - **Завершено с ошибкой** – при обновлении баз произошла ошибка.
    - **Не выполнено** – обновление баз не выполнялось.

  - **Дата и время выпуска**

    Дата и время выпуска антивирусных баз. Отображаются в формате, установленном в параметрах операционной системы.

    Если антивирусные базы устарели более чем на сутки, текст в этом поле выделяется красным цветом.

Если блок **Антивирусные базы** и поле **Дата и время выпуска** в этом блоке выделены красным цветом, требуется обновить базы Антивируса (см. раздел "Запуск обновления баз вручную" на стр. 167). При необходимости вы можете настроить параметры обновления антивирусных баз (см. раздел "Настройка обновления баз программы по расписанию" на стр. 167).
Если последнее обновление антивирусных баз Антивируса завершилось с ошибкой, блок **Антивирусные базы** выделяется красным цветом, а в поле **Статус** отображается сообщение об ошибке.

По ссылке **Перейти к настройке параметров обновления** открывается рабочая область узла **Обновления**.

- В блоке параметров **Статистика** отображаются счетчики, содержащие информацию о количестве сообщений, помещенных в карантин для повторной проверки на спам (см. стр. 118):
  - **Количество сообщений сейчас на карантине**

    Количество сообщений, находящихся в карантине в текущий момент.
  - **Всего сообщений помещено на карантин за время работы программы**

    Количество сообщений, помещенных в карантин с момента начала получения статистики.

  Под счетчиками в блоке параметров **Статистика** отображаются графики, содержащие статистическую информацию о работе модулей программы за последние семь дней:
  - **Анти-Спам**

    График содержит следующие сведения:
    - **Всего сообщений**. Количество сообщений, поступивших на проверку.
    - **С фишингом или спамом**. Количество проверенных сообщений, содержащих спам или фишинговые ссылки.
    - **Непроверенных**. Количество непроверенных сообщений.
    - **Чистых**. Количество сообщений, относящихся к следующим категориям:
      - Проверенные сообщения, не содержащие спам или фишинговые ссылки.
      - Сообщения, исключенные из проверки с помощью белых списков отправителей или получателей.
    - **Остальных**. Количество сообщений, относящихся к следующим категориям:
      - Возможный спам.
      - Формальное оповещение.
      - Массовая рассылка.
      - Сообщение, попадающее под действие черных списков отправителей.
      - Сообщения, поступившие через доверительные соединения (если проверка доверительных соединений отключена).
  - **Антивирус для роли Транспортный концентратор**

    В блоке отображается следующая статистическая информация:
    - **Всего сообщений**. Количество сообщений, поступивших на проверку.
    - **Зараженных**. Количество сообщений, в которых были обнаружены вредоносные объекты.
    - **Отфильтрованных**. Количество сообщений, в которых по результатам фильтрации вложений были обнаружены файлы, совпадающие с критериями фильтрации.
    - **Непроверенных**. Количество сообщений, которые на были проверены программой (например, в результате ошибок в работе программы).
    - **Признанных чистыми**. Количество сообщений, в которых по результатам проверки Антивирусом не были обнаружены вредоносные объекты, и по результатам фильтрации вложений не были обнаружены файлы, совпадающие с критериями фильтрации.
    - **Остальных**. Количество сообщений, относящихся к категории Возможно зараженные.
  - **Антивирус для роли Почтовый ящик**

    График содержит следующие сведения:

- **Имя сервера**. Имя подключенного сервера.
- **Всего сообщений**. Количество обработанных сообщений.
- **Зараженных**. Количество обнаруженных зараженных сообщений.
- **Непроверенных**. Количество непроверенных сообщений.
- **Признанных чистыми**. Количество проверенных сообщений, не содержащих угроз.
- **Остальных**. Количество сообщений, относящихся к категориям Возможно зараженные и Защищенные.

Набор графиков может быть сокращенным в зависимости от конфигурации программы.

Просмотр сведений о состоянии защиты серверов Microsoft Exchange одного профиля

► *Чтобы просмотреть сведения о состоянии защиты серверов Microsoft Exchange одного профиля, выполните следующие действия:*

1. Запустите Консоль управления, выбрав в меню операционной системы **Пуск** пункт **Программы → Kaspersky Security 9.0 для Microsoft Exchange Servers → Kaspersky Security 9.0 для Microsoft Exchange Servers**.
2. В дереве Консоли управления в узле **Профиль** выберите узел профиля (см. раздел "Управление профилями" на стр. 157), сведения о состоянии защиты серверов Microsoft Exchange которого вы хотите просмотреть.

В рабочей области выбранного профиля отображаются следующие сведения:

- В блоке параметров **Профиль** отображаются сведения о состоянии ключа Сервера безопасности, добавленного на входящие в профиль Сервера безопасности:
  - **Функциональность**

    Функциональность программы, определяемая действующей лицензией. Может принимать следующие значения:

    - **Полная функциональность**.
    - **Срок действия лицензии истек. Обновление баз и техническая поддержка недоступны**. Срок действия лицензии истек. Обновление баз программы и техническая поддержка недоступны.
    - **Только управление**.
    - **Только обновление**. Только обновление баз программы.
  - **Статус**
  - Поле **Статус** отображается только для активных ключей. Возможны следующие статусы ключа Сервера безопасности и соответствующие им ограничения программы:
    - **Действующая лицензия**. Функциональность модулей Антивирус и Анти-Спам не ограничена.
    - **Срок действия пробной лицензии истек**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.

- **Срок действия лицензии истек**. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network. Функциональность модулей Антивирус и Анти-Спам доступна.
- **Базы повреждены**. Базы Антивируса или базы Анти-Спама отсутствуют или повреждены.
- **Ключ отсутствует**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
- **Ключ заблокирован**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
- **Черный список ключей поврежден или не найден**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
- **Не удается обновить статус лицензии**. Функциональность модулей Антивирус и Анти-Спам не ограничена. Вы можете просмотреть описание ошибки в блоке **Состояние серверов** в поле **Статус лицензии.**

Если в поле **Статус** в блоке **Профиль** отображается значение, отличное от *Действующая лицензия*, блок выделяется красным цветом. В этом случае требуется добавить активный ключ (см. раздел "Активация программы с помощью ключа для Сервера безопасности" на стр. 70), перейдя к узлу **Лицензирование** по ссылке **Перейти к управлению ключами**.

- **Дата окончания**

  Дата окончания срока действия лицензии.

Если поле **Дата окончания** выделено красным цветом, вам требуется продлить срок действия лицензии, например, добавив резервный ключ (см. раздел "Активация программы с помощью ключа для Сервера безопасности" на стр. 70), перейдя к узлу **Лицензирование** по ссылке **Перейти к управлению ключами**.

Период времени до окончания срока действия лицензии, в течение которого поле выделяется красным цветом, задается в параметре **Уведомить заранее об истечении срока действия лицензии (дни) (см. раздел "Настройка уведомления о скором истечении срока действия лицензии" на стр. 72).** Параметр находится в рабочей области узла **Лицензирование** (см. раздел "**Узел Лицензирование**" на стр. 75). По умолчанию – 15 дней.

- **Количество почтовых ящиков**

  Максимальное количество почтовых ящиков, которые может защитить программа по этому ключу.

- **Резервный ключ**

  Информация о наличии резервного ключа: **Добавлен** или **Отсутствует**.

По ссылке **Перейти к управлению ключами** открывается рабочая область узла **Лицензирование**, в которой вы можете добавлять и удалять ключи.

- В блоке параметров **Состояние серверов** отображается таблица, столбцы которой содержат информацию о состоянии Серверов безопасности профиля, обновлений баз программы, модулей программы и SQL-сервера:
  - **Сервер**

    Имя сервера Microsoft Exchange, на котором установлен добавленный в профиль Сервер безопасности. Может принимать следующие значения:

    - <Доменное имя сервера Microsoft Exchange>, если в профиль добавлен Сервер безопасности, установленный на одиночном сервере Microsoft Exchange.
    - <Имя DAG – Доменное имя сервера Microsoft Exchange>, если в профиль добавлен Сервер безопасности, установленный на сервере Microsoft Exchange в составе группы DAG.

  - **Статус лицензии**

Статус лицензии может принимать следующие значения:

- **Действующая лицензия**. Функциональность модулей Антивирус и Анти-Спам не ограничена.
- **Срок действия пробной лицензии истек**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
- **Срок действия лицензии истек**. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network. Функциональность модулей Антивирус и Анти-Спам доступна.
- **Базы повреждены**. Базы Антивируса или базы Анти-Спама отсутствуют или повреждены.
- **Ключ отсутствует**. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
- **Ключ заблокирован**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.
- **Черный список ключей поврежден или не найден**. Недоступна функциональность модулей Антивирус и Анти-Спам. Доступно только обновление баз Антивируса и баз Анти-Спама.

Если в поле **Статус** значение **Не удается обновить статус лицензии**, в поле **Статус лицензии** вы можете прочитать описание ошибки.

- **Статус обновлений**

  Статус обновления баз программы на Сервере безопасности. Может принимать следующие значения:

  - **Базы актуальны** – базы программы успешно обновлены.
  - **Ошибка баз** – при обновлении баз программы произошла ошибка, базы устарели, базы повреждены или обновление не выполнялось.
  - **Сервер недоступен** – Сервер безопасности недоступен по сети или выключен.

- **Модуль Антивирус**

  Состояние модуля Антивирус. Может принимать следующие значения:

  - **Выключен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт или модуль Антивирус для роли Почтовый ящик установлен, антивирусная проверка сообщений отключена.
  - **Не работает или работает с ошибками** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт или модуль Антивирус для роли Почтовый ящик установлен, антивирусная проверка сообщений

включена, но модуль Антивирус не проверяет сообщения на вирусы и другие угрозы из-за ошибок, связанных с лицензией, ошибок баз Антивируса или ошибок проверки.

- **Не установлен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт или модуль Антивирус для роли Почтовый ящик не установлены.
- **Включен** – модуль Антивирус для ролей Транспортный концентратор и Пограничный транспорт или модуль Антивирус для роли Почтовый ящик установлен, антивирусная проверка сообщений включена, модуль Антивирус проверяет сообщения на вирусы и другие угрозы.

- **Фильтрация вложений и содержимого**

  Состояние модуля Фильтрация вложений и содержимого. Может принимать следующие значения:

  - **Выключен** – Модуль Фильтрация вложений и содержимого установлен, но находится в неактивном состоянии.
  - **Не работает или работает с ошибками** – Модуль Фильтрация вложений и содержимого установлен и находится в активном состоянии, но не выполняет фильтрацию в сообщениях из-за ошибок, связанных с лицензией или ошибок проверки.
  - **Не установлен** – Модуль Фильтрация вложений и содержимого не установлен.
  - **Включен** – Модуль Фильтрация вложений и содержимого установлен и активен.

- **Модуль Анти-Спам**

  Состояние модуля Анти-Спам. Отображается, если Сервер безопасности установлен на сервере Microsoft Exchange, который развернут в роли Транспортный концентратор или Пограничный транспорт. Может принимать следующие значения:

  - **Выключен** – модуль Анти-Спам установлен, проверка сообщений на спам отключена.
  - **Не работает или работает с ошибками** – модуль Анти-Спам установлен, проверка сообщений на спам включена, но модуль Анти-Спам не проверяет сообщения на спам из-за ошибок, связанных с лицензией, ошибок баз Анти-Спама или ошибок проверки.
  - **Не установлен** – модуль Анти-Спам не установлен.
  - **Включен** – модуль Анти-Спам установлен, проверка сообщений на спам включена.

- **SQL-сервер**

  Состояние SQL-сервера. Может принимать следующие значения:

  - **Доступен**.
  - **Недоступен**.

Если Сервер безопасности недоступен, в столбце **Статус обновлений** отображается статус *Сервер недоступен*, а столбцы **Статус обновлений**, **Модуль Антивирус**, **Модуль Анти-Спам** выделяются красным цветом.
Если в столбце **Статус обновлений** отображается значение, отличное от *Базы актуальны*, столбец выделяется красным цветом.
Если статус Антивируса или Анти-Спама *Выключен* или *Не работает или работает с ошибками*, соответствующий модулю столбец выделяется красным цветом.

По ссылке на имени Сервера безопасности в столбце **Сервер** открывается рабочая область узла этого Сервера безопасности.

Узел Защита сервера

Рабочая область этого узла содержит закладки, позволяющие настроить параметры Антивируса, Анти-Спама, Антифишинга,а также фильтрации вложений и содержимого и фильтрации однотипных сообщений.

Защита для роли Почтовый ящик

Защита для роли Транспортный концентратор

Дополнительные параметры Антивируса

О Kaspersky Security Network и Kaspersky Private Security Network

Kaspersky Security Network – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о следующих данных:

- репутации файлов, веб-сайтов и программ;
- категориях файлов, веб-сайтов и программ (например, файл операционной системы, компьютерная игра, веб-сайт категории Для взрослых);
- частоте обнаружения файлов во всех странах мира и о географическом распространении файлов;
- статистике доверия к файлам и веб-сайтам среди пользователей программ "Лаборатории Касперского" во всем мире (Kaspersky Application Advisor);
- отзывах вирусными аналитиками "Лаборатории Касперского" отдельных вирусных записей в локальных базах антивирусных программ (например, изменение оценки объекта с "опасный" на "безопасный").

Данные Kaspersky Security Network используются в программах «Лаборатории Касперского» для следующих целей:

- обеспечения более высокой скорости реакции программ на объекты, информация о которых еще не вошла в базы антивирусных программ;
- снижения вероятности ложных срабатываний Анти-Спама;
- повышения эффективности работы некоторых компонентов защиты.

  Например, на основании данных Kaspersky Security Network антивирусная программа может выполнять следующие действия:

  - блокировать доступ пользователя к вредоносным веб-сайтам;
  - блокировать запуск вредоносных файлов на компьютере пользователя;
  - ограничивать доступ к отдельным категориям файлов и веб-сайтов (например, ограничивать запуск файлов или веб-сайтов категории Компьютерные игры в рабочее время).

Если пользователь участвует в Kaspersky Security Network, программа "Лаборатории Касперского", установленная на компьютере пользователя, получает информацию из Kaspersky Security Network, а также отправляет в "Лабораторию Касперского" данные о предположительно опасных объектах, обнаруженных на

компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

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

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет программам "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику и файлы в "Лабораторию Касперского". Для получения подробной информации см. Руководство администратора Kaspersky Private Security Network.

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Службы программы, которые используют в своей работе KPSN, не требуют подключения к интернету. Другие компоненты Kaspersky Security, например служба быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service, компоненты, выполняющие обновление баз программы, компоненты, выполняющие активацию программы, требуют подключения к интернету.

Данные, которыми программа обменивается с серверами KPSN, передаются только в пределах локальной сети организации. Данные, которые программа передает в KPSN, не включают в себя статистику. Программа передает статистику только на серверы KSN.

Модуль Анти-Спам передает на серверы KPSN следующие данные:

- IP-адрес отправителя сообщения электронной почты.
- IP-адрес промежуточных серверов, участвовавших в пересылке сообщения, и почтовых серверов, через которые проходило сообщение.
- Имена доменов отправителя сообщения из SMTP-сессии и MIME-заголовка.
- Веб-адреса, содержащиеся в проверяемом письме. Если такие адреса содержали пароли, то пароли не передаются на серверы KPSN.
- Короткие текстовые сигнатуры по тексту сообщения. Текстовыми сигнатурами являются необратимые свертки текста, по которым нельзя восстановить исходный текст. Сам текст

сообщения не передается. Программа использует короткие текстовые сигнатуры, чтобы фильтровать известные спам-рассылки и выносить вердикты по результатам такой фильтрации.

- Контрольная сумма (MD5) от адреса электронной почты отправителя проверяемого сообщения.
- Контрольные суммы (MD5) от графических объектов, находящихся в сообщении.
- Категории базы контентной фильтрации.
- Категория тематической принадлежности текста, которую определила программа.
- Список категорий, которые определила программа при проверке эвристическим анализатором.
- Контрольная сумма (MD5) от имени файла, вложенного в сообщение.

Модуль Анти-Фишинг передает на серверы KPSN веб-адреса, которые программа обнаружила в сообщении при проверке сообщения на содержание фишинговых ссылок.

Модуль Антивирус передает на серверы KPSN следующие данные:

- Контрольные суммы обрабатываемых файлов (MD5, SHA2-256).

Идентификатор и версию записи, связанной с угрозой в антивирусной базе.

См. также

О Kaspersky Private Security Network 99

kaspersky

О Kaspersky Security Network

Kaspersky Security Network – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о следующих данных:

- репутации файлов, веб-сайтов и программ;
- категориях файлов, веб-сайтов и программ (например, файл операционной системы, компьютерная игра, веб-сайт категории Для взрослых);
- частоте обнаружения файлов во всех странах мира и о географическом распространении файлов;
- статистике доверия к файлам и веб-сайтам среди пользователей программ "Лаборатории Касперского" во всем мире (Kaspersky Application Advisor);
- отзывах вирусными аналитиками "Лаборатории Касперского" отдельных вирусных записей в локальных базах антивирусных программ (например, изменение оценки объекта с "опасный" на "безопасный").

Данные Kaspersky Security Network используются в программах «Лаборатории Касперского» для следующих целей:

- обеспечения более высокой скорости реакции программ на объекты, информация о которых еще не вошла в базы антивирусных программ;
- снижения вероятности ложных срабатываний Анти-Спама;
- повышения эффективности работы некоторых компонентов защиты.

  Например, на основании данных Kaspersky Security Network антивирусная программа может выполнять следующие действия:

  - блокировать доступ пользователя к вредоносным веб-сайтам;
  - блокировать запуск вредоносных файлов на компьютере пользователя;
  - ограничивать доступ к отдельным категориям файлов и веб-сайтов (например, ограничивать запуск файлов или веб-сайтов категории Компьютерные игры в рабочее время).

Если пользователь участвует в Kaspersky Security Network, программа "Лаборатории Касперского", установленная на компьютере пользователя, получает информацию из Kaspersky Security Network, а также отправляет в "Лабораторию Касперского" данные о предположительно опасных объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

В этом разделе

kaspersky

Участие в Kaspersky Security Network

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

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Ваше участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках угроз, разрабатывать способы их нейтрализации и обрабатывать спам-сообщения с высокой точностью.

Если вы участвуете в Kaspersky Security Network, определенная статистика, полученная в результате работы Kaspersky Security, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Обработка данных может иметь особенности в зависимости от нахождения пользователя в том или ином регионе в соответствии с местным законодательством. Если вы участвуете в Kaspersky Security Network, то при пересечении границ регионов вы будете получать предупреждения в журнале событий Windows о переходе в другой сегмент KSN. Если настроено получение уведомлений о возникновении системных ошибок, предупреждение будет дополнительно отправлено на указанные адреса электронной почты.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

Вы можете включать и отключать использование Kaspersky Security Network в работе Антивируса (см. раздел "Включение и выключение использования Kaspersky Private Security Network в Антивирусе" на стр. 103) и Анти-Спама (см. раздел "Включение и выключение использования Kaspersky Private Security Network в Анти-Спаме" на стр. 102) отдельно.

Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать обновления для программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае вы будете получать предупреждения об ограниченном режиме работы KSN в журнале событий Windows. При возвращении в нормальный режим работы вы будете так же получать уведомление в журнале событий Windows. Если настроено получение уведомлений о возникновении системных ошибок, предупреждение и уведомление будут дополнительно отправлены на указанные адреса электронной почты.

О Kaspersky Private Security Network

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

kaspersky

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет программам "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику и файлы в "Лабораторию Касперского". Для получения подробной информации см. Руководство администратора Kaspersky Private Security Network.

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Службы программы, которые используют в своей работе KPSN, не требуют подключения к интернету. Другие компоненты Kaspersky Security, например, служба быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service, компоненты, выполняющие обновление баз программы, компоненты, выполняющие активацию программы, требуют подключения к интернету.

Данные, которыми программа обменивается с серверами KPSN, передаются только в пределах локальной сети организации. Данные, которые программа передает в KPSN, не включают в себя статистику. Программа передает статистику только на серверы KSN.

Модуль Анти-Спам передает на серверы KPSN следующие данные:

- IP-адрес отправителя сообщения электронной почты.
- IP-адрес промежуточных серверов, участвовавших в пересылке сообщения, и почтовых серверов, через которые проходило сообщение.
- Имена доменов отправителя сообщения из SMTP-сессии и MIME-заголовка.
- Веб-адреса, содержащиеся в проверяемом письме. Если такие адреса содержали пароли, то пароли не передаются на серверы KPSN.
- Короткие текстовые сигнатуры по тексту сообщения. Текстовыми сигнатурами являются необратимые свертки текста, по которым нельзя восстановить исходный текст. Сам текст сообщения не передается. Программа использует короткие текстовые сигнатуры, чтобы фильтровать известные спам-рассылки и выносить вердикты по результатам такой фильтрации.
- Контрольная сумма (MD5) от адреса электронной почты отправителя проверяемого сообщения.
- Контрольные суммы (MD5) от графических объектов, находящихся в сообщении.
- Категории базы контентной фильтрации.
- Категория тематической принадлежности текста, которую определила программа.
- Список категорий, которые определила программа при проверке эвристическим анализатором.
- Контрольная сумма (MD5) от имени файла, вложенного в сообщение.

Модуль Анти-Фишинг передает на серверы KPSN веб-адреса, которые программа обнаружила в сообщении при проверке сообщения на содержание фишинговых ссылок. Модуль Антивирус передает на серверы KPSN следующие данные:

- Контрольные суммы обрабатываемых файлов (MD5, SHA2-256).
- Идентификатор и версию записи, связанной с угрозой в антивирусной базе.

См. также

Настройка параметров проверки на спам и фишинг 123

Настройка параметров подключения к Kaspersky Private Security Network 101

О Kaspersky Security Network 98

Включение и выключение использования Kaspersky Private Security Network в Анти-Спаме 102

Настройка параметров подключения к Kaspersky Private Security Network

► *Чтобы настроить параметры подключения к Kaspersky Private Security Network, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить параметры подключения к Kaspersky Private Security Network для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите настроить параметры подключения к Kaspersky Private Security Network для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры подключения к Kaspersky Private Security Network.
2. Выберите узел **Настройка**.
3. В рабочей области раскройте блок параметров **Параметры KSN**.
4. Установите флажок **Использовать Kaspersky Private Security Network (KPSN)**.

   Активируется кнопка **Импортировать**.
5. Нажмите на кнопку **Импортировать**.

   Откроется окно **Открыть папку**.
6. В окне **Открыть папку** выберите папку, в которой находятся файлы с параметрами подключения к серверам службы Kaspersky Private Security Network.

   Файлы предоставляются "Лабораторией Касперского" в следующем составе:
   - Файлы с параметрами подключения к серверам службы Kaspersky Private Security Network:
     - kc_private.xms;
     - kh_private.xms.
   - ksncli_private.dat – файл с публичным RSA-ключом для шифрования канала передачи данных между программой и серверами службы Kaspersky Private Security Network.

Более подробную информацию вы можете получить, обратившись в Службу технической поддержки.

Если вы получили файлы с параметрами подключения к серверам службы Kaspersky Private Security Network, имена которых отличаются от указанных в этой справке, то измените имена файлов в соответствии с именами, указанными в этой справке.

7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**.

Программа импортирует файлы с параметрами подключения и применит полученные параметры для соединения с серверами службы Kaspersky Private Security Network.

Если вы используете Kaspersky Private Security Network, чтобы не передавать данные вашей организации через интернет, убедитесь, что вы отключили другие дополнительные службы Kaspersky Security, например, службу быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service, которая требует подключения к интернету для обмена данными с серверами "Лаборатории Касперского".

См. также

О Kaspersky Private Security Network 99

Включение и выключение использования Kaspersky Private Security Network в Анти-Спаме 102

Включение и выключение использования Kaspersky Private Security Network в Анти-Спаме

Убедитесь, что вы настроили параметры подключения к службе KPSN.

► *Чтобы включить / выключить использование Kaspersky Private Security Network в Анти-Спаме, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел нужного Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Параметры проверки на спам**.
4. В нижней части блока установите флажок **Использовать Kaspersky Security Network**.

Флажок **Использовать Kaspersky Security Network** доступен, если в блоке **Параметры KSN** в узле **Настройка** выбран вариант **Использовать Kaspersky Private Security Network (KPSN)**. Все параметры службы Kaspersky Security Network распространяются на службу Kaspersky Private Security Network.

5. Если требуется, укажите максимальное время ожидания ответа на запросы к серверу KSN в поле с прокруткой **Максимальное время ожидания при запросе в KSN**.

   Значение по умолчанию – 5 сек.

6. Нажмите на кнопку **Сохранить**.

Если вы используете профили для управления Серверами безопасности, расположенными в разных регионах (распределенная инфраструктура), то применение сделанных изменений произойдет после репликации данных Active Directory в организации. Если вам необходимо применить изменения ранее, выполните принудительную синхронизацию данных Active Directory.

См. также

О Kaspersky Private Security Network 99

Настройка параметров подключения к Kaspersky Private Security Network..... 101

Включение и выключение использования Kaspersky Private Security Network в Антивирусе

Убедитесь, что вы настроили параметры подключения к службе KPSN.

► *Чтобы включить / выключить использование Kaspersky Private Security Network в Антивирусе, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел нужного Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.
4. В нижней части блока установите флажок **Использовать Kaspersky Security Network**.

   Флажок **Использовать Kaspersky Security Network** доступен, если в блоке **Параметры KSN** в узле **Настройка** выбран вариант **Использовать Kaspersky Private Security Network (KPSN)**. Все параметры службы Kaspersky Security Network распространяются на службу Kaspersky Private Security Network.

5. Если требуется, укажите максимальное время ожидания ответа на запросы к серверу KSN в поле с прокруткой **Максимальное время ожидания при запросе в KSN**.

   Значение по умолчанию – 5 сек.

6. Нажмите на кнопку **Сохранить**.

Если вы используете профили для управления Серверами безопасности, расположенными в разных регионах (распределенная инфраструктура), то применение сделанных изменений произойдет после репликации данных Active Directory в организации. Если вам необходимо применить изменения ранее, выполните принудительную синхронизацию данных Active Directory.

См. также

kaspersky

Антивирусная защита

Одной из главных задач Kaspersky Security является антивирусная защита, в рамках которой программа проверяет на вирусы и наличие других угроз компьютерной безопасности почтовый поток и сообщения в почтовых ящиках, а также лечит зараженные сообщения и другие объекты Microsoft Exchange, такие как сообщения, задачи или записи в общих папках.

Здесь и далее, любая информация и инструкции по выполнению действий с сообщениями без потери общности также применимы к другим объектам Microsoft Exchange (таким как задачи, встречи, собрания, записи), если специально не указано другое.

Общие принципы работы Антивируса

Антивирус проверяет сообщения с помощью последней загруженной версии баз, эвристического анализатора, а также с помощью облачных служб Kaspersky Security Network, если использование этих служб в Антивирусе включено (см. раздел "Включение и выключение использования Kaspersky Private Security Network в Антивирусе" на стр. 103).

Антивирус проверяет содержимое сообщений (body) и присоединенные к ним файлы любых форматов.

Kaspersky Security различает следующие виды проверяемых объектов: простой объект (содержимое сообщения, простое вложение, например, в виде исполняемого файла) и объект-контейнер (объект, состоящий из нескольких объектов, например, архив, сообщение с любым вложенным сообщением).

При проверке многотомных архивов каждый том архива обрабатывается программой как отдельный объект. В этом случае Антивирус сможет обнаружить вредоносный код, только если он целиком содержится в одном из томов. Если при частичной загрузке данных вредоносный код также будет разделен на части, он не будет обнаружен при проверке. В такой ситуации не исключена вероятность распространения вредоносного кода после восстановления целостности объекта. Многотомные архивы могут быть проверены после сохранения на диске антивирусной программой, установленной на компьютере пользователя.

В случае необходимости вы можете определять перечень объектов, не подлежащих антивирусной проверке. Из проверки могут исключаться архивы, все объекты-контейнеры выше заданного уровня вложенности, файлы по маскам имен и сообщения, адресованные определенным получателям (см. раздел "Настройка исключений из антивирусной проверки" на стр. 111).

Файлы размером более 1 МБ сохраняются для обработки в служебной папке store, расположенной в папке data – папке хранения данных программы. Также в папке data расположено хранилище временных файлов – папка tmp. Требуется исключать папку store и папку tmp из проверки антивирусными программами, работающими на компьютерах с установленным сервером Microsoft Exchange.

По результатам проверки Антивирус присваивает каждому сообщению один из следующих статусов:

- *Зараженный* – проверен, содержит как минимум один из известных вирусов.
- *Незараженный* – проверен, не содержит вирусов.
- *Защищенный* – не проверен, защищен паролем.

Если сообщение или его часть заражена, Антивирус обрабатывает обнаруженный вредоносный объект в соответствии с заданными параметрами.

В параметрах Антивируса вы можете настроить действия, которые программа выполняет над сообщениями, содержащими вредоносные объекты. Вы можете настроить следующие действия:

- **Пропускать**. Антивирус пропускает сообщение и содержащийся в нем вредоносный объект.
- **Удалять объект**. Антивирус удаляет вредоносный объект, но пропускает сообщение.
- **Удалять сообщение**. Антивирус удаляет сообщение вместе с вредоносным объектом.

При удалении вредоносного объекта на сервере Microsoft Exchange сообщение или вложение, содержащее вредоносный объект, заменяется текстовым файлом, который содержит название вредоносного объекта, дату выпуска баз, с помощью которых был обнаружен вредоносный объект, и имя сервера Microsoft Exchange, на котором он был обнаружен.

Перед обработкой Антивирусом копия элемента может быть сохранена в резервном хранилище (см. раздел "Резервное хранилище" на стр. 178).

Антивирус состоит из двух модулей программы: **Антивирус для роли Транспортный концентратор** и **Антивирус для роли Почтовый ящик**.

Антивирус для роли Транспортный концентратор

Антивирус для роли Транспортный концентратор проверяет поступающие на сервер Microsoft Exchange сообщения в режиме реального времени. Он обрабатывает входящий и исходящий почтовый поток, а также проверяет поток транзитных сообщений. Если антивирусная защита сервера включена, запуск и остановка проверки почтового потока выполняется одновременно с запуском и остановкой сервера Microsoft Exchange.

Антивирус для роли Почтовый ящик

Антивирус для роли Почтовый ящик проверяет на вирусы и наличие других угроз компьютерной безопасности сообщения и другие элементы Microsoft Exchange, находящиеся в почтовых ящиках пользователей организации и в общих папках.

Защита Антивируса для роли Почтовый ящик распространяется на все почтовые ящики и общие папки, которые находятся в защищаемых хранилищах почтовых ящиков.

Если пользователь, чьи почтовые ящики защищены, создает сообщения в общих папках незащищенных серверов Microsoft Exchange, то Kaspersky Security не проверяет такие сообщения. При переносе сообщений из общих папок незащищенного хранилища в защищенное они проверяются программой. При репликации данных между защищенными и незащищенными хранилищами не синхронизируются изменения, внесенные программой в результате антивирусной проверки.

О предотвращении задержки сообщений Антивирусом

В исключительных случаях при сбое в работе антивирусного ядра время проверки сообщений Антивирусом может значительно увеличиваться. В таких случаях для предотвращения задержки сообщений Антивирус временно переходит в режим ограниченной проверки. В этом режиме некоторые сообщения могут быть пропущены без антивирусной проверки.

kaspersky

В этом разделе

Включение и выключение антивирусной защиты сервера

Если антивирусная защита сервера включена, то вместе с запуском и остановкой сервера Microsoft Exchange происходит соответственно запуск и остановка антивирусной проверки почтового потока. Фоновая проверка хранилищ (см. раздел "Настройка параметров фоновой проверки" на стр. 142) может быть запущена вручную или автоматически по расписанию.

Выключение антивирусной защиты сервера значительно повышает вероятность проникновения вредоносных программ через почтовую систему. Не рекомендуется выключать антивирусную защиту без необходимости.

Антивирусная защита сервера Microsoft Exchange, развернутого в ролях Почтовый ящик и Транспортный концентратор, включается раздельно.

► *Чтобы включить или выключить антивирусную защиту сервера Microsoft Exchange в роли Почтовый ящик, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите включить или выключить антивирусную защиту нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите включить или выключить антивирусную защиту Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить антивирусную защиту.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Почтовый ящик** в блоке параметров **Параметры проверки Антивируса** выполните одно из следующих действий:
   - установите флажок **Включить антивирусную защиту для роли Почтовый ящик**, если вы хотите включить антивирусную защиту сервера Microsoft Exchange;
   - снимите флажок Включить антивирусную защиту для роли Почтовый ящик, если вы хотите выключить антивирусную защиту сервера Microsoft Exchange.

4. Нажмите на кнопку **Сохранить**.

Если программа работает в DAG серверов Microsoft Exchange, антивирусная защита сервера в роли Почтовый ящик, включенная на одном из серверов, автоматически включается на остальных серверах, входящих в эту DAG. На остальных серверах этой DAG включать антивирусную защиту сервера для роли Почтовый ящик не требуется.

► *Чтобы включить антивирусную защиту сервера Microsoft Exchange в роли Транспортный концентратор, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите включить или выключить антивирусную защиту нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите включить или выключить антивирусную защиту Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, антивирусную защиту Серверов безопасности которого вы хотите настроить.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** в блоке параметров **Параметры проверки Антивируса** выполните одно из следующих действий:
   - установите флажок **Включить антивирусную защиту для роли Транспортный концентратор**, если вы хотите включить антивирусную защиту сервера Microsoft Exchange;
   - снимите флажок **Включить антивирусную защиту для роли Транспортный концентратор**, если вы хотите выключить антивирусную защиту сервера Microsoft Exchange.
4. Нажмите на кнопку **Сохранить**.

Настройка параметров антивирусной обработки объектов: Антивирус для роли Транспортный концентратор

Вы можете настроить параметры антивирусной обработки объектов, выбрав действие, которое Антивирус для роли Транспортный концентратор выполняет с каждым типом объектов.

► *Чтобы настроить параметры антивирусной обработки объектов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры антивирусной обработки объектов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры антивирусной обработки объектов для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры антивирусной обработки объектов.
2. Выберите узел **Защита сервера**.

3. На закладке **Защита для роли Транспортный концентратор** раскройте блок **Параметры проверки Антивируса**.
4. В разделе **Параметры обработки объектов** настройте следующий параметр:

   Зараженный объект

   В раскрывающемся списке **Зараженный объект** можно выбрать действие программы при обнаружении зараженного объекта.

   Для выбора доступны следующие варианты:

   - **Пропускать**. Программа доставляет адресату сообщение с зараженным объектом в неизмененном виде.

     Если установлены флажки **Добавлять метку в тему сообщения** или **Метка для внешних получателей**, программа добавляет к теме сообщения дополнительный текст (метку). Флажок **Добавлять метку в тему сообщения** добавляет метку к сообщениям для внутренних получателей, а флажок **Метка для внешних получателей** – для внешних получателей. Текст меток можно изменить. Значение меток по умолчанию: `[Обнаружен зараженный объект]`.

   - **Удалять объект**. Программа пытается вылечить зараженный объект. Если лечение не удалось, программа удаляет зараженный объект и доставляет адресату сообщение.

     Если установлены флажки **Добавлять метку в тему сообщения** или **Метка для внешних получателей**, программа добавляет к теме сообщения дополнительный текст (метку). Флажок **Добавлять метку в тему сообщения** добавляет метку к сообщениям для внутренних получателей, а флажок **Метка для внешних получателей** – для внешних получателей. Текст меток можно изменить. Значение меток по умолчанию: `[Удален зараженный объект]`.

   - **Удалять сообщение**. Программа полностью удаляет сообщение, содержащее зараженный объект.
5. Если вы хотите, чтобы перед обработкой объекта его копия сохранялась в резервном хранилище (см. раздел "Резервное хранилище" на стр. 178), установите флажок **Сохранять копию объекта в резервном хранилище**.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, параметры антивирусной обработки объектов для роли Транспортный концентратор требуется настраивать отдельно на каждом из серверов, входящих в группу DAG.

Параметры проверки на спам

Раскрывающийся блок **Параметры проверки на спам** позволяет настроить параметры проверки сообщений на спам и фишинг:

- **Включить проверку сообщений на спам**
  Включение / выключение проверки входящих сообщений на спам с помощью модуля Анти-Спам.
  Если флажок установлен, программа проверяет входящие сообщения на наличие спама.
  Если флажок снят, проверка входящих сообщений на спам не выполняется.
  По умолчанию флажок установлен.

- **Уровень чувствительности**

  Ползунок устанавливает уровень чувствительности проверки на спам. Анти-Спам учитывает значение этого параметра при классификации сообщения как спама или возможного спама. Доступны следующие значения уровня чувствительности проверки сообщений на спам:

  - **максимальный**. Этот уровень чувствительности следует использовать, если вы получаете спам очень часто. При выборе этого уровня чувствительности может возрасти частота распознавания полезной почты как спама.
  - **высокий**. Этот уровень чувствительности следует использовать, если вы часто получаете спам. При выборе этого уровня чувствительности уменьшается частота распознавания полезной почты как спама (по сравнению с уровнем **максимальный**). Скорость проверки увеличивается.
  - **низкий**. Этот уровень чувствительности обеспечивает оптимальное сочетание скорости и качества проверки. При выборе этого уровня чувствительности уменьшается частота распознавания полезной почты как спама (по сравнению с уровнем **высокий**). Скорость проверки увеличивается.

  Этот уровень чувствительности установлен по умолчанию.

  - **минимальный**. Этот уровень чувствительности следует использовать, если вы редко получаете спам.

  Ползунок доступен, если установлен флажок **Включить проверку сообщений на спам**.

- **Обрабатывать b2b-предложения как массовую рассылку**

  Если флажок установлен, программа обрабатывает B2B-предложения как массовую рассылку. Эта функциональность распространяется на все ящики и группы, защищаемые от массовой рассылки. Если флажок снят, программа не относит B2B-предложения к массовой рассылке.

  Флажок снят по умолчанию.
  Некоторые различия массовой рассылки от B2B-рассылки:

  - В отличие от массовой рассылки, B2B-рассылка может быть таргетированной.
  - B2B-рассылка может быть не массовой, а представлять собой отдельное (личное) письмо с бизнес-предложением.
  - Массовая рассылка больше ориентирована на количество получателей, тогда как в B2B-рассылке главным аттрибутом является тематика рассылки.

- **Обрабатывать спуфинг корпоративной посты (BEC) как спам**

  Если флажок установлен, программа использует функциональность защиты от атак класса BEC (Business Email Compromise), в частности спуфинга корпоративной почты.

  При установке программы автоматически создается группа KSE BEC Protected Users в Active Directory. В эту группу администратор организации добавляет сотрудников, под которых с наибольшей вероятностью ожидается маскировка злоумышленников.

  Каждое входящее письмо проверяется на предмет маскировки отправителя под пользователя из группы. Если обнаруживается попытка спуфинга, письма обрабатываются как спам.

  Если группа KSE BEC Protected Users не создалась автоматически при установке программы, рекомендуется создать такую группу вручную.

Вы можете создать только одну группу. Общее количество адресов электронной почты в группе не должно превышать 10 000. При превышении этого количества в проверке будут участвовать только первые 10 000 адресов электронной почты.

При установке KSE на Edge-сервере настройка защиты от BEC-атак не работает, независимо от наличия или отсутствия домена Active Directory.

Настройка параметров антивирусной обработки объектов: Антивирус для роли Почтовый ящик

Вы можете настроить параметры антивирусной обработки объектов, выбрав действие, которое Антивирус для роли Почтовый ящик выполняет с каждым типом объектов.

► *Чтобы настроить параметры антивирусной обработки объектов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры антивирусной обработки объектов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры антивирусной обработки объектов для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры антивирусной обработки объектов.
2. Выберите узел **Защита сервера**.
3. На закладке **Защита для роли Почтовый ящик** раскройте блок параметров **Параметры проверки Антивируса**.
4. В разделе **Параметры обработки объектов** настройте следующие параметры:
   - **Зараженный объект**

     В раскрывающемся списке **Зараженный объект** можно выбрать действие программы при обнаружении зараженного объекта.

     Для выбора доступны следующие варианты:

     - **Пропускать**. Программа доставляет адресату сообщение с зараженным объектом в неизмененном виде.
     - **Удалять объект**. Программа пытается вылечить зараженный объект. Если лечение не удалось, программа удаляет зараженный объект и доставляет адресату сообщение.
     - **Удалять сообщение**. Программа полностью удаляет сообщение, содержащее зараженный объект.
   - **Защищенный объект**

     В раскрывающемся списке **Защищенный объект** можно выбрать действие программы при обнаружении защищенного паролем объекта.

     Для выбора доступны следующие варианты:

     - **Пропускать**. Программа доставляет адресату сообщение с защищенным паролем объектом в неизмененном виде.
     - **Удалять сообщение**. Программа полностью удаляет сообщение, содержащее защищенный паролем объект.
5. Если вы хотите, чтобы перед обработкой объекта его копия сохранялась в резервном хранилище (см. раздел "Резервное хранилище" на стр. 178), установите флажок **Сохранять копию объекта в резервном хранилище**.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, параметры антивирусной обработки объектов для роли Почтовый ящик, настроенные для сервера, автоматически распространяются на остальные серверы, входящие в группу DAG. На остальных серверах этой группы DAG настраивать параметры антивирусной обработки объектов для роли Почтовый ящик не требуется.

kaspersky

Настройка исключений из антивирусной проверки

Для уменьшения нагрузки на сервер при выполнении антивирусной проверки вы можете настроить исключения из проверки, ограничив перечень проверяемых объектов. Исключения из антивирусной проверки действуют как при проверке почтового потока, так и при фоновой проверке хранилищ.

Вы можете настроить исключения из антивирусной проверки следующими способами:

- Отключить проверку архивов и объектов-контейнеров (см. раздел "Настройка параметров проверки вложенных объектов-контейнеров и архивов" на стр. 115).
- Настроить исключения по маске имен файлов (см. раздел "Настройка исключений по маске имен файлов" на стр. 114).

  Файлы, имена которых соответствуют указанным маскам, не будут проверяться на вирусы.
- Настроить исключения по адресам получателей (см. раздел "Настройка исключений по адресам получателей" на стр. 112).

  Сообщения, адресованные указанным получателям, не будут проверяться на вирусы.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, исключения из проверки, настроенные на одном из серверов, автоматически распространяются на остальные серверы Microsoft Exchange, входящие в эту группу DAG. На остальных серверах, входящих в эту группу DAG, настраивать исключения из проверки не требуется.

В этом разделе

О доверенных адресатах

Вы можете исключить из антивирусной проверки сообщения, адресованные определенным получателям, указав адреса этих получателей в списке *доверенных адресатов* (см. раздел "*Настройка исключений по адресам получателей*" на стр. 112). По умолчанию список пуст.

Вы можете добавлять в список доверенных адресатов адреса получателей в виде записей следующих типов:

- Объекты Active Directory:
  - Простые пользователи (User).
  - Контакты (Contact).
  - Группы рассылки (Distribution Group).
  - Группы безопасности (Security Group).

Рекомендуется добавлять адреса в виде записей этого типа.

- SMTP-адреса в формате `mailbox@domain.com`.

  Записи этого типа требуется добавлять, если установлен Антивирус для роли Транспортный концентратор и исключаемый адрес не может быть найден в Active Directory.

  > Чтобы исключить общую папку (Public Folder) из проверки Антивирусом для роли Транспортный концентратор, требуется добавить в список доверенных получателей все ее SMTP-адреса, если их несколько. Если какие-то из SMTP-адресов общей папки отсутствуют в списке, сообщения, поступающие в общую папку, могут быть проверены Антивирусом.

- Имена пользователей или групп (Display Name).

  Записи этого типа требуется добавлять, если установлен Антивирус для роли Почтовый ящик и исключаемый адрес не может быть найден в Active Directory.

- Общие папки (Public Folder).

  Записи этого типа требуется добавлять, если установлен Антивирус для роли Почтовый ящик. Общие папки невозможно выбрать из Active Directory. Записи этого типа требуется добавлять, указывая полный путь к общей папке.

> Если установлены Антивирус для роли Почтовый ящик и Антивирус для роли Транспортный концентратор и исключаемый адрес не может быть найден в Active Directory, в список доверенных адресатов требуется включить две записи, соответствующие адресу: SMTP-адрес и имя пользователя / группы. В противном случае сообщения, поступающие на этот адрес, не будут исключены из проверки.

Адреса получателей, заданные в виде объектов Active Directory, исключаются из антивирусной проверки согласно следующим правилам:

- Если адрес получателя задан в виде простого пользователя, контакта или общей папки, сообщения для него исключаются из проверки.
- Если адрес задан в виде группы рассылки, сообщения, адресованные этой группе рассылки, исключаются из проверки. Однако сообщения, адресованные участникам группы рассылки персонально, не исключаются из проверки, если они не были добавлены в список отдельно.
- Если адрес задан в виде группы безопасности, сообщения, адресованные этой группе рассылки и участникам этой группы рассылки, исключаются из проверки.

Программа автоматически обновляет адреса получателей, полученные из Active Directory, при изменении соответствующих записей Active Directory (например, если изменился адрес электронной почты пользователя или если в группу безопасности был добавлен новый участник). Обновление выполняется один раз в сутки.

Настройка исключений по адресам получателей

Вы можете исключить из антивирусной проверки сообщения, адресованные определенным получателям, указав адреса этих получателей в списке доверенных адресатов.

► *Чтобы настроить исключения по адресам получателей, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить исключения по адресам получателей для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите настроить исключения по адресам получателей для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить исключения.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.
4. Установите флажок **Не проверять сообщения для адресатов**.
5. Добавьте адрес получателя в список доверенных адресов. Для этого выполните следующие действия:
   - Чтобы добавить в список запись из Active Directory, выполните следующие действия:
     a. Нажмите на кнопку .
     b. В открывшемся окне найдите нужную запись Active Directory и нажмите на кнопку **OK**.

     Адреса, выбранные из Active Directory, обозначаются в списке следующими значками:
     - – простые пользователи, контакты, группы рассылки;
     - – группы безопасности.
   - Чтобы добавить в список SMTP-адрес, имя пользователя или общую папку, выполните следующие действия:
     - Чтобы добавить SMTP-адрес или имя пользователя, введите его в поле ввода и нажмите на кнопку .
     - Чтобы добавить общую папку, введите путь к папке и нажмите на кнопку .

     Адреса, добавленные таким способом, обозначаются в списке значком .

     > Адреса, добавленные таким способом, не проходят проверку на наличие в Active Directory.
6. Чтобы удалить адрес получателя из списка доверенных адресатов, выделите строку с адресатом в списке и нажмите на кнопку .
7. Чтобы экспортировать список доверенных адресатов в файл, выполните следующие действия:
   a. Нажмите на кнопку .
   b. В открывшемся окне укажите название файла в поле **Имя файла**.
   c. Нажмите на кнопку **Сохранить**.
8. Чтобы импортировать список доверенных адресатов из файла, выполните следующие действия:
   a. Нажмите на кнопку .
   b. В открывшемся окне в поле **Имя файла** укажите файл со списком доверенных адресатов.
   c. Нажмите на кнопку **Открыть**.
9. Нажмите на кнопку **Сохранить**.

Настройка исключений по маске имен файлов

► *Чтобы настроить исключения по маске имен файлов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить исключения по маске имен файлов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить исключения по маске имен файлов для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить исключения.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.
4. Установите флажок **Не проверять файлы по маскам**.
5. Добавьте маску имен файлов (далее также маску) в список масок. Для этого выполните следующие действия:
   a. Введите маску в поле ввода.

      Примеры разрешенных масок имен файлов:
      - *.txt – все файлы с расширением txt, например, readme.txt или notes.txt;
      - readme.??? – все файлы с именем readme и расширением из трех символов, например, readme.txt или readme.doc;
      - test – все файлы с именем test без расширения.

   b. Нажмите на кнопку , расположенную справа от поля ввода.
6. Чтобы удалить маску из списка масок, выделите строку с маской в списке и нажмите на кнопку .
7. Чтобы экспортировать список масок в файл, выполните следующие действия:
   a. нажмите на кнопку ;
   b. в открывшемся окне укажите название файла в поле **Имя файла**;
   c. нажмите на кнопку **Сохранить**.
8. Чтобы импортировать список масок из файла, выполните следующие действия:
   a. нажмите на кнопку ;
   b. в открывшемся окне в поле **Имя файла** укажите файл со списком масок;
   c. нажмите на кнопку **Открыть**.
9. Нажмите на кнопку **Сохранить**.

Этот параметр учитывается при фильтрации вложений и содержимого (см. раздел "Фильтрация вложений и содержимого" на стр. 146). Файлы, исключенные из антивирусной проверки по именам и / или маскам имен файлов, также исключаются из фильтрации вложений.

Настройка параметров проверки вложенных объектов-контейнеров и архивов

По умолчанию Kaspersky Security проверяет архивы и объекты-контейнеры, вложенные в сообщения. Чтобы оптимизировать работу Kaspersky Security, сократить нагрузку на сервер и уменьшить время обработки почтового потока, вы можете отключить проверку вложений или ограничить уровень вложенности таких объектов. Не рекомендуется отключать проверку вложений надолго, так как они могут содержать вирусы и другие вредоносные объекты.

► *Чтобы настроить проверку вложенных объектов-контейнеров и архивов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить проверку вложенных объектов-контейнеров и архивов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить проверку вложенных объектов-контейнеров и архивов для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите выполнить настройку.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.
4. Включите / отключите проверку вложенных объектов-контейнеров и архивов, выполнив одно из следующих действий:
   - Если вы хотите, чтобы программа проверяла такие объекты, установите флажок **Проверять вложенные контейнеры/архивы**.
   - Если вы хотите, чтобы программа не проверяла такие объекты, снимите этот флажок.
5. Если вы хотите ограничить допустимый уровень вложенности проверяемых контейнеров и архивов, установите флажок **Проверять вложенные контейнеры/архивы с уровнем вложенности не более** и укажите ограничение в поле ввода с прокруткой.
6. Нажмите на кнопку **Сохранить**.

Если программа работает в DAG серверов Microsoft Exchange, параметры проверки вложенных объектов-контейнеров и архивов, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в DAG. На остальных серверах этой DAG настраивать параметры проверки вложенных объектов-контейнеров и архивов не требуется.

Редактирование сообщения об удалении вложения модулем Антивирус

Если по результатам антивирусной проверки программа удаляет файл вложения из сообщения электронной почты, то к исходному сообщению прикрепляется файл формата TXT. Файл содержит текст, информирующий пользователя о действии программы. По умолчанию в текст включен список удаленных объектов. Вы можете отредактировать содержание этого информационного сообщения и включить туда инструкции и другие сведения, актуальные для сотрудников вашей организации.

► *Чтобы отредактировать сообщение, информирующее пользователя об удалении вложенного объекта модулем Антивирус, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел нужного Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.

Нажмите на кнопку **Редактировать** (*Сообщение об удалении вложения Антивирусом*).

1. В открывшемся окне в поле **Текст сообщения** отредактируйте содержание сообщения.
2. Нажмите **ОК**.
3. Нажмите на кнопку **Сохранить**.

О предотвращении задержки сообщений модулем Антивирус

В исключительных случаях при работе модуля Антивирус время проверки сообщений антивирусным ядром может значительно увеличиться. Это возможно при сбое в работе антивирусного ядра. Увеличение времени проверки может привести к образованию очереди сообщений, ожидающих проверки Антивирусом. В результате доставка сообщения пользователю может быть задержана или может увеличиться время ожидания пользователя при открытии уже полученных сообщений.

Для решения этой проблемы в программе предусмотрена возможность предотвращения задержки сообщений модулем Антивирус. При обнаружении сбоя антивирусного ядра программа выполняет следующие действия:

- на короткое время переключает Антивирус в режим работы, в котором он может пропускать без проверки ожидающие сообщения;
- отображает сообщение об ошибке в окне состояния защиты сервера в рабочей области узла <Имя сервера> (см. раздел "Просмотр сведений о состоянии защиты сервера Microsoft Exchange" на стр. 85);
- записывает сообщение об ошибке в журнал программы (см. раздел "Журналы программы" на стр. 199);
- уведомляет об ошибке по электронной почте, если настроены уведомления о системных ошибках (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 175).

По истечении заданного периода времени Антивирус возобновляет проверку сообщений в обычном режиме. Если к этому моменту сбой в работе антивирусного ядра не устранен, описанный процесс повторяется.

По умолчанию функция предотвращения задержки сообщений модулем Антивирус работает и не может быть выключена в интерфейсе программы. Для выключения этой функции или получения дополнительных сведений вы можете обратиться в Службу технической поддержки "Лаборатории Касперского".

kaspersky

Окно Типы файлов вложений

В этом окне вы можете сформировать список типов файлов, который программа использует для фильтрации вложений по типу файла.

Типы файлов

Иерархический список, в котором перечислены распространенные типы файлов, сгруппированные по функциональному назначению (например, Исполняемые файлы, Изображения).

Типы файлов и группы типов файлов, флажки для которых установлены, участвуют в фильтрации вложений. Программа проверяет файлы вложений на соответствие этим типам файлов.

Программа определяет тип файла вложения по содержимому файла, а не по его расширению. Это позволяет выполнять фильтрацию правильно даже в случае, если расширение файла вложения не соответствует типу этого файла (например, если расширение было намеренно изменено).

По умолчанию все флажки сняты.

Окно Имена файлов вложений

В этом окне вы можете сформировать список имен файлов, который программа использует для фильтрации вложений по имени файла.

Допустимо указывать в именах файлов маски (wildcards), например, `attach*.*`, `report?.doc*`.

Для формирования списка вы можете использовать поле ввода и следующие кнопки:

- – добавить в список запись, указанную в поле ввода.
- – удалить выбранную запись из списка.
- – экспортировать список в файл.
- – импортировать список из файла.

kaspersky

Защита от спама и фишинга

Одной из главных задач Kaspersky Security является фильтрация спама в почтовом потоке, проходящем через сервер Microsoft Exchange. Модуль Анти-Спам фильтрует входящую почту до того, как сообщения попадут в почтовые ящики пользователей.

Анти-Спам проверяет следующие типы данных:

- Внутренний и внешний почтовый поток, следующий по протоколу SMTP с анонимной проверкой подлинности на сервере.
- Сообщения, попадающие на сервер через анонимные внешние подключения (edge-сервер).
- Исходящие сообщения электронной почты.

Анти-Спам не проверяет следующие типы данных:

- Внутренний почтовый поток организации.
- Внешний почтовый поток, поступающий на сервер через аутентифицируемые сессии. Проверку такого почтового потока можно включить вручную (см. раздел "Настройка дополнительных параметров проверки на спам и фишинг" на стр. 125), при помощи параметра **Проверять на спам сообщения, поступающие через доверительные соединения**.
- Сообщения, поступающие от других серверов почтовой инфраструктуры Microsoft Exchange, поскольку соединения между серверами одной инфраструктуры Microsoft Exchange считаются доверительными. При этом если сообщения поступили в инфраструктуру через сервер, на котором отсутствует или неактивен Анти-Спам, они не будут проверены на спам и на всех последующих серверах данной инфраструктуры по пути следования сообщений. Включить проверку таких сообщений можно вручную (см. раздел "Настройка дополнительных параметров проверки на спам и фишинг" на стр. 125), при помощи параметра **Проверять на спам сообщения, поступающие через доверительные соединения**.

Анти-Спам проверяет заголовок сообщения, содержимое сообщения, вложенные файлы, элементы оформления и другие атрибуты сообщения. При проверке Анти-Спам использует лингвистические и эвристические алгоритмы, основанные на сравнении проверяемого сообщения с сообщениями-образцами, а также дополнительные и облачные службы, такие как Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 99).

По результатам фильтрации Анти-Спам присваивает сообщениям один из следующих статусов:

- *Спам*. Сообщение имеет признаки, характерные для спама.
- *Возможный спам*. Сообщение имеет признаки, характерные для спама, но значение спам-рейтинга сообщения не позволяет классифицировать его как спам.
- *Массовые рассылки*. Сообщение относится к рассылке (как правило, новостного или рекламного характера), но не имеет признаков, достаточных, чтобы считать его спамом.
- *Формальное оповещение*. Техническое сообщение, например о доставке сообщения адресату.
- *Чистое*. Сообщение не имеет признаков, характерных для спама.
- *Внесено в черный список*. IP-адрес отправителя сообщения или адрес его электронной почты входит в черный список адресов.

При проверке внутреннего почтового потока, следующего по протоколу SMTP, и при включении проверки на спам сообщений, поступающих через доверительные соединения, Анти-Спам присваивает статус *Чистое* следующим сообщениям: сообщения рассылок, технические сообщения и сообщения, значение спам-рейтинга которых не позволяет классифицировать их как спам.

Вы можете выбирать действия, которые программа должна выполнять над сообщениями с определенным статусом (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123). Для выбора доступны следующие действия:

- **Пропускать**. Сообщение будет доставлено адресату без изменений.
- **Отклонять**. Сервер-отправитель получит сообщение об ошибке при отправке сообщения (код ошибки 500), сообщение не будет доставлено адресату.
- **Удалять**. Сервер-отправитель сообщения получит уведомление об отправке сообщения (код 250), но сообщение не будет доставлено адресату.
- **Добавлять SCL-оценку**. Сообщениям будет даваться оценка вероятности нежелательной почты (SCL). Оценка SCL представляет собой число в диапазоне от 1 до 9. Высокая оценка SCL означает, что сообщение с большой вероятностью является спамом. SCL-оценка рассчитывается путем деления спам-рейтинга сообщения на 10. Если в результате вычисления получается цифра больше 9, то SCL-оценка принимается равной 9. SCL-оценка, присвоенная сообщениям, учитывается при дальнейшей обработке сообщений инфраструктурой Microsoft Exchange.
- **Добавлять метку в тему сообщения**. Сообщения, которым присвоены статусы *Спам*, *Возможный спам*, *Массовые рассылки* или *Внесен в черный список*, отмечаются в теме сообщения специальными метками `[!!SPAM]`, `[!!Probable Spam]`, `[!!Mass Mail]` или `[!!Blacklisted]` соответственно. Вы можете изменять текст этих меток (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123).

Программа поддерживает четыре уровня чувствительности проверки на спам:

- *Максимальный*. Этот уровень чувствительности следует использовать, если вы получаете спам очень часто. При выборе этого уровня чувствительности может возрасти частота распознавания полезной почты как спама.
- *Высокий*. При выборе этого уровня чувствительности сокращается (по сравнению с уровнем *Максимальный*) частота распознавания полезной почты как спама и увеличивается скорость проверки. Уровень чувствительности *Высокий* следует использовать, если вы часто получаете спам.
- *Низкий*. При выборе этого уровня чувствительности сокращается (по сравнению с уровнем *Высокий*) частота распознавания полезной почты как спама и увеличивается скорость проверки. Уровень чувствительности *Низкий* обеспечивает оптимальное сочетание скорости и качества проверки.
- *Минимальный*. Этот уровень чувствительности следует использовать, если вы редко получаете спам.

По умолчанию защита от спама осуществляется на уровне чувствительности *Низкий*. Вы можете повысить или понизить уровень чувствительности (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123). В зависимости от уровня чувствительности и в соответствии со спам-рейтингом, полученным в результате проверки, сообщению может быть присвоен статус *Спам* или *Возможный спам* (см. таблицу ниже).

Таблица 7. Пороговые значения спам-рейтинга на разных уровнях чувствительности проверки на спам

Уровень чувствительности	Возможный спам	Спам
Максимальный	60	75
Высокий	70	80
Низкий	80	90
Минимальный	90	100

В исключительных случаях при сбое в работе ядра Анти-Спама время проверки сообщений на спам может значительно увеличиваться. В таких случаях для предотвращения задержки сообщений Анти-Спам временно переходит в режим ограниченной проверки. В этом режиме некоторые сообщения могут быть пропущены без проверки на спам.

В этом разделе

Включение и выключение защиты сервера от спама

Выключение защиты сервера от спама значительно повышает вероятность получения нежелательной почты. Не рекомендуется выключать защиту от спама без необходимости.

► *Чтобы включить или выключить защиту сервера Microsoft Exchange от спама, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите включить или выключить защиту от спама для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите включить или выключить защиту от спама для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить защиту от спама.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** в блоке **Параметры проверки на спам** выполните одно из следующих действий:
   - Если вы хотите включить защиту от спама, установите флажок **Включить проверку сообщений на спам**.
   - Если вы хотите выключить защиту от спама, снимите этот флажок.
4. Нажмите на кнопку **Сохранить**.

О проверке на фишинг

В программе Kaspersky Security предусмотрена проверка сообщений на наличие фишинговых и вредоносных ссылок.

Фишинговые ссылки ведут на мошеннические сайты, целью которых является кража персональных данных пользователей, таких как информация о банковских счетах. Частным примером фишинг-атаки может служить сообщение якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, но реально находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших персональных данных.

Вредоносные ссылки ведут на веб-ресурсы, которые предназначены для распространения вредоносного программного обеспечения.

Для защиты сервера Microsoft Exchange от фишинга и вредоносных ссылок программа использует базы адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые и вредоносные. Базы регулярно обновляются и входят в поставку программы Kaspersky Security.

При проверке сообщений на наличие фишинга и вредоносных ссылок программа анализирует не только ссылки на веб-адреса, но и заголовки сообщений, содержимое сообщений, вложенные файлы, элементы оформления и другие атрибуты сообщений. При проверке также используются эвристические алгоритмы и

запросы к облачным службам Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 99) (KSN), если использование KSN в Анти-Спаме включено (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123). Использование KSN позволяет программе получать актуальную информацию о фишинговых и вредоносных веб-ресурсах до их включения в базы "Лаборатории Касперского".

При обнаружении в сообщении фишинговых или вредоносных ссылок программа присваивает сообщению статус *Фишинг*. Вы можете выбирать действия, которые программа должна выполнять над сообщениями с этим статусом. Для выбора доступны следующие действия:

- **Пропускать**. Сообщение будет доставлено адресату без изменений.
- **Отклонять**. Сервер-отправитель получит сообщение об ошибке при отправке сообщения (код ошибки 500), сообщение не будет доставлено адресату.
- **Удалять**. Сервер-отправитель сообщения получит уведомление об отправке сообщения (код 250), но сообщение не будет доставлено адресату.
- **Добавлять SCL и PCL оценку**. Сообщениям будет присваиваться оценка вероятности нежелательной почты (SCL), равная 9, и оценка вероятности фишинга (PCL), равная 8. При поступлении в почтовую инфраструктуру Microsoft Exchange сообщений с высоким значением PCL-оценки (более 3), они автоматически попадают в папки "Нежелательная почта" ("Junk E-Mail"), а все ссылки в них – деактивируются.
- **Добавлять метку в тему сообщения**. Сообщения, которым присвоен статус *Фишинг*, будут отмечены специальной меткой `[!!Phishing]` в теме сообщения. Вы можете изменить текст этой метки (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123).

Включение и выключение проверки сообщений на фишинг

Вы можете включить проверку сообщений на фишинг, только если включена защита сервера Microsoft Exchange от спама (см. раздел "Включение и выключение защиты сервера от спама" на стр. 121). Проверка сообщений на фишинг включает также проверку на вредоносные ссылки.

► *Чтобы включить или выключить проверку сообщений на фишинг, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите включить или выключить проверку сообщений на фишинг для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите включить или выключить проверку сообщений на фишинг для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить проверку на фишинг.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** в блоке **Параметры проверки на спам** выполните одно из следующих действий:
   - Если вы хотите включить проверку сообщений на фишинг, установите флажок **Включить проверку сообщений на наличие фишинга**.
   - Если вы хотите выключить проверку сообщений на фишинг, снимите этот флажок.
4. Нажмите на кнопку **Сохранить**.

Настройка параметров проверки на спам и фишинг

► *Чтобы настроить параметры проверки на спам и фишинг, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить параметры проверки на спам и фишинг нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите настроить параметры проверки на спам и фишинг Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры проверки на спам и фишинг.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Параметры проверки на спам**.
4. Установите флажок **Включить проверку сообщений на спам**, если вы хотите, чтобы программа проверяла сообщения на спам с помощью модуля Анти-Спам.
5. С помощью ползунка **Уровень чувствительности** установите уровень чувствительности проверки на спам (см. раздел "Защита от спама и фишинга" на стр. 118): **максимальный**, **высокий**, **низкий**, **минимальный**.
6. В блоке **Параметры обработки спама** в раскрывающемся списке **Действие** выберите действие, которое программа должна выполнять над сообщениями с каждым из перечисленных статусов (*Спам*, *Возможный спам*, *Формальное оповещение*, *Адрес в черном списке*, *Массовая рассылка*):
   - **Пропускать**. Сообщение будет доставлено адресату без изменений.
   - **Отклонять**. Сервер-отправитель получит сообщение об ошибке при отправке сообщения (код ошибки 500), сообщение не будет доставлено адресату.
   - **Удалять**. Сервер-отправитель получит уведомление об отправке сообщения (код 250), но сообщение не будет доставлено адресату.

     Если в вашей организации есть несколько серверов Microsoft Exchange, через которые проходят сообщения, Microsoft Exchange обрабатывает спам-сообщения следующим образом: если спам-сообщение не было удалено на первом сервере, но это спам-сообщение было удалено на последующем сервере, то спам-сообщение хранится в теневой очереди (shadow redundancy queue) первого сервера в течение периода, установленного в параметрах Microsoft Exchange. Такая обработка сообщений в Microsoft Exchange приводит к увеличению теневой очереди на первом сервере.
7. В блоке **Параметры обработки спама** укажите дополнительные действия, которые программа должна выполнять над сообщениями с каждым из перечисленных статусов. Установите флажки для нужных параметров:
   - **Добавлять SCL-оценку**. К сообщению будет добавлена оценка вероятности нежелательной почты (SCL-оценка). SCL-оценка может быть числом в диапазоне от 1 до 9. Высокая SCL-оценка означает, что сообщение с большой вероятностью является спамом. SCL-оценка, присвоенная сообщениям, учитывается при дальнейшей обработке сообщений инфраструктурой Microsoft Exchange.
   - **Сохранять копию**. Копия сообщения будет сохранена в резервном хранилище.

- **Добавлять метку в тему сообщения**. Сообщения, которым присвоены статусы *Спам*, *Возможный спам*, *Формальное оповещение*, *Адрес в черном списке* и *Массовая рассылка*, отмечаются специальными метками в теме сообщения: `[!!Spam]`, `[!!Probable Spam]`, `[!!Formal]`, `[!!Blacklisted]` и `[!!Mass Mail]` соответственно. Если требуется, измените текст этих меток в полях ввода, соответствующих статусам.

8. Установите флажок **Включить проверку сообщений на наличие фишинга**, если вы хотите, чтобы программа проверяла сообщения на наличие фишинговых ссылок.
9. В блоке **Параметры обработки спама** под флажком **Включить проверку сообщений на наличие фишинга** в раскрывающемся списке **Действие** выберите действие, которое программа должна выполнять над сообщениями со статусом *Фишинг*:
   - **Пропускать**. Сообщение будет доставлено адресату без изменений.
   - **Отклонять**. Сервер-отправитель получит сообщение об ошибке при отправке сообщения (код ошибки 500), сообщение не будет доставлено адресату.
   - **Удалять**. Сервер-отправитель получит уведомление об отправке сообщения (код 250), но сообщение не будет доставлено адресату.
10. В блоке **Параметры обработки спама** под флажком **Включить проверку сообщений на наличие фишинга** укажите дополнительные действия, которые программа должна выполнять над сообщениями со статусом *Фишинг*. Установите флажки для нужных параметров:
    - **Добавлять SCL и PCL оценку**. Сообщениям будет присваиваться оценка вероятности нежелательной почты (SCL), равная 9, и оценка вероятности фишинга (PCL), равная 8.Сообщения с высоким значением PCL-оценки (более 3), при поступлении в почтовую инфраструктуру Microsoft Exchange автоматически попадают в папки "Нежелательная почта" ("Junk E-Mail"), а все ссылки в них – деактивируются.
    - **Сохранять копию**. Копия сообщения будет сохранена в резервном хранилище.
    - **Добавлять метку в тему сообщения**. Сообщения, которым присвоен статус *Фишинг*, отмечаются специальной меткой в теме сообщения: `[!!Phishing]`. Если требуется, измените текст этой метки в поле ввода справа.
11. В блоке **Параметры обработки спама** настройте параметры использования дополнительных служб проверки на спам (см. раздел "О дополнительных службах, функциях и технологиях защиты от спама" на стр. 128):
    - Если вы хотите включить использование служб Kaspersky Security Network (KSN) при проверке на спам и фишинг, выполните следующие действия:
      a. Установите флажок **Использовать Kaspersky Security Network**.
      b. Если требуется, укажите максимальное время ожидания ответа на запросы к серверу KSN в поле **Максимальное время ожидания при запросе в KSN**.

         Значение по умолчанию – 5 сек.

      Флажок **Использовать Kaspersky Security Network** доступен, если в блоке **Параметры KSN** в узле **Настройка** выбран вариант **Я принимаю Положение о KSN. Использовать Kaspersky Security Network** или вариант **Использовать Kaspersky Private Security Network (KPSN).** Все параметры службы Kaspersky Security Network распространяются на службу Kaspersky Private Security Network.

- Если вы хотите включить использование репутационной службы Reputation Filtering, установите флажок **Использовать Reputation Filtering**. Флажок **Reputation Filtering** доступен, если установлен флажок **Использовать Kaspersky Security Network**.
- Если вы хотите включить использование службы быстрых обновлений баз Анти-Спама Enforced Anti-Spam Updates Service, установите флажок **Использовать Enforced Anti-Spam Updates Service**.

> Если в вашей организации для доступа в интернет используется прокси-сервер, вы можете настроить подключение программы к службам Kaspersky Security Network и Enforced Anti-Spam Updates Service через прокси-сервер (см. раздел "Настройка параметров прокси-сервера" на стр. 169).

12. Установите флажок **Проверять исходящие сообщения и удалять сообщения, являющиеся спамом или содержащие фишинговую ссылку** в блоке **Параметры обработки исходящих сообщений**, если вы хотите включить проверку исходящих сообщений на спам и фишинг.
13. Нажмите на кнопку **Сохранить**.

Настройка дополнительных параметров проверки на спам и фишинг

Вы можете настраивать дополнительные параметры проверки на спам и фишинг, такие как ограничения проверки сообщений по времени и размеру или возможности проверки на спам вложенных в сообщение файлов Microsoft Office.

► *Чтобы настроить ограничения проверки сообщений на спам и фишинг по времени и размеру, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить ограничения проверки сообщений на спам и фишинг для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить ограничения проверки сообщений на спам и фишинг Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить ограничения проверки.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Дополнительные параметры Анти-Спама**.
4. В блоке параметров **Ограничения** в поле ввода с прокруткой укажите **Максимальное время проверки сообщения** в секундах.

   Если время проверки сообщения превысит указанное, проверка сообщений на спам и фишинг будет остановлена. Значение по умолчанию равно 60 сек. Если включено добавление к сообщению служебных заголовков, они будут содержать запись о превышении максимального времени проверки.
5. В блоке параметров **Ограничения** в поле ввода с прокруткой укажите **Максимальный размер проверяемого объекта** в килобайтах.

   Если размер сообщения со всеми вложениями превысит указанный размер, проверка на спам и фишинг осуществляться не будет, сообщение будет доставлено получателю. Значение по

умолчанию равно 1536 КБ (1,5 МБ). Максимальное значение – 2096128 КБ (2047 МБ), минимальное значение – 1 КБ. Если включено добавление к сообщению служебных заголовков, они будут содержать запись о превышении максимального размера проверяемого объекта.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

► *Чтобы настроить параметры проверки файлов Microsoft Office на спам, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры проверки файлов Microsoft Office на спам и фишинг для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры проверки файлов Microsoft Office на спам и фишинг Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры проверки файлов Microsoft Office.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Дополнительные параметры Анти-Спама**.
4. В блоке параметров **Параметры проверки файлов Microsoft Office** выполните следующие действия:
   - Если вы хотите, чтобы программа проверяла на спам содержимое документов Microsoft Word, установите флажок **Проверять файлы формата DOC**.
   - Если вы хотите, чтобы программа проверяла на спам содержимое документов RTF установите флажок **Проверять файлы формата RTF**.

     Эти параметры не оказывают влияние на проверку документов на фишинг.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

► *Чтобы настроить использование дополнительных параметров проверки на спам и фишинг, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить использование дополнительных параметров проверки сообщений на спам и фишинг для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить использование дополнительных параметров проверки сообщений на спам и фишинг Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить использование дополнительных параметров проверки.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Дополнительные параметры Анти-Спама**.
4. Если вы хотите, чтобы изображения, приложенные к сообщению, проверялись с использованием технологии GSG (технология анализа изображений), установите флажок **Использовать технологию анализа изображений**.

С помощью этой технологии изображения проверяются на соответствие образцам, имеющимся в базе Анти-Спама. В случае нахождения соответствий спам-рейтинг сообщения будет увеличен.

5. Установите флажок **Проверять на спам сообщения, поступающие через доверительные соединения**, чтобы включить проверку сообщений, полученных по доверительным соединениям (Trusted Connection), на спам.

   Проверка на наличие вредоносных ссылок (фишинг) сообщений, полученных по доверительным соединениям, включена постоянно.

6. Установите флажок **Не проверять сообщения для адреса Postmaster**, чтобы отключить проверку на спам и фишинг сообщений, полученных для адреса Postmaster.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка увеличения спам-рейтинга сообщений

Вы можете настраивать параметры Анти-Спама, влияющие на определение специальной характеристики сообщений – спам-рейтинга. Эти параметры позволяют настраивать увеличение спам-рейтинга сообщений по результатам анализа адреса электронной почты отправителя и темы сообщения, а также в случае, когда сообщение написано на иностранном языке.

► *Чтобы настроить увеличение спам-рейтинга сообщений по результатам анализа адреса отправителя, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить увеличение спам-рейтинга сообщений для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить увеличение спам-рейтинга сообщений для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить увеличение спам-рейтинга сообщений.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Параметры определения спам-рейтинга**.
4. В блоке параметров **Увеличить спам-рейтинг, если** установите нужные флажки для следующих параметров:
   - **Поле "Кому" не содержит адресов**. Если поле «Кому» не заполнено, спам-рейтинг сообщения будет увеличен.
   - **Адрес отправителя сообщения содержит цифры**. Если адрес отправителя содержит цифры, спам-рейтинг сообщения будет увеличен.
   - **Адрес отправителя сообщения (находящийся в теле сообщения) не содержит доменной части**. Если адрес отправителя не содержит имени домена, спам-рейтинг сообщения будет увеличен.
5. Нажмите на кнопку **Сохранить**.

► *Чтобы настроить увеличение спам-рейтинга сообщений по результатам анализа темы сообщения, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить увеличение спам-рейтинга сообщений для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить увеличение спам-рейтинга сообщений для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить увеличение спам-рейтинга сообщений.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок параметров **Параметры определения спам-рейтинга**.
4. В блоке параметров **Увеличить спам-рейтинг, если тема сообщения содержит** установите нужные флажки для следующих параметров:
   - **Более 250 символов**. Если тема сообщения содержит больше 250 символов, спам-рейтинг сообщения будет увеличен.
   - **Много знаков пробелов и/или точек**. Если тема сообщения содержит много пробелов и / или точек, спам-рейтинг сообщения будет увеличен.
   - **Метку времени**. Если тема сообщения содержит цифровой идентификатор или метку времени (timestamp), спам-рейтинг сообщения будет увеличен.
5. Нажмите на кнопку **Сохранить**.

► *Чтобы настроить увеличение спам-рейтинга сообщений по результатам анализа языка, на котором написано сообщение, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить увеличение спам-рейтинга сообщений для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить увеличение спам-рейтинга сообщений для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить увеличение спам-рейтинга сообщений.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок параметров **Параметры определения спам-рейтинга**.
4. В блоке параметров **Увеличить спам-рейтинг, если язык сообщения** установите флажки для тех языков, сообщения на которых вы не ожидаете получать:
   - **Китайский**, если вы не ожидаете сообщений на китайском языке.
   - **Корейский**, если вы не ожидаете сообщений на корейском языке.
   - **Тайский**, если вы не ожидаете сообщений на тайском языке.
   - **Японский**, если вы не ожидаете сообщений на японском языке.
5. Нажмите на кнопку **Сохранить**.

kaspersky

О дополнительных службах, функциях и технологиях защиты от спама

Для более тщательной защиты почты от спама программа использует следующие дополнительные функции, технологии и службы «Лаборатории Касперского»:

- DNSBL (Domain Name System Block List). Служба получения информации с DNSBL-серверов, содержащих общедоступные списки IP-адресов, уличенных в рассылке спама.
- SURBL (Spam URI Realtime Block List). Служба получения информации с SURBL-серверов, содержащих общедоступные списки ссылок, которые ведут на интернет-ресурсы, рекламируемые отправителями спама. Таким образом, если сообщение содержит веб-адреса из этого списка ссылок, оно с большей вероятностью является спамом.

  При расчете спам-рейтинга учитывается вес каждого ответившего DNSBL- и SURBL-сервера. Если суммарный рейтинг ответивших серверов больше 100, программа присваивает сообщению статус *Адрес в черном списке* и выполняет действие, указанное (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123) для этого статуса. Если суммарный рейтинг ответивших серверов меньше 100, программа увеличивает спам-рейтинг сообщения.
- KSN (Kaspersky Security Network). Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

  По умолчанию использование KSN отключено (см. раздел "Участие в Kaspersky Security Network" на стр. 99). Чтобы начать использование KSN, вам нужно принять специальное Положение о KSN, регламентирующее порядок получения и использования информации с компьютера, на котором работает Kaspersky Security.
- Enforced Anti-Spam Updates Service. Служба быстрых обновлений баз Анти-Спама. Если использование Enforced Anti-Spam Updates Service включено, программа постоянно связывается с серверами "Лаборатории Касперского" и обновляет собственные базы Анти-Спама сразу после появления новых описаний спам-сообщений на серверах "Лаборатории Касперского". Это позволяет увеличить скорость реагирования Анти-Спама на появление новых рассылок спама.

  Для работы Enforced Anti-Spam Updates Service требуется выполнение следующих условий:

  - постоянное соединение с интернетом компьютера, на котором установлен Сервер безопасности;
  - регулярное обновление баз Анти-Спама (рекомендуемая частота обновления – каждые пять минут).
- Reputation Filtering. Облачная репутационная служба дополнительной проверки сообщений, которая помещает сообщения, требующие дополнительной проверки, в специальное временное хранилище – *карантин*. В течение определенного времени (50 минут) программа выполняет повторную проверку сообщения, используя дополнительные сведения, получаемые от серверов "Лаборатории Касперского" (например, из сети KSN). Если в течение заданного времени программа не классифицирует сообщение как спам, она пропускает сообщение. Применение службы Reputation Filtering позволяет повысить точность распознавания спама и снизить вероятность ложных срабатываний Анти-Спама.

  Для использования службы Reputation Filtering вам нужно подтвердить свое участие в Kaspersky Security Network (KSN) и принять специальное Положение о KSN.

  > Сообщения, помещенные службой Reputation Filtering в карантин и не классифицированные как спам, будут доставлены получателям по истечении 50 минут, даже если работа программы будет завершена или приостановлена.

- Динамический DNS-клиент. Функция, которая определяет потенциальную принадлежность IP-адреса отправителя к бот-сети по его обратной DNS-зоне. Эту функцию можно использовать при условии, что защищаемый SMTP-сервер не обслуживает собственных пользователей, использующих xDSL- или Dial-up-соединение.
- Технология SPF (Sender Policy Framework). Технология, позволяющая проверить, не подделан ли домен отправителя. С помощью технологии SPF домены предоставляют право на рассылку почты от своего имени определенным компьютерам. Если отправитель сообщения не входит в список авторизованных отправителей, спам-рейтинг сообщения будет увеличен.

Использование внешних служб проверки на спам

► *Чтобы включить использование внешних служб (см. раздел "О дополнительных службах, функциях и технологиях защиты от спама" на стр. 128) проверки на спам, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить использование внешних служб проверки на спам для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите настроить использование внешних служб проверки на спам для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить использование внешних служб проверки на спам.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок параметров **Использование внешних служб Анти-Спама**.
4. Если вы хотите, чтобы при проверке на спам программа учитывала результаты работы внешних служб проверки IP-адресов и веб-адресов, установите флажок **Использовать внешние ресурсы проверки на спам**.
5. Если вы хотите использовать свой список DNS-имен серверов, предоставляющих черные списки DNS-имен, и назначать им весовые коэффициенты, установите флажок **Использовать набор черных списков DNSBL**. Чтобы сформировать пользовательский список выполните следующие действия:
   - Если вы хотите добавить запись в пользовательский список, укажите DNS-имя сервера и весовой коэффициент в соответствующих полях и нажмите на кнопку .
   - Если вы хотите удалить запись из пользовательского списка, нажмите на кнопку .
   - Если вы хотите импортировать пользовательский список, нажмите на кнопку .
   - Если вы хотите экспортировать пользовательский список, нажмите на кнопку .
6. Если вы хотите использовать свой список SURBL-имен серверов, предоставляющих черные списки URL, и назначать им весовые коэффициенты, установите флажок **Использовать набор черных списков SURBL**. Чтобы сформировать пользовательский список, выполните следующие действия:
   - Если вы хотите добавить запись в пользовательский список, укажите DNS-имя сервера и весовой коэффициент в соответствующих полях и нажмите на кнопку .
   - Если вы хотите удалить запись, нажмите на кнопку .
   - Если вы хотите импортировать пользовательский список, нажмите на кнопку .

- Если вы хотите экспортировать пользовательский список, нажмите на кнопку  .

7. Если вы хотите включить проверку наличия записи в обратной зоне для IP-адреса отправителя в DNS, установите флажок **Проверять наличие IP-адреса отправителя в DNS**.
8. Если вы хотите включить использование технологии SPF, установите флажок **Использовать технологию SPF**.
9. Если вы хотите включить проверку IP-адреса отправителя на потенциальную принадлежность к бот-сети по его обратной DNS-зоне, установите флажок **Проверять принадлежность IP-адреса отправителя динамическому DNS**.

   В случае положительного результата проверки спам-рейтинг сообщения будет увеличен.
10. В поле ввода с прокруткой **Максимальное время ожидания при DNS-запросе** укажите максимальное время ожидания в секундах.

    Значение по умолчанию составляет 5 сек. После истечения времени ожидания программа проверяет сообщение на спам без использования проверки принадлежности IP-адреса отправителя динамическому DNS.

О черном и белом списках адресов электронной почты

Черный и белый списки позволяют указывать адреса электронной почты, которые вы хотите обрабатывать в соответствии с параметрами, настроенными отдельно для этих списков. Например, вы можете добавить адрес в белый список и отключить проверку на спам для сообщений, отправленных с этого адреса, или настроить удаление всех сообщений, отправленных с адреса, добавленного в черный список.

Белый список адресов Анти-Спама

Белый список позволяет пропускать сообщения независимо от значений параметров Анти-Спама, установленных в блоке **Параметры обработки спама**.

Белый список может содержать адреса двух видов, различных по назначению:

- Адреса отправителей сообщений. Сообщения, полученные с таких адресов Анти-Спам пропускает независимо от установленных параметров проверки на спам. Адреса отправителей могут быть заданы в виде адреса электронной почты, маски адресов электронной почты, либо IP-адреса.
- Адреса получателей сообщений. Сообщения, отправленные на такие адреса, Анти-Спам пропускает независимо от установленных параметров проверки на спам. Адреса получателей могут быть заданы в виде адреса электронной почты, маски адресов электронной почты, а также учетной записи или группы учетных записей для адресов внутри организации.

Анти-Спам может пропускать сообщения без проверки на спам любого типа, включая массовые рассылки, или только без проверки на массовые рассылки в зависимости от параметров, установленных для адреса, добавленного в белый список:

- **Спам, фишинг и массовые рассылки**. Анти-Спам пропускает сообщения, классифицированные как *Спам*, *Возможный спам*, *Формальное оповещение*, *Фишинг и Массовая рассылка*.
- **Массовые рассылки**. Анти-Спам пропускает сообщения, классифицированные только как *Массовая рассылка*.

> Антивирусная проверка полученных и отправленных сообщений выполняется независимо от наличия адресов получателей и отправителей сообщений в белом списке.

По умолчанию белый список пуст.

Черный список адресов Анти-Спама

Черный список позволяет обрабатывать особым образом сообщения, поступающие от отправителей, адреса которых перечислены в этом списке. Программа присваивает сообщениям от таких отправителей статус *Адрес в черном списке* и выполняет действие, указанное для этого статуса в блоке **Параметры обработки спама**, например, отклоняет такие сообщения.

Адреса отправителей в черном списке могут быть заданы в виде адреса электронной почты, маски адресов электронной почты, либо IP-адреса.

По умолчанию черный список пуст.

Приоритеты черного и белого списков при обработке сообщений

Программа применяет черный и белый списки к сообщениям согласно их приоритетам:

1. Записи в белом списке с областью действия "Спам, фишинг и массовые рассылки" обладают наибольшим приоритетом.
2. Записи в черном списке обладают меньшим приоритетом, чем записи в белом списке с областью действия "Спам, фишинг и массовые рассылки".
3. Записи в белом списке с областью действия "Массовые рассылки" обладают наименьшим приоритетом.

Если адрес отправителя добавлен одновременно в записи белого и черного списков, результат обработки сообщений от этого отправителя будет зависеть от области действия записи белого списка.

Таблица 8. Порядок обработки сообщений от отправителя, добавленного в черный и белый списки

Условия	Результат обработки сообщения
Адрес отправителя добавлен в черный список и в белый список с областью действия "Спам, фишинг и массовые рассылки".	Запись белого списка имеет приоритет. Программа пропускает сообщения от этого отправителя независимо от установленных параметров проверки на спам.
Адрес отправителя добавлен в черный список и в белый список с областью действия "Массовые рассылки"	Запись черного списка имеет приоритет. Программа присваивает сообщениям статус *Адрес в черном списке* и обрабатывает их в соответствии с параметрами, указанными для этого статуса.

Формирование белого списка адресов Анти-Спама

► *Чтобы добавить адрес в белый список адресов Анти-Спама, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите сформировать белый список для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите сформировать белый список для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите сформировать белый список.

2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Белый список адресов Анти-Спама**.
4. Чтобы добавить новый адрес в список, выполните следующие действия:
   a. Нажмите на кнопку **Добавить получателя**, чтобы добавить в список адрес получателя, или на кнопку **Добавить отправителя**, чтобы добавить адрес отправителя.
   b. В открывшемся окне **Параметры записи белого списка** настройте следующие параметры:

Адрес электронной почты или маска

Добавление отправителей или получателей сообщений в белый список по адресу электронной почты или по маске адресов. Этот вариант выбран по умолчанию.

Если вы добавляете в белый список отправителей сообщений, программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, отправленные с указанных адресов электронной почты.

Если вы добавляете в белый список получателей сообщений, программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, адресованные указанным получателям.

Учетная запись Active Directory или группа

Добавление получателей сообщений в белый список по учетной записи в Active Directory. Программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, адресованные получателям, которых определяют указанные учетные записи.

Этот вариант доступен только при добавлении или изменении адреса получателя сообщений. См. также раздел О доверенных адресатах (на стр. 111).

IP-адрес

Добавление отправителя в белый список по IP-адресу. Программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, поступающие с заданного IP-адреса.

Этот вариант доступен только при добавлении или изменении адреса отправителя сообщений.

Не проверять сообщения на наличие следующего содержимого

В этом блоке вы можете указать, какие проверки вы хотите исключить для сообщений с указанными отправителями или получателями. Доступны следующие варианты:

- **Спам, фишинг и массовые рассылки**. Программа будет пропускать сообщения со спамом и массовые рассылки.
- **Массовые рассылки**. Программа будет пропускать только массовые рассылки.

Комментарий

Дополнительная информация о записи. Например, причина добавления адреса в список. Максимальная длина комментария – 200 символов.

a. Нажмите на кнопку **OK**.

Новая запись будет добавлена в список.

1. Нажмите на кнопку **Сохранить**.

Изменения, внесенные в белый список адресов Анти-Спама, будут сохранены.

Вы также можете:

- настроить параметры записи по кнопке **Изменить**;
- удалить одну или несколько записей из списка по кнопке **Удалить**;
- скопировать отмеченные в списке записи в текстовый файл (например, с помощью комбинаций клавиш **CTRL+C**, **CTRL+V**);
- экспортировать записи списка в файл формата XML по кнопке **Экспортировать**;
- импортировать записи в список из ранее экспортированного файла формата XML или файла формата TXT по кнопке **Импортировать**; при импортировании файла формата TXT файл будет распознан как список адресов электронной почты отправителей.

Формирование черного списка адресов Анти-Спама

► *Чтобы добавить адрес в черный список адресов Анти-Спама, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите сформировать черный список для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите сформировать черный список для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите сформировать черный список.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Черный список адресов Анти-Спама**.
4. Чтобы добавить новый адрес отправителя в список, выполните следующие действия:
   a. Нажмите на кнопку **Добавить отправителя**.
   b. В открывшемся окне **Параметры записи черного списка** настройте следующие параметры:
      - **Адрес электронной почты или маска**

        Добавление отправителей сообщений в черный список по адресу электронной почты или по маске адресов. Программа будет присваивать сообщениям, отправленным с указанных адресов электронной почты, статус *Адрес в черном списке* и выполнять над ними действия, настроенные для сообщений с этим статусом.

      - **IP-адрес**

Добавление отправителя в черный список по IP-адресу. Программа будет присваивать сообщениям, поступающим с заданного IP-адреса, статус *Адрес в черном списке* и выполнять над ними действия, настроенные для сообщений с этим статусом.

- **Комментарий**

  Дополнительная информация о записи. Например, причина добавления адреса в список. Максимальная длина комментария – 200 символов.

a. Нажмите на кнопку **OK**.

Новая запись будет добавлена в список.

1. Нажмите на кнопку **Сохранить**.

Изменения, внесенные в черный список, будут сохранены.

Вы также можете:

- настроить параметры записи по кнопке **Изменить**;
- удалить одну или несколько записей из списка по кнопке **Удалить**;
- скопировать отмеченные в списке записи в текстовый файл (например, с помощью комбинаций клавиш **CTRL+C**, **CTRL+V**);
- экспортировать записи списка в файл по кнопке **Экспортировать**;
- импортировать записи в список из файла по кнопке **Импортировать**.

Окно Параметры записи белого списка

В этом окне вы можете настроить параметры записи белого списка.

Адрес электронной почты или маска

Добавление отправителей или получателей сообщений в белый список по адресу электронной почты или по маске адресов. Этот вариант выбран по умолчанию.

Если вы добавляете в белый список отправителей сообщений, программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, отправленные с указанных адресов электронной почты.

Если вы добавляете в белый список получателей сообщений, программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, адресованные указанным получателям.

Учетная запись Active Directory или группа

Добавление получателей сообщений в белый список по учетной записи в Active Directory. Программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, адресованные получателям, которых определяют указанные учетные записи.

Этот вариант доступен только при добавлении или изменении адреса получателя сообщений. См. также раздел О доверенных адресатах (на стр. 111).

IP-адрес

Добавление отправителя в белый список по IP-адресу. Программа будет пропускать без проверки на спам и / или массовые рассылки сообщения, поступающие с заданного IP-адреса.

Этот вариант доступен только при добавлении или изменении адреса отправителя сообщений.

Не проверять сообщения на наличие следующего содержимого

В этом блоке вы можете указать, какие проверки вы хотите исключить для

сообщений с указанными отправителями или получателями. Доступны следующие варианты:

- **Спам, фишинг и массовые рассылки**. Программа будет пропускать сообщения со спамом и массовые рассылки.
- **Массовые рассылки**. Программа будет пропускать только массовые рассылки.

Комментарий

Дополнительная информация о записи. Например, причина добавления адреса в список. Максимальная длина комментария – 200 символов.

Окно Параметры записи черного списка

В этом окне вы можете настроить параметры записи черного списка.

Адрес электронной почты или маска

Добавление отправителей сообщений в черный список по адресу электронной почты или по маске адресов. Программа будет присваивать сообщениям, отправленным с указанных адресов электронной почты, статус *Адрес в черном списке* и выполнять над ними действия, настроенные для сообщений с этим статусом.

IP-адрес

Добавление отправителя в черный список по IP-адресу. Программа будет присваивать сообщениям, поступающим с заданного IP-адреса, статус *Адрес в черном списке* и выполнять над ними действия, настроенные для сообщений с этим статусом.

Комментарий

Дополнительная информация о записи. Например, причина добавления адреса в список. Максимальная длина комментария – 200 символов.

Информирование "Лаборатории Касперского" о ложных срабатываниях Анти-Спама

Вы можете отправлять на исследование в "Лабораторию Касперского" сообщения, которые по вашему мнению Kaspersky Security ошибочно классифицировал как спам (см. раздел "Защита от спама и фишинга" на стр. 118) (сообщения со статусами *Спам* или *Возможный спам*), формальные оповещения (сообщения со статусом *Формальное оповещение*) или сообщения, относящиеся к массовым рассылкам (сообщения со статусом *Массовая рассылка*).

Вместе с сообщением, вызвавшим ложное срабатывание Анти-Спама, в "Лабораторию Касперского" также отправляется служебная информация Анти-Спама, связанная с обработкой сообщения Анти-Спамом. Получив это сообщение и служебную информацию Анти-Спама, специалисты "Лаборатории Касперского" могут провести исследование случая ложного срабатывания Анти-Спама и внести изменения в базы Анти-Спама.

Сообщения и служебная информация Анти-Спама отправляются от имени учетной записи, заданной в параметрах отправки уведомлений (см. раздел "Настройка общих параметров отправки уведомлений" на стр. 174).

► *Чтобы отправить сообщение, вызвавшее ложное срабатывание Анти-Спама, на исследование в "Лабораторию Касперского", выполните следующие действия:*

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Резервное хранилище**.
3. В рабочей области узла в списке объектов резервного хранилища выберите сообщение, которое вы хотите отправить на исследование в "Лабораторию Касперского". Вы можете выбрать сообщение со статусом Спам, Возможный спам, *Формальное оповещение* или *Массовая рассылка.*
4. Нажмите на правую кнопку мыши и в контекстном меню этого сообщения выберите пункт **Пожаловаться на ложное срабатывание Анти-Спама**.

   Откроется окно **Отправка объекта в «Лабораторию Касперского»**.
5. Укажите в поле **Адрес электронной почты для обратной связи** ваш адрес электронной почты, по которому специалисты "Лаборатории Касперского" могут связаться с вами. При необходимости специалисты "Лаборатории Касперского" свяжутся с вами для получения дополнительных сведений.
6. Прочитайте и примите условия отправки объекта в "Лабораторию Касперского", установив флажок **Я принимаю условия отправки объекта**. Условия отправки объекта вы можете просмотреть в поле **Информация об отправке объекта**.
7. Нажмите на кнопку **OK**.

Выбранное сообщение будет отправлено в "Лабораторию Касперского" на исследование по поводу ложного срабатывания Анти-Спама.

О повышении точности обнаружения спама на серверах Microsoft Exchange 2013

При установке программы на сервере Microsoft Exchange 2013, развернутом в единственной роли Сервер клиентского доступа, в списке компонентов для установки доступен компонент Перехватчик CAS. Этот компонент предназначен для повышения точности обнаружения спама. Этот компонент рекомендуется устанавливать на всех серверах Microsoft Exchange 2013, развернутых в единственной роли Сервер клиентского доступа.

На серверах Microsoft Exchange 2013, развернутых в роли Почтовый ящик, этот компонент устанавливается автоматически вместе с компонентом Анти-Спам, если компонент Анти-Спам выбран для установки (см. раздел "Шаг 4. Выбор компонентов и модулей программы" на стр. 28).

О проверке исходящей почты на спам и фишинг

Вы можете включать / выключать проверку исходящих сообщений на спам и фишинг с помощью модуля Анти-Спам. Если с какого-либо адреса в вашей организации отправляются сообщения, содержащие спам или фишинг, это может означать, что какой-либо компьютер в вашей организации заражен.

Если модуль Анти-Спам обнаруживает сообщение, содержащее спам или фишинг, статус сообщения принимает значение **Спам** или **Фишинг.** Программа удаляет исходящее сообщение с обнаруженным спамом или фишингом, сохраняя копию исходного сообщения в резервном хранилище.

Поле **Тип отправителя** у исходящих сообщений в резервном хранилище имеет значение **Внутренний**. Чтобы определить, заражен ли какой-либо компьютер, рассылающий спам или фишинг, в вашей организации, вы можете просмотреть список копий исходящих сообщений в резервном хранилище, список событий в журнале событий Windows или список событий в журнале событий Kaspersky Security Center.

Модуль Анти-Спам проверяет сообщения исходящей почты, адресованные на внешние адреса электронной почты. Модуль не проверяет сообщения, относящиеся к следующим категориям:

- Сообщения, адресованные на внутренние адреса электронной почты.
- Сообщения, у которых адреса получателей сообщений находятся в белом списке.

Модуль Анти-Спам определяет статус сообщения по содержанию текста и заголовку сообщения. В результатах проверки программа учитывает только наличие спама или фишинга в сообщениях, которым Модуль Анти-Спам присвоил статусы **Спам** или **Фишинг.** В результатах проверки программа не учитывает срабатывания в сообщениях со статусами:

- **Возможный спам**. Сообщение является возможным спамом.
- **Формальное оповещение**. Сообщение является формальным оповещением.
- **Массовая рассылка**. Сообщение является массовой рассылкой.

Проверка на спам и фишинг в исходящих сообщениях не использует репутационную службу Reputation Filtering.

Включение и выключение проверки исходящих сообщений на наличие спама и фишинга

► *Чтобы включить или выключить проверку исходящих сообщений на спам и фишинг, выполните следующие действия:*

1. В дереве Консоли управления раскройте один из следующих узлов:
   - Если вы хотите включить или выключить проверку исходящих сообщений на спам и фишинг для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите включить или выключить проверку исходящих сообщений на спам и фишинг для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить проверку исходящих сообщений на спам и фишинг.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Транспортный концентратор** раскройте блок **Параметры проверки на спам**.
4. В блоке **Параметры обработки исходящих сообщений** выполните одно из следующих действий:
   - Если вы хотите включить проверку исходящих сообщений на спам и фишинг, установите флажок **Проверять исходящие сообщения и удалять сообщения, являющиеся спамом или содержащие фишинговую ссылку**.

     Флажок **Проверять исходящие сообщения и удалять сообщения, являющиеся спамом или содержащие фишинговую ссылку** доступен, если установлен флажок **Включить проверку сообщений на спам**
   - Если вы хотите выключить проверку исходящих сообщений на спам и фишинг, снимите флажок **Проверять исходящие сообщения и удалять сообщения, являющиеся спамом или содержащие фишинговую ссылку**.
5. Нажмите на кнопку **Сохранить**.

Настройка параметров защиты почтовых ящиков и общих папок

Программа может защищать то количество почтовых ящиков, которое не превышает ограничение активного ключа (см. раздел "Просмотр информации о добавленных ключах" на стр. 73). Если этого количества недостаточно, вы можете перенести защиту с одних почтовых ящиков на другие. Для этого вы можете перенести ящики, у которых вы хотите снять защиту, в хранилища, которые не будут защищаться. По умолчанию защите подлежат также все общие папки почтового сервера. Вы можете снять защиту с общих папок, если считаете, что их проверка избыточна.

По умолчанию программа защищает те хранилища почтовых ящиков сервера Microsoft Exchange, которые уже существовали в момент установки программы, а также все новые хранилища.

► *Чтобы настроить параметры защиты почтовых ящиков и общих папок, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры защиты почтовых ящиков и общих папок для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры защиты почтовых ящиков и общих папок для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры защиты почтовых ящиков и общих папок.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Почтовый ящик** раскройте блок параметров **Защита почтовых ящиков**.

   В списке **Защищаемые хранилища почтовых ящиков** перечислены хранилища почтовых ящиков и общих папок защищаемого сервера Microsoft Exchange.

   > Если программа работает в DAG серверов Microsoft Exchange, в этом списке перечислены хранилища почтовых ящиков и общих папок, находящиеся на всех серверах, входящих в эту DAG.
   > При просмотре из профиля в списке **Защищаемые хранилища почтовых ящиков** отображаются только защищаемые хранилища тех серверов Microsoft Exchange, на которых установлен модуль Антивирус для роли Почтовый ящик.

4. В списке **Защищаемые хранилища почтовых ящиков** установите флажки для тех хранилищ почтовых ящиков, для которых вы хотите включить защиту.
5. Нажмите на кнопку **Сохранить**.

kaspersky

Фоновая проверка и проверка по требованию

Фоновая проверка – это режим работы Антивируса для роли Почтовый ящик, при котором Антивирус проверяет на вирусы и наличие других угроз сообщения, хранящиеся на сервере Microsoft Exchange, и другие объекты Microsoft Exchange с использованием последней версии антивирусных баз. Вы можете запускать фоновую проверку вручную (см. раздел "Запуск фоновой проверки вручную" на стр. 143) или задать расписание запуска (см. раздел "Настройка параметров фоновой проверки" на стр. 142). Использование фоновой проверки позволяет снизить нагрузку на серверы в часы пик и повысить уровень безопасности почтовой инфраструктуры в целом.

Проверка по требованию – это режим работы Антивируса для роли Почтовый ящик, при котором Антивирус проверяет на вирусы и наличие других угроз сообщения и другие объекты Microsoft Exchange, хранящиеся в выбранных почтовых ящиках и общих папках на сервере Microsoft Exchange. Вы можете запускать проверку по требованию выбранных почтовых ящиков и общих папок вручную. Использование проверки по требованию позволяет ограничить область проверки и сократить время проверки. Если проверка по требованию была прервана, то при последующем запуске она начинается сначала, то есть программа проверяет все выбранные объекты повторно.

Здесь и далее, любая информация и инструкции по выполнению действий с сообщениями также применимы к другим объектам Microsoft Exchange (таким как задачи, встречи, собрания, записи), если специально не указано иное.

Фоновая проверка одних и тех же сообщений может выполняться неоднократно. Антивирус выполняет повторную фоновую проверку проверенных ранее сообщений после обновления антивирусных баз. Проверка по требованию одних и тех же сообщений в выбранных ящиках и общих папках выполняется однократно.

Если фоновая проверка была прервана, то при последующем запуске программа проверяет только те почтовые ящики и общие папки, которые не были проверены в предыдущий раз. Если фоновая проверка была завершена, то при последующем запуске она начинается сначала, то есть программа проверяет все выбранные объекты.

Фоновая проверка может вызвать замедление работы сервера Microsoft Exchange. Рекомендуется запускать фоновую проверку в период минимальной нагрузки на почтовые серверы, например, в ночное время. Если вы хотите выполнить проверку определенных почтовых ящиков или общих папок, вы можете использовать проверку по требованию.

Во время фоновой проверки и проверки по требованию:

1. Kaspersky Security в соответствии с установленными параметрами (см. раздел "Настройка параметров защиты почтовых ящиков и общих папок" на стр. 139) получает от сервера Microsoft Exchange сообщения электронной почты и другие объекты Microsoft Exchange (например, задачи, встречи, собрания, записи), размещенные в следующих областях:
   - Фоновая проверка – объекты, размещенные в защищаемых хранилищах.
   - Проверка по требованию – объекты, размещенные в выбранных почтовых ящиках и общих папках.

2. Kaspersky Security передает на обработку модулю Антивирус для роли Почтовый ящик следующие сообщения:

   - Фоновая проверка – сообщения, которые не были проверены с использованием последней версии антивирусных баз.
   - Проверка по требованию – сообщения, которые находятся в выбранных почтовых ящиках и общих папках и удовлетворяют настройкам параметров проверки по требованию (см. раздел "Настройка параметров и запуск проверки по требованию" на стр. 144).

3. При обнаружении зараженных объектов во время фоновой проверки и проверки по требованию Антивирус обрабатывает их в соответствии с параметрами, установленными в параметрах Антивируса для роли Почтовый ящик (см. раздел "Настройка параметров антивирусной обработки объектов: Антивирус для роли Почтовый ящик" на стр. 109) по следующему алгоритму:

   Если в сообщении или другом объекте Microsoft Exchange обнаружен зараженный объект и в параметрах Антивируса установлено действие **Удалять объект** или **Удалять сообщение**, Антивирус пытается вылечить объект.

   Если лечение удалось, Антивирус заменяет зараженный объект на вылеченный.

   Если лечение не удалось, Антивирус выполняет действия, приведенные в таблице ниже.

Таблица 9. Действия Антивируса, если лечение зараженного объекта не удалось

Место обнаружения зараженного объект	Установленное действие	Действие Антивируса
В сообщении	Удалять сообщение	Антивирус удаляет сообщение вместе с зараженным объектом.
	Удалять объект	Антивирус заменяет зараженный объект (вложение) текстовым файлом с информацией о том, что зараженный объект был удален.
В другом объекте Microsoft Exchange (например, в задаче, встрече, записи)	Удалять сообщение	
	Удалять объект	

Антивирус не удаляет полностью объекты Microsoft Exchange, не являющиеся сообщениями, такие как задачи, встречи, собрания, записи. Из них могут быть удалены только зараженные вложения.

Сохранение копии объекта в резервном хранилище при фоновой проверке и проверке по требованию

Если в параметрах Антивируса для роли Почтовый ящик установлен флажок **Сохранять копию объекта в резервном хранилище**, Kaspersky Security перед обработкой объекта помещает его копию в резервное хранилище. Если у помещаемого объекта (например, у задачи) отсутствует поле **От** или **Кому**, это поле в резервном хранилище заполняется адресом пользователя, в почтовом ящике которого находится объект.

Особенности фоновой проверки и проверки по требованию

Функции фоновой проверки и проверки по требованию имеют следующие особенности:

- Использование службы EWS (Exchange Web Services). Программа использует для проверки службу EWS, выполняющуюся локально на защищаемом сервере Microsoft Exchange. Проверка на серверах профиля выполняется параллельно с использованием локальных служб EWS на каждом из защищаемых серверов. Если локальная служба EWS недоступна, программа записывает в журнал событий защищаемого сервера Microsoft Exchange сообщение с информацией об ошибке.

- Роль учетной записи службы программы. Выполнение проверки возможно, только если учетной записи службы программы назначена роль ApplicationImpersonation из набора встроенных ролей Role Based Access Control (RBAC) сервера Microsoft Exchange. В противном случае при попытке запуска проверки Kaspersky Security записывает в журнал событий Microsoft Windows сообщение об ошибке. Мастер установки программы назначает эту роль учетной записи службы программы автоматически в процессе установки или обновления программы. Если это назначение не было выполнено мастером установки программы из-за ошибки, необходимо выполнить его вручную средствами управления Microsoft Exchange.
- Ограничения проверки общих папок. Антивирус проверяет только те общие папки, для которых существует как минимум один пользователь, обладающий следующим набором прав доступа к этой общей папке:
  - Folder visible.
  - Read items.
  - Edit all.
  - Delete all.

В этом разделе

Настройка параметров фоновой проверки

Программа выполняет фоновую проверку тех хранилищ почтовых ящиков и общих папок, которые отмечены в списке **Защищаемые хранилища почтовых ящиков**. Перед запуском фоновой проверки выберите хранилища, которые должны быть проверены (см. раздел "Настройка параметров защиты почтовых ящиков и общих папок" на стр. 139), и сохраните изменения.

Если программа работает на сервере Microsoft Exchange в составе группы DAG, параметры фоновой проверки, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту группу DAG. На остальных серверах этой группы DAG настраивать параметры фоновой проверки не требуется.

► *Чтобы настроить параметры фоновой проверки, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры фоновой проверки для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;

- если вы хотите настроить параметры фоновой проверки для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры фоновой проверки.

2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Почтовый ящик** раскройте блок параметров **Защита почтовых ящиков**.
4. В разделе **Фоновая проверка** в раскрывающемся списке **Расписание** настройте режим запуска фоновой проверки:
   - **Вручную**. Запуск фоновой проверки выполняется вручную.
   - **Ежедневно**. Фоновая проверка выполняется ежедневно. Укажите точное время проверки в поле ввода времени в формате **<ЧЧ:ММ>**.
   - **В выбранный день**. Фоновая проверка выполняется в выбранные дни. Установите флажки напротив дней недели, в которые должна запускаться фоновая проверка, и укажите точное время запуска фоновой проверки в поле ввода времени в формате **<ЧЧ:ММ>**.
   - **Ежемесячно**. Фоновая проверка выполняется один раз в месяц. В поле ввода с прокруткой укажите день месяца, в который должна запускаться фоновая проверка, и укажите точное время запуска фоновой проверки в поле ввода времени в формате **<ЧЧ:ММ>**.
5. Если вы хотите чтобы программа проверяла содержимое (body) сообщения при фоновой проверке, установите флажок **Проверять текст сообщения**.
6. Если вы хотите чтобы программа проверяла только сообщения, полученные или измененные в течение определенного периода времени до начала фоновой проверки, установите флажок **Проверять только недавние сообщения** и укажите количество суток в поле ввода с прокруткой **Проверять сообщения, полученные до запуска фоновой проверки не раньше, чем за (сут)**.

   Максимальное значение параметра – 364 дня.
7. Установите флажок **Ограничить проверку по времени** и задайте значение параметра **Остановить проверку через (ч),** чтобы оптимизировать время проверки.

   Максимальное значение параметра – 168 часов.
8. Нажмите на кнопку **Сохранить**.

Запуск фоновой проверки вручную

Программа выполняет фоновую проверку тех хранилищ почтовых ящиков и общих папок, которые отмечены в списке **Защищаемые хранилища почтовых ящиков**. Перед запуском фоновой проверки выберите хранилища, которые должны быть проверены (см. раздел "Настройка параметров защиты почтовых ящиков и общих папок" на стр. 139), и сохраните изменения.

► *Чтобы запустить фоновую проверку вручную, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности, установленный на сервере Microsoft Exchange, на котором вы хотите запустить фоновую проверку.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Почтовый ящик** раскройте блок параметров **Защита почтовых ящиков**.
4. В блоке **Фоновая проверка** нажмите на кнопку **Запустить проверку**.

В процессе фоновой проверки доступна кнопка остановки задачи, а также отображаются этапы выполнения задачи (*Подготовка к проверке*, *Этап 1 из 2. Проверка почтовых ящиков*, *Этап 2 из 2. Проверка общих папок*). По окончании операции выводится отчет о проверке (время завершения, количество проверенных почтовых ящиков и общих папок).

5. Чтобы остановить фоновую проверку до ее завершения, нажмите на кнопку **Остановить**.

   Запуск и остановка фоновой проверки происходят в течение минуты после нажатия на кнопку **Запустить проверку** / **Остановить**.

Настройка параметров и запуск проверки по требованию

Программа выполняет проверку по требованию тех почтовых ящиков и общих папок, которые указаны в поле **Область проверки**.

► *Чтобы настроить параметры и запустить проверку по требованию, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел нужного Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области на закладке **Защита для роли Почтовый ящик** раскройте блок параметров **Проверка по требованию**.
4. Если вы хотите, чтобы программа проверяла содержимое (body) сообщения при проверке по требованию, установите флажок **Проверять текст сообщения**.
5. Если вы хотите, чтобы программа проверяла только сообщения, полученные или измененные в течение определенного периода времени до начала проверки по требованию, установите флажок **Проверять только недавние сообщения** и укажите количество суток в поле **Проверять сообщения, полученные до запуска фоновой проверки не раньше, чем за (сут)**. Программа выполняет проверку по требованию сообщений и других объектов Microsoft Exchange, измененных (в том числе и полученных) в течение указанного количества суток до запуска проверки по требованию.

   Максимальное значение параметра – 364 дня.
6. Если вы хотите ограничить проверку по требованию по времени, установите флажок **Ограничить проверку по времени** и укажите максимальную продолжительность проверки по требованию в поле **Остановить проверку через (ч)**. Программа прекращает проверку по требованию, если она выполняется дольше указанного времени.

   Максимальное значение параметра – 168 часов.
7. Укажите почтовые ящики и общие папки, которые вы хотите проверить, в поле **Область проверки**. Выполните следующие действия:

   a. Нажмите на кнопку  .

   b. В окне **Область проверки** выполните одно из следующих действий:

      - Если вы хотите добавить почтовый ящик в поле **Область проверки**, нажмите на кнопку **Добавить пользователя** и добавьте пользователя, почтовый ящик которого вы хотите проверить.

- Если вы хотите добавить общую папку в поле **Область проверки**, нажмите на кнопку **Добавить общую папку** и установите флажки напротив папок, которые вы хотите проверить.

c. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**.
9. Если вы хотите запустить проверку по требованию, нажмите на кнопку **Запустить проверку**.

   В процессе проверки по требованию отображается кнопка остановки.

   В процессе проверки по требованию отображается индикатор выполнения и этапы выполнения проверки (*Подготовка к проверке*, *Этап 1 из 2. Проверка почтовых ящиков*, *Этап 2 из 2. Проверка общих папок*). По окончании операции выводится отчет о проверке (время завершения, количество проверенных почтовых ящиков и общих папок, количество зараженных или защищенных паролем объектов в почтовых ящиках и общих папках).
10. Чтобы остановить проверку по требованию до ее завершения, нажмите на кнопку **Остановить**.

    Запуск и остановка проверки по требованию происходят в течение минуты после нажатия на кнопку **Запустить проверку** / **Остановить**.

Окно Области проверки

В этом окне вы можете сформировать список почтовых ящиков пользователей и общих папок сервера Microsoft Exchange, который программа использует для проверки по требованию.

Добавить пользователя

Кнопка, по которой вы можете добавить пользователя из Active Directory, почтовый ящик которого вы хотите проверить.

При нажатии на кнопку открывается окно выбора пользователя из Active Directory. Программа добавляет выбранных пользователей в поле **Область проверки.**

Добавить общую папку

Кнопка, по которой вы можете добавить общие папки, которые вы хотите проверить.

При нажатии на кнопку открывается окно **Выбор общих папок**.

Удалить

Кнопка, по которой вы можете удалить пользователей и общие папки из списка.

Окно Выбор общих папок

Окно, в котором вы можете выбрать общие папки для проверки по требованию.

В списке находятся только общие папки верхнего уровня.

Если установлены флажки напротив названий общих папок, то программа включает эти папки в проверку по требованию. Программа добавляет выбранные общие папки в поле **Область проверки.**

kaspersky

Фильтрация вложений и содержимого

Фильтрация вложений и содержимого позволяет фильтровать файлы вложений по определенным критериям, а так же проверять текст в сообщениях и в темах сообщений электронной почты на наличие запрещенных слов. Во время фильтрации вложений и содержимого Kaspersky Security ищет в сообщениях электронной почты текст и файлы вложений, соответствующие указанным критериям фильтрации, и применяет к ним действие, настроенное администратором: удаляет файл вложения, удаляет сообщение целиком или пропускает сообщение.

Фильтрация вложений и содержимого осуществляется по индивидуально настроенным правилам (см. раздел "Работа с правилами фильтрации вложений и содержимого" на стр. 147).

Kaspersky Security может вести запись событий, связанных с фильтрацией вложений и содержимого, в журнал событий Windows. Вы можете настроить запись событий в журнал событий Windows в узле **Уведомления** (см. раздел "**Настройка уведомлений о событиях в работе программы**" на стр. 175).

Kaspersky Security удаляет сообщения и вложения без возможности восстановления. Рекомендуется сохранять копии сообщений в резервном хранилище, чтобы избежать потери данных. Вы можете настроить эту функцию в параметрах фильтрации (см. раздел "Работа с правилами фильтрации вложений и содержимого" на стр. 147).

Kaspersky Security может уведомлять о действиях при фильтрации вложений и содержимого по электронной почте. Вы можете настроить отправку автоматических уведомлений в узле **Уведомления** (см. раздел "**Настройка уведомлений о событиях в работе программы**" на стр. 175).

Статистика по фильтрации вложений и содержимого отображается в узле **<Имя сервера>**, а также включается в отчеты для роли Транспортный концентратор (см. раздел "Отчеты" на стр. 188).

Фильтрация вложений и содержимого доступна, если на сервере Microsoft Exchange установлен компонент Антивирус для роли Транспортный концентратор.

О предотвращении задержки сообщений при фильтрации вложений и содержимого

В исключительных случаях при сбое в работе антивирусного ядра время фильтрации вложений и содержимого в сообщениях может значительно увеличиваться. В таких случаях для предотвращения задержки сообщений модуль фильтрации вложений и содержимого временно переходит в режим ограниченной проверки. В этом режиме некоторые сообщения могут быть пропущены без фильтрации вложений и содержимого.

В этом разделе

Включение фильтрации вложений и содержимого

► *Чтобы включить фильтрацию вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите включить или выключить фильтрацию вложений и содержимого на нераспределенном Сервере безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите включить или выключить фильтрацию вложений и содержимого на Серверах безопасности, входящих в профиль, раскройте узел **Профили** и в нем выберите узел того профиля, на Серверах безопасности которого вы хотите включить или выключить фильтрацию вложений и содержимого.
2. Выберите узел **Защита сервера**.
3. Выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация вложений и содержимого** установите флажок **Включить фильтрацию вложений и содержимого**.
5. Нажмите на кнопку **Сохранить**.

Фильтрация вложений и содержимого будет включена. Правила фильтрации будут доступны для настройки. Если ни одно правило не настроено, фильтрация вложений и содержимого неактивна.

Работа с правилами фильтрации вложений и содержимого

Правило – это совокупность условий, которые должны выполняться, для того чтобы программа применила к файлу вложения или содержимому сообщения электронной почты заданное действие.

Для каждого правила фильтрации вложений и содержимого администратор задает следующие условия:

- параметры файла вложения и содержимого сообщения;
- получатели и / или отправители сообщения;
- исключения из правила (при необходимости).

В качестве условий фильтрации вложений и содержимого вы можете указать следующие параметры (см. раздел "Настройка общих параметров и условий правила фильтрации вложений и содержимого" на стр. 149):

- Защита файла паролем.
- Ключевые слова.

  Программа проверяет текст и темы сообщений на наличие определенных слов, запрещенных в организации. Список ключевых слов или регулярных выражений может быть добавлен в правило фильтрации вручную или из файла формата TXT.
- Имя и / или расширение файла.

  Вы можете указать имена файлов целиком или использовать маски имен файлов.
- Наличие макросов в файле.
- Размер файла в мегабайтах.
- Формат файла.

Программа определяет формат файла по его структуре (т.е по способу хранения файла или его отображения на экране). Это позволяет выполнять фильтрацию вложений, если расширение файла вложения не совпадает с форматом этого файла (например, если расширение было намеренно изменено).

При выборе нескольких параметров правило будет применяться, если вложенный файл или содержимое сообщения соответствует хотя бы одному из них.

С отфильтрованными сообщениями программа может выполнить одно из следующих действий (см. раздел "Настройка общих параметров и условий правила фильтрации вложений и содержимого" на стр. 149):

- удалить сообщение;
- удалить объект из вложения (или вложение);
- пропустить сообщение.

Программа может применять правила фильтрации к сообщениям для / от конкретных пользователей или групп пользователей (см. раздел "Настройка списков пользователей для правила фильтрации вложений и содержимого" на стр. 151).

Вы можете детализировать правила фильтрации вложений и содержимого, исключая сообщения из фильтрации (см. раздел "Настройка исключений из фильтрации вложений и содержимого" на стр. 152). Вы можете исключать сообщения из проверки следующим образом:

- По адресу электронной почты отправителя.

  Программа не будет применять правила фильтрации к вложениям и содержимому сообщений от указанных отправителей.

- По адресу электронной почты получателя.

  Программа не будет применять правила фильтрации к вложениям и содержимому сообщений для указанных адресатов.

- По имени или маске имени файла.

  Программа не будет применять правила фильтрации к файлам вложений, которые соответствуют указанным именам или маскам имен.

- По формату файла.

  Программа не будет применять правила фильтрации к файлам указанных форматов.

Создание правила фильтрации вложений и содержимого

► *Чтобы создать правило фильтрации вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выберите узел соответствующего Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация вложений и содержимого** нажмите на кнопку **Добавить правило**.
5. Нажмите на кнопку **Сохранить**.

Правило будет добавлено в список в левой части рабочей области. Имя по умолчанию – **Новое правило**. Параметры и условия выполнения правила будут доступны для настройки.

Настройка общих параметров и условий правила фильтрации вложений и содержимого

► *Чтобы настроить общие параметры и условия правила фильтрации вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выберите узел соответствующего Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация вложений и содержимого** выделите правило, которое вы хотите настроить.
5. На закладке **Общие параметры** оставьте установленным флажок **Включить правило**, если вы хотите, чтобы правило стало активным сразу после настройки.

   Если вы не хотите применять правило сразу после настройки, снимите флажок.
6. В поле **Имя правила** измените имя правила или оставьте значение по умолчанию.
7. В раскрывающемся списке **Действие** выберите действие программы с вложениями и содержимым, которые соответствуют хотя бы одному из критериев фильтрации:
   - **Пропускать**. Программа разрешает пересылку сообщения электронной почты с запрещенными вложениями или содержимым. Этот вариант выбран по умолчанию. Для получения информации об отфильтрованных объектах вы можете настроить уведомления или запись событий в журнал событий Windows.
   - **Удалять объект**. Программа удаляет объект из вложения или вложение из сообщения электронной почты. К такому сообщению программа добавляет файл формата TXT (см. раздел "Редактирование сообщения об удалении вложения во время фильтрации" на стр. 153), который содержит информацию обо всех удаленных вложениях.
   - **Удалять сообщение**. Программа удаляет сообщение электронной почты с отфильтрованным вложением или содержимым без возможности восстановления этого сообщения. При выборе этого варианта рекомендуется сохранять копии сообщений в резервном хранилище, чтобы избежать потери данных.
8. Установите флажок **Добавлять метку в тему сообщения,** если вы хотите, чтобы программа добавляла к теме сообщения с отфильтрованным вложением или содержимым дополнительный текст (метку). Текст меток можно изменить. Значение меток по умолчанию: `[Запрещенное вложение или содержимое]`.

   Добавление метки доступно при выборе действия **Пропускать** или **Удалять объект**.
9. Если вы хотите, чтобы перед обработкой объекта его копия сохранялась в резервном хранилище (см. раздел "Резервное хранилище" на стр. 178), установите флажок **Сохранять копию объекта в резервном хранилище**.
10. В раскрывающемся блоке **Добавить условие** выберите критерии, которым должен соответствовать объект для применения к нему правила фильтрации:
    - **Защита паролем**
    - **Ключевые слова**

      Фильтрация содержимого сообщений по ключевым словам или регулярным выражениям.

При выборе данного пункта меню становится доступна кнопка  . При нажатии на кнопку открывается окно **Ключевые слова**, в котором вы можете указать ключевые слова и / или регулярные выражения вручную. Вы также можете импортировать список ключевых слов и / или регулярных выражений из файла формата TXT. Указанные ключевые слова и / или регулярные выражения отобразятся в поле **Список ключевых слов**.

Поиск ключевых слов производится по подстроке, без учета регистра.

Вы так же можете добавлять сообщениям оценку вероятности нежелательной почты (SCL). Для этого установите флажок **Добавлять SCL-оценку**.

По умолчанию флажок снят.

- **Маска имени файла**

  Фильтрация файлов вложений и вложенных архивов по имени или расширению файла.

  При выборе данного пункта меню становится доступна кнопка  . При нажатии на кнопку открывается окно **Маски имен файлов**, в котором вы можете указать имена и / или маски имен файлов вручную. Вы также можете импортировать список имен и / или масок имен файлов из файла формата TXT. Указанные имена и / или маски имен файлов отобразятся в поле **Файлы со следующими масками**.

  Программа проверяет файлы вложений и файлы во вложенных архивах. При обнаружении файлов, соответствующих критериям фильтрации, программа применяет к проверяемым сообщениям действие, заданное правилом.

- **Наличие макросов**
- **Ограничение размера файла**

Фильтрация вложений по размеру файла вложения.

При выборе данного пункта меню становится активно поле с прокруткой справа. В поле с прокруткой вы можете указать максимальный размер файлов вложений, пересылаемых в сообщениях электронной почты. Вы можете указать размер вложений в диапазоне от 1 до 999 МБ. По умолчанию установлено значение 20 МБ. Если программа обнаруживает вложения, которые превышают указанный размер, то применяет к ним действие, настроенное в параметрах фильтрации.

- **Формат файла**

  Фильтрация файлов вложений и вложенных архивов по формату файла.

  Программа определяет формат файла по его структуре (т.е по способу хранения файла или его отображения на экране). Это позволяет выполнять фильтрацию вложений, если расширение файла вложения не совпадает с форматом этого файла (например, если расширение было намеренно изменено).

При выборе данного пункта меню, становится доступна кнопка  . При нажатии на кнопку открывается окно **Форматы файлов**, в котором вы можете выбрать форматы файлов, к которым программа будет применять правило фильтрации. Выбранные форматы отобразятся в поле **Файлы следующих форматов**.

Программа проверяет файлы вложений и файлы во вложенных архивах. При обнаружении файлов указанных форматов программа применяет к проверяемым сообщениям действие, заданное правилом фильтрации.

Программа будет применять правило к объектам, соответствующим хотя бы одному из заданных условий.

1. Чтобы удалить условие, нажмите на кнопку ✕ рядом с соответствующим критерием.
2. Нажмите на кнопку **Сохранить**.

Настройка списков пользователей для правила фильтрации вложений и содержимого

► *Чтобы настроить список пользователей, к сообщениям от / для которых будет применяться правило фильтрации вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выберите узел соответствующего Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация вложений и содержимого** выделите правило, к которому вы хотите применить изменения, и выберите закладку **Пользователи**.
5. Чтобы указать получателей сообщения, выберите один из следующих вариантов в блоке **Применять правило к сообщениям для следующих получателей**:
   - **Все пользователи**, если вы хотите применять правило к сообщениям для любых получателей;
   - **Только внешние пользователи**, если вы хотите применять правило к сообщениям для получателей, которые не принадлежат к вашей организации;
   - **Отдельные пользователи или группы пользователей**, если вы хотите применять правило к сообщениям для конкретных получателей или групп Active Directory.
6. Чтобы указать отправителей сообщения, выберите один из следующих вариантов в блоке **Применять правило к сообщениям от следующих отправителей**:
   - **Все пользователи**, если вы хотите применять правило к сообщениям от любых отправителей;
   - **Только внешние пользователи**, если вы хотите применять правило к сообщениям от отправителей, которые не принадлежат к вашей организации;
   - **Отдельные пользователи или группы пользователей**, если вы хотите применять правило к сообщениям от конкретных отправителей или групп Active Directory.

Получатели и отправители, на которых распространяется правило, объединяются логическим оператором "И".

7. Нажмите на кнопку **Сохранить**.

► *Чтобы добавить в любой из списков запись из Active Directory, выполните следующие действия:*

1. В блоке настроек для соответствующего типа пользователей нажмите на кнопку .
2. В открывшемся окне найдите нужную запись Active Directory и нажмите на кнопку **OK**.
3. Адреса, выбранные из Active Directory, обозначаются в списке следующими значками:
   - – простые пользователи, контакты, группы рассылки;
   - – группы безопасности.

► *Чтобы добавить в любой из списков SMTP-адрес или имя пользователя, выполните следующие действия:*

1. Чтобы добавить SMTP-адрес или имя пользователя, введите его в поле ввода и нажмите на кнопку .

   Адреса, добавленные таким способом, обозначаются в списке значком .

   Адреса, добавленные таким способом, не проходят проверку на наличие в Active Directory.

2. Чтобы удалить SMTP-адрес или имя пользователя, выделите соответствующую строку и нажмите на кнопку .

► *Чтобы экспортировать список пользователей в файл, выполните следующие действия:*

1. Нажмите на кнопку .
2. В открывшемся окне укажите название файла в поле **Имя файла.**
3. Нажмите на кнопку **Сохранить**.

► *Чтобы импортировать список пользователей из файла, выполните следующие действия:*

1. Нажмите на кнопку .
2. В открывшемся окне в поле **Имя файла** укажите файл со списком пользователей.
3. Нажмите на кнопку **Открыть**.
4. Нажмите на кнопку **Сохранить**.

Настройка исключений из фильтрации вложений и содержимого

► *Чтобы настроить исключения из правила фильтрации вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выберите узел соответствующего Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.

4. В раскрывающемся блоке **Фильтрация вложений и содержимого** выделите правило, к которому вы хотите применить изменения, и выберите закладку **Исключения**.
5. В раскрывающемся блоке **Добавить условие** выберите критерии, по которым программа будет исключать объект из проверки:

   Маска имени файла

   Отдельные отправители

   Отдельные получатели

   Формат файла

   Программа не будет применять правило фильтрации к объектам, соответствующим хотя бы одному из условий исключения.
6. Чтобы удалить условие исключения, нажмите на кнопку ✕ рядом с соответствующим критерием.
7. Нажмите на кнопку **Сохранить**.

Параметры исключений из фильтрации будут сохранены.

Удаление правила фильтрации вложений и содержимого

► *Чтобы удалить правило фильтрации вложений и содержимого, выполните следующие действия:*

1. В дереве Консоли управления выберите узел соответствующего Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация вложений и содержимого** выберите правило, которое хотите удалить.
5. Нажмите на кнопку **Удалить правило**.
6. Нажмите на кнопку **Сохранить**.

Правило будет удалено.

Редактирование сообщения об удалении вложения во время фильтрации

Если по результатам фильтрации вложений программа удаляет файл вложения из сообщения электронной почты, то к исходному сообщению прикрепляется файл формата TXT. Файл содержит текст, информирующий пользователя о действии программы. По умолчанию в текст включен список удаленных объектов. Вы можете отредактировать содержание этого информационного сообщения и включить туда инструкции и другие сведения, актуальные для сотрудников вашей организации.

► *Чтобы отредактировать сообщение, информирующее пользователя об удалении вложенного объекта во время фильтрации, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел нужного Сервера безопасности.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Дополнительные параметры Антивируса**.

4. Нажмите на кнопку **Редактировать** (*Сообщение об удалении вложения по правилу фильтрации*).
5. В открывшемся окне в поле **Текст сообщения** отредактируйте содержание сообщения.
6. Нажмите **OK**.
7. Нажмите на кнопку **Сохранить**.

Фильтрация однотипных сообщений

Фильтрация однотипных сообщений позволяет настроить ограничение по количеству сообщений, отправляемых пользователем вашей организации за единицу времени. Основная цель данного ограничения – контроль над ситуацией, когда зараженный почтовый ящик автоматически генерирует бесконечный поток сообщений, отправляемых внутренним и внешним адресатам. Во время фильтрации однотипных сообщений Kaspersky Security ищет сообщения, соответствующие указанным критериям фильтрации. Фильтрация однотипных сообщений доступна, если на сервере Microsoft Exchange установлен компонент Антивирус для роли Транспортный концентратор.

Сообщения классифицируются как однотипные при наличии у них одного из следующих признаков:

- Одинаковая тема сообщения.

  Программа определяет сообщения с одинаковой темой. При анализе темы сообщения учитывается регистр.

- Одинаковые вложения.

  Программа определяет сообщения, которые содержат вложенные файлы с одинаковым расширением и одинаковым названием с учетом регистра.

- Одинаковые вложения или тема сообщения.

  Программа определяет сообщения, которые удовлетворяют как минимум одному из критериев.

Вы также можете применить ограничение к любым сообщениям, отправляемым внутренними адресатами, независимо от наличия у них общих признаков.

К сообщениям, количество которых превышает установленное ограничение, программа может применить одно из следующих действий:

- разрешить пересылку сообщений получателям;
- удалить избыточные сообщения без возможности восстановления.

Программа ведет отдельный подсчет количества сообщений для каждого Сервера безопасности.

При необходимости вы можете настроить исключения (на стр. 156) по адресу электронной почты и не применять ограничения к определенным пользователям вашей организации.

Программа может вести запись событий, связанных с фильтрацией однотипных сообщений, в журнал событий Windows, а также уведомлять вас об этих событиях по электронной почте. Вы можете настроить необходимые параметры в узле **Уведомления** (см. раздел "**Настройка уведомлений о событиях в работе программы**" на стр. 175).

kaspersky

В этом разделе

Включение и выключение фильтрации однотипных сообщений

► *Чтобы включить фильтрацию однотипных сообщений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите включить или выключить фильтрацию однотипных сообщений на нераспределенном Сервере безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите включить или выключить фильтрацию однотипных сообщений на Серверах безопасности, входящих в профиль, раскройте узел **Профили** и в нем выберите узел того профиля, на Серверах безопасности которого вы хотите включить или выключить фильтрацию однотипных сообщений.
2. Выберите узел **Защита сервера**.
3. Выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация однотипных сообщений** установите флажок **Ограничить количество однотипных сообщений, отправляемых внутренним пользователем**.
5. Нажмите на кнопку **Сохранить**.

Фильтрация однотипных сообщений будет включена. Параметры фильтрации (см. раздел "Настройка параметров фильтрации однотипных сообщений" на стр. 155) будут доступны для настройки. Программа будет проверять сообщения в соответствии с критериями фильтрации.

Настройка параметров фильтрации однотипных сообщений

► *Чтобы настроить параметры фильтрации однотипных сообщений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить параметры однотипных сообщений на нераспределенном Сервере безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите настроить параметры фильтрации однотипных сообщений на Серверах безопасности, входящих в профиль, раскройте узел **Профили** и в нем выберите узел того профиля, на Серверах безопасности которого вы хотите настроить параметры фильтрации однотипных сообщений.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация однотипных сообщений** настройте следующие параметры:

- **Максимально допустимое количество сообщений**
- **Период времени (мин.)**
- **Применить ограничение к следующим типам сообщений**
- **Действие**

5. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены. Программа будет фильтровать однотипные сообщения в соответствии с настроенными параметрами. Вы можете детализировать параметры фильтрации, настроив исключения (на стр. 156).

► *Чтобы настроить исключения из фильтрации однотипных сообщений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить параметры фильтрации однотипных сообщений на нераспределенном Сервере безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите настроить параметры фильтрации однотипных сообщений на Серверах безопасности, входящих в профиль, раскройте узел **Профили** и в нем выберите узел того профиля, на Серверах безопасности которого вы хотите настроить параметры фильтрации однотипных сообщений.
2. Выберите узел **Защита сервера**.
3. В рабочей области выберите закладку **Защита для роли Транспортный концентратор**.
4. В раскрывающемся блоке **Фильтрация однотипных сообщений** настройте параметр **Не применять ограничение к следующим внутренним отправителям**.
5. Нажмите на кнопку **Сохранить**.

Параметры исключений из фильтрации будут сохранены.

kaspersky

Управление профилями

Если в сети организации присутствует несколько серверов Microsoft Exchange с установленной программой, у вас может возникнуть необходимость одновременно управлять параметрами программы в группе серверов. Это могут быть, например, серверы Microsoft Exchange с одинаковыми требованиями безопасности. Для управления одинаковыми параметрами в группе Серверов безопасности в программе Kaspersky Security предназначены *профили*. Профиль – это совокупность одинаковых параметров, применяемых одновременно к нескольким Серверам безопасности. Использование профилей позволяет настроить одинаковые параметры для всех однотипных Серверов безопасности одновременно и избежать необходимости настраивать все параметры для каждого Сервера безопасности отдельно.

Использование профилей может быть полезно в следующих случаях:

- В сети организации присутствует несколько серверов Microsoft Exchange с установленной программой, и вам нужно управлять этими серверами одинаково. В этом случае вы можете создать один профиль, добавить в него все Серверы безопасности и настроить в профиле параметры программы.
- В сети организации есть две или более группы Серверов безопасности, и для этих групп вам нужно настроить разные параметры. В этом случае возможны следующие варианты использования профилей:
  - Вы можете настроить избирательный доступ пользователей к управлению Серверами безопасности с помощью профильных ролей.
  - Если каждая группа включает более одного Сервера безопасности, вы можете создать несколько профилей с разными параметрами и добавить в них разные Серверы безопасности.
  - Если один из Серверов безопасности требует индивидуальной настройки параметров, вы можете создать профиль для группы серверов с одинаковыми параметрами и настроить параметры этих серверов с помощью созданных профилей. Для Сервера безопасности, который не входит в группу, нет необходимости создавать профиль, вы можете настроить его параметры отдельно. Сервер безопасности, не входящий ни в один профиль, называется *нераспределенным Сервером безопасности*. Вы можете настроить параметры нераспределенного Сервера безопасности отдельно в узле этого Сервера безопасности.

Использование профилей не обязательно. Вы также можете настраивать параметры Серверов безопасности отдельно в узле каждого Сервера безопасности.

При наличии нескольких сайтов в организации нужно учитывать задержки репликации при создании и редактировании профилей, так как информацию о профилях программа хранит в Active Directory.

Создавать / удалять профили, добавлять в профили / удалять из профилей Серверы безопасности и настраивать доступ к профилям могут только администраторы из группы Kse Administrators в Active Directory.

Для использования профилей вам нужно выполнить следующие действия:

1. Создать профиль (см. раздел "Создание профиля" на стр. 159).
2. Настроить параметры профиля (см. раздел "Настройка параметров Серверов безопасности в профиле" на стр. 159).
3. Добавить в профиль Серверы безопасности (см. раздел "Добавление Серверов безопасности в профиль" на стр. 161).
4. Настроить доступ к профилю (см. раздел "Управление доступом к профилю" на стр. 162).

Параметры Сервера безопасности могут быть недоступны для изменения в случае, если Сервер безопасности добавлен в профиль и наследует параметры профиля (см. раздел "Настройка параметров Серверов безопасности в профиле" на стр. 159). При этом рядом с недоступным параметром отображается атрибут "замок". Для того чтобы задать для Сервера безопасности значения параметров, отличные от параметров профиля, нужно удалить Сервер безопасности из профиля (см. раздел "Удаление Сервера безопасности из профиля" на стр. 163).

Вы можете создавать неограниченное количество профилей, а также произвольно добавлять в них Серверы безопасности и удалять Серверы безопасности из профилей (см. раздел "Удаление Сервера безопасности из профиля" на стр. 163).

Вам может потребоваться удалить Сервер безопасности из профиля, например, в следующих случаях:

- если вам нужно настроить для Сервера безопасности параметры, отличные от параметров профиля;
- если вам нужно добавить Сервер безопасности в другой профиль (в этом случае вам нужно сначала удалить Сервер безопасности из профиля, в который он добавлен).

Если вам больше не нужен созданный профиль, вы можете удалить этот профиль из конфигурации программы (см. раздел "Удаление профиля" на стр. 164).

В этом разделе

Создание профиля

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

1. В дереве Консоли управления раскройте узел **Профили**.
2. Добавьте новый профиль одним из следующих способов:
   - выбрав пункт **Добавить профиль** в меню **Действие**;
   - выбрав пункт **Добавить профиль** в контекстном меню узла **Профили**;
   - нажав на кнопку **Добавить профиль** в рабочей области Консоли управления;
   - по ссылке **Добавить профиль** в панели быстрого доступа.
3. В открывшемся окне **Создать новый профиль** введите имя профиля.
4. Нажмите на кнопку **ОК**.

Вложенный узел с именем созданного профиля отобразится в узле **Профили**.

Для использования профиля вам нужно настроить параметры профиля (см. раздел "Настройка параметров Серверов безопасности в профиле" на стр. 159), добавить в профиль Серверы безопасности (см. раздел "Добавление Серверов безопасности в профиль" на стр. 161) и настроить доступ к профилю (см. раздел "Управление доступом к профилю" на стр. 162).

Настройка параметров Серверов безопасности в профиле

Вы можете выполнить следующие общие действия для Серверов безопасности одного профиля (во вложенных узлах профиля):

- настроить параметры антивирусной защиты (см. раздел "Настройка параметров антивирусной обработки объектов: Антивирус для роли Почтовый ящик" на стр. 109) и защиты от спама (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123), а также дополнительные параметры Антивируса (см. раздел "Настройка исключений из антивирусной проверки" на стр. 111) в узле **Защита сервера**;
- настроить расписание автоматического обновления баз (см. раздел "Настройка обновления баз программы по расписанию" на стр. 167) и источник обновлений (см. раздел "Выбор источника обновлений" на стр. 168) в узле **Обновления**;
- настроить параметры уведомлений (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 175) в узлах **Уведомления** и **Настройка**;
- настроить параметры журналов событий (см. раздел "Настройка параметров журналов программы" на стр. 204) и уровень диагностики (см. раздел "Настройка детализации журналов программы" на стр. 205) в узле **Настройка**;
- управлять ключами и настроить параметры уведомления об истечении срока действия лицензии (см. раздел "Настройка уведомления о скором истечении срока действия лицензии" на стр. 72) в узле **Лицензирование**;
- настроить параметры отчетов в узле **Отчеты**.

При этом не изменятся следующие индивидуальные параметры Серверов безопасности и действия, которые программа выполняет для Серверов безопасности:

- запуск фоновой проверки (см. раздел "Настройка параметров фоновой проверки" на стр. 142) в узле **Защита сервера**;

- запуск обновления баз (см. раздел "Запуск обновления баз вручную" на стр. 167) в узле **Обновления**;
- параметры центра обновлений (см. раздел "Назначение сервера центром обновлений и настройка его параметров" на стр. 170) в узле **Обновления**;
- тестовая отправка уведомления (см. раздел "Настройка общих параметров отправки уведомлений" на стр. 174) в узлах **Уведомления** и **Настройка**;
- параметры резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 186) в узле **Настройка**.

Вы по-прежнему сможете настраивать параметры и выполнять действия только отдельно для каждого Сервера безопасности (во вложенных узлах каждого Сервера безопасности или в узле профиля в дереве узла **Серверы** для каждого Сервера безопасности).

Особенности управления профилями в группе доступности баз данных Microsoft Exchange

Если в Консоли управления Exchange вы вносите изменения в конфигурацию DAG, которая добавлена в профиль в программе Kaspersky Security, требуется учитывать следующие особенности параметров Серверов безопасности этой DAG в программе Kaspersky Security:

- Если вы устанавливаете программу Kaspersky Security на сервер Microsoft Exchange, входящий в DAG, добавленную в профиль, то после установки к соответствующему Серверу безопасности в Kaspersky Security применяются параметры этого профиля.
- Если в Консоли управления Exchange вы добавляете в DAG, которая добавлена в профиль в программе Kaspersky Security, сервер Microsoft Exchange с установленной программой Kaspersky Security, то к соответствующему Серверу безопасности в Kaspersky Security применяются параметры этого профиля. Если DAG не добавлена в профиль, то к соответствующему Серверу безопасности в Kaspersky Security применяются индивидуальные параметры этой DAG.
- Если в Консоли управления Exchange вы объединяете в новую DAG несколько добавленных в профиль серверов Microsoft Exchange с установленной программой, то к соответствующим Серверам безопасности в Kaspersky Security применяются параметры этой DAG, то есть устанавливаются общие параметры по умолчанию (кроме списка защищаемых хранилищ), а индивидуальные параметры серверов остаются такими же, как до добавления серверов в DAG.

  При этом если до объединения в DAG серверы были добавлены в профили, то после объединения они по-прежнему отображаются не только в списке серверов DAG, но и в этих профилях, но вы не сможете управлять параметрами этих серверов из профилей. Вы сможете управлять параметрами этих серверов только из профиля, в который добавлена DAG, или через индивидуальные параметры DAG (если DAG не добавлена в профиль). При необходимости вы можете вручную удалить из профилей отображаемые в них серверы.
- Если в Консоли управления Exchange вы исключаете сервер Microsoft Exchange с установленной программой из DAG, которая добавлена в профиль в программе Kaspersky Security, то соответствующий Сервер безопасности исключается из профиля в Kaspersky Security и получает параметры по умолчанию. После исключения из DAG этот Сервер безопасности не отображается в списке серверов профиля, вам требуется вручную добавить его в список защищаемых серверов Microsoft Exchange (см. раздел "Добавление Серверов безопасности к Консоли управления" на стр. 81) или в один из профилей (см. раздел "Добавление Серверов безопасности в профиль" на стр. 161) и настроить его параметры (см. раздел "Настройка параметров Серверов безопасности в профиле" на стр. 159).

Добавление Серверов безопасности в профиль

► *Чтобы добавить Серверы безопасности в профиль, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили**.
2. Выберите узел профиля, в который вы хотите добавить Сервер безопасности, или раскройте узел профиля и выберите узел **Серверы**.
3. Откройте мастер добавления сервера в профиль одним из следующих способов:
   - выбрав пункт **Добавить сервер** в меню **Действие**;
   - выбрав пункт **Добавить сервер** в контекстном меню узла;
   - по ссылке **Добавить сервер** в панели быстрого доступа;
   - нажав на кнопку **Добавить сервер** в рабочей области Консоли управления (только при выбранном узле профиля).
4. В окне мастера **Добавление сервера в профиль <Имя профиля>** в поле **Нераспределенные серверы** выберите Серверы безопасности, которые вы хотите добавить в профиль.

   В поле **Нераспределенные серверы** отображаются Серверы безопасности, не добавленные ни в один профиль.
5. Нажмите на кнопку **>>**.

   Выбранные Серверы безопасности появятся в поле **Добавляемые в профиль**.
6. Нажмите на кнопку **Далее**.
7. В следующем окне мастера нажмите на кнопку **Завершить**.

Добавленные Серверы безопасности появятся в списке серверов в рабочей области узла профиля и в узле профиля в дереве узла **Серверы**. К Серверам безопасности, добавленным в профиль, программа в течение 5 минут применит общие параметры Серверов безопасности профиля (см. раздел "Настройка параметров Серверов безопасности в профиле" на стр. 159).

Вы можете добавить в профиль серверы, входящие в DAG серверов, только все вместе одновременно. При добавлении DAG в профиль все серверы и все их роли (включая роль Транспортный концентратор) добавляются в этот профиль.

Вы не можете добавить в профиль Сервер безопасности, установленный на компьютере, на котором развернут сервер Microsoft Exchange в роли Пограничный транспорт (Edge Transport).

После добавления в профиль Сервера безопасности на него распространяется лицензия на уровне профиля, даже если до добавления в профиль для этого Сервера безопасности действовала другая лицензия.

Управление доступом к профилю

Доступ пользователей к просмотру сведений и к настройкам профиля осуществляется путем назначения им профильных ролей.

► *Чтобы предоставить доступ пользователям или группам пользователей к профилю, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили** и в нем раскройте узел профиля, доступ к которому вы хотите настроить.
2. Выберите узел **Настройка**.

   В рабочей области в блоке **Управление доступом** отображается список ролей для пользователей профиля:

   - **Администратор профиля**.
   - **Специалист антивирусной безопасности профиля**.
   - **Оператор антивирусной безопасности профиля**.
3. Установите флажки напротив ролей, которые требуется назначить пользователям или группам пользователей для доступа к профилю.
4. Нажмите на кнопку  напротив выбранной роли.
5. Выберите и добавьте пользователя или группу пользователей, которым вы хотите предоставить доступ к профилю в выбранной роли.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить сделанные изменения.

Пользователям будут предоставлены права доступа к профилю в соответствии с назначенными ролями.

► *Чтобы отменить доступ к профилю для выбранных пользователей или групп пользователей, выполните следующие действия:*

1. Выполните пункты 1–2 предыдущей инструкции.
2. Снимите флажки напротив ролей, права доступа которых нужно отменить для выбранных пользователей или групп пользователей профиля.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить сделанные изменения.

► *Чтобы обновить права доступа к профилю для выбранных пользователей или групп пользователей, выполните следующие действия:*

1. Выполните пункты 1–2 предыдущей инструкции.
2. Снимите флажки напротив ролей, права доступа которых нужно обновить для выбранных пользователей или групп пользователей профиля.

3. Нажмите на кнопку **Сохранить**.
4. Снова установите флажки напротив ролей, права доступа которых необходимо обновить для выбранных пользователей или групп пользователей профиля.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить сделанные изменения.

Удаление Сервера безопасности из профиля

► *Чтобы удалить Сервер безопасности из профиля, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили**.
2. Выберите Сервер безопасности, который вы хотите удалить, одним из следующих способов:
   - выберите узел профиля, из которого вы хотите удалить Сервер безопасности, и в рабочей области в списке серверов выберите Сервер безопасности, который вы хотите удалить;
   - раскройте узел профиля, из которого вы хотите удалить Сервер безопасности, раскройте узел **Серверы** и в списке серверов выберите Сервер безопасности, который вы хотите удалить.
3. Удалите выбранный Сервер безопасности одним из следующих способов:
   - Если вы выбрали Сервер безопасности в рабочей области, нажмите на кнопку **Удалить сервер**.
   - Если вы выбрали Сервер безопасности в списке серверов узла **Серверы**, удалите Сервер безопасности одним из следующих способов:
     - выберите пункт **Удалить из профиля** в меню **Действие**;
     - выберите пункт **Удалить из профиля** в контекстном меню узла;
     - по ссылке **Удалить из профиля** в панели быстрого доступа.
4. В открывшемся окне подтвердите удаление сервера.

   Программа в течение 5 минут удалит Сервер безопасности из списка серверов в рабочей области узла профиля и из узла **Серверы** в дереве узла профиля. При этом параметры Сервера безопасности не изменятся, но вы больше не сможете настраивать их из профиля, вы сможете настраивать их только отдельно для Сервера безопасности в узле этого Сервера безопасности.

В конфигурации с группой DAG вы можете удалить из профиля все серверы, входящие в группу DAG, только одновременно.

После удаления из профиля Сервера безопасности на него по-прежнему распространяется действие лицензии профиля, из которого он был удален.

Удаление профиля

► *Чтобы удалить профиль, выполните следующие действия:*

1. В дереве Консоли управления выберите профиль, который вы хотите удалить, одним из следующих способов:
   - выберите узел **Профили** и в рабочей области в списке профилей выберите профиль, который вы хотите удалить;
   - раскройте узел **Профили** и в списке узлов выберите узел профиля, который вы хотите удалить.
2. Удалите выбранный профиль одним из следующих способов:
   - Если вы выбрали профиль в рабочей области, нажмите на кнопку **Удалить профиль**.
   - Если вы выбрали узел профиля, вложенный в узел **Профили**, удалите профиль одним из следующих способов:
     - выберите пункт **Удалить** в меню **Действие**;
     - выберите пункт **Удалить** в контекстном меню узла профиля;
     - по ссылке **Удалить** в панели быстрого доступа.
3. В открывшемся окне подтвердите удаление профиля.

Программа удалит профиль из дерева узла **Профили**. Серверы безопасности, входящие в профиль, станут нераспределенными. При этом параметры нераспределенных Серверов безопасности не изменятся, но вы сможете настраивать все параметры для каждого Сервера безопасности только отдельно в узле каждого сервера.

kaspersky

Обновления

Обновление баз программы Kaspersky Security обеспечивает актуальность защиты серверов Microsoft Exchange.

Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу, а также новые виды спама. Информация об угрозах и спаме и способах их нейтрализации содержится в *базах программы*, то есть базах Антивируса и Анти-Спама. Чтобы своевременно обнаруживать угрозы и спам-сообщения, требуется регулярно обновлять базы программы. Программа определяет базы Антивируса как устаревшие через 24 часа, а базы Анти-Спама – через 5 часов с момента последнего обновления.

Рекомендуется обновить базы программы сразу после установки программы, поскольку базы, входящие в состав установочного пакета, к моменту установки могут потерять актуальность. На серверах "Лаборатории Касперского" антивирусные базы обновляются каждый час. Базы Анти-Спама обновляются каждые пять минут. Рекомендуется с той же периодичностью настроить обновление баз по расписанию (см. раздел "Настройка обновления баз программы по расписанию" на стр. 167).

Kaspersky Security может получать обновления баз программы из следующих источников обновлений:

- с серверов обновлений "Лаборатории Касперского" в интернете;
- с другого HTTP-сервера / FTP-сервера (например, вашего интранет-сервера);
- из локального источника обновлений – локальной или сетевой папки;
- из центра обновлений – одного из серверов Microsoft Exchange с установленной программой Kaspersky Security, который назначен центром обновлений (см. раздел "О центрах обновлений" на стр. 165).

Обновление баз может выполняться вручную или по расписанию.

В этом разделе

О центрах обновлений

Любой сервер Microsoft Exchange с установленной программой Kaspersky Security может быть назначен центром обновлений (см. раздел "Назначение сервера центром обновлений и настройка его параметров" на стр. 170). Центры обновлений получают актуальные базы с серверов "Лаборатории Касперского" и могут служить источниками обновлений баз программы (см. раздел "Выбор источника обновлений" на стр. 168) для других серверов Microsoft Exchange, на которых установлена программа.

Использование центров обновлений может быть полезно в следующих случаях:

- Если в сети организации присутствует несколько серверов Microsoft Exchange с установленной программой, вы можете назначить один из серверов Microsoft Exchange центром обновлений, получающим базы с серверов "Лаборатории Касперского", и указать его в качестве источника обновлений для остальных серверов Microsoft Exchange сети организации. Это позволит сократить сетевой трафик, получаемый из интернета, поддерживать базы на всех серверах Microsoft Exchange в одинаковом состоянии, а также избежать необходимости настраивать соединение с интернетом для каждого сервера Microsoft Exchange и обеспечивать безопасность этих соединений.
- Если в сети организации имеются географически распределенные сегменты серверов, связанные медленными каналами связи, вы можете создать для каждого из региональных сегментов собственный центр обновлений, получающий базы с серверов "Лаборатории Касперского". Это позволит сократить сетевой трафик между региональными сегментами и ускорить распространение обновлений на все серверы сети организации.

Об обновлении баз в конфигурациях с группой DAG серверов Microsoft Exchange

В конфигурациях с группой DAG серверов Microsoft Exchange параметры обновления баз антивирусной защиты являются едиными для всей группы DAG. Это позволяет настраивать централизованное обновление баз антивирусной защиты на всех серверах, входящих в конфигурацию.

Настройка централизованного обновления баз для защиты от спама и фишинга недоступна для конфигураций с группой DAG серверов.

Вы можете настроить следующие способы централизованного обновления баз антивирусной защиты:

- **С серверов обновлений "Лаборатории Касперского"**. При использовании этого способа каждый из серверов группы DAG подключается к серверам обновлений "Лаборатории Касперского" в заданное время независимо от других серверов, что ведет к увеличению интернет-трафика. Поэтому этот способ не рекомендуется использовать в конфигурациях с большим количеством серверов. Недостатком этого способа также является необходимость настраивать соединение с интернетом на каждом из серверов, входящих в конфигурацию. Преимуществом способа является повышенная надежность, поскольку обновление выполняется непосредственно с серверов "Лаборатории Касперского" без промежуточных звеньев.
- **С промежуточного сервера или из сетевой папки**. При использовании этого способа серверы, входящие в группу DAG, загружают обновления с промежуточного HTTP-сервера, FTP-сервера или из сетевой папки, находящейся за пределами конфигурации серверов Microsoft Exchange. Этот способ позволяет сократить интернет-трафик организации, а также добиться высокой скорости и синхронности обновления на всех серверах конфигурации, однако требует расходов на обслуживание дополнительного промежуточного оборудования.
- **Из центра обновлений**. Этот способ требует назначения одного из серверов, входящих в группу DAG, центром обновлений (см. раздел "Назначение сервера центром обновлений и настройка его параметров" на стр. 170). Преимуществами этот способа являются сокращение интернет-трафика организации, высокая скорость и синхронность обновления на всех серверах конфигурации. Однако при использовании этого способа предъявляются повышенные требования к надежности сервера, назначенного центром обновлений.

Запуск обновления баз вручную

► *Чтобы просмотреть информацию об обновлении баз Антивируса и обновить их вручную, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Обновления**.
3. В рабочей области в блоке параметров **Обновление антивирусных баз** отображается следующая информация:
   - **Результат последнего обновления**. Информация о статусе обновления антивирусных баз.
   - **Время выпуска баз**. Время публикации антивирусных баз, которые в настоящий момент используются в программе, на сервере "Лаборатории Касперского".
4. Если вы хотите обновить антивирусные базы, нажмите на кнопку **Запустить обновление**.
5. Чтобы остановить обновление, нажмите на кнопку **Остановить**.

Если программа работает в DAG серверов Microsoft Exchange, требуется вручную обновить базы Антивируса на каждом из серверов, входящем в эту DAG.

► *Чтобы просмотреть информацию об обновлении баз Анти-Спама и обновить базы Анти-Спама вручную, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Обновления**.
3. В рабочей области в блоке параметров **Обновление баз Анти-Спама** отображается следующая информация:
   - **Результат последнего обновления**. Информация о статусе обновления баз Анти-Спама.
   - **Время выпуска баз**. Время публикации баз Анти-Спама, которые в данный момент используются в программе, на сервере "Лаборатории Касперского".
4. Если вы хотите обновить базы Анти-Спама, нажмите на кнопку **Запустить обновление**.
5. Чтобы остановить обновление, нажмите на кнопку **Остановить**.

Настройка обновления баз программы по расписанию

► *Чтобы настроить обновление баз программы по расписанию, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить обновление баз программы по расписанию для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить обновление баз программы по расписанию для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить обновление баз Антивируса.

2. Выберите узел **Обновления**.
3. Выполните одно из следующих действий:
   - если вы хотите настроить обновление баз Антивируса по расписанию, раскройте блок параметров **Обновление антивирусных баз**;
   - если вы хотите настроить обновление баз Анти-Спама по расписанию, раскройте блок параметров **Обновление баз Анти-Спама**.
4. В раскрывающемся списке **Режим запуска** выберите один из следующих вариантов:
   - **Периодически**. В поле ввода **каждые** укажите частоту обновления баз программы в минутах / часах / сутках.
   - **Ежедневно**. В поле ввода с прокруткой справа укажите точное локальное время сервера, когда требуется обновлять базы программы.
   - **В выбранный день**. Установите флажки напротив дней недели, в которые необходимо обновлять базы программы, и укажите время обновления.
5. Нажмите на кнопку **Сохранить**.

Если программа работает на сервере Microsoft Exchange в составе группы DAG, параметры обновления баз Антивируса по расписанию, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту группу DAG. На остальных серверах этой группы DAG настраивать обновление по расписанию не требуется.

Выбор источника обновлений

► *Чтобы выбрать источник обновлений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите выбрать источник обновлений для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите выбрать источник обновлений для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите выбрать источник обновлений.
2. Выберите узел **Обновления**.
3. Выполните одно из следующих действий: если вы хотите выбрать источник обновлений для баз Анти-Спама, раскройте блок параметров **Обновление баз Анти-Спама**; если вы хотите выбрать источник обновлений для баз Антивируса, раскройте блок параметров **Обновление антивирусных баз**.
4. В списке **Источник обновлений** выберите один из следующих вариантов:
   - Если вы хотите загружать обновления с серверов "Лаборатории Касперского", выберите пункт **Серверы обновлений "Лаборатории Касперского"**.

     Этот источник обновлений установлен по умолчанию.

- Если вы хотите загружать обновления с промежуточного сервера, локальной или сетевой папки, выберите пункт **HTTP-сервер, FTP-сервер, локальная или сетевая папка**. Затем в поле ввода укажите адрес сервера или полный путь к локальной или сетевой папке.
- Если вы хотите загружать обновления из центра обновлений, выберите пункт **Хранилище центра обновлений**. Затем в раскрывающемся списке выберите сервер, являющийся центром обновлений.

  Вы можете установить этот источник обновлений, если в вашей конфигурации создан хотя бы один центр обновлений (см. раздел "Назначение сервера центром обновлений и настройка его параметров" на стр. 170). Если сервер Microsoft Exchange, для которого вы выбираете источник обновлений, развернут в роли Пограничный транспорт (Edge Transport), имя сервера, являющегося центром обновлений, может отсутствовать в раскрывающемся списке. В этом случае введите имя сервера, являющегося центром обновлений, вручную.

5. Нажмите на кнопку **Сохранить**.

Если программа работает в конфигурации с DAG серверов Microsoft Exchange, параметры обновления баз Антивируса (в частности, источник обновлений), настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту DAG. На остальных серверах настраивать параметры обновления не требуется.

Настройка параметров прокси-сервера

► *Чтобы настроить параметры прокси-сервера, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры подключения к прокси-серверу для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры подключения к прокси-серверу для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры подключения к прокси-серверу.
2. Выберите узел **Настройка**.
3. Установите флажок **Использовать прокси-сервер**, если вы хотите настроить подключение программы к службам Анти-Спама Kaspersky Security Network, Enforced Anti-Spam Updates Service, источникам обновлений и серверам активации "Лаборатории Касперского" через прокси-сервер.

   При подключении к серверам активации "Лаборатории Касперского" для профиля Серверов безопасности используются локальные параметры подключения к прокси-серверу компьютера, на котором установлена Консоль управления. В рабочей области раскройте блок параметров **Параметры прокси-сервера**.

4. В поле **Адрес прокси-сервера** введите адрес прокси-сервера.

5. В поле **Порт** укажите номер порта прокси-сервера.

   По умолчанию используется порт 8080.

6. Если для подключения к прокси-серверу требуется аутентификация, установите флажок **Использовать аутентификацию** и укажите имя учетной записи в поле **Учетная запись** и пароль в поле **Пароль**.
7. Если вы не хотите использовать прокси-сервер для подключения к локальным ресурсам, установите флажок **Не использовать прокси-сервер для локальных адресов**.
8. Нажмите на кнопку **Сохранить**.

Назначение сервера центром обновлений и настройка его параметров

Не рекомендуется назначать центр обновлений и настраивать его параметры во время перехода на новую версию программы на серверах, работающих в конфигурации с DAG серверов Microsoft Exchange. Действия, описанные в этом разделе, требуется выполнять только после завершения перехода всех серверов на новую версию программы (см. стр. 50).

Не рекомендуется назначать центром обновлений виртуальный сервер Microsoft Exchange.

Сервер Microsoft Exchange, являющийся центром обновлений, должен иметь постоянное подключение к интернету и 500 МБ дополнительного дискового пространства.

► *Чтобы назначить сервер центром обновлений и настроить его параметры, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Обновления**.
3. В рабочей области раскройте блок **Параметры центра обновлений**.
4. Установите флажок **Сервер является центром обновлений**.
5. Выберите источник обновлений, из которого центр обновлений будет получать базы:
   - Если вы хотите загружать в центр обновлений обновления с серверов "Лаборатории Касперского", выберите пункт **Серверы обновлений "Лаборатории Касперского"**.

     Этот источник обновлений установлен по умолчанию.

   - Если вы хотите загружать в центр обновлений обновления с промежуточного сервера, локальной или сетевой папки, выберите пункт **HTTP-сервер, FTP-сервер, локальная или сетевая папка**. Затем в поле ввода укажите адрес сервера или полный путь к локальной или сетевой папке.

- Если вы хотите загружать в центр обновлений обновления из другого центра обновлений, выберите пункт **Хранилище центра обновлений**. Затем в раскрывающемся списке выберите сервер, являющийся центром обновлений.

6. Настройте для центра обновлений расписание обновления баз. Для этого в раскрывающемся списке **Режим запуска** выберите один из следующих вариантов:
   - **Периодически**. В поле ввода **каждые** укажите частоту обновления баз.
   - **Ежедневно**. Укажите точное локальное время сервера в поле **в ЧЧ**:**ММ**.
   - **В выбранный день**. Установите флажки напротив дней недели, в которые необходимо обновлять базы, и укажите время обновления.

   Не рекомендуется выбирать режим запуска обновления баз **Вручную** для центра обновлений, так как при этом режиме запуска невозможно обеспечить актуальность баз в центре обновлений и на всех серверах, которые используют его в качестве источника обновлений.

7. Нажмите на кнопку **Сохранить**.

Выбранный сервер Microsoft Exchange будет назначен центром обновлений. В дальнейшем он может быть выбран в качестве источника обновлений для других серверов (см. раздел "Выбор источника обновлений" на стр. 168).

kaspersky

Уведомления

Уведомление – это сообщение, которое содержит информацию о событии в работе Kaspersky Security на защищаемом сервере Microsoft Exchange.

Вы можете настроить получение уведомлений о следующих событиях в работе программы:

- обнаружение зараженных или защищенных паролем объектов в сообщениях;
- обнаружение спам-сообщений, массовых рассылок и сообщений, содержащих фишинговые ссылки;
- обнаружение содержимого и вложений, соответствующих критериям фильтрации;
- обнаружение потока однотипных сообщений, отправляемых с внутреннего почтового ящика организации;
- изменение статуса и состояния баз Антивируса и Анти-Спама;
- истечение срока действия лицензии и другие события, связанные с лицензированием;
- возникновение системных ошибок.

В зависимости от типа события, программа может отправлять уведомление о нем в виде сообщения электронной почты или записывать информацию в журнал событий Windows.

Вы можете включить запись в журнал событий Windows для всех уведомлений, кроме информации о статусе баз Антивируса и Анти-Спама и системных ошибках в работе программы.

Если в организации настроено управление программой через Kaspersky Security Center и включена запись событий в журнал событий Windows, то информация о следующих событиях дополнительно передается в Kaspersky Security Center:

- обнаружение зараженных или защищенных паролем объектов в сообщениях;
- обнаружение содержимого и вложений, соответствующих критериям фильтрации;
- истечение срока действия лицензии и другие события, связанные с лицензиями.

Kaspersky Security не отправляет уведомления об обнаружении спам-сообщений, массовых рассылок и сообщений, содержащих фишинговые ссылки, по электронной почте. Для данных событий вы можете включить запись в журнал событий Windows.

Уведомления содержат подробную информацию о сообщении, в котором был обнаружен объект, и о действиях, выполненных программой в связи с данным обнаружением. Текст уведомлений формируется на основе заданных шаблонов. Для некоторых событий доступно создание индивидуальных шаблонов уведомлений.

Отправка уведомлений по электронной почте

Kaspersky Security отправляет уведомления о событиях по электронной почте. Для отправки уведомлений программа использует веб-службу сервера Microsoft Exchange. Перед использованием уведомлений вам нужно указать адрес веб-службы и параметры аутентификации на сервере Microsoft Exchange (см. раздел «Настройка общих параметров отправки уведомлений» на стр. 174).

Вы можете указать адресатов уведомлений для каждого события (см. раздел «Настройка уведомлений о событиях в работе программы» на стр. 175).

Получателем любого уведомления, отправляемого по электронной почте, может быть назначен администратор или любой другой адрес электронной почты. Об обнаружении зараженных или защищенных паролем объектов, а также об отфильтрованных вложениях и содержимом вы можете дополнительно

уведомлять отправителя и получателей сообщения. Получателем считается почтовый ящик, указанный в поле «Кому» сообщения. При обнаружении объекта в почтовом ящике внутреннего пользователя организации отправка уведомлений будет выполняться, даже если сообщения фактически не отправлялись из почтового ящика (например, сохранены в папке Черновики с заполненным полем «Кому»).

По умолчанию адресаты уведомлений не заданы.

Отправка уведомлений внешним отправителям и получателям сообщений

По умолчанию Kaspersky Security разрешает отправку уведомлений об обработке объектов только на внутренние адреса электронной почты отправителей и получателей проверенных сообщений.

Внутренними считаются адреса электронной почты, принадлежащие к доменам, которые перечислены в списках Accepted Domains защищаемых серверов Microsoft Exchange вашей организации.

Если в адресной книге вашей организации есть контакты с адресами из другой организации, такие адреса считаются внешними.

Вы можете включить отправку уведомлений об обработке объектов на адреса внешних отправителей и получателей сообщений (см. раздел «Разрешение отправки уведомлений внешним отправителям и получателям сообщений» на стр. 176).

Уведомления по результатам проверки модулем Антивирус

Kaspersky Security позволяет получать отдельные уведомления при возникновении следующих событий:

- обнаружение зараженного объекта;
- обнаружение защищенного паролем объекта;
- обнаружение в сообщении вложения или содержимого, соответствующего критериям фильтрации;
- превышение ограничения по количеству однотипных сообщений, отправленных с внутреннего адреса электронной почты.

Kaspersky Security отправляет по одному уведомлению об обнаружении в сообщении объектов каждого типа независимо от количества обнаруженных объектов. Например, если в сообщении обнаружено пять зараженных и два защищенных паролем объекта, Kaspersky Security отправит одно уведомление об обнаружении зараженных объектов и одно уведомление об обнаружении защищенных паролем объектов.

Уведомления по результатам проверки модулем Анти-Спам

Kaspersky Security может записывать информацию о следующих событиях в журнал событий Windows:

- обнаружение спам-сообщения;
- обнаружение сообщения, содержащего фишинговую ссылку;
- обнаружение сообщения, содержащего массовую рассылку.

Уведомления о событиях, связанных с лицензиями

Kaspersky Security формирует следующие уведомления о событиях, связанных с лицензиями:

- Уведомление о занесении ключа в черный список ключей.

  Уведомление отправляется после каждого обновления баз программы на Сервере безопасности, если активный ключ Сервера безопасности находится в черном списке ключей. Каждый Сервер безопасности, на который добавлен ключ, найденный в черном списке, отправляет уведомление.

- Уведомление о скором истечении срока действия лицензии.

  Уведомление отправляется один раз в сутки (00:00 UTC) в соответствии со значением параметра (см. раздел "Настройка уведомления о скором истечении срока действия лицензии" на стр. 72), заданным в поле **Уведомить заранее об истечении срока действия лицензии (дни)** в узле **Уведомления**. При отправке уведомления учитывается срок действия активного и резервного ключей Сервера безопасности.

- Уведомление об ошибке обновления статуса лицензии.

  Уведомление отправляется один раз в сутки (00:00 UTC), если в течение продолжительного времени программе не удалось связаться с серверами активации "Лаборатории Касперского", чтобы подтвердить статус лицензии.

- Уведомление об истекшем сроке действия лицензии.

  Уведомление отправляется один раз в сутки (00:00 UTC), если истек срок действия активного ключа, при этом резервный ключ отсутствует, или завершился период действия подписки.

- Уведомление о неудачной попытке обновления статуса лицензии и об истекшем сроке обновления лицензии.

  Уведомление отправляется один раз в сутки (00:00 UTC), если не удалось обновить статус лицензии, так как в течение продолжительного времени программе не удалось связаться с серверами активации "Лаборатории Касперского", чтобы подтвердить статус лицензии, и срок обновления статуса лицензии истек.

В этом разделе

Настройка общих параметров отправки уведомлений

► *Чтобы настроить параметры отправки уведомлений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить параметры отправки уведомлений для нераспределенного Сервера безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите настроить параметры отправки уведомлений для Серверов безопасности профиля, раскройте узел **Профили** и в нем выберите узел того профиля, для Серверов безопасности которого вы хотите настроить параметры отправки уведомлений.
2. Выберите узел **Уведомления**.

   В рабочей области отобразятся блоки **Параметры отправки уведомлений** и **Уведомления о событиях**.
3. В блоке **Параметры отправки уведомлений** укажите следующие параметры:
   - **Адрес сервера**

     Адрес веб-службы сервера Microsoft Exchange, с помощью которой программа отправляет уведомления. По умолчанию на сервере Microsoft Exchange используется адрес `https://<имя_сервера_клиентского_доступа>/ews/exchange.asmx`.

- **Учетная запись** и **Пароль**

  Учетная запись, от имени которой программа отправляет уведомления, и пароль для этой учетной записи. Учетная запись должна иметь в почтовой инфраструктуре Microsoft Exchange почтовый ящик, доступный через Outlook® Web Access (OWA). Эта учетная запись также используется для отправки отчетов.

  Вы можете выбрать учетную запись, нажав на кнопку  .

- **Адрес администратора**

  Адрес или список адресов электронной почты администраторов программы. Программа отправляет уведомления на эти адреса электронной почты при наступлении событий, для которых в списке адресатов установлен флажок **Администратор**. Вы можете указать несколько адресов электронной почты, разделяя их точкой с запятой.

  Если вы настраиваете параметры уведомлений для нераспределенного Сервера безопасности, вы можете отправить тестовое сообщение на адрес электронной почты администратора, нажав на кнопку **Тест**.

4. Нажмите на кнопку **ОК**.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, параметры отправки уведомлений, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту группу DAG. На остальных серверах этой группы DAG настраивать параметры отправки уведомлений не требуется.

При некорректном срабатывании механизма отправки уведомлений по протоколу EWS, вы можете воспользоваться возможностью отправки уведомлений по протоколу SMTP, выбрав соответствующий протокол в блоке **Параметры отправки уведомлений**.

В настройках отправки уведомлений по протоколу SMTP вы можете указать:

- Адрес SMTP-сервера (адрес вводится вручную).

  Также вы можете добавить номер порта в адрес SMTP-сервера (по умолчанию порт 587).

- Учетную запись и пароль (вы можете указать учетную запись из списка Active Directory или ввести вручную).

  При отправке уведомлений без аутентификации указывать учетную запись и пароль не требуется.

- Адрес электронной почты отправителя.
- Адрес электронной почты администратора.

Для отправки уведомлений по протоколам EWS и SMTP:

Убедитесь, что установлен флажок **Использовать TLS** для установки защищенного соединения, шифрования сообщений и их безопасной передачи в сети.

Отключать использование TLS стоит только в случаях, если сервер по какой-то причине не поддерживает корректную установку защищенного соединения и исправить ситуацию со стороны сервера Microsoft Echange или SMTP-сервера невозможно.

Возможны ситуации, когда соединение не устанавливается из-за того, что сертификат сервера не является доверенным на машине с KSE. В таком случае необходимо добавить этот сертификат в системное хранилище сертификатов, не отключая использование TLS.

Настройка уведомлений о событиях в работе программы

► *Чтобы настроить уведомления о событиях в работе программы, выполните следующие действия:*

1. В дереве Консоли управления выберите узел **Уведомления**.

   В рабочей области отобразятся блоки **Параметры отправки уведомлений** и **Уведомления о событиях**.

2. В блоке **Уведомления о событиях** настройте параметры уведомлений следующим образом:

   a. В левой части блока в списке **Темы уведомлений** выберите событие, уведомление о котором вы хотите отправлять. В зависимости от типа выбранного события, в правой части блока отобразится список адресатов, доступных для отправки уведомлений, и / или флажок для включения записи в журнал событий Windows.

      При выборе пункта **Спам и фишинг** отобразится список событий Анти-Спама и Анти-Фишинга.

   b. Если для выбранного типа событий доступна отправка уведомлений по электронной почте, установите флажок напротив адресатов, которых вы хотите информировать о наступлении события. При выборе варианта **Дополнительные адреса,** укажите адрес электронной почты

получателя уведомлений в поле ввода. Вы можете добавить несколько адресов электронной почты, разделяя их точкой с запятой.

При выборе пункта **Спам и фишинг** установите флажок напротив событий Анти-Спама и/или Анти-Фишинга. Вы можете выбрать следующие события:

- **Спам**. Событие записывается, если программа обнаружила спам-сообщение.
- **Массовая рассылка**. Событие записывается, если программа обнаружила сообщение, содержащее массовую рассылку.
- **Фишинг**. Событие записывается, если программа обнаружила сообщение, содержащее фишинговую ссылку.

c. Если для выбранного типа событий доступно создание индивидуального шаблона уведомлений, вы можете отредактировать текст уведомления, нажав на кнопку **Шаблон**.

d. Если вы хотите, чтобы программа записывала информацию о событии в журнал событий Windows и Kaspersky Security Center, установите флажок **Записывать события в журнал Windows**.

Этот параметр недоступен для уведомлений о статусе баз и системных ошибках. События Анти-Спама, Анти-Фишинга и фильтрации однотипных сообщений записываются только в журнал событий Windows.

3. Нажмите на кнопку **Сохранить**.

Настроенные параметры уведомлений будут сохранены.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, параметры уведомлений, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту группу DAG. На остальных серверах этой группы DAG настраивать параметры уведомлений не требуется.

Разрешение отправки уведомлений внешним отправителям и получателям сообщений

По умолчанию Kaspersky Security запрещает отправку уведомлений об обработке объектов на внешние, то есть, расположенные за пределами организации, адреса электронной почты отправителей и получателей проверенных сообщений. Например, если в списке получателей зараженного сообщения указаны внутренние и внешние получатели, то, если включена отправка уведомлений об обнаружении зараженного объекта получателям сообщений (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 175), уведомление будет отправлено только внутренним получателям. Внутренними считаются адреса электронной почты, принадлежащий к доменам, которые перечислены в списках Accepted Domains защищаемых серверов Microsoft Exchange вашей организации. Если в адресной книге вашей организации есть контакты с адресами из другой организации, такие адреса считаются внешними.

Запрет не распространяется на адреса администраторов и на дополнительные адреса.

Вы можете разрешить отправку уведомлений об обработке объектов внешним отправителям и получателям сообщений.

Если вы разрешите отправку уведомлений на внешние адреса, то информация об обработанных объектах станет доступна третьим лицам за пределами организации.

► *Чтобы разрешить отправку уведомлений на внешние адреса электронной почты отправителей и получателей сообщений, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите настроить отправку уведомлений внешним отправителям и получателям сообщений для нераспределенного Сервера безопасности, выберите узел этого Сервера безопасности.
   - Если вы хотите настроить отправку уведомлений внешним отправителям и получателям сообщений для Серверов безопасности профиля, раскройте узел **Профили** и в нем выберите узел того профиля, для Серверов безопасности которого вы хотите выполнить настройку.
2. Выберите узел **Уведомления**.

   В рабочей области отобразятся блоки **Параметры отправки уведомлений** и **Уведомления о событиях**.
3. Чтобы разрешить отправку уведомлений об обработанных объектах любым (как внутренним, так и внешним по отношении к организации) отправителям и получателям проверенных сообщений, снимите этот флажок **Отсылать уведомления только внутренним пользователям**, расположенный в блоке **Уведомления о событиях**.
4. Нажмите на кнопку **Сохранить**.

   Отправка уведомлений на внешние адреса электронной почты отправителей и получателей сообщений будет разрешена.

Если программа работает в конфигурации с группой DAG серверов Microsoft Exchange, параметры уведомлений, настроенные на одном из серверов, автоматически распространяются на остальные серверы, входящие в эту группу DAG. На остальных серверах этой группы DAG настраивать параметры уведомлений не требуется.

kaspersky

Резервное хранилище

Kaspersky Security может сохранять в *резервном хранилище* копии сообщений перед обработкой этих сообщений модулями программы. Копии сообщений помещаются в резервное хранилище вместе со всеми вложениями.

Kaspersky Security сохраняет копии сообщений в резервном хранилище в следующих случаях:

- после проверки сообщений модулем Антивирус перед тем, как выполнить изменение сообщения в результате действия **Удалять сообщение** или **Удалять объект**, если разрешено сохранение копий сообщений в резервном хранилище при антивирусной проверке (см. раздел "Настройка параметров антивирусной обработки объектов: Антивирус для роли Почтовый ящик" на стр. 109);
- после проверки сообщений на спам и фишинг перед тем, как выполнить над сообщением действие `Удалять` или `Отклонять`, если разрешено сохранение копий сообщений в резервном хранилище при проверке на спам и фишинг (см. раздел "Настройка параметров проверки на спам и фишинг" на стр. 123);
- при выполнении фильтрации вложений и содержимого, если разрешено сохранение копий сообщений в резервном хранилище при фильтрации вложений и содержимого (см. раздел "Работа с правилами фильтрации вложений и содержимого" на стр. 147).

Вы можете выполнять следующие действия над копиями сообщений в резервном хранилище:

- Просматривать содержимое резервного хранилища (см. раздел "Просмотр объектов резервного хранилища" на стр. 179).
- Получать информацию о сообщениях в резервном хранилище (см. раздел "Просмотр свойств объектов в резервном хранилище" на стр. 180).
- Фильтровать информацию о сообщениях в резервном хранилище для удобства просмотра и поиска информации о сообщениях (см. раздел "Фильтрация списка объектов резервного хранилища" на стр. 181).
- Сохранять сообщения из резервного хранилища на диск в целях получения информации, содержащейся в сообщении (см. раздел "Сохранение объектов из резервного хранилища на диск" на стр. 182). Вы также можете попытаться еще раз проверить сохраненное сообщение Антивирусом с использованием обновленной версии баз.
- Доставлять сообщения из резервного хранилища получателям (см. раздел "Отправка объектов из резервного хранилища исходным получателям" на стр. 182). Сохраненные объекты будут доставлены получателям.
- Отправлять сообщения из резервного хранилища на адреса электронной почты, указанные вручную (см. раздел "Отправка объектов из резервного хранилища на другие адреса электронной почты" на стр. 183).
- Удалять копии сообщений из резервного хранилища (см. раздел "Удаление объектов из резервного хранилища" на стр. 184).

Данные об объектах резервного хранилища хранятся в базе данных SQL, указанной при установке программы (см. раздел "Шаг 5. Создание базы данных и настройка подключения программы к SQL-серверу" на стр. 30). Если несколько Серверов безопасности используют одну базу данных SQL (например, в конфигурации серверов с DAG), в резервном хранилище сохраняются сообщения, полученные от каждого из этих Серверов безопасности.

Копии сообщений хранятся в резервном хранилище в зашифрованном виде, обеспечивая отсутствие риска заражения и сокращение времени работы Антивируса (файлы в формате резервного хранилища не определяются как зараженные).

Общее количество объектов в резервном хранилище ограничено одним миллионом. Вы можете дополнительно ограничить объем резервного хранилища, установив ограничения по размеру резервного хранилища и по времени хранения объектов в нем (см. раздел "Настройка параметров резервного хранилища" на стр. 186).

Проверка соблюдения ограничений выполняется каждую минуту. По результатам проверки программа может выполнять следующие действия:

- если превышено допустимое количество сообщений в хранилище, программа удаляет необходимое количество наиболее "старых" объектов;
- если установлено ограничение на размер хранилища в мегабайтах и при помещении в хранилище очередного сообщения оно превышено, программа освобождает необходимый объем за счет удаления наиболее "старых" объектов;
- если установлено ограничение на срок хранения сообщений, программа удаляет сообщения, срок хранения которых закончился.

В этом разделе

Просмотр объектов резервного хранилища

Вы можете просматривать информацию обо всех сохраненных в резервном хранилище объектах (копиях сообщений и вложениях).

► *Чтобы просмотреть объекты резервного хранилища, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Резервное хранилище**.

   В рабочей области отображается таблица, содержащая информацию об объектах, сохраненных в резервном хранилище.

В нижней части рабочей области под таблицей отображается информация о том, сколько всего объектов находится в резервном хранилище, и какой объем они занимают, а также количество отфильтрованных объектов, если используется фильтр.

По умолчанию вы можете просмотреть в таблице следующую информацию для каждого объекта в резервном хранилище:

- **От**. Адрес отправителя сообщения, указанный в поле сообщения "От" .
- **Кому**. Адрес или список адресов получателей сообщения, указанных в полях сообщения "Кому" и "СК".
- **Тема**. Тема сообщения.
- **Статус**. Статус проверки объекта (*Заражен*, *Возможно зараженный*, *Вылечен*, *Защищен*, *Спам*, *Возможный спам*, *Формальное оповещение*, *Адрес в черном списке*, *Доверенный*, *Массовая рассылка*, *Фишинг*, *Запрещенное вложение удалено*, *Сообщение удалено*, *Сообщение с запрещенным вложением или содержимым пропущено*).
- **Получено**. Точное время поступления сообщения на сервер Microsoft Exchange.

Вы можете настроить вид рабочей области, изменяя набор и порядок отображения столбцов таблицы.

► *Чтобы настроить вид рабочей области, выполните следующие действия:*

1. Нажмите на кнопку **Выбрать столбцы**, чтобы добавить или удалить столбцы таблицы.
2. В открывшемся окне выполните следующие действия:
   - установите флажки рядом с теми столбцами таблицы, которые вы хотите просматривать в рабочей области;
   - снимите флажки рядом с теми столбцами таблицы, которые вы не хотите просматривать.

Вы можете сортировать информацию в таблице по любому из столбцов таблицы, нажав на название нужного столбца, например, **От**, **Кому**, **Тема**.

В рабочей области одновременно отображается ограниченное количество объектов. Чтобы просмотреть другие объекты, нужно воспользоваться кнопками перехода, расположенными в правом нижнем углу рабочей области. Между двумя парами кнопок перехода расположен индикатор номера текущего окна. Чтобы перейти к следующему окну, нужно нажать на кнопку со значком **>**. Чтобы перейти к предыдущему окну, нужно нажать на кнопку со значком **<**. Чтобы перейти к последнему окну, нужно нажать на кнопку со значком **>>**. Чтобы вернуться к самому первому окну, нужно нажать на кнопку со значком **<<**.

Просмотр свойств объектов в резервном хранилище

► *Чтобы просмотреть свойства объекта в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Резервное хранилище**.
3. В таблице со списком объектов резервного хранилища выберите объект, свойства которого вы хотите просмотреть.
4. Нажмите на кнопку **Свойства**, расположенную над списком объектов.

Откроется окно **Свойства**. В этом окне вы можете просмотреть следующую информацию:

- **Компонент**. Модуль, поместивший объект в резервное хранилище: Антивирус, Анти-Спам, Анти-Фишинг или Фильтрация вложений и содержимого.
- **Обнаружение**. Название угрозы, если сообщение заражено, или имя сработавшего правила фильтрации вложений и содержимого.
- **Тип объекта**. Тип объекта: Сообщение целиком, Текст сообщения или Вложение.
- **Ключевые слова**. Обнаруженные слова, соответствующие условиям сработавшего правила фильтрации вложений и содержимого.
- **От**. Адрес отправителя.
- **Кому**. Адрес получателя сообщения.
- **Имя объекта**. Имя файла сообщения или вложения.
- **Тема**. Тема сообщения.
- **ID сообщения**. Идентификатор сообщения. Соответствует полю "Message-Id" в заголовке сообщения.
- **Имя сервера.** Имя сервера, поместившего объект в резервное хранилище.
- **Получено.** Точное время доставки сообщения (число, месяц, год, часы, минуты).
- **Отправлено.** Точное время отправки сообщения (число, месяц, год, часы, минуты).
- **Время выпуска баз**. Время выпуска баз программы, с помощью которых был проверен объект.
- **Статус**. Статус, присвоенный сообщению программой (*Заражен*, *Возможно зараженный*, *Вылечен*, *Защищен*, *Спам*, *Возможный спам*, *Формальное оповещение*, *Адрес в черном списке*, *Доверенный*, *Массовая рассылка*, *Фишинг*, *Запрещенное вложение удалено*, *Сообщение удалено*, *Сообщение с запрещенным вложением или содержимым пропущено*).
- **Размер**. Размер объекта в килобайтах.

Фильтрация списка объектов резервного хранилища

Вы можете отфильтровать список объектов резервного хранилища по одному или нескольким условиям с помощью фильтра. Условия фильтра применяются к столбцам таблицы. Добавляя условия, вы можете составлять сложные фильтры. Условия в фильтре комбинируются логической операцией "И". Объекты резервного хранилища, которые не соответствуют условиям фильтра, не отображаются в списке.

► *Чтобы отфильтровать список объектов резервного хранилища, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Резервное хранилище**.
3. В блоке **Фильтр хранилища** настройте условия фильтрации:
   a. В раскрывающемся списке выберите столбец, к которому должно быть применено условие.

      В зависимости от выбранного столбца оставшиеся параметры условия могут принимать следующий вид:

      - раскрывающийся список;
      - раскрывающийся список и поле ввода.

b. Выберите значение параметра (параметров) из раскрывающегося списка и / или укажите вручную.

4. При необходимости добавьте дополнительные критерии фильтрации, нажав на кнопку **Добавить условие**. Удалите ненужные условия с помощью кнопки , расположенной в правой части строки с условием.
5. Нажмите на кнопку **Поиск**, чтобы отфильтровать список объектов резервного хранилища

Программа отобразит в таблице объекты резервного хранилища, соответствующие условиям фильтра. Объекты резервного хранилища, не соответствующие условиям фильтра, будут скрыты.

После применения фильтра вы также можете сортировать информацию в таблице по возрастанию или убыванию данных любого столбца таблицы. Для этого нажмите на название нужного столбца, например, **От**, **Кому**, **Тема**.

Сохранение объектов из резервного хранилища на диск

Сохранение объектов из резервного хранилища может привести к заражению вашего компьютера.

► *Чтобы сохранить объект из резервного хранилища на диск, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел Сервера безопасности.
2. Выберите узел **Резервное хранилище**.
3. В рабочей области в таблице со списком объектов резервного хранилища выберите объект, который вы хотите сохранить.
4. Нажмите на кнопку **Сохранить на диск**, расположенную в верхней части рабочей области над списком объектов.
5. В открывшемся окне укажите папку, в которую вы хотите сохранить объект и, если требуется, введите или измените имя объекта.
6. Нажмите на кнопку **Сохранить**.
7. В открывшемся окне ознакомьтесь с текстом предупреждения и нажмите **Да**, если вы принимаете риск и хотите выполнить действие.

Выбранный объект будет расшифрован, его копия будет сохранена в указанной папке под заданным именем. Сохраненный объект имеет тот же формат, в котором объект поступил на обработку программе. После успешного сохранения объекта программа выводит на экран компьютера уведомление: "Выбранный объект сохранен на диск".

Отправка объектов из резервного хранилища исходным получателям

В результате отправки объектов из резервного хранилища компьютеры получателей сообщения могут быть заражены.

Вы можете отправлять сохраненные в резервном хранилище объекты получателям, которым они изначально предназначались.

Для отправки объектов типа *Текст сообщения* или *Вложение* необходимо указать параметры веб-службы Microsoft Exchange для Сервера безопасности, на котором был обнаружен объект.

Для отправки объектов типа *Сообщение целиком* необходимо учитывать следующие условия:

- на сервере Microsoft Exchange, на котором был обнаружен объект, должен быть настроен каталог преобразования;
- учетная запись, от имени которой запускается служба Kaspersky Security 9.0 для Microsoft Exchange Servers, должна обладать необходимыми правами для записи в каталог преобразования.

В целях безопасности программа подписывает каждое сообщение, отправленное из резервного хранилища, заголовком, который содержит зашифрованный хеш сообщения. Ключ для расшифровки подписи генерируется автоматически при установке или обновлении программы.

Чтобы программа не проверяла отправленное сообщение повторно и не возвращала его в резервное хранилище, на всех защищаемых серверах Microsoft Exchange должны присутствовать идентичные наборы ключей для расшифровки подписи. Для этого вам нужно вручную экспортировать ключ (см. раздел "Работа с ключом для расшифровки подписи сообщений" на стр. 221) Транспортного сервера-концентратора и импортировать его на Пограничный транспортный сервер и наоборот.

Чтобы отправить объект из резервного хранилища адресатам, выполните следующие действия:

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Резервное хранилище**.
3. В рабочей области в таблице со списком объектов резервного хранилища выберите объект, который вы хотите отправить адресатам.
4. Нажмите на кнопку **Отправить,** расположенную в верхней части рабочей области над списком объектов, и выберите пункт меню **Отправить исходным получателям**.
5. В открывшемся окне ознакомьтесь с текстом предупреждения и нажмите **Да**, если вы принимаете риск и хотите выполнить действие.

Программа отправит выбранный объект адресатам исходного сообщения.

Отправка объектов из резервного хранилища на другие адреса электронной почты

В результате отправки объектов из резервного хранилища компьютеры получателей сообщения могут быть заражены.

Вы можете пересылать сохраненные в резервном хранилище объекты на любые адреса электронной почты, указанные вручную. В данном случае объект доставляется получателю в виде вложенного файла. В теле сообщения содержится информация об объекте.

Функциональность доступна пользователям, включенным в группы (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Kse Administrators и Kse AV Security Officers.

Для отправки объектов необходимо указать параметры веб-службы Microsoft Exchange для Сервера безопасности, на котором был обнаружен объект.

В целях безопасности программа подписывает каждое сообщение, отправленное из резервного хранилища, заголовком, который содержит зашифрованный хеш сообщения. Ключ для расшифровки подписи генерируется автоматически при установке или обновлении программы.

Чтобы программа не проверяла отправленное сообщение повторно и не возвращала его в резервное хранилище, на всех защищаемых серверах Microsoft Exchange должны присутствовать идентичные наборы ключей для расшифровки подписи. Для этого вам нужно вручную экспортировать ключ (см. раздел "Работа с ключом для расшифровки подписи сообщений" на стр. 221) Транспортного сервера-концентратора и импортировать его на Пограничный транспортный сервер и наоборот.

Чтобы отправить объект из резервного хранилища на адреса электронной почты, указанные вручную, выполните следующие действия:

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Резервное хранилище**.
3. В рабочей области в таблице со списком объектов резервного хранилища выберите объект, который вы хотите отправить.
4. Нажмите на кнопку **Отправить,** расположенную в верхней части рабочей области над списком объектов, и выберите пункт меню **Отправить на другие адреса**.

   При нажатии на кнопку открывается окно **Отправка объекта резервного хранилища**.
5. В поле **Укажите адреса, на которые будет отправлен объект** введите адреса электронной почты получателей сообщения. Вы можете указать несколько адресов, разделяя их точкой с запятой.
6. При необходимости измените тему сообщения в поле **Тема сообщения**. Тема по умолчанию: `Объект отправлен из резервного хранилища Kaspersky Security`.
7. При необходимости измените текст в поле **Информация об объекте**. По умолчанию поле содержит информацию о свойствах объекта резервного хранилища (см. раздел "Просмотр свойств объектов в резервном хранилище" на стр. 180).
8. В нижней части окна ознакомьтесь с текстом предупреждения и установите флажок напротив него, если вы принимаете риск и хотите выполнить действие.
9. Нажмите **ОК**.

Программа отправит выбранный объект на указанные адреса.

Удаление объектов из резервного хранилища

Объекты, сохраненные в резервном хранилище, могут быть удалены автоматически и вручную.

Программа автоматически удаляет из резервного хранилища следующие объекты:

- наиболее "старый" объект, если размещение нового объекта приведет к превышению ограничения на максимально допустимое количество объектов в резервном хранилище (ограничение на количество объектов в резервном хранилище равно одному миллиону);
- наиболее "старый" объект, если в параметрах резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 186) установлено ограничение на размер резервного хранилища и при размещении нового объекта это ограничение будет превышено;

- объекты, срок хранения которых закончился, если параметрах резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 186) установлено ограничение на срок хранения объекта.

Вы также можете удалять объекты из резервного хранилища вручную. Вы можете удалять объекты выборочно или удалить все объекты, находящиеся в списке.

Удаление объектов вручную доступно только для пользователей, которым назначена роль "Администратор".

Удаление объектов из резервного хранилища выборочно

► *Чтобы удалить объекты из резервного хранилища выборочно, выполните следующие действия:*

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Резервное хранилище**.
3. В рабочей области в таблице со списком объектов резервного хранилища выберите объект или объекты, которые вы хотите удалить. Для поиска объектов можно использовать фильтр (см. раздел "Фильтрация списка объектов резервного хранилища" на стр. 181).
4. Нажмите на кнопку **Удалить** и выберите пункт **Удалить**.

   Откроется окно подтверждения.
5. В окне подтверждения нажмите на кнопку **Да**.

Программа удалит выбранные объекты из резервного хранилища.

Удаление из резервного хранилища объектов, находящихся в списке

Эта функция позволяет решить следующие задачи:

- Удалить из резервного хранилища объекты, соответствующие выбранным критериям (найденные с помощью фильтра).
- Очистить резервное хранилище, удалив из него все объекты (если фильтр не применен).

► *Чтобы удалить из резервного хранилища объекты, находящиеся в списке, выполните следующие действия:*

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Резервное хранилище**.
3. Если требуется, выполните поиск объектов, которые вы хотите удалить из резервного хранилища, с помощью фильтра (см. раздел "Фильтрация списка объектов резервного хранилища" на стр. 181).
4. Нажмите на кнопку **Удалить** и выберите пункт **Удалить все**.

   Откроется окно подтверждения.
5. В окне подтверждения нажмите на кнопку **Да**.

Если к резервному хранилищу применен фильтр, программа удалит из резервного хранилища объекты, соответствующие критериям фильтра. Если фильтр не применен, программа удалит из резервного хранилища все объекты.

Настройка параметров резервного хранилища

Резервное хранилище создается при установке Сервера безопасности. Для параметров резервного хранилища задаются значения по умолчанию, они могут быть изменены администратором.

► *Чтобы изменить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли управления выберите узел сервера Microsoft Exchange.
2. Выберите узел **Настройка**.
3. Если вы хотите ограничить размер резервного хранилища, выполните следующие действия:
   - в рабочей области в группе параметров **Хранение данных** установите флажок **Ограничить размер резервного хранилища**;
   - в поле ввода с прокруткой **Размер резервного хранилища не должен превышать** укажите максимальный размер резервного хранилища.

     По умолчанию максимальный размер резервного хранилища равен 5120 МБ.
4. Если вы хотите ограничить срок хранения объектов в резервном хранилище, выполните следующие действия:
   - в рабочей области в группе параметров **Хранение данных** установите флажок **Ограничить срок хранения объектов в резервном хранилище**;
   - в поле ввода с прокруткой **Хранить объекты не дольше** укажите нужное количество дней.

     По умолчанию срок хранения объектов в резервном хранилище составляет 45 дней.
5. Нажмите на кнопку **Сохранить**.

Если ни один флажок в группе параметров **Хранение данных** не установлен, действует только ограничение на общее количество объектов в резервном хранилище (не более одного миллиона объектов).

Независимо от конфигурации программы (одиночный сервер или группа DAG) параметры резервного хранилища требуется настраивать отдельно на каждом физическом сервере.

Выбор базы данных резервного хранилища для просмотра его содержимого из профиля

Данные об объектах резервного хранилища хранятся в базе данных SQL, указанной при установке программы (см. раздел "Шаг 5. Создание базы данных и настройка подключения программы к SQL-серверу" на стр. 30).

При добавлении нескольких Серверов безопасности в профиль в узле профиля по умолчанию отображается узел того резервного хранилища, имя SQL-сервера с базой данных которого идет первым по алфавиту в списке в формате <имя SQL-сервера>\<экземпляр>.

Вы можете выбрать в профиле базу данных SQL, в которой хранятся данные об объектах резервного хранилища, содержимое которого вы хотите просматривать.

► *Чтобы выбрать в профиле базу данных резервного хранилища для просмотра его содержимого, выполните следующие действия:*

1. В дереве Консоли управления раскройте узел **Профили**.
2. Раскройте узел профиля, содержащего Сервер безопасности, использующий нужную базу данных SQL.
3. Выберите узел **Резервное хранилище**.
4. Нажмите на кнопку **Выбрать**.

   Откроется окно **База данных**, которое содержит все базы данных SQL, используемые хотя бы одним Сервером безопасности профиля.
5. В окне **База данных** выберите Сервер безопасности, на котором расположена база данных SQL нужного резервного хранилища.
6. Нажмите на кнопку **ОК**.

В случае удаленного подключения к базе данных на SQL-сервере нужно убедиться, что на этом SQL-сервере включена поддержка TCP/IP в качестве клиентского протокола.

Окно Отправка объекта в "Лабораторию Касперского"

В этом окне вы можете отправить выбранный объект на исследование по поводу ложного срабатывания Анти-Спама.

Адрес электронной почты для обратной связи

Адрес электронной почты, по которому специалисты "Лаборатории Касперского" смогут связаться с вами для получения дополнительной информации об отправляемом объекте.

Информация об отправке объекта

Условия отправки объекта в "Лабораторию Касперского" и служебная информация Анти-Спама, необходимая для исследования случая ложного срабатывания Анти-Спама.

Я принимаю условия отправки объекта

Флажок, разрешающий отправку объекта на исследование по поводу ложного срабатывания Анти-Спама в "Лабораторию Касперского".

Если флажок установлен, вы принимаете условия отправки объекта.

Если флажок снят, вы не принимаете условия отправки объекта. Отправка объекта при этом невозможна.

По умолчанию флажок снят.

kaspersky

Отчеты

Kaspersky Security предоставляет возможность создавать и просматривать отчеты о работе модулей Антивирус и Анти-Спам. Для каждого модуля может быть создан отдельный отчет о его работе за период от одного дня.

Вы можете использовать следующие способы создания отчетов:

- Создавать отчеты вручную (см. раздел "Создание отчета вручную" на стр. 192).
- Создавать отчеты с помощью задач формирования отчетов (см. раздел "Создание задачи формирования отчетов" на стр. 193). Задачи формирования отчетов могут быть запущены вручную или автоматически по заданному расписанию. Вы можете создавать новые задачи формирования отчетов, удалять имеющиеся, изменять параметры уже созданных задач.

В программе предусмотрены стандартные и подробные отчеты, с уровнем детализации "Стандартный" и "Подробный", соответственно. Стандартные отчеты содержат информацию об объектах, обработанных за весь отчетный период, без указания временного интервала. В подробных отчетах указаны временные интервалы, по каждому из которых приводятся сведения об обработанных объектах.

Размер временных интервалов зависит от величины выбранного отчетного периода:

- если отчетный период равен одним суткам, временной интервал равен одному часу;
- если отчетный период составляет от двух до семи суток, минимальный временной интервал равен шести часам;
- если отчетный период составляет более восьми суток, минимальный временной интервал равен одним суткам.

В отчеты включаются статистические данные, полученные за время, когда соответствующие модули программы включены. Программа не получает статистические данные по модулям, находящимся в выключенном состоянии.

Вы можете просматривать отчеты в программе или получать их по электронной почте. Отчеты, отправляемые по электронной почте, прикрепляются к сообщению в виде вложения. Сообщение содержит следующий пояснительный текст: `Вложенный файл содержит отчет о работе Kaspersky Security 9.0 для Microsoft Exchange Servers`.

kaspersky

В этом разделе

Отчет о работе Антивируса для роли Почтовый ящик

Отчет о работе Антивируса для роли Почтовый ящик содержит результаты работы модуля Антивирус для роли Почтовый ящик за указанный отчетный период.

В верхней части отчета отображается следующая информация:

- **<Дата>**. Дата формирования отчета.
- **<Время>**. Время формирования отчета.
- **<Название отчета>**. "Стандартный отчет Антивируса для роли Почтовый ящик" или "Подробный отчет Антивируса для роли Почтовый ящик".
- **Имя сервера**. Имя Сервера безопасности, на котором был сформирован отчет.
- **Отчетный период**. Период, за который сформирован отчет.
- **Серверы, по которым был сформирован отчет**. Список Серверов безопасности, данные по которым вошли в отчет.

В таблице отчета отображаются результаты обработки (статусы) объектов в сообщениях электронной почты модулем Антивирус для роли Почтовый ящик. Таблица содержит информацию об объектах со следующими статусами:

- **Признано чистыми**. Проверенные объекты, в которых не найдено вредоносных программ.
- **Вылечено**. Зараженные объекты, которые удалось вылечить.
- **Обнаруженные проблемы**:
  - **Заражено**. Объекты, зараженные вирусом или другой программой, содержащей угрозу.
  - **Возможно заражено**. Объекты, которые могут быть заражены неизвестным вирусом или другой программой, содержащей угрозу.

  - **Защищено паролем**. Объекты, защищенные паролем, например, архивы с паролем.
- **Не проверено по причинам**:
  - **Проблем с лицензией**. Объекты, которые не были проверены из-за проблемы с лицензией.
  - **Ошибок баз Антивируса**. Объекты, которые не были проверены из-за ошибок, возникших по причине повреждения или отсутствия баз Антивируса.
  - **Ошибок обработки**. Объекты, при проверке которых произошла ошибка.
- **Всего**. Все объекты, поступившие на проверку.
- **Из них обнаружено службой KSN** (применимо для отчета с уровнем детализации "Стандартный"). Вредоносные объекты, обнаруженные с помощью служб (см. раздел "О Kaspersky Security Network" на стр. 98) Kaspersky Security Network или Kaspersky Private Security Network.

Отчет с уровнем детализации "Стандартный" отображает сведения о количестве, доле и размере объектов с перечисленными статусами, вычисленные за отчетный период:

- **Количество объектов**. Общее количество объектов с указанным статусом.
- **Процент от общего числа**. Доля объектов с указанным статусом среди всех объектов, поступивших на проверку.
- **Размер**. Суммарный размер объектов с указанным статусом.

В отчете с уровнем детализации "Подробный" отчетный период разбит на равные временные интервалы, за которые приводятся сведения о количестве объектов с перечисленными статусами. Размер временных интервалов зависит от величины выбранного отчетного периода (см. раздел "Отчеты" на стр. 188).

Отчет о работе Антивируса для роли Транспортный концентратор

Отчет о работе Антивируса для роли Транспортный концентратор содержит результаты работы модуля Антивирус для роли Транспортный концентратор за определенный отчетный период.

Отчет состоит из заголовка и таблицы.

В заголовке отчета отображаются следующие сведения:

- **<Дата>**. Дата формирования отчета.
- **<Время>**. Время формирования отчета.
- **<Название отчета>**. "Стандартный отчет Антивируса для роли Транспортный концентратор" или "Подробный отчет Антивируса для роли Транспортный концентратор".
- **Имя сервера**. Имя Сервера безопасности, на котором был сформирован отчет.
- **Отчетный период**. Период, за который сформирован отчет.
- **Серверы, по которым был сформирован отчет**. Список Серверов безопасности, данные по которым вошли в отчет.

В таблице отображаются результаты обработки (статусы) объектов в сообщениях электронной почты модулем Антивируса для роли Транспортный концентратор. Таблица содержит сведения об объектах со следующими статусами:

- **Признано чистыми**. Проверенные объекты, в которых не найдено вирусов или других программ, содержащих угрозу, и которые не попадают под действие условий фильтрации вложений и содержимого.

- **Вылечено**. Объекты, которые удалось вылечить.
- **Обнаруженные проблемы**:
  - **Заражено**. Объекты, зараженные вирусом или другой программой, содержащей угрозу.
  - **Возможно заражено**. Объекты, которые могут быть заражены неизвестным вирусом или другой программой, содержащей угрозу.
- **Отфильтровано вложений и содержимого**. Сообщения, в которых обнаружено содержимое или вложения, попадающие под действие условий фильтрации вложений и содержимого.
- **Не проверено по причинам**:
  - **Проблем с лицензией**. Объекты, которые не были проверены из-за проблемы с лицензией.
  - **Ошибок баз Антивируса**. Объекты, которые не были проверены из-за ошибок, возникших по причине повреждения или отсутствия баз Антивируса.
  - **Ошибок обработки**. Объекты, при проверке которых произошла ошибка.
- **Всего**. Все объекты, поступившие на проверку.
- **Из них обнаружено службой KSN** (применимо для отчета с уровнем детализации "Стандартный"). Вредоносные объекты, обнаруженные с помощью служб (см. раздел "О Kaspersky Security Network" на стр. 98) Kaspersky Security Network или Kaspersky Private Security Network.

Отчет с уровнем детализации "Стандартный" отображает сведения о количестве, доле и размере объектов с перечисленными статусами, вычисленные за отчетный период:

- **Количество объектов**. Общее количество объектов с указанным статусом.
- **Процент от общего числа**. Доля объектов с указанным статусом среди всех объектов, поступивших на проверку.
- **Размер**. Суммарный размер объектов с указанным статусом.

В отчете с уровнем детализации "Подробный" отчетный период разбит на равные временные интервалы, за которые приводятся сведения о количестве объектов с перечисленными статусами. Размер временных интервалов зависит от величины выбранного отчетного периода (см. раздел "Отчеты" на стр. 188).

Отчет о работе Анти-Спама

Отчет о работе Анти-Спама содержит результаты работы модуля Анти-Спам за определенный отчетный период.

Отчет состоит из заголовка и таблицы.

В заголовке отчета отображаются следующие сведения:

- **<Дата>**. Дата формирования отчета.
- **<Время>**. Время формирования отчета.
- **<Название отчета>**. "Стандартный отчет Анти-Спама" или "Подробный отчет Анти-Спама".
- **Имя сервера**. Имя Сервера безопасности, на котором был сформирован отчет.
- **Отчетный период**. Период, за который сформирован отчет.
- **Серверы, по которым был сформирован отчет**. Список Серверов безопасности, данные по которым вошли в отчет.

В таблице отображаются результаты обработки (статусы) сообщений электронной почты модулем Анти-Спам. Таблица содержит сведения о сообщениях со следующими статусами:

- **Чистые**. Сообщения, относящихся к следующим категориям:
  - Проверенные сообщения, не содержащие спам или фишинговые ссылки.
  - Сообщения, исключенные из проверки с помощью белых списков отправителей или получателей.
- **Доверенные**. Сообщения, поступившие через доверительные соединения (Trusted Connection) (см. раздел "Настройка дополнительных параметров проверки на спам и фишинг" на стр. 125).
- **Спам**. Сообщения, которые являются спамом.
- **Возможный спам**. Сообщения, которые, возможно (по результатам эвристического анализа), являются спамом.
- **Формальное оповещение**. Сервисные сообщения, такие как уведомления о доставке сообщения адресату.
- **Адрес в черном списке**. Сообщения от отправителей, адреса которых были внесены в черный список.
- **Фишинг**. Сообщения, которые содержат фишинговые ссылки.
- **Массовая рассылка**. Сообщения, которые являются результатом рассылок и не относятся к спаму.
- **Не проверено**. Сообщения, которые не были проверены Анти-Спамом.
- **Всего**. Все сообщения, поступившие на проверку.
- **Из них обнаружено службой KSN** (применимо для отчета с уровнем детализации "Стандартный"). Спам-сообщения и сообщения, содержащие фишинговые ссылки, обнаруженные с помощью служб (см. раздел "О Kaspersky Security Network" на стр. 98) Kaspersky Security Network или Kaspersky Private Security Network.

Отчет с уровнем детализации "Стандартный" отображает сведения о количестве, доле и размере сообщений с перечисленными статусами, вычисленные за отчетный период:

- **Количество сообщений**. Общее количество сообщений с указанным статусом.
- **Процент от общего числа**. Доля сообщений с указанным статусом среди всех сообщений, поступивших на проверку.
- **Размер**. Суммарный размер сообщений с указанным статусом.

В отчете с уровнем детализации "Подробный" отчетный период разбит на равные временные интервалы, за которые приводятся сведения о количестве и суммарном размере сообщений с перечисленными статусами. Размер временных интервалов зависит от величины выбранного отчетного периода (см. раздел "Отчеты" на стр. 188).

Создание отчета вручную

► *Чтобы создать отчет вручную, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите создать отчет для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;

- если вы хотите создать отчет для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите создать отчет.

2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Формирование и просмотр отчетов** нажмите на кнопку **Новый отчет**.
4. В открывшемся окне **Параметры формирования отчета** в раскрывающемся списке **Модуль** выберите модуль, о работе которого вы хотите создать отчет:
   - **Антивирус для роли Почтовый ящик**.
   - **Антивирус для роли Транспортный концентратор**.
   - **Анти-Спам**.
5. В раскрывающемся списке **Уровень детализации** выберите один из следующих уровней детализации отчета (см. раздел "Отчеты" на стр. 188):
   - **Стандартный**;
   - **Подробный**.
6. В полях **с** и **по** укажите даты начала и окончания отчетного периода вручную или выберите даты в календаре.
7. Если вы создаете отчет для Серверов безопасности одного профиля, в блоке параметров **Формировать отчет по статистике** выполните следующие действия:
   - Выберите вариант **Всех Серверов безопасности профиля**, если вы хотите создать отчет, содержащий информацию обо всех Серверах безопасности, входящих в профиль. В раскрывающемся списке справа выберите Сервер безопасности, на котором будет сформирован отчет.
   - Выберите вариант **Одного Сервера безопасности**, если вы хотите создать отчет, содержащий информацию об одном Сервере безопасности профиля. В раскрывающемся списке справа выберите Сервер безопасности, отчет о данных которого вы хотите создать.
8. Нажмите на кнопку **OK**, чтобы создать отчет на основании заданных параметров.

Программа откроет окно отчета в браузере сразу после формирования отчета и отобразит информацию об отчете в блоке **Формирование и просмотр отчетов**.

Создание задачи формирования отчетов

► *Чтобы создать задачу формирования отчетов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите создать задачу формирования отчетов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите создать задачу формирования отчетов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите создать задачу формирования отчетов.
2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Задачи формирования отчетов** нажмите на кнопку **Новая задача**.

4. В открывшемся окне **Параметры задачи** в поле **Имя** введите название создаваемой задачи. Это имя будет присваиваться отчетам, созданным с помощью этой задачи.
5. На закладке **Параметры формирования отчета** в раскрывающемся списке **Модуль** выберите выберите модуль, о работе которого будут формироваться отчеты при выполнении этой задачи:
   - **Антивирус для роли Почтовый ящик**.
   - **Антивирус для роли Транспортный концентратор**.
   - **Анти-Спам**.
6. В раскрывающемся списке **Уровень детализации** выберите один из следующих уровней детализации отчета (см. раздел "Отчеты" на стр. 188):
   - **Стандартный**;
   - **Подробный**.
7. Если вы хотите, чтобы программа отправляла сформированные отчеты по электронной почте, выполните следующие действия:
   a. Если вы хотите, чтобы программа отправляла сформированные отчеты на адрес электронной почты администратора, установите флажок **Отправить администратору**.
   b. Если вы хотите, чтобы программа отправляла сформированные отчеты на указанные вами адреса электронной почты, установите флажок **Отправить получателям**. В поле ввода укажите адреса электронной почты, на которые вы хотите отправлять отчеты.
   c. В узле **Уведомления** укажите параметры отправки уведомлений (см. раздел "Настройка общих параметров отправки уведомлений" на стр. 174): адрес веб-службы Exchange (EWS), учетную запись, от имени которой программа отправляет уведомления, и пароль для этой учетной записи, а также адреса администраторов (если вы установили флажок **Отправить администратору**). Программа использует эти параметры для отправки отчетов по электронной почте.
8. Если вы создаете отчет для Серверов безопасности одного профиля, в блоке параметров **Формировать отчет по статистике** выполните следующие действия:
   - Выберите вариант **Всех Серверов безопасности профиля**, если вы хотите формировать отчеты, содержащие информацию обо всех Серверах безопасности, входящих в профиль. В раскрывающемся списке справа выберите Сервер безопасности, на котором будет сформирован отчет.
   - Выберите вариант **Одного Сервера безопасности**, если вы хотите формировать отчеты, содержащие информацию об одном Сервере безопасности профиля. В раскрывающемся списке справа выберите Сервер безопасности, отчеты о данных которого вы хотите формировать.
9. На закладке **Расписание** установите флажок **Формировать отчет по расписанию**, если вы хотите, чтобы отчеты формировались согласно заданному расписанию.
10. Если вы установили флажок **Формировать отчет по расписанию**, выберите периодичность создания отчетов по расписанию:
    - **Каждые N дней**. В поле ввода **Каждые N дней** укажите периодичность в днях, с которой программа должна формировать отчеты. В поле ввода **Время запуска** укажите время формирования отчетов.
    - **Еженедельно**. В блоке **День запуска** выберите дни недели, в которые программа должна формировать отчеты. В поле ввода **Время запуска** укажите время формирования отчетов.
    - **Ежемесячно**. В поле ввода **День месяца** укажите день месяца, в который программа должна формировать отчеты. В поле ввода **Время запуска** укажите время формирования отчетов.

11. Нажмите на кнопку **OK**.

Программа отобразит созданную задачу формирования отчетов в блоке **Задачи формирования отчетов**. Отчеты будут формироваться по указанному в задаче расписанию. Вы также можете запустить задачу вручную (см. раздел "Запуск задачи формирования отчетов" на стр. 196).

Просмотр списка задач формирования отчетов

► *Чтобы просмотреть список задач формирования отчетов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите просмотреть задачи формирования отчетов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите просмотреть задачи формирования отчетов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, задачи формирования отчетов для Серверов безопасности которого вы хотите просмотреть.
2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Задачи формирования отчетов** в таблице отображаются все созданные задачи. Для каждой задачи отображается следующая информация:
   - **Имя задачи**. Имя созданной задачи формирования отчетов.
   - **Модуль**. Модуль, о работе которого формируется отчет при выполнении этой задачи: Анти-Спам, Антивирус для роли Почтовый ящик или Антивирус для роли Транспортный концентратор.
   - **Уровень детализации**. Уровень детализации формируемых отчетов: "Подробный" или "Стандартный".
   - **Область действия**. Профиль или Сервер безопасности, данные которых отображаются в формируемых отчетах.
   - **Расписание**. Заданное расписание формирования отчетов.
   - **Время последнего изменения**. Дата и время последнего изменения задачи формирования отчетов.
   - **Следующий запуск**. Дата и время следующего запуска задачи формирования отчетов по расписанию.
   - **Автоматический запуск**. Информация о том, задан ли запуск задачи на выполнение по расписанию.
   - **Сервер формирования отчета**. Сервер безопасности, на котором формируются отчеты.

Изменение параметров задачи формирования отчетов

► *Чтобы изменить параметры задачи формирования отчетов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите изменить параметры задачи формирования отчетов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;

- если вы хотите изменить параметры задачи формирования отчетов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, параметры задачи формирования отчетов для Серверов безопасности которого вы хотите изменить.

2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Задачи формирования отчетов** в таблице задач выберите задачу, параметры которой вы хотите изменить.
4. Нажмите на кнопку **Изменить** над таблицей задач.
5. В открывшемся окне **Параметры задачи** измените нужные параметры (см. раздел "Создание задачи формирования отчетов" на стр. 193).
6. Нажмите на кнопку **ОК**.

Запуск задачи формирования отчетов

► *Чтобы запустить задачу формирования отчетов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите запустить задачу формирования отчетов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите запустить задачу формирования отчетов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, задачу формирования отчетов для Серверов безопасности которого вы хотите запустить.
2. Выберите узел **Отчеты**.
3. В блоке **Задачи формирования отчетов** в таблице задач выберите задачу, которую вы хотите запустить.
4. Нажмите на кнопку **Запустить**.

Программа откроет окно отчета в браузере сразу после завершения формирования отчета и отобразит информацию об отчете в блоке **Задачи формирования отчетов**.

Удаление задачи формирования отчетов

► *Чтобы удалить задачу формирования отчетов, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите удалить задачу формирования отчетов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите удалить задачу формирования отчетов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, задачу формирования отчетов для Серверов безопасности которого вы хотите удалить.
2. Выберите узел **Отчеты**.
3. В блоке **Задачи формирования отчетов** в таблице задач выберите задачу, которую вы хотите удалить.
4. Нажмите на кнопку **Удалить** над таблицей задач.

Откроется окно подтверждения.

5. В окне подтверждения нажмите на кнопку **Да**.

Выбранная задача будет удалена из таблицы задач в блоке **Задачи формирования отчетов**.

Просмотр отчета

Сформированные отчеты хранятся в списке отчетов и доступны для просмотра.

► *Чтобы просмотреть отчет, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите просмотреть отчет для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите просмотреть отчет для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, отчеты для Серверов безопасности которого вы хотите просмотреть.
2. Выберите узел **Отчеты**.
3. В рабочей области в блоке **Формирование и просмотр отчетов** в таблице отображаются все созданные отчеты. Для каждого отчета отображается следующая информация:
   - **Имя**. Имя отчета. Если отчет создан вручную, то название отчета: "Отчет <модуль, о работе которого сформирован отчет>", если отчет создан с помощью задачи формирования отчета, название отчета аналогично названию задачи.
   - **Создан**. Дата и время создания отчета.

     В этом столбце отображается время, установленное в региональных параметрах компьютера, на котором запущена Консоль управления.

   - **Период**. Период времени, за который отображаются данные в отчете.
   - **Источник данных**. Имя Сервера безопасности, профиля или группы DAG (только для отчета для Антивируса для роли Почтовый ящик), данные которых отображаются в отчете.
   - **Модуль**. Модуль, о работе которого сформирован отчет: Анти-Спам, Антивирус для роли Почтовый ящик или Антивирус для роли Транспортный концентратор.
   - **Уровень детализации**. Уровень детализации отчета: "Подробный" или "Стандартный".
   - **Сервер формирования отчета**. Сервер безопасности, на котором сформирован отчет.
4. Для просмотра отчета выберите его в списке и нажмите на кнопку **Просмотреть**.

Выбранный отчет откроется в окне браузера, установленного по умолчанию.

См. также

Сохранение отчета на диск

Вы можете сохранять готовые отчеты на диск вашего компьютера и просматривать их без Консоли управления. Отчеты сохраняются на диске в файлах формата HTML.

► *Чтобы сохранить отчет на диск, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите сохранить отчет для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите сохранить отчет для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, отчет для Серверов безопасности которого вы хотите сохранить.
2. Выберите узел **Отчеты**.
3. В блоке **Формирование и просмотр отчетов** в таблице отчетов выберите отчет, который вы хотите сохранить, и нажмите на кнопку **Сохранить**.
4. В открывшемся окне **Сохранить как** укажите папку, в которую вы хотите сохранить отчет и, если требуется, введите или измените имя отчета.
5. Нажмите на кнопку **Сохранить**.

Удаление отчета

Вы можете удалять ненужные отчеты из списка отчетов. Вы можете удалять отчеты по одному или удалить сразу несколько отчетов.

Удаленные отчеты невозможно восстановить.

► *Чтобы удалить отчет, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите удалить отчет для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите удалить отчет для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, отчет для Серверов безопасности которого вы хотите удалить.

2. Выберите узел **Отчеты**.
3. В блоке **Формирование и просмотр отчетов** в таблице отчетов выберите отчет, который вы хотите удалить, и нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.
4. В окне подтверждения нажмите на кнопку **Да**.

Выбранный отчет будет удален из таблицы отчетов.

Журналы программы

Kaspersky Security записывает информацию о своей работе (например, сообщения об ошибках программы или предупреждения) в журнал событий Windows и в журналы событий Kaspersky Security.

О журнале событий Windows

В журнал событий Windows записывается информация о работе Kaspersky Security, на основании которой администратор Kaspersky Security или специалист по информационной безопасности могут контролировать работу программы.

События, связанные с работой Kaspersky Security, регистрируются в журнале событий Windows от имени источника KSE и отображаются в **Журналах приложений и служб** в разделе **Kaspersky Security для Exchange Servers**. Базовые события, связанные с работой программы, имеют фиксированные коды событий (см. раздел "События Kaspersky Security в журнале событий Windows" на стр. 200). Вы можете использовать код события для поиска и фильтрации событий в журнале.

О журналах событий Kaspersky Security

Журналы событий Kaspersky Security представляют собой файлы формата TXT, которые хранятся локально в папке `<Папка установки программы>\logs`. Вы можете задать для хранения журналов другую папку (см. раздел "Настройка параметров журналов программы" на стр. 217).

Подробность ведения журналов событий программы зависит от установленных параметров детализации журналов (см. раздел "Настройка детализации журналов программы" на стр. 218).

Kaspersky Security ведет журналы событий по следующему алгоритму:

- Программа записывает информацию в конец самого нового журнала.
- Когда размер журнала достигает 100 МБ, программа архивирует его и создает новый журнал.
- По умолчанию программа хранит файлы журналов в течение 14 дней с момента внесения последнего изменения в журнал, а затем удаляет их. Вы можете установить другой срок хранения журналов (см. раздел "Настройка параметров журналов программы" на стр. 217).

Для каждого Сервера безопасности создаются отдельные журналы независимо от варианта развертывания программы.

В папке с журналами программы и в папке с данными программы (`<Папка установки программы>\data`) могут содержаться конфиденциальные данные. Программа не обеспечивает защиту от несанкционированного доступа к данным в этих папках. Вам необходимо предпринять собственные меры по защите данных в этих папках от несанкционированного доступа.

kaspersky

В этом разделе

События Kaspersky Security в журнале событий Windows

В этом разделе собрана информация о базовых событиях в работе программы, которые записываются в журнал событий Windows. События, связанные с работой Kaspersky Security, регистрируются в журнале событий Windows от имени источника KSE. Такие события имеют фиксированный *код события*. События в таблице отсортированы по возрастанию кода события.

Таблица 10. Базовые события в работе программы

Код события	Уровень важности события	Описание
1000	Ошибка	Событие записывается, если программа обнаруживает, что базы Антивируса устарели более чем на сутки. В записи о событии указывается тип баз и дата выпуска баз.
	Предупреждение	Событие записывается, если программа обнаруживает, что базы Анти-Спама устарели более чем на пять часов. В записи о событии указывается тип баз и дата выпуска баз.
1001	Сведения	Событие записывается, если программа обнаруживает зараженный или защищенный объект, либо файл вложения, который соответствует критериям фильтрации вложений, а также в рабочей области узла **Уведомления** установлен флажок **Записывать события в журнал Windows** для соответствующих типов уведомлений.
1004	Предупреждение	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления**, настроен параметр **Уведомить заранее об истечении срока действия лицензии (дни)** и срок действия лицензии скоро истечет. В записи о событии указывается ключ, дата окончания срока действия лицензии и количество дней, оставшихся до окончания этого срока.
1005	Ошибка	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и срок действия лицензии истек. В записи о событии указывается ключ и дата окончания срока действия лицензии.
1007	Ошибка	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и активный ключ не обнаружен.

Код события	Уровень важности события	Описание
1008	Сведения	Событие записывается, если базы программы были обновлены до последней версии. В записи о событии указывается тип баз и дата выпуска баз.
1009	Ошибка	Событие записывается, если программа зафиксировала ошибки в работе компонента. В записи о событии указывается название компонента и описание ошибки.
	Предупреждение	Событие записывается, если программа зафиксировала выключение компонента. В записи о событии указывается название компонента.
	Сведения	Событие записывается, если программа зафиксировала включение компонента. В записи о событии указывается название компонента.
1010	Ошибка	Событие записывается, если произошла ошибка на SQL-сервере и база данных перестала быть доступна. В записи о событии указывается имя базы данных, имя SQL-сервера и описание ошибки.
	Сведения	Событие записывается, если доступ к базе данных на SQL-сервере восстановлен и ошибки в работе устранены. В записи о событии указывается имя базы данных и имя SQL-сервера.
1011	Сведения	Событие записывается, если пользователь запросил запуск фоновой проверки. В записи о событии указывается учетная запись пользователя.
1012	Сведения	Событие записывается, если пользователь запросил остановку фоновой проверки. В записи о событии указывается учетная запись пользователя.

Код события	Уровень важности события	Описание
1013	Сведения	Событие записывается, если фоновая проверка была запущена вручную или автоматически по расписанию. В записи о событии указывается тип запуска.
1014	Сведения	Событие записывается, если фоновая проверка была остановлена. В записи о событии указывается причина остановки проверки.
1015	Предупреждение	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и программе не удалось обновить статус лицензии. В записи о событии указывается ключ, дата окончания срока действия лицензии и количество дней, оставшихся до перехода в режим ограниченной функциональности.
1016	Ошибка	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления**, программе не удалось обновить статус лицензии и срок обновления лицензии истек. В записи о событии указывается описание причины возникновения ошибки.
1025	Сведения	Событие записывается, если в узле **Уведомления** для события **Спам и фишинг** в блоке **Параметры уведомлений** установлен флажок **Спам** и программа обнаружила сообщение, содержащее спам или возможный спам. В записи о событии указывается информация о сообщении.
1026	Сведения	Событие записывается, если в узле **Уведомления** для события **Спам и фишинг** в блоке **Параметры уведомлений** установлен флажок **Массовая рассылка** и программа обнаружила сообщение, содержащее массовую рассылку. В записи о событии указывается информация о сообщении.
1027	Сведения	Событие записывается, если в узле **Уведомления** для события **Спам и фишинг** в блоке **Параметры уведомлений** установлен флажок **Фишинг** и программа обнаружила сообщение, содержащее фишинговую ссылку. В записи о событии указывается информация о сообщении.
1028	Сведения	Событие записывается, если в узле **Уведомления** для события **Фильтрация однотипных сообщений** в блоке **Параметры уведомлений** установлен флажок **Записывать события в журнал Windows** и программа обнаружила превышение ограничения по количеству сообщений, отправленных с внутреннего адреса электронной почты. В записи о событии указывается информация о последнем отфильтрованном сообщении.
11010	Сведения	Событие записывается, если Консоль управления была запущена. В записи о событии указывается учетная запись пользователя, запустившего Консоль управления.
11011	Сведения	Событие записывается, если Консоль управления была закрыта. В записи о событии указывается учетная запись пользователя, закрывшего Консоль управления.

Код события	Уровень важности события	Описание
11020	Ошибка	Событие записывается, если компонент программы перешел в режим ограниченной проверки. В записи о событии указывается название компонента и время его перехода в режим ограниченной проверки (см. раздел "О предотвращении задержки сообщений модулем Антивирус" на стр. 116).
11100	Предупреждение	Событие записывается, если использование KSN ограничено. В записи о событии указывается об использовании KSN в ограниченном режиме.
11103	Сведения	Событие записывается, если использование KSN не ограничено. В записи о событии указывается об использовании KSN без ограничений.
11106	Предупреждение	Событие записывается, если регион работы KSN был изменен. В записи о событии указываются наименования предыдущего и текущего регионов работы KSN.
2055	Ошибка	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и при автоматическом обновлении статуса лицензии возникла ошибка. В записи о событии указывается описание причины возникновения ошибки.
30000	Сведения	Событие записывается, если параметры программы были изменены. В записи о событии указывается учетная запись пользователя, изменившего параметры, область изменений (например, Anti-Spam), значение измененного параметра.
31000	Сведения	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и статус ключа, дата окончания срока действия лицензии, количество пользователей или тип лицензии изменились. В записи о событии указывается ключ, тип лицензии, дата окончания срока действия лицензии и количество пользователей лицензии.
31022	Сведения	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и пользователь выполнил действия с ключом Сервера безопасности. В записи о событии указывается учетная запись пользователя.
42404	Сведения	Событие записывается, если удален объект из резервного хранилища. В записи о событии указывается подробная информация об объекте и учетная запись пользователя, если объект был удален пользователем. Программа удаляет объект в соответствии с настройками параметров резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 186).
42405	Сведения	Событие записывается, если пользователь отправил возможно зараженный объект из резервного хранилища на исследование в "Лабораторию Касперского". В записи о событии указывается учетная запись пользователя и подробная информация об объекте.

Код события	Уровень важности события	Описание
42406	Сведения	Событие записывается, если пользователь отправил объект из резервного хранилища исходным получателям. В записи о событии указывается учетная запись пользователя и подробная информация об объекте.
42421	Сведения	Событие записывается, если пользователь отправил объект, ложно идентифицированный программой как спам, из резервного хранилища на исследование в "Лабораторию Касперского". В записи о событии указывается учетная запись пользователя и подробная информация об объекте.
42422	Сведения	Событие записывается, если пользователь сохранил на диск объект из резервного хранилища. В записи о событии указывается учетная запись пользователя и подробная информация об объекте.
42423	Сведения	Событие записывается, если пользователь отправил объект из резервного хранилища на адреса электронной почты, указанные вручную. В записи о событии указывается учетная запись пользователя и подробная информация об объекте.
42706	Ошибка	Событие записывается, если базы программы не удалось обновить. В записи о событии указывается тип баз и описание ошибки.
42707	Сведения	Событие записывается, если ошибка обновления баз программы устранена и базы обновлены успешно. В записи о событии указывается тип баз и дата выпуска баз.
48808	Сведения	Событие записывается, если программа обнаружила исходящее сообщение электронной почты, содержащее спам или фишинг. В записи о событии содержатся сведения о сообщении.

Настройка параметров журналов программы

► *Чтобы настроить параметры журналов программы, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить параметры журналов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить параметры журналов для Серверов безопасности одного профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить параметры журналов.
2. Выберите узел **Настройка**.
3. Раскройте блок параметров **Диагностика** и выполните следующие действия:
   a. В поле **Папка с журналами** укажите путь к папке, предназначенной для хранения журналов. По ссылке **По умолчанию** вы можете вернуть путь, установленный по умолчанию (`<Папка установки программы>\logs`).

      В строке не допускается использование системных переменных, таких как %TEMP%.

      Не рекомендуется использовать в качестве папки с журналами сетевые папки. Их работоспособность не поддерживается программой.

Вы можете указать путь к папке хранения журналов отдельно для каждого Сервера безопасности. Этот параметр нельзя задать для профиля.

Если вы укажете другую папку хранения журналов, программа начинает создавать файлы журналов в новой папке. При этом старые файлы журналов остаются в прежней папке хранения журналов. Если новая папка хранения журналов не существует, она будет создана. Если доступ к новой папке отсутствует (например, из-за отсутствия прав), программа записывает журналы в папку, установленную по умолчанию, до тех пор, пока доступ к новой папке не будет обеспечен. Переход к использованию новой папки хранения журналов выполняется в течение 30 минут после предоставления доступа к папке.

b. В поле ввода с прокруткой **Срок хранения журналов** укажите временной интервал, в течение которого журналы хранятся в папке после создания. По истечении этого времени программа удаляет журналы.

   Значение по умолчанию – 14 дней.

c. Настройте уровень детализации (см. раздел "Настройка детализации журналов программы" на стр. 205). Уровень детализации определяет степень подробности ведения журналов.

4. Нажмите на кнопку **Сохранить**.

Программа начнет записывать события в журналы в соответствии с установленными параметрами.

Если программа работает на сервере Microsoft Exchange в составе группы DAG, параметры журналов, настроенные на одном из серверов Microsoft Exchange, автоматически распространяются на остальные серверы Microsoft Exchange, входящие в эту группу DAG. На остальных серверах Microsoft Exchange в составе этой группы DAG настраивать параметры журналов не требуется.

Настройка детализации журналов программы

► *Чтобы настроить детализацию журналов программы, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - если вы хотите настроить уровень детализации журналов для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности;
   - если вы хотите настроить уровень детализации журналов для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел профиля, для Серверов безопасности которого вы хотите настроить уровень детализации журналов.
2. Выберите узел **Настройка**.
3. Раскройте блок параметров **Диагностика**.
4. Нажмите на кнопку **Настройка** в блоке параметров **Детализация журналов.**

   Откроется окно **Параметры диагностики**.
5. Установите флажки напротив тех событий, информацию о которых программа должна записывать в журнал.
6. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно.

Если вы выбрали несколько событий в окне, то уровень детализации изменится на **Пользовательский**. Программа будет записывать основные события в работе программы, а также подробную информацию для указанных вами событий.

Если вы выбрали все события в окне, то уровень детализации изменится на **Максимальный**. Программа будет записывать в журналы подробную информацию о всех событиях.

Ведение подробных журналов программы может замедлять работу программы.
В подробные журналы могут быть записаны конфиденциальные данные из содержимого сообщений и сетевых запросов.

7. Если необходимо сбросить настроенную детализацию журнала, нажмите на кнопку **Сбросить**.

   Программа изменит уровень детализации на **Минимальный**. В журналы будут записываться только основные события в работе программы: результат проверки объектов, результат загрузки обновлений баз и результат добавления ключа.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить сделанные изменения.

Если программа работает на сервере Microsoft Exchange в составе группы DAG, уровень детализации, настроенный на одном из серверов Microsoft Exchange, автоматически распространяется на остальные серверы Microsoft Exchange, входящие в эту группу DAG. На остальных серверах Microsoft Exchange в составе этой группы DAG настраивать уровень детализации не требуется.

Журнал событий аудита

Этот раздел содержит информацию о журнале событий аудита в работе программы, а также инструкции по включению записи и просмотру событий, записанных в этот журнал.

В этом разделе

О журнале событий аудита

Kaspersky Security позволяет вести запись событий аудита, связанных с управлением и работой программы. Журнал событий аудита хранится на локальном компьютере в формате CSV.

Информацию о событиях, сохраненных в журнале событий аудита, вы можете просмотреть с помощью оболочки Windows PowerShell (см. раздел «Просмотр событий системного аудита» на стр. 209). Программа сохраняет в журнал событий аудита информацию о следующих событиях в работе программы:

Таблица 11. События, сохраняемые в журнале системного аудита

Событие	Информация о событии
Запуск и остановка сервиса Kaspersky Security for Microsoft Exchange Servers	Дата и время события (UTC). Тип события (запуск или остановка). Результат события (успешно или не успешно). Полное доменное имя сервера.
Включение и выключение антивирусной защиты	Дата и время события (UTC). Тип события (включение или выключение). Результат события (успешно или не успешно). Имя сервера или фермы серверов. Имя пользователя, инициировавшего событие.
Изменение параметров антивирусной защиты	Дата и время события (UTC). Измененные параметры настройки. Результат события (успешно или не успешно). Имя сервера или фермы серверов. Имя пользователя, инициировавшего событие.
Обновление антивирусных баз	Дата и время события (UTC). Имя сервера или фермы серверов. Результат события (успешно или не успешно). Дата и время выпуска антивирусных баз. Имя пользователя, инициировавшего событие. При автоматическом запуске обновления в журнал записывается название службы.
Создание и удаление задачи проверки по требованию	Дата и время события (UTC). Тип события (создание или удаление). Результат события (успешно или не успешно). Название задачи проверки по требованию. Имя пользователя, инициировавшего событие.
Запуск и остановка задачи проверки по требованию	Дата и время события (UTC). Тип события (запуск или остановка). Результат события (успешно или не успешно). Имя сервера или фермы серверов. Имя пользователя, инициировавшего событие. При автоматическом запуске задачи в журнал записывается название службы.

Событие	Информация о событии
Изменение параметров задачи проверки по требованию	Дата и время события (UTC). Измененные параметры настройки. Результат события (успешно или не успешно). Название задачи проверки по требованию. Имя пользователя, инициировавшего событие.
Обнаружение вредоносного файла	Дата и время события (UTC). Тип обнаруженного файла (зараженный, поврежденный или защищенный паролем). Имя файла. Версия файла. Полный путь к файлу. Действие программы с файлом. Режим проверки (проверка при обращении или проверка по требованию). Параметры проверки. Пользователь, инициировавший событие.

Включение и выключение ведения журнала событий аудита

Чтобы включить ведение журнала событий аудита, выполните следующие действия:

1. Запустите Windows PowerShell от имени администратора.

   Запуск Windows PowerShell необходимо выполнять на сервере Exchange, на котором установлены Сервер безопасности и Консоль управления.

2. В среде PowerShell выполните команду `Import-Module '<полный путь к папке установки программы>\Enterprise.Automation.dll'`.

   Библиотека Enterprise.Automation подключится и будет доступна для использования. Если библиотека была подключена ранее, пропустите этот шаг.

3. Выполните команду `Enable-Audit`.

Запись событий в журнал будет включена. Программа будет сохранять в журнал событий аудита информацию о событиях в работе программы.

Чтобы выключить ведение журнала событий аудита, выполните следующие действия:

1. Запустите Windows PowerShell от имени администратора.
2. В среде PowerShell выполните команду `Enable-Audit -Disable`.

Запись событий в журнал будет выключена.

Если установлен пароль для работы в Консоли управления, программа будет запрашивать его при выполнении каждой команды.

Чтобы установить пароль, выполните следующие действия:

1. Запустите Windows PowerShell от имени администратора.

   Запуск Windows PowerShell необходимо выполнять на компьютере, на который установлена Консоль управления.

2. В среде Windows PowerShell выполните команду `Import-Module '<полный путь к папке установки программы>\Enterprise.Automation.dll'`.

   Библиотека Enterprise.Automation подключится и будет доступна для использования.

3. Выполните команду `Set-Password`.

4. Введите пароль и подтвердите его.

   Пароль будет установлен. Программа будет запрашивать пароль при запуске Консоли управления, а также при управлении Kaspersky Security с помощью команд в среде Windows PowerShell.

Чтобы снять пароль, выполните следующие действия:

1. Выполните команду `Reset-Password`.

2. Введите текущий пароль, чтобы подтвердить выполнение команды.

   Пароль будет снят. Программа не будет запрашивать пароль при запуске Консоли управления и при управлении Kaspersky Security с помощью команд в среде Windows PowerShell. В Дереве Консоли управления не будет отображаться узел **Авторизация**.

Просмотр событий системного аудита

Чтобы просмотреть события системного аудита, выполните следующие действия:

1. Запустите Windows PowerShell от имени администратора.
2. В среде PowerShell выполните команду `Import-Module '<полный путь к папке установки программы>\Enterprise.Automation.dll`.

   Библиотека Enterprise.Automation подключится и будет доступна для использования. Если библиотека была подключена ранее, пропустите этот шаг.

3. Выполните команду `Get-Log`.

   В среде PowerShell отобразится список всех событий, сохраненных в журнале системного аудита.

   Вы можете работать со списком событий с помощью следующих параметров команды `Get-Log`.

Filter.

Этот параметр позволяет находить события, записи о которых содержат заданный текст. Например, `Get-Log -Filter "удален"`. При выполнении этой команды в среде PowerShell отобразятся события, в записях которых содержится слово «удален», например, события, связанные с удалением объекта во время антивирусной проверки.

Sorting.

Этот параметр позволяет сортировать события по времени их возникновения. Например, `Get-Log -Sorting descending`. В среде PowerShell отобразятся события, начиная с последнего сохраненного события. По умолчанию события отображаются, начиная с первого сохраненного события.

Format-Table.

Параметр Format-Table позволяет отображать события, сохраненные в журнале системного аудита, в среде PowerShell в виде таблицы. Например, `Get-Log | ft`.

Вы можете использовать несколько параметров в одной команде. Например, `Get-Log -Sorting descending -Filter "запуск" | ft`.

Если установлен пароль для работы в Консоли управления, программа будет запрашивать его при выполнении каждой команды.

Сохранение информации из журнала событий аудита в текстовый файл

Чтобы сохранить информацию из журнала событий аудита в текстовый файл, выполните следующие действия:

1. Запустите Windows PowerShell от имени администратора.

Выполните команду `Get-Log > <путь к файлу><имя файла>.txt`.

Программа запросит пароль доступа. Если пароль доступа не установлен, выполнение команды будет прекращено.

Введите пароль.

Программа создаст по указанному пути файл и сохранит в него информацию из журнала событий аудита событий.

kaspersky

Работа с Kaspersky Security в среде Windows PowerShell

В этом разделе содержится информация и инструкции по выполнению команд в среде Windows PowerShell для просмотра состояния защиты серверов Microsoft Exchange и статистических данных о работе модулей программы.

В этом разделе

О командах Windows PowerShell

С помощью команд, выполняемых в среде PowerShell, вы можете получать информацию о работе программы без запуска Консоли управления.

В комплект поставки программы входит библиотека Kse.Powershell, содержащая команды Windows PowerShell, которые позволяют выполнять следующие действия:

- просмотреть состояние защиты сервера Microsoft Exchange;
- просмотреть статистику работы модулей Антивируса и фильтрации вложений и содержимого;
- просмотреть статистику работы модуля Анти-Спама;
- просмотреть белый и черный списки адресов Анти-Спама;
- добавлять адреса в белый и черный списки адресов Анти-Спама;
- удалять адреса из белого и черного списков адресов Анти-Спама;
- синхронизировать белые или черные списки адресов Анти-Спама.

Вы можете выполнять команды Windows PowerShell с любого компьютера организации, на котором установлена Консоль управления Kaspersky Security.

Для выполнения команд необходимо наличие установленной среды Windows PowerShell версии 4.0.

Подключение библиотеки Kse.Powershell

► *Чтобы подключить библиотеку Kse.Powershell, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator).
2. В среде Windows PowerShell выполните команду:

   ```
   Import-Module '<полный путь к папке установки программы>\Kse.Powershell.dll'
   ```

Библиотека Kse.Powershell подключится и будет доступна для использования.

Просмотр состояни защиты сервера Microsoft Exchange

Просматривать состояние защиты сервера Microsoft Exchange в среде Windows PowerShell могут пользователи, обладающие одной из следующих ролей (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58):

- Администратор;
- Специалист по антивирусной безопасности;
- Оператор антивирусной безопасности.

► *Чтобы просмотреть состояние защиты сервера Microsoft Exchange, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEServerStatus -ServerFqdn <имя сервера>
   ```

   где <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес.

В среде Windows PowerShell отобразится следующая информация:

- ServerFqdn – имя защищаемого сервера Microsoft Exchange.
- LicenseStatus – статус ключа Сервера безопасности:
  - *Valid* – действующая лицензия. Функциональность Антивируса и Анти-Спама не ограничена.
  - *Expired* – срок действия лицензии истек. Обновление баз Антивируса и баз Анти-Спама запрещено, недоступно использование Kaspersky Security Network.

  - *NoLicenseKey* – ключ отсутствует. Недоступна функциональность модулей Антивирус и Анти-Спам, обновление баз Антивируса и баз Анти-Спама запрещено.
  - *InconsistentUpdate* – базы программы недоступны или повреждены.
  - *BlackListed* – ключ заблокирован. Доступно только обновление баз Антивируса и баз Анти-Спама. Недоступна функциональность модулей Антивирус и Анти-Спам.
- LicenseExpirationDate – дата окончания срока действия лицензии Сервера безопасности (если ключ Сервера безопасности отсутствует, отображается значение DateTime.MinValue, равное 1/1/0001 12:00:00 AM).
- TransportAntivirusStatus – статус модуля Антивирус для роли Транспортный концентратор:
  - *Running* – модуль включен.
  - *WorksWithErrors* – модуль работает с ошибками.
  - *TurnedOff* – модуль выключен.
  - *NotInstalled* – модуль не установлен.
  - *ImpossibleToInstall* – модуль не может быть установлен в данной конфигурации сервера Microsoft Exchange.
- MailboxAntivirusStatus – статус модуля Антивирус для роли Почтовый ящик (*Running*, *WorksWithErrors*, *TurnedOff*, *NotInstalled*, *ImpossibleToInstall*). Значения параметра те же, что и для TransportAntivirusStatus.
- AntispamStatus – статус модуля Анти-Спам (*Running*, *WorksWithErrors*, *TurnedOff*, *NotInstalled*, *ImpossibleToInstall*). Значения параметра те же, что и для TransportAntivirusStatus.
- AttachmentFilteringStatus – статус модуля фильтрации вложений и содержимого (*Running*, *WorksWithErrors*, *TurnedOff*, *NotInstalled*, *ImpossibleToInstall*). Значения параметра те же, что и для TransportAntivirusStatus.
- SqlServerStatus – статус соединения с SQL-сервером:
  - *Running* – SQL-сервер доступен.
  - *TurnedOff* – SQL-сервер недоступен.
  - *WorksWithErrors* – SQL-сервер работает с ошибками.
- AntivirusBasesCumulativeStatus – состояние баз Антивируса:
  - *UpToDate* – базы Антивируса находятся в актуальном состоянии.
  - *Outdated* – базы Антивируса устарели.
  - *Error* – при обновлении баз Антивируса произошла ошибка.
  - *NotAvailable* – базы Антивируса недоступны.
- AntivirusBasesIssueDateUtc – дата и время (UTC) выпуска используемой версии баз Антивируса.
- AntispamBasesCumulativeStatus – состояние баз Анти-Спама (*UpToDate*, *Outdated*, *Error*, *NotAvailable*). Значения параметра те же, что и для AntivirusBasesCumulativeStatus.
- AntispamBasesIssueDateUtc – дата и время (UTC) выпуска используемой версии баз Анти-Спама.

Если служба программы Kaspersky Security for Microsoft Exchange Servers (KSCM8) не запущена, команда Get-KSEServerStatus возвращает исключение System.ServiceModel.EndpointNotFoundException.

Просмотр статистики работы модулей Антивируса и фильтрации вложений и содержимого

Просматривать статистику работы модулей Антивируса и фильтрации вложений и содержимого в среде Windows PowerShell могут пользователи, обладающие одной из следующих ролей (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58):

- Администратор;
- Специалист по антивирусной безопасности;
- Оператор антивирусной безопасности.

► *Чтобы просмотреть статистику работы модулей Антивируса и фильтрации вложений и содержимого, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEAVServerStatistics -ServerFqdn <имя сервера> -From <начало периода> -To <конец периода> -AntivirusRole <роль>
   ```

   где:

   - <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес.
   - <начало периода> – дата начала периода, за который вы хотите просмотреть статистику.
   - <конец периода> – дата окончания периода, за который вы хотите просмотреть статистику.
   - <роль> – роль, в которой развернута программа. Возможны следующие значения:
     - Mailbox – Антивирус для роли Почтовый ящик;
     - Transport – Антивирус для роли Транспортный концентратор.

   В среде Windows PowerShell отобразится следующая информация:

   - TotalCheckedObjects – общее количество сообщений, проверенных модулем за указанный период;
   - CleanObjects – количество незараженных сообщений;
   - InfectedObjects – количество зараженных сообщений;
   - DisinfectedObjects – количество вылеченных сообщений;
   - PasswordProtectedObjects – количество сообщений с файлами, защищенными паролем (параметр применим для роли Mailbox);
   - SuspiciousObjects – количество возможно зараженных сообщений;
   - AttachmentFilteredObjects – количество сообщений, попадающих под действие критериев фильтрации вложений и содержимого (параметр применим для роли Transport, для роли Mailbox значение всегда равно 0);
   - SkippedByLicenseErrorObjects – количество сообщений, не проверенных из-за проблемы с лицензией;

- SkippedByTimeoutObjects – количество сообщений, не проверенных из-за истечения времени ожидания;
- SkippedByProcessingErrorObjects – количество сообщений, не проверенных из-за ошибок обработки.

Пример команды, которая выводит статистику работы модулей Антивирус для роли Транспортный концентратор и фильтрации вложений и содержимого на сервере server.domain.com за последние сутки:

```
Get-KSEAVServerStatistics -ServerFqdn server.domain.com -From $(Get-Date).AddDays(-1) -To $(Get-Date)-AntivirusRole Transport
```

Если служба программы Kaspersky Security for Microsoft Exchange Servers (KSCM8) не запущена, команда Get-KSEAVServerStatistics возвращает исключение System.ServiceModel.EndpointNotFoundException.

Просмотр статистики работы модуля Анти-Спам

Просматривать статистику работы модуля Анти-Спам в среде Windows PowerShell могут пользователи, обладающие одной из следующих ролей (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58):

- Администратор;
- Специалист по антивирусной безопасности;
- Оператор антивирусной безопасности.

► *Чтобы просмотреть статистику работы модуля Анти-Спам, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEASServerStatistics -ServerFqdn <имя сервера> -From <начало периода> -To <конец периода>
   ```

   где:

   - <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес.
   - <начало периода> – дата начала периода, за который вы хотите просмотреть статистику.
   - <конец периода> – дата окончания периода, за который вы хотите просмотреть статистику.

   В среде Windows PowerShell отобразится следующая информация:

   - TotalCheckedMessages – общее количество сообщений, поступивших на проверку за указанный период;

- CleanMessages – количество сообщений, в которых не обнаружен спам и фишинговые ссылки (со статусом *Чистые*);
- SpamMessages – количество сообщений со статусом *Спам*;
- ProbableSpamMessages – количество сообщений со статусом *Возможный спам*;
- FormalMessages – количество сообщений со статусом *Формальное оповещение*;
- BlackListedMessages – количество сообщений со статусом *Адрес в черном списке*;
- TrustedMessages – количество сообщений со статусом *Доверенные*;
- MassMailMessages – количество сообщений со статусом *Массовая рассылка*;
- PhishingMessages – количество сообщений со статусом *Фишинг*;
- NotCheckedMessages – количество сообщений, не проверенных Анти-Спамом.

Пример команды, которая выводит статистику работы Анти-Спама на сервере server.domain.com за последний час:

```
Get-KSEASServerStatistics -ServerFqdn server.domain.com -From $(Get-Date).AddHours(-1) -To $(Get-Date)
```

Если служба программы Kaspersky Security for Microsoft Exchange Servers (KSCM8) не запущена, команда Get-KSEASServerStatistics возвращает исключение System.ServiceModel.EndpointNotFoundException.

Просмотр белого списка адресов Анти-Спама

Просматривать белые списки адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

► *Чтобы просмотреть белый список адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните одну из следующих команд:
   - `Get-KSEAntiSpamWhiteList -Server <имя сервера>`
   - `Get-KSEAntiSpamWhiteList -Profile <имя профиля>`

   где:
   - <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес.
   - <имя профиля> – имя существующего профиля, если используется.

   В среде Windows PowerShell будут выведены записи белого списка, содержащие следующую информацию:

- AuditDataUserLogin – служебная информация Kaspersky Security.
- Comment – комментарий к записи, если есть.
- Id – уникальный идентификатор записи (GUID).
- IsMassMailExclusionOnly – область действия записи (True – по записи пропускаются массовые рассылки, False – по записи пропускаются спам и массовые рассылки).
- IsSender – назначение адреса в записи (True – адрес отправителя, False – адрес получателя).
- ItemType – способ указания адреса (EmailAddress – адрес электронной почты, IpAddress – IP-адрес, AdUser – пользователь Active Directory, AdGroup – группа пользователей Active Directory).
- ItemValue – адрес электронной почты, маска адресов электронной почты, IP-адрес или GUID учетной записи или группы Active Directory.
- ModificationDateTimeUtc – дата и время последнего изменения записи (UTC).
- ModifiedByUser – учетная запись пользователя, который выполнил последнее изменение записи.

Пример команды, которая выводит записи белого списка на сервере server.domain.com:

```
Get-KSEAntiSpamWhiteList -Server server.domain.com
```

Просмотр черного списка адресов Анти-Спама

Просматривать черные списки адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

► *Чтобы просмотреть черный список адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните одну из следующих команд:
   - `Get-KSEAntiSpamBlackList -Server <имя сервера>`
   - `Get-KSEAntiSpamBlackList -Profile <имя профиля>`

   где:
   - <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес.
   - <имя профиля> – имя существующего профиля, если используется.

   В среде Windows PowerShell будут выведены записи черного списка, содержащие следующую информацию:
   - AuditDataUserLogin – служебная информация Kaspersky Security.
   - Comment – комментарий к записи, если есть.
   - Id – уникальный идентификатор записи (GUID).

- ItemType – способ указания адреса (EmailAddress – адрес электронной почты, IpAddress – IP-адрес).
- ItemValue – адрес электронной почты или IP-адрес.
- ModificationDateTimeUtc – дата и время последнего изменения записи (UTC).
- ModifiedByUser – учетная запись пользователя, который выполнил последнее изменение записи.

Пример команды, которая выводит записи черного списка на сервере server.domain.com:

```
Get-KSEAntiSpamBlackList -Server server.domain.com
```

Добавление адресов в белый список адресов Анти-Спама

Добавлять адреса в белый список адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

Вы можете:

- добавить новую запись в белый список;
- скопировать в белый список записи из другого белого списка, например, расположенного на другом защищаемом сервере.

► *Чтобы добавить запись в белый список адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Add-KSEAntiSpamWhiteList -Server <имя сервера> -Type <тип> -Value <адрес> -Role <роль> -Scope <область действия> -Comment <текст комментария>
   ```

   где:

   - <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес. Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>;`
   - <область действия> – область действия записи (MassMail – по записи пропускаются массовые рассылки, All – по записи пропускаются спам и массовые рассылки);
   - <роль> – назначение адреса в записи (Sender – адрес отправителя, Recipient – адрес получателя);
   - <тип> – способ указания адреса (EmailAddress – адрес электронной почты, IpAddress – IP-адрес, AdUser – пользователь Active Directory, AdGroup – группа пользователей Active Directory);

- <адрес> – адрес электронной почты, маска адресов электронной почты, IP-адрес или GUID учетной записи или группы Active Directory;
- <текст комментария> – комментарий к записи. Необязательный параметр.

В список будет добавлена запись с указанными параметрами.

► *Чтобы скопировать в белый список на сервере 1 записи из белого списка на сервере 2, выполните следующие действия:*

1. Выполните команду:

   ```
   Get-KSEAntiSpamWhiteList -Server <имя сервера 2> | Add-
   KSEAntiSpamWhiteListItem -Server <имя сервера 1>
   ```

   где:

   - <имя сервера 1> – имя сервера, в белый список которого вы хотите добавить записи;
   - <имя сервера 2> – имя сервера, из белого списка которого вы хотите скопировать записи.

     Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

   Записи из белого списка на сервере 2 будут добавлены в белый список на сервере 1. Для каждой добавленной записи будет создан новый идентификатор записи (Id). Если адрес в записи, копируемой с сервера 2, уже используется в какой-либо записи на сервере 1, то такая запись не будет скопирована.

   Вы можете выбирать в списке записи, которые хотите добавить, с помощью команд фильтрации (см. примеры).

Примеры:

1. Добавление в белый список на сервере server.domain.com записи, содержащей адрес отправителя, заданный в виде IP-адреса 192.168.1.1:

```
Add-KSEAntiSpamWhiteListItem -Server server.domain.com -Type IpAddress -
Value "192.168.1.1" -Role Sender -Scope All -Comment "Comment text"
```

2. Добавление в белый список на сервере server.domain.com записи, содержащей адрес получателя, заданный именем учетной записи username:

```
Add-KSEAntiSpamWhiteListItem -Server server.domain.com -Type AdUser -
Value (Get-ADUser username).ObjectGUID -Role Recipient -Scope All -
Comment "Comment text"
```

3. Копирование записей из белого списка на сервере server1.domain.com в белый список на сервере server2.domain.com:

```
Get-KSEAntiSpamWhiteList -Server server1.domain.com | Add-
KSEAntiSpamWhiteListItem -Server server2.domain.com
```

4. Копирование записей, содержащих адреса отправителей из белого списка в профиле profile1 в белый список в профиле profile2:

```
Get-KSEAntiSpamWhiteList -Profile profile1 | Where-Object {$_.IsSender -
eq "True"} | Add-KSEAntiSpamWhiteListItem -Profile profile2
```

kaspersky

Добавление адресов в черный список адресов Анти-Спама

Добавлять адреса в черный список адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

Вы можете:

- добавить новую запись в черный список;
- скопировать в черный список записи из другого черного списка, например, расположенного на другом защищаемом сервере.

► *Чтобы добавить запись в черный список адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Add-KSEAntiSpamBlackList -Server <имя сервера> -Type <тип> -Value <адрес> -Comment <текст комментария>
   ```

   где:

   - <имя сервера> – имя защищаемого сервера Microsoft Exchange в формате FQDN. Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.
   - <тип> – способ указания адреса (EmailAddress – адрес электронной почты, IpAddress – IP-адрес).
   - <адрес> – адрес электронной почты, маска адресов электронной почты или IP-адрес.
   - <текст комментария> – комментарий к записи. Необязательный параметр.

   В список будет добавлена запись с указанными параметрами.

► *Чтобы скопировать в черный список на сервере 1 записи из черного списка на сервере 2, выполните следующие действия:*

1. Выполните команду:

   ```
   Get-KSEAntiSpamBlackList -Server <имя сервера 2> | Add-KSEAntiSpamBlackListItem -Server <имя сервера 1>
   ```

   где:

   - <имя сервера 1 > - имя сервера, в черный список которого вы хотите добавить записи;
   - <имя сервера 2> - имя сервера, из черного списка которого вы хотите скопировать записи.

     Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

Записи из черного списка на сервере 2 будут добавлены в черный список на сервере 1. Для каждой добавленной записи будет создан новый идентификатор записи (Id). Если адрес в записи, копируемой с сервера 2, уже используется в какой-либо записи на сервере 1, то такая запись не будет скопирована.

Вы можете выбирать в списке записи, которые хотите добавить, с помощью команд фильтрации (см. примеры).

Примеры:

1. Добавление в черный список на сервере server.domain.com записи, содержащей адрес отправителя, заданный в виде адреса электронной почты user@mail.com.

```
Add-KSEAntiSpamBlackListItem -Server server.domain.com -Type EmailAddress
-Value "user@mail.com" -Comment "Comment text"
```

2. Копирование записей из черного списка профиля profilename в черный список на сервере server.domain.com.

```
Get-KSEAntiSpamBlackList -Profile profilename | Add-
KSEAntiSpamBlackListItem -Server server.domain.com
```

3. Копирование записей, содержащих IP-адреса, из черного списка на сервере server1.domain.com в черный список на сервере server2.domain.com.

```
Get-KSEAntiSpamBlackList -Server server1.domain.com | Where-Object
{$_.ItemType -eq "IpAddress"} | Add-KSEAntiSpamBlackListItem -Server
server2.domain.com
```

Удаление адресов из белого списка адресов Анти-Спама

Удалять адреса из белого списка адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

Вы можете:

- удалить одну, несколько или все записи из белого списка;
- удалить из белого списка те записи, которые есть в другом белом списке, например, расположенном на другом защищаемом сервере.

► *Чтобы удалить все записи из белого списка адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEAntiSpamWhiteList -Server <имя сервера> | Remove-
   KSEAntiSpamWhiteListItem -Server <имя сервера>
   ```

   где <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес. Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

Из белого списка на сервере или в профиле будут удалены все записи.

Вы можете удалить из списка одну или несколько записей. Для этого выберите с помощью команд фильтрации записи, которые хотите удалить (см. примеры).

► *Чтобы удалить из белого списка на сервере 1 все записи, которые есть в белом списке на сервере 2, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEAntiSpamWhiteList -Server <имя сервера 2> | Remove-
   KSEAntiSpamWhiteListItem -Server <имя сервера 1>
   ```

   где:

   - <имя сервера 1 > – имя сервера, из белого списка которого вы хотите удалить записи;
   - <имя сервера 2> – имя сервера, в белом списке которого содержатся записи, которые вы хотите удалить из белого списка на сервере 1.

     Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

Из белого списка на сервере 1 будут удалены все записи, которые присутствуют в белом списке на сервере 2.

Вы можете удалить из списка одну или несколько записей. Для этого выберите с помощью команд фильтрации записи, которые хотите удалить (см. примеры).

Примеры:

1. Очистка белого списка на сервере server.domain.com:

```
Get-KSEAntiSpamWhiteList -Server server.domain.com | Remove-
KSEAntiSpamWhiteListItem -Server server.domain.com
```

2. Удаление из белого списка профиля profile2 записей, которые присутствуют в белом списке профиля profile1:

```
Get-KSEAntiSpamWhiteList -Profile profile1 | Remove-
KSEAntiSpamWhiteListItem -Profile profile2
```

3. Удаление из белого списка на сервере server.domain.com записей, адреса в которых оканчиваются на ".mail.com":

```
Get-KSEAntiSpamWhiteList -Server server.domain.com | Where-Object
{$_.ItemValue -like "*.mail.com"} | Remove-KSEAntiSpamWhiteListItem -
Server server.domain.com
```

4. Удаление из белого списка в профиле profilename записей, адреса в которых заданы в виде группы учетных записей Active Directory:

```
Get-KSEAntiSpamWhiteList -Profile profilename | Where-Object {$_.ItemType
-eq "AdGroup"} | Remove-KSEAntiSpamWhiteListItem -Profile profilename
```

kaspersky

Удаление адресов из черного списка адресов Анти-Спама

Удалять адреса из черного списка адресов Анти-Спама в среде Windows PowerShell могут пользователи, обладающие ролью (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58) Администратор.

Вы можете:

- удалить одну, несколько или все записи из черного списка;
- удалить из черного списка те записи, которые есть в другом черном списке, например, расположенном на другом защищаемом сервере.

► *Чтобы удалить все записи из черного списка адресов Анти-Спама, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEAntiSpamBlackList -Server <имя сервера> | Remove-
   KSEAntiSpamBlackListItem -Server <имя сервера>
   ```

   где <имя сервера> – имя защищаемого сервера Microsoft Exchange. Рекомендуется указывать полный адрес сервера в формате FQDN или IP-адрес. Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

Из черного списка на сервере будут удалены все записи.

Вы можете удалить из списка одну или несколько записей. Для этого выберите с помощью команд фильтрации записи, которые хотите удалить (см. примеры).

► *Чтобы удалить из черного списка на сервере 1 все записи, которые есть в черном списке на сервере 2, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Get-KSEAntiSpamBlackList -Server <имя сервера 2> | Remove-
   KSEAntiSpamBlackListItem -Server <имя сервера 1>
   ```

   где:

   - <имя сервера 1 > – имя сервера, из черного списка которого вы хотите удалить записи.
   - <имя сервера 2> – имя сервера, в черном списке которого содержатся записи, которые вы хотите удалить из черного списка на сервере 1.

     Если вы используете профили для управления серверами, вы можете заменить `-Server <имя сервера>` на `-Profile <имя профиля>`.

Из черного списка на сервере 1 будут удалены все записи, которые присутствуют в черном списке на сервере 2.

Вы можете удалить из списка одну или несколько записей. Для этого выберите с помощью команд фильтрации записи, которые хотите удалить (см. примеры).

Примеры:

1. Очистка черного списка на сервере server.domain.com:

```
Get-KSEAntiSpamBlackList -Server server.domain.com | Remove-
KSEAntiSpamBlackListItem -Server server.domain.com
```

2. Удаление из черного списка на сервере server.domain.com записей, которые присутствуют в черном списке профиля profilename:

```
Get-KSEAntiSpamBlackList -Profile profilename | Remove-
KSEAntiSpamBlackListItem -Server server.domain.com
```

3. Удаление из черного списка на сервере server.domain.com записей, в комментариях к которым присутствует слово "obsolete":

```
Get-KSEAntiSpamBlackList -Server server.domain.com | Where-Object
{$_.Comment -like "*obsolete*"} | Remove-KSEAntiSpamBlackListItem -Server
server.domain.com
```

kaspersky

Синхронизация белых / черных списков адресов Анти-Спама

Вы можете синхронизировать белые или черные списки, расположенные на разных серверах Microsoft Exchange или в разных профилях, с помощью комбинаций команд добавления адресов в белый / черный списки и удаления адресов из белого / черного списков адресов Анти-Спама.

Синхронизация списков выполняется путем полной замены одного списка другим. Синхронизация состоит из двух этапов:

1. Удаление всех записей из списка, который нужно синхронизировать с другим списком.
2. Добавление всех записей из другого списка в имеющийся пустой список.

Примеры:

1. Синхронизация белого списка на сервере server2.domain.com с белым списком на сервере server1.domain.com:

```
Get-KSEAntiSpamWhiteList -Server server2.domain.com | Remove-
KSEAntiSpamWhiteListItem -Server server2.domain.com

Get-KSEAntiSpamWhiteList -Server server1.domain.com | Add-
KSEAntiSpamWhiteListItem -Server server2.domain.com
```

2. Синхронизация черного списка в профиле profile2 с черным списком в профиле profile1:

```
Get-KSEAntiSpamBlackList -Profile profile2 | Remove-
KSEAntiSpamBlackListItem -Profile profile2

Get-KSEAntiSpamBlackList -Profile profile1 | Add-KSEAntiSpamBlackListItem
-Profile profile2
```

Работа с ключом для расшифровки подписи сообщений

В целях безопасности программа подписывает каждое сообщение, отправляемое адресатам из резервного хранилища (см. раздел "Отправка объектов из резервного хранилища исходным получателям" на стр. 182), заголовком, который содержит зашифрованный хеш сообщения.

Ключ для расшифровки подписи генерируется автоматически при установке или обновлении программы. При необходимости вы также можете сгенерировать ключ повторно.

Производить действия с ключом для расшифровки подписи сообщений в среде Windows PowerShell на Транспортном сервере-концентраторе могут пользователи, включенные в группу Kse Administrators (см. раздел "Ролевое разграничение доступа пользователей к функциям и службам программы" на стр. 58). Для работы с ключом на Пограничном транспортном сервере достаточно запустить Windows PowerShell от имени администратора.

► *Чтобы экспортировать ключ, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

```
Export-MessageSignKey -FileName <путь к файлу> -Server <имя сервера>
```

где:

- <путь к файлу> – путь к файлу, в который будет экспортирован ключ, включая название файла;
- <имя сервера> – , имя сервера Microsoft Exchange, обрабатывающего запрос.

Ключ будет сохранен в указанный файл.

При выполнении команды на сервере, развернутом в роли "Транспортный концентратор", производится экспорт ключей всех серверов Microsoft Exchange, добавленных в домен. Все ключи записываются в один файл.

При выполнении команды на сервере, развернутом в роли "Пограничный транспорт", экспортируется только ключ данного сервера.

► *Чтобы импортировать ключ, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Import-MessageSignKey -FileName <путь к файлу> -Server <имя сервера>
   ```

   где:

   - <путь к файлу> – путь к файлу ключа, включая название файла.
   - <имя сервера> – , имя сервера Microsoft Exchange, на котором выполняется импорт ключа.

Ключ будет импортирован на сервер.

► *Чтобы повторно сгенерировать ключ, выполните следующие действия:*

1. Запустите Windows PowerShell от имени администратора (Run as Administrator) и подключите библиотеку Kse.Powershell (см. раздел "Подключение библиотеки Kse.Powershell" на стр. 208).
2. Выполните команду:

   ```
   Regenerate-MessageSignKey -Server <имя сервера>
   ```

   где <имя сервера> – имя сервера Microsoft Exchange, ключ для которого создается повторно.

Ключ будет перевыпущен.

kaspersky

Экспорт и импорт конфигурации программы

Этот раздел содержит информацию о том, как экспортировать конфигурацию программы в файл и импортировать ее из файла. Файл с конфигурацией имеет формат XML.

Вы можете импортировать конфигурацию только в программу той же версии, из которой был произведен экспорт конфигурации.

В специальных случаях поведение программы может быть изменено путем создания файла параметров специального вида и размещения файла в папке установки программы. Более подробную информацию вы можете получить, обратившись в Службу технической поддержки.

В этом разделе

Экспорт конфигурации программы в файл

► *Чтобы экспортировать конфигурацию программы в файл, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите экспортировать конфигурацию программы для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите экспортировать конфигурацию программы для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел нужного профиля.
2. Выберите узел **Настройка**.
3. В рабочей области в блоке параметров **Управление конфигурацией** нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Параметры конфигурации** установите флажки для тех групп параметров, которые вы хотите экспортировать:
   - **Все параметры**. Все параметры, составляющие конфигурацию программы.
   - **Защита для роли Транспортный концентратор**. Группа параметров, относящихся к модулям Анти-Спам и Антивирус для роли Транспортный концентратор.
   - **Защита для роли Почтовый ящик**. Группа параметров, относящихся к модулю Антивирус для роли Почтовый ящик.

- **Дополнительные параметры Антивируса**. Дополнительные параметры Антивируса, такие как параметры KSN, параметры проверки архивов и объектов-контейнеров и исключения из антивирусной проверки.
- **Обновления**. Параметры обновления баз программы.
- **Запись событий в журнал**. Параметры диагностики и журналов программы.
- **Отчеты**. Параметры отчетов.
- **Уведомления**. Параметры уведомлений.
- **Инфраструктура**. Группа, включающая следующие параметры:
  - параметры подключения к Microsoft SQL Server: имя SQL-сервера и имя базы данных SQL;
  - параметры подключения к прокси-серверу.

5. Нажмите на кнопку **ОК**.
6. В открывшемся окне **Сохранить как** введите имя файла, выберите папку назначения и нажмите на кнопку **Сохранить**.

Программа сохранит выбранные параметры конфигурации в файл с расширением kseconfig.

Импорт конфигурации программы из файла

Вы можете импортировать конфигурацию только в программу той же версии, из которой был произведен экспорт конфигурации.

► *Чтобы импортировать конфигурацию программы из файла, выполните следующие действия:*

1. В дереве Консоли управления выполните следующие действия:
   - Если вы хотите импортировать конфигурацию программы для нераспределенного Сервера безопасности, раскройте узел нужного Сервера безопасности.
   - Если вы хотите импортировать конфигурацию программы для Серверов безопасности профиля, раскройте узел **Профили** и в нем раскройте узел нужного профиля.
2. Выберите узел **Настройка**.
3. В рабочей области в блоке параметров **Управление конфигурацией** нажмите на кнопку **Импортировать**.
4. В открывшемся окне **Открыть** выберите файл с конфигурацией программы, которую вы хотите импортировать, и нажмите на кнопку **Открыть**.

   Вы можете выбирать только файлы с расширением kseconfig.

Программа импортирует конфигурацию из выбранного файла. Значения параметров, загруженные из файла, автоматически заменят текущие значения параметров программы.

kaspersky

Управление программой с помощью Kaspersky Security Center

Kaspersky Security Center – это программа, предназначенная для централизованного управления программами "Лаборатории Касперского" в сети организации. Для получения подробной информации об установке и использовании Kaspersky Security Center см. Руководство администратора Kaspersky Security Center.

С помощью Kaspersky Security Center вы можете решать следующие задачи по работе с Kaspersky Security для Microsoft Exchange Servers:

- распространять ключи на защищаемые серверы Microsoft Exchange;
- просматривать сведения о состоянии защиты серверов Microsoft Exchange;
- просматривать статистику работы программы на серверах Microsoft Exchange;
- сохранять информацию о работе программы в журнале событий Сервера администрирования Kaspersky Security Center;
- распространять пакеты обновлений для баз Антивируса и Анти-Спама на защищаемые серверы Microsoft Exchange, сетевые параметры которых запрещают обращаться к внешним сетевым ресурсам.

О плагине управления

Плагин управления Kaspersky Security для Microsoft Exchange Servers обеспечивает интерфейс для управления Kaspersky Security для Microsoft Exchange Servers через Kaspersky Security Center. Плагин входит в комплект поставки Kaspersky Security для Microsoft Exchange Servers. Плагин должен быть установлен на том компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

Для установки плагина управления требуется версия Kaspersky Security Center 4.2.

Права на управление

Учетные записи всех компьютеров, на которых установлен Kaspersky Security для Microsoft Exchange Servers, должны быть добавлены в группу KSE Administrators для управления Kaspersky Security для Microsoft Exchange Servers с помощью Консоли администрирования Kaspersky Security Center.

В этом разделе

kaspersky

Установка плагина управления Kaspersky Security

Для установки плагина управления требуется версия Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

► *Чтобы установить плагин управления Kaspersky Security, выполните следующие действия:*

1. Скопируйте на компьютер, где установлена Консоль администрирования Kaspersky Security Center, файл klcfginst.msi из комплекта поставки Kaspersky Security и запустите его.
2. Выполните шаги мастера установки.

   Плагин управления будет установлен на компьютер.

Kaspersky Security Center начнет использовать плагин управления Kaspersky Security для подключения к серверам Microsoft Exchange организации с установленной программой Kaspersky Security. Для получения подробной информации см. *Руководство администратора Kaspersky Security Center*.

Об активации программы через Kaspersky Security Center

Если вы управляете Kaspersky Security для Microsoft Exchange Servers через Kaspersky Security Center, вы можете активировать программу с помощью ключа. Kaspersky Security Center позволяет автоматически распространять ключи на *управляемые устройства*. Вы можете добавить ключ сервера безопасности Kaspersky Security для Microsoft Exchange Servers в хранилище соответствующего Сервера администрирования с помощью файла ключа или кода активации. Вы можете использовать функцию автоматического распространения ключа на управляемые устройства в свойствах ключа как в момент добавления ключа в хранилище Сервера администрирования, так и в любое другое время.

Для получения подробных сведений об особенностях работы Kaspersky Security Center с ключами программ "Лаборатории Касперского" см. Руководство администратора Kaspersky Security Center.

Автоматически распространенный ключ добавляется в качестве активного ключа на серверах Kaspersky Security для Microsoft Exchange Servers, подключенных к текущему Серверу администрирования, у которых отсутствует активный ключ или истек срок действия лицензии.

Если срок действия лицензии скоро истекает и резервный ключ отсутствует, ключ добавляется в качестве резервного. Программа автоматически переходит на его использование по истечении срока действия активного ключа. Вы не можете распространять ключ, добавленный с помощью кода активации в качестве резервного ключа.

При подключении к Серверу администрирования новых серверов Kaspersky Security для Microsoft Exchange Servers действие ключа распространяется на них автоматически.

Если автоматически распространенный ключ добавлен хотя бы для одного сервера безопасности из профиля управления несколькими серверами безопасности, программа Kaspersky Security использует этот ключ как активный ключ профиля Kaspersky Security.

При удалении автоматически распространенного ключа из хранилища Сервера администрирования ключ продолжает использоваться на том Сервере безопасности, на который ключ был автоматически распространен. В этом случае управление ключом и просмотр информации о нем будут доступны только через интерфейс Kaspersky Security для Microsoft Exchange Servers.

Сценарий распространения ключа на серверы Kaspersky Security для Microsoft Exchange Servers с помощью задачи распространения ключа не поддерживается.

Обновление баз программы через Kaspersky Security Center

Вы можете использовать Kaspersky Security Center для централизованной загрузки обновлений баз Антивируса и Анти-Спама. В этом случае пакеты обновлений будут сохраняться в сетевой папке и передаваться программе через внутреннюю сеть организации. Данный способ позволит сократить внешний сетевой трафик и оптимизировать обновление баз программы на защищаемых серверах, сетевые параметры которых запрещают обращаться к внешним сетевым ресурсам.

► *Для настройки такого способа обновления баз программы выполните следующие действия:*

- В Консоли администрирования Kaspersky Security Center создайте задачу загрузки обновлений в хранилище и укажите желаемую сетевую папку для сохранения обновлений. Для получения подробной информации см. Руководство администратора Kaspersky Security Center.

  Убедитесь, что настройки сети разрешают обмен данными между выбранной сетевой папкой и защищаемыми серверами Microsoft Exchange.
- В Консоли управления Kaspersky Security для Microsoft Exchange Servers перейдите в узел **Обновления**. В блоках **Обновление антивирусных баз** и **Обновление баз Анти-Спама** выберите пункт **HTTP-сервер, FTP-сервер, локальная или сетевая папка** и укажите сетевую папку, заданную в Kaspersky Security Center, как источник обновлений.

События Kaspersky Security в Kaspersky Security Center

В этом разделе собрана информация о событиях в работе программы, которые записываются в журнал событий Сервера администрирования Kaspersky Security Center.

Kaspersky Security Center также позволяет экспортировать события Kaspersky Security в SIEM-системы по протоколу Syslog.

Для получения подробных сведений о работе с событиями и политиками программы с помощью Сервера администрирования Kaspersky Security Center см. *Руководство администратора Kaspersky Security Center*.

Таблица 12. События Kaspersky Security, связанные со срабатываниями, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Включен режим ограниченной проверки	Критическое событие	Событие записывается, если компонент программы перешел в режим ограниченной проверки. В записи о событии указывается название компонента и время его перехода в режим ограниченной проверки (см. раздел "О предотвращении задержки сообщений модулем Антивирус" на стр. 116).
Обнаружен зараженный или защищенный паролем объект	Информационное сообщение	Событие записывается, если в узле **Уведомления** установлен флажок **Записывать события в журнал Windows** в соответствующей событию теме уведомления и обнаружен зараженный или защищенный объект.
Обнаружен файл вложения или содержимое, параметры которого соответствуют условиям фильтрации	Информационное сообщение	Событие записывается, если в узле **Уведомления** установлен флажок **Записывать события в журнал Windows** в соответствующей событию теме уведомления и обнаружен зараженный файл во вложении, который соответствует критериям фильтрации вложений.
Обнаружено исходящее сообщение, являющееся спамом или содержащее фишинговую ссылку	Информационное сообщение	Событие записывается, если программа обнаружила исходящее сообщение электронной почты, содержащее спам или фишинг. В записи о событии содержатся сведения о сообщении.
Ошибка в работе компонента программы	Критическое событие	Событие записывается, если программа зафиксировала ошибки в работе компонента. В записи о событии указывается название компонента и описание ошибки.

По умолчанию события, связанные со срабатываниями, хранятся в журнале событий Kaspersky Security Center 30 дней. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Таблица 13. События Kaspersky Security, связанные с базой Антивируса и базой Анти-Спама, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Антивирусные базы обновлены	Информационное сообщение	Событие записывается, если антивирусные базы программы были обновлены до последней версии. В записи о событии указывается дата выпуска баз.
Антивирусные базы устарели	Критическое событие	Событие записывается, если антивирусные базы программы устарели более чем на сутки.
Базы Анти-Спама устарели	Предупреждение	Событие записывается, если базы Анти-Спама устарели более чем на 5 часов.
Ошибка обновления антивирусных баз устранена. Антивирусные базы успешно обновлены	Информационное сообщение	Событие записывается, если устранена ошибка обновления антивирусных баз программы, и базы обновлены успешно. В записи о событии указывается тип баз и дата выпуска баз.
Ошибка обновления баз	Критическое событие	Событие записывается, если базы программы не удалось обновить. В записи о событии указывается тип баз и описание ошибки.
Базы Анти-Спама обновлены	Информационное сообщение	Событие записывается, если базы Анти-Спама обновлены до последней версии. В записи о событии указывается тип баз и дата выпуска баз.
Ошибка обновления баз Анти-Спама устранена. Базы Анти-Спама успешно обновлены	Информационное сообщение	Событие записывается, если в программе устранена ошибка обновления баз Анти-Спама, и базы успешно обновлены. В записи о событии указывается тип баз и дата выпуска баз.

По умолчанию события, связанные с базой данных программы, хранятся в журнале событий Kaspersky Security Center 30 дней. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Таблица 14. События Kaspersky Security, связанные с доступом программы к SQL-серверу, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Ошибка соединения с SQL-сервером	Критическое событие	Событие записывается, если программа зафиксировала ошибку на SQL-сервере. В записи о событии указывается имя базы данных, имя SQL-сервера и описание ошибки.
Соединение с SQL-сервером восстановлено	Информационное сообщение	Событие записывается, если доступ к базе данных на SQL-сервере восстановлен.

По умолчанию события, связанные с базой данных программы, хранятся в журнале событий Kaspersky Security Center 30 дней. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Таблица 15. События Kaspersky Security, связанные с лицензированием программы, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Выполнено действие с ключом Сервера безопасности	Информационное сообщение	Событие записывается, если статус ключа, дата окончания срока действия лицензии, количество пользователей или тип лицензии изменились. В записи о событии указывается ключ, тип лицензии, дата окончания срока действия лицензии и количество пользователей лицензии.
Пользователь выполнил действие с ключом Сервера безопасности	Информационное сообщение	Событие записывается, если пользователь выполнил действия с ключом Сервера безопасности. В записи о событии указывается учетная запись пользователя.

Событие	Уровень важности события	Описание
Активный ключ не обнаружен	Критическое событие	Событие записывается, если в узле **Уведомления** установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в соответствующей событию теме уведомления и активный ключ не обнаружен.
Срок действия лицензии истек	Критическое событие	Событие записывается, если в узле **Уведомления** установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в соответствующей событию теме уведомления и настроен параметр **Уведомить заранее об истечении срока действия лицензии (дни)** и основная лицензия истекла. В записи о событии указывается ключ, дата окончания срока действия лицензии и количество дней, оставшихся до окончания этого срока.
Срок действия лицензии скоро истекает	Предупреждение	Событие записывается, если в узле **Уведомления** установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в соответствующей событию теме уведомления и основная лицензия скоро истечет. В записи о событии указывается ключ, дата окончания срока действия лицензии и количество дней, оставшихся до окончания этого срока.
Статус лицензии давно не обновлялся	Предупреждение	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления** и программе не удалось обновить статус лицензии. В записи о событии указывается ключ, дата окончания срока действия лицензии и количество дней, оставшихся до перехода в режим ограниченной функциональности.

Событие	Уровень важности события	Описание
Произошла ошибка при обновлении статуса лицензии	Критическое событие	Событие записывается, если установлен флажок **Записывать события в журналы Windows и Kaspersky Security Center** в узле **Уведомления**, программе не удалось обновить статус лицензии и срок обновления лицензии истек. В записи о событии указывается описание причины возникновения ошибки.

По умолчанию события, связанные с лицензированием программы, хранятся в журнале событий Kaspersky Security Center 30 дней. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Таблица 16. События Kaspersky Security, связанные с мониторингом и аудитом, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Антивирус для роли Транспортный концентратор включен	Информационное сообщение	Событие записывается, если программа зафиксировала включение компонента Антивирус для роли Транспортный концентратор.
Антивирус для роли Транспортный концентратор выключен	Предупреждение	Событие записывается, если программа зафиксировала выключение компонента Антивирус для роли Транспортный концентратор.
Антивирус для роли Почтовый ящик включен	Информационное сообщение	Событие записывается, если программа зафиксировала включение компонента Антивирус для роли Почтовый ящик.
Антивирус для роли Почтовый ящик выключен	Предупреждение	Событие записывается, если программа зафиксировала выключение компонента Антивирус для роли Почтовый ящик.
Анти-Спам включен	Информационное сообщение	Событие записывается, если программа зафиксировала включение компонента Анти-Спам.
Анти-Спам выключен	Предупреждение	Событие записывается, если программа зафиксировала выключение компонента Анти-Спам.

Событие	Уровень важности события	Описание
Задача фоновой проверки остановлена	Информационное сообщение	Событие записывается, если фоновая проверка была остановлена. В записи о событии указывается причина остановки проверки.
Запущена задача фоновой проверки	Информационное сообщение	Событие записывается, если фоновая проверка была запущена вручную или автоматически по расписанию. В записи о событии указывается тип запуска.
Пользователь изменил параметры программы	Информационное сообщение	Событие записывается, если пользователь изменил параметры программы. В записи о событии указывается учетная запись пользователя, изменившего параметры, подробная информация об изменении параметра программы.
Пользователь попытался запустить фоновую проверку	Информационное сообщение	Событие записывается, если пользователь запросил запуск задачи проверки по требованию. В записи о событии указывается учетная запись пользователя.
Пользователь попытался остановить фоновую проверку	Информационное сообщение	Событие записывается, если пользователь попытался остановить задачу фоновой проверки. В записи о событии указывается учетная запись пользователя и причина остановки задачи.
Фильтрация вложений и содержимого включена	Информационное сообщение	Событие записывается, если программа зафиксировала включение компонента Фильтрация вложений.
Фильтрация вложений и содержимого выключена	Предупреждение	Событие записывается, если программа зафиксировала выключение компонента Фильтрация вложений.

По умолчанию события, связанные с мониторингом и аудитом, хранятся в журнале событий Kaspersky Security Center 30 дней. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Таблица 17. События Kaspersky Security, связанные с резервным хранилищем, в журнале событий Kaspersky Security Center

Событие	Уровень важности события	Описание
Пользователь отправил объект из резервного хранилища исходным получателям	Информационное сообщение	Событие записывается, если пользователь попытался отправить объект из резервного хранилища исходным получателям. В записи о событии указывается подробная информация об объекте и учетная запись пользователя.
Пользователь отправил объект из резервного хранилища на указанные вручную адреса электронной почты	Информационное сообщение	Событие записывается, если пользователь попытался отправить объект из резервного хранилища на адреса электронной почты, указанные вручную. В записи о событии указывается подробная информация об объекте и учетная запись пользователя.
Пользователь отправил объект из резервного хранилища на исследование в "Лабораторию Касперского"	Информационное сообщение	Событие записывается, если пользователь отправил возможно зараженный объект из резервного хранилища на исследование в "Лабораторию Касперского". В записи о событии указывается подробная информация об объекте и учетная запись пользователя.

Событие	Уровень важности события	Описание
Пользователь отправил сообщение, определенное как спам, на исследование в "Лабораторию Касперского"	Информационное сообщение	Событие записывается, если пользователь попытался отправить объект, ложно идентифицированный программой как спам, из резервного хранилища на исследование в "Лабораторию Касперского". В записи о событии указывается подробная информация об объекте и учетная запись пользователя.
Пользователь попытался сохранить на диске объект из резервного хранилища	Информационное сообщение	Событие записывается, если пользователь запросил сохранение на диск объекта из резервного хранилища. В записи о событии указывается подробная информация об объекте и учетная запись пользователя.
Пользователь удалил объект из резервного хранилища	Информационное сообщение	Событие записывается, если удален объект из резервного хранилища. В записи о событии указывается подробная информация об объекте и учетная запись пользователя, если объект был удален пользователем. Программа удаляет объект в соответствии с настройками параметров резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 186).

По умолчанию события, связанные с резервным хранилищем, не хранятся в журнале событий Kaspersky Security Center. Вы можете изменить этот параметр в консоли Kaspersky Security Center.

Просмотр сведений о состоянии защиты сервера Microsoft Exchange

► *Чтобы просмотреть сведения о состоянии защиты сервера Microsoft Exchange, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center и подключитесь к Серверу администрирования Kaspersky Security Center. Для получения подробных сведений о подключении см. *Руководство администратора Kaspersky Security Center*.
2. В дереве Консоли администрирования выберите узел **Управляемые устройства**, выберите группу управляемых устройств, в которую входит сервер Microsoft Exchange, и в рабочей области выберите закладку **Устройства**.

   На закладке отображается таблица со списком клиентских устройств организации. В списке могут находиться серверы Microsoft Exchange и другие компьютеры организации с установленными программами "Лаборатории Касперского". Для получения подробных сведений об отображаемой в

таблице информации см. *Руководство администратора Kaspersky Security Center*. Ниже приведена информация, специфическая для серверов Microsoft Exchange.

В столбце **Статус** отображается актуальное состояние защиты серверов Microsoft Exchange: *ОК*, *Предупреждение, Критический*. Актуальное состояние защиты также обозначается цветом: *ОК* – зеленым, *Предупреждение* – желтым, *Критический* – красным.

В столбце **Описание статуса** отображаются причины изменения статуса сервера Microsoft Exchange на *Критический* или *Предупреждение*. Возможны следующие причины изменения статуса:

- Для статуса *Предупреждение*:
  - *KSE: Антивирус для роли Почтовый ящик выключен*.
  - *KSE: Антивирус для роли Транспортный концентратор выключен*.
  - *KSE: Анти-Спам выключен*.
  - *KSE: Базы Анти-Спама устарели*.
  - *KSE: Срок действия лицензии Сервера безопасности скоро истечет*.
  - *KSE: Не удалось обновить статус лицензии.*
  - *KSE: Соединение с SQL-сервером недоступно*.
- Для статуса *Критический*:
  - *KSE: Программа остановлена или недоступна*.
  - *KSE: Доступ к программе запрещен*.
  - *KSE: Антивирус работает с ошибками*.
  - *KSE: Анти-Спам работает с ошибками*.
  - *KSE: Срок действия лицензии Сервера безопасности истек*.
  - *KSE: Проблема с лицензией Сервера безопасности*.
  - *KSE: Отсутствует ключ Сервера безопасности*.
  - *KSE: Не удалось обновить статус лицензии. Срок обновления истек.*
  - *KSE: Антивирусные базы устарели*.
  - *KSE: Ошибка при обновлении антивирусных баз*.
  - *KSE: Ошибка при обновлении баз Анти-Спама*.

Перечисленные статусы отображаются в случае, если в свойствах соответствующей группы управляемых устройств в списках **Условия для статуса компьютера "Критический"** и **Условия для статуса компьютера "Предупреждение"** установлен флажок **Определяемый программой** (**<Группа управляемых устройств>** → **Свойства** → **Статус устройства**). Для получения подробной информации см. *Руководство администратора Kaspersky Security Center*.

В таблице также отображается информация о статусах компонентов Kaspersky Security:

- **Статус антивирусной защиты почтовых серверов** – общее состояние антивирусной защиты в Kaspersky Security Center. Определяется двумя статусами компонентов программы: статусом Антивируса для роли Почтовый ящик и статусом Антивируса для роли Транспортный концентратор (см. таблицу ниже).

- **Статус защиты от спама** – состояние защиты от спама.

Статус может принимать следующие значения:

- *Неизвестно* – информация о статусе недоступна или компонент не установлен.
- *Остановлена* – компонент выключен.
- *Выполняется* – компонент включен.
- *Сбой* – компонент работает с ошибками.

*Таблица 18. Определение значения **Статуса антивирусной защиты почтовых серверов** по статусам компонентов программы*

Статус компонента в программе (1)	Статус компонента в программе (2)	Статус антивирусной защиты почтовых серверов
Не установлен	Не установлен	Неизвестно
Не установлен	Отключен	Остановлена
Не установлен	Работает	Выполняется
Не установлен	Ошибки работы	Сбой
Отключен	Отключен	Остановлена
Отключен	Работает	Остановлена
Отключен	Ошибки работы	Сбой
Работает	Работает	Выполняется
Работает	Ошибки работы	Сбой
Ошибки работы	Ошибки работы	Сбой

Статистика работы программы в Kaspersky Security Center

Kaspersky Security Center позволяет просматривать статистическую информацию о работе таких модулей программы, как Антивирус и Анти-Спам. Для получения подробных сведений о работе со статистикой см. *Руководство администратора Kaspersky Security Center*.

При работе с Kaspersky Security для Microsoft Exchange Servers вы можете добавить информационные панели, отражающие статусы объектов по результатам проверки соответствующим модулем программы. При добавлении информационной панели вы можете указать период времени, за который на диаграмме будет представлена статистика.

Статистика Антивируса

На диаграмме представлена общая информация о работе Антивируса на всех серверах Kaspersky Security для Microsoft Exchange Servers, подключенных к текущему Серверу администрирования. Возможные статусы объектов по результатам проверки:

- **Признанных чистыми**. Количество проверенных объектов, в которых не найдено вредоносных программ.
- **Зараженных**. Количество объектов, содержащих вирус или другую угрозу.
- **Защищенных паролем**. Количество объектов, защищенных паролем.
- **Отфильтрованных**. Количество объектов, нарушающих допустимые условия фильтрации вложений и содержимого.
- **Ошибок обработки**. Количество объектов, не проверенных в результате ошибок в работе программы или из-за проблемы с лицензией.

При одновременном срабатывании компонентов Антивируса и фильтрации вложений и содержимого объект расценивается как зараженный.

Подробная статистика Антивируса

На диаграмме представлена информация о проблемах, обнаруженных Антивирусом на всех серверах Kaspersky Security для Microsoft Exchange Servers, подключенных к текущему Серверу администрирования. При работе с данной информационной панелью вы можете просмотреть статистику работы программы за отдельный временной интервал в рамках выбранного периода времени. Возможные статусы объектов по результатам проверки:

- **Зараженных**. Количество объектов, содержащих вирус или другую угрозу.
- **Защищенных паролем**. Количество объектов, защищенных паролем.
- **Отфильтрованных**. Количество объектов, нарушающих допустимые условия фильтрации вложений и содержимого.
- **Ошибок обработки**. Количество объектов, не проверенных в результате ошибок в работе программы или из-за проблемы с лицензией.

При одновременном срабатывании компонентов Антивируса и фильтрации вложений и содержимого объект расценивается как зараженный.

Статистика Анти-Спама

На диаграмме представлена общая информация о работе Анти-Спама на всех серверах Kaspersky Security для Microsoft Exchange Servers, подключенных к текущему Серверу администрирования. Возможные статусы сообщений по результатам проверки:

- **Чистые**. Количество сообщений, относящихся к следующим категориям:
  - Проверенные сообщения, не содержащие спам или фишинговые ссылки.
  - Сообщения, исключенные из проверки с помощью белых списков отправителей или получателей.
- **Спам**. Количество сообщений, которые являются спамом.
- **Возможный спам**. Сообщения, которые, возможно (по результатам эвристического анализа), являются спамом.
- **Формальное оповещение**. Сервисные сообщения, такие как уведомления о доставке сообщения адресату.

- **Адрес в черном списке**. Сообщения от отправителей, адреса которых были внесены в черный список.
- **Доверенные**. Сообщения, поступившие через доверительные соединения (Trusted Connection).
- **Массовая рассылка**. Сообщения, которые являются результатом рассылок и не относятся к спаму.
- **Фишинг**. Сообщения, которые содержат фишинговые ссылки.
- **Не проверено**. Сообщения, которые не были проверены Анти-Спамом.

Подробная статистика Анти-Спама

На диаграмме представлена информация за установленный в Kaspersky Security Center период времени о проблемах, обнаруженных Анти-Спамом на всех серверах Kaspersky Security для Microsoft Exchange Servers, подключенных к текущему Серверу администрирования. Возможные статусы сообщений по результатам проверки:

- **Спам**. Сообщения, которые являются спамом.
- **Возможный спам**. Сообщения, которые, возможно (по результатам эвристического анализа), являются спамом.
- **Формальное оповещение**. Сервисные сообщения, такие как уведомления о доставке сообщения адресату.
- **Адрес в черном списке**. Сообщения от отправителей, адреса которых были внесены в черный список.
- **Доверенные**. Сообщения, поступившие через доверительные соединения (Trusted Connection).
- **Массовая рассылка**. Сообщения, которые являются результатом рассылок и не относятся к спаму.
- **Фишинг**. Сообщения, которые содержат фишинговые ссылки.
- **Не проверено**. Сообщения, которые не были проверены Анти-Спамом.

Для каждого управляемого устройства вы можете просмотреть список событий

► *Чтобы просмотреть журнал событий защиты сервера Microsoft Exchange, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center и подключитесь к Серверу администрирования Kaspersky Security Center. Для получения подробных сведений о подключении см. *Руководство администратора Kaspersky Security Center*.
2. В дереве Консоли администрирования выберите узел **Управляемые устройства**, выберите группу управляемых устройств, в которую входит сервер Microsoft Exchange, и в рабочей области выберите закладку **Устройства**.

   На закладке отображается таблица со списком клиентских устройств организации. В списке могут находиться серверы Microsoft Exchange и другие компьютеры организации с установленными программами "Лаборатории Касперского". Для получения подробных сведений об отображаемой в таблице информации см. *Руководство администратора Kaspersky Security Center*. Ниже приведена информация, специфическая для серверов Microsoft Exchange.
3. В таблице со списком клиентских устройств организации выберите сервер Microsoft Exchange, на котором установлен Kaspersky Security.
4. Выберите пункт **События** в контекстном меню клиентского устройства.

   Появится окно с журналом событий в виде таблицы.

kaspersky

Мониторинг работы программы с помощью System Center Operations Manager

Для наблюдения за состоянием программы с помощью System Center Operations Manager вы можете использовать Kaspersky Security for Microsoft Exchange Servers Monitoring Management Pack. Пакет управления доступен только на английском языке. Вы можете использовать его с любой языковой версией программы.

Минимальные программные требования

Поддерживаемые операционные системы Сервера безопасности:

- Windows Server 2012;
- Windows Server 2012 R2.

Поддерживаемые версии System Center Operations Manager:

- System Center 2012 Operations Manager;
- System Center 2012 R2 Operations Manager.

На серверах, за которыми ведется наблюдение, должен быть установлен Windows PowerShell 3.0 или более поздней версии.

Импорт пакета управления

Импорт пакета управления осуществляется по стандартной процедуре, предусмотренной используемой версией System Center Operations Manager (см. сопроводительную документацию для System Center Operations Manager).

Учетная запись сервера, за которым ведется наблюдение, должна быть включена в одну из следующих групп Active Directory: Kse Administrators, Kse AV Operators, Kse AV Security Officers.

kaspersky

Функциональность Kaspersky Security for Microsoft Exchange Servers Monitoring Management Pack

Для получения информации о работе программы в пакете управления предусмотрены следующие мониторы:

- **KSE Aggregate Monitor** - централизованное наблюдение за состоянием всех мониторов программы.
- **KSCM8 Service Monitor** - наблюдение за состоянием службы Kaspersky Security for Microsoft Exchange Servers (KSCM8).
- **KSE Anti-Virus for the Hub Transport Role Monitor** - наблюдение за статусом работы Антивируса для роли Транспортный концентратор.
- **KSE Anti-Virus for the Mailbox Role Monitor** - наблюдение за статусом работы Антивируса для роли Почтовый ящик.
- **KSE Anti-Spam Engine Monitor** - наблюдение за статусом работы Анти-Спама.
- **KSE Anti-Virus Databases Monitor** - наблюдение за состоянием баз Антивируса.
- **KSE Anti-Spam Databases Monitor** - наблюдение за состоянием баз Анти-Спама.
- **KSE SQL Database Monitor** - наблюдение за состоянием соединения программы с базой данных SQL.
- **KSE Licensing Monitor** - наблюдение за статусом лицензии.

Если в работе какого-либо компонента программы происходит сбой, то на соответствующем мониторе отображается предупреждение. В зависимости от серьезности ошибки, предупреждение получает статус *Предупреждение* или *Критичное*.

Таблица 19. Типы предупреждений и причины их возникновения

Название монитора	Предупреждение	Критичное
KSE Aggregate Monitor	Как минимум один из мониторов программы находится в статусе *Предупреждение.*	Как минимум один из мониторов программы находится в статусе *Критичное.*
KSCM8 Service Monitor	Не применимо	Служба Kaspersky Security for Microsoft Exchange Servers не запущена.
KSE Anti-Virus for the Hub Transport Role Monitor	• Не удалось получить информацию о состоянии работы Антивируса для роли Транспортный концентратор. • Антивирус для роли Транспортный концентратор выключен.	Антивирус для роли Транспортный концентратор включен, но работает с ошибками.
KSE Anti-Virus for the Mailbox Role Monitor	• Не удалось получить информацию о состоянии работы Антивируса для роли Почтовый ящик. • Антивирус для роли Почтовый ящик выключен.	Антивирус для роли Почтовый ящик включен, но работает с ошибками.
KSE Anti-Spam Engine Monitor	• Не удалось получить информацию о состоянии работы Анти-Спама. • Анти-Спам выключен.	Анти-Спам включен, но работает с ошибками.
KSE Anti-Virus Databases Monitor	Не удалось получить информацию о состоянии баз Антивируса.	• Базы Антивируса не обновлены. • Базы Антивируса повреждены.
KSE Anti-Spam Databases Monitor	Невозможно получить информацию о состоянии баз Анти-Спама.	• Базы Анти-Спама не обновлены. • Базы Анти-Спама повреждены.
KSE SQL Database Monitor	• Не удалось установить соединение с базой данных SQL.	• Не применимо
KSE Licensing Monitor	• Срок действия лицензии истекает через 15 дней или ранее. • Не удалось получить информацию о статусе лицензии.	• Срок действия лицензии истек. • Ключ не добавлен или подписка не активирована. • Добавленный ключ занесен в черный список.

kaspersky

Приложение. Скрипт отправки спама на исследование

Этот раздел содержит информацию о скрипте отправки спама на исследование специалистам "Лаборатории Касперского" и настройке его параметров.

В этом разделе

О скрипте отправки спама на исследование

Модуль Анти-Спам блокирует спам-сообщения, используя известные ему на текущий момент характеристики спам-рассылок. Если в почтовый ящик пользователя попадают спам-сообщения, пока не известные модулю Анти-Спам, пользователь может передать эти неотфильтрованные образцы спама на обработку специалистами "Лаборатории Касперского". Это позволит оперативно добавить новые записи в базу данных модуля Анти-Спам, быстрее заблокировать спам-рассылку и тем самым предотвратить ее дальнейшую доставку.

Передать образцы спама в "Лабораторию Касперского" пользователи могут, переместив их в папку "Нежелательная почта" ("Junk E-Mail"). Для поиска сообщений в папке "Нежелательная почта" почтовых ящиков указанных пользователей и пересылки их на указанный адрес предназначен *скрипт отправки спама на исследование*. Скрипт пересылает только те сообщения, которые были добавлены в папку "Нежелательная почта" не ранее заданного количества дней и не были отмечены другими системами защиты почты от спама.

Скрипт пересылает в "Лабораторию Касперского" сообщения из папок "Нежелательная почта" со всем содержимым. Необходимо уведомить пользователей почтовых ящиков, что перенося сообщения в папку "Нежелательная почта", они подтверждают, что в сообщениях отсутствуют конфиденциальные данные.

Скрипт выполняется от имени учетной записи, имеющей адрес электронной почты в инфраструктуре Microsoft Exchange организации и имеющей доступ к Exchange Web Services. Эта учетная запись должна иметь права на изменение папок "Нежелательная почта" всех обрабатываемых почтовых ящиков.

Для ведения журнала работы скрипта и работы с конфигурационным файлом параметров скрипта учетная запись, от имени которой запущен скрипт, должна иметь права на запись в папку, в которой он расположен (<Папка установки программы\SpamForwarder>).

Чтобы открыть папку со скриптом,

выберите в меню **Пуск** пункт **Программы → Kaspersky Security 9.0 для Microsoft Exchange Servers → Скрипт отправки спама на исследование**.

Для работы скрипта отправки спама на исследование необходим программный интерфейс Microsoft Exchange Web Services Managed API 2.0. Программный модуль этого интерфейса нужно загрузить по ссылке: http://www.microsoft.com/en-us/download/details.aspx?id=35371 и записать в папку со скриптом, в подпапку `bin`.

Режимы работы скрипта

Для работы скрипта отправки спама на исследование необходим программный интерфейс Microsoft Exchange Web Services Managed API 2.0. Программный модуль этого интерфейса нужно загрузить по ссылке: http://www.microsoft.com/en-us/download/details.aspx?id=35371 и записать в папку со скриптом, в подпапку `bin`.

Предусмотрено два режима работы скрипта:

- режим назначения прав;
- обычный режим работы.

Режим назначения прав

В режиме назначения прав скрипт назначает права для обрабатываемых почтовых ящиков пользователю, от имени которого будет впоследствии запускаться скрипт. Вам нужно запустить скрипт в этом режиме перед началом работы, а также каждый раз после добавления новых почтовых ящиков в конфигурационный файл.

Почтовые ящики, для которых уже назначены права, отмечаются в конфигурационном файле специальным атрибутом и при последующих запусках скрипта в этом режиме не обрабатываются.

Вы можете привести выданные скриптом права в исходное состояние вручную.

► *Чтобы привести выданные скриптом разрешения в исходное состояние вручную, выполните следующие действия:*

1. Откройте почтовый ящик пользователя в Microsoft Outlook.
2. Откройте контекстное меню папки "Нежелательная почта".
3. Выберите пункт **Свойства**.
4. На закладке **Разрешения** окна свойств папки "Нежелательная почта" удалите запись, связанную с учетной записью, от имени которой выполняется скрипт.
5. Нажмите **ОК**.
6. Откройте конфигурационный файл скрипта (см. раздел "Настройка конфигурационного файла скрипта" на стр. 246).
7. В блоке `<users>` удалите запись, касающуюся почтового ящика пользователя.

Если вы планируете в дальнейшем продолжить обработку спам-сообщений для этого почтового ящика, достаточно убрать из записи в конфигурационном файле атрибут `rightsAssigned`. Это остановит обработку почтового ящика до очередного запуска скрипта в режиме назначения прав или до возвращения атрибута `rightsAssigned` в исходный вид.

В режиме назначения прав скрипт выполняется в Exchange Management Shell от имени пользователя, имеющего права на редактирование разрешений в почтовых ящиках пользователей.

Для работы скрипта требуется Windows PowerShell версии 2.0 или выше.

Обычный режим работ скрипта

В этом режиме скрипт последовательно выбирает спам-сообщения из папок "Нежелательная почта" почтовых ящиков пользователей, которые указаны в конфигурационном файле в блоке `<users>` и для которых назначены соответствующие права.

Применяются следующие критерии отбора:

- сообщение не является отчетом о невозможности доставки (NDR);
- сообщение не старше количества дней, указанного в параметре `<oldMessages>` конфигурационного файла;
- поле "Тема" сообщения не содержит меток, указанных в блоке `<subjectMarks>` конфигурационного файла.

Каждое такое спам-сообщение помещается в сообщение в виде вложения с сохранением внутренней структуры спам-сообщения и отправляется на адрес электронной почты, указанный в параметре `<recipientEmail>` конфигурационного файла. После этого к полю "Тема" сообщения добавляется метка, имеющая атрибут `default` в конфигурационном файле.

Эта процедура повторяется для всех почтовых ящиков, указанных в блоке `<users>` конфигурационного файла.

Для постоянной работы скрипта требуется средствами вашей операционной системы создать задачу, выполняемую по расписанию.

Параметры запуска скрипта

Для работы скрипта отправки спама на исследование необходим программный интерфейс Microsoft Exchange Web Services Managed API 2.0. Программный модуль этого интерфейса нужно загрузить по ссылке: http://www.microsoft.com/en-us/download/details.aspx?id=35371 и записать в папку со скриптом, в подпапку `bin`.

Независимо от режима работы скрипт должен запускаться с параметром –IWantToForwardEmailFromJunkEmailFolderToKasperskyLab. Этот параметр переключает скрипт в активный режим. При попытке запуска скрипта без этого параметра скрипт не выполняется, а в консоли Windows PowerShell отображается текст программного исключения.

В качестве входных параметров для запуска скрипта вы можете указать следующие параметры:

- `workFolder` – путь к папке, в которой расположен скрипт. По умолчанию путь к текущей папке. Этот параметр позволяет запустить скрипт в обычном режиме работы.

Пример запуска скрипта в обычном режиме:

```
.\spamForwarder.ps1 –workFolder c:\temp\spamForwarder -
IWantToForwardEmailFromJunkEmailFolderToKasperskyLab
```

- `grantPermissions` – параметр, позволяющий запустить скрипт в режиме назначения прав.

Пример запуска скрипта в режиме назначения прав:

```
.\spamForwarder.ps1 –grantPermissions -
IWantToForwardEmailFromJunkEmailFolderToKasperskyLab
```

Настройка конфигурационного файла скрипта

Для работы скрипта отправки спама на исследование необходим программный интерфейс Microsoft Exchange Web Services Managed API 2.0. Программный модуль этого интерфейса нужно загрузить по ссылке: http://www.microsoft.com/en-us/download/details.aspx?id=35371 и записать в папку со скриптом, в подпапку `bin`.

Конфигурационный файл скрипта config.xml используется для настройки скрипта и имеет следующую структуру:

```
<config>
   <senderEmail>administrator@company.com</senderEmail>
   <recipientEmail>Probable_KSEspam@spam.kaspersky.com</recipientEmail>
   <exchangeVersion>Exchange2013</exchangeVersion>
   <envelopeSubject>Example of SPAM Message</envelopeSubject>
   <envelopeBody>This message contains SPAM sample in
   attachment</envelopeBody>
   <logSize>10</logSize>
   <oldMessages>3</oldMessages>
   <ews>https://kseserver.company.com/EWS/Exchange.asmx</ews>
   <users>
      <user rightsAssigned="True">user@company.com</user>
      <user>user1@company.com</user>
      <user>user2@company.com</user>
      </users>
```

```
    <subjectMarks>
       <mark>[KL SPAM]</mark>
       <mark default="True">[!! SPAM]</mark>
       <mark>[!!SPAM]</mark>
       <mark>[!!Spam]</mark>
       <mark>[!!Probable Spam]</mark>
       <mark>[!!Blacklisted]</mark>
    </subjectMarks>
 </config>
```

Вы можете настраивать следующие параметры конфигурационного файла скрипта:

- `senderEmail` – адрес электронной почты, с которого отправляются сообщения с образцами спама на исследование в "Лабораторию Касперского".

  Учетная запись, от имени которой запущен скрипт, должна иметь полные права на работу с почтовым ящиком, с которого отправляются сообщения в "Лабораторию Касперского".

- `recipientEmail` – адрес электронной почты, на который отсылаются образцы спама. По умолчанию Probable_KSEspam@spam.kaspersky.com.
- `exchangeVersion` – параметр, указывающий версию сервера Microsoft Exchange для инициализации EWS API, может принимать одно из следующих значений (вам нужно выбрать наиболее подходящее):
  - Exchange2013 (для Microsoft Exchange 2013);
  - Exchange2013_SP1 (для Microsoft Exchange 2013 SP1 и более поздних версий);
  - Exchange2016 (для Microsoft Exchange 2016).
- `envelopeSubject` – заголовок сообщения, в которое вкладываются образцы спама перед отправкой. Не рекомендуется менять это значение.
- `envelopeBody` – текст сообщения, в которое вкладываются образцы спама перед отправкой. Не рекомендуется менять это значение.
- `logSize` – максимальный размер журнала работы скрипта (в мегабайтах), при достижении которого выполняется ротация. Вы можете указать любое значение.
- `oldMessages` – максимальная давность сообщений (в днях), которые скрипт отбирает для отправки. Значение по умолчанию – 3 дня. Не рекомендуется менять это значение.
- `ews` – адрес сервера Exchange Web Services. Если этот параметр присутствует в конфигурационном файле, скрипт не использует функцию автоматического определения CA сервера. Не рекомендуется использовать этот параметр.
- `users` – блок с адресами электронной почты пользователей, почтовые ящики которых обрабатываются скриптом. Этот блок может содержать произвольное количество записей об отдельных почтовых ящиках пользователей.
- `user` – запись, содержащая адрес электронной почты ящика, подлежащего обработке скриптом. Атрибут `rightsAssigned` проставляется автоматически на этапе добавления прав. Не рекомендуется менять его значение вручную, за исключением случая, когда нужно повторно назначить права на почтовый ящик пользователя. Записи о почтовых ящиках, для которых этот атрибут не установлен, не участвуют в процессе обработки скриптом.

- `subjectMarks` – блок, содержащий возможные метки, добавляемые системами защиты от спама к теме сообщения. Блок может содержать произвольное количество записей, но количество разных меток может влиять на скорость поиска сообщений в почтовых ящиках пользователей.
- `mark` – запись, содержащая отдельную запись о метке. Атрибут `default` указывает на запись, которая используется скриптом для отметки отправленных на анализ сообщений. Не рекомендуется указывать атрибут `default` для нескольких меток, так как это нарушит работу скрипта.

Журнал работы скрипта

Результаты работы скрипта сохраняются в файле журнала. Журнал работы скрипта находится в папке, в которой расположен скрипт, в подпапке `log`.

При каждом запуске скрипта производится оценка размера текущего файла журнала. Если размер файла журнала превышает значение, указанное в параметре `<logSize>` конфигурационного файла скрипта, выполняется архивирование файла журнала методом GZIP. Также на этом этапе проверяется наличие архивов файлов журнала, которые старше двух месяцев. Такие архивы удаляются.

kaspersky

Приложение. Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.

Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 20. Параметры и их значения для программы в сертифицированном состоянии

Функциональность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Защита для роли Почтовый ящик – параметры проверки Антивируса	**Включить антивирусную защиту для роли Почтовый ящик**	Флажок установлен
Защита для роли Почтовый ящик – параметры проверки Антивируса	**Параметры обработки объектов – зараженный объект**	Одно из следующих значений: • **Удалять объект**; • **Удалять сообщение**.
Защита для роли Почтовый ящик – параметры проверки Антивируса	**Параметры обработки объектов – сохранять копию объекта в резервном хранилище**	Флажок установлен
Защита для роли Транспортный концентратор – параметры проверки Антивируса	**Включить антивирусную защиту для роли Транспортный концентратор**	Флажок установлен
Защита для роли Транспортный концентратор – параметры проверки Антивируса	**Параметры обработки объектов – действие для зараженных объектов**	Одно из следующих значений: • **Удалять объект**; • **Удалять сообщение**.
Защита для роли Транспортный концентратор – параметры проверки Антивируса	**Параметры обработки объектов – сохранять копию объекта в резервном хранилище**	Флажок установлен
Дополнительные параметры Антивируса	**Проверять вложенные контейнеры/архивы**	Флажок установлен
Дополнительные параметры Антивиуса	**Проверять вложенные контейнеры/архивы с уровнем вложенности не более …**	Рекомендуется использовать параметры по умолчанию. Уменьшение уровня вложенности для проверяемых архивов/контейнеров может привести к выходу из сертифицированного состояния.
Обновления	**Обновление баз Антивируса – источник обновлений**	Одно из следующих значений: • **Серверы обновлений «Лаборатории Касперского»**; • **HTTP-сервер, FTP-сервер, локальная или сетевая папка**.
Обновления	**Обновление баз Антивируса – режим запуска**	Рекомендуется обновлять базы Антивируса не реже 1 раза

Функциональность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
		в 7 дней
Уведомления	**Уведомления о событиях – зараженные объекты – Администратор**	Флажок установлен
Настройка	**Хранение данных**	Рекомендуется использовать параметры по умолчанию. Уменьшение размера хранилища или срока хранения объектов может привести к выходу из сертифицированного состояния.
Настройка	**Параметры KSN**	Одно из следующих значений: • **Не использовать службы «Лаборатории Касперского»**; • **Использовать Kaspersky Private Security Network**. Настройка параметров KPSN описана в разделе "Настройка параметров подключения к Kaspersky Private Security Network".
Лицензирование	**Активный ключ**	В сертифицированном состоянии активный ключ должен быть установлен и иметь статус *Действующая лицензия*.

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 программе (см. раздел "Источники информации о программе" на стр. 253), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

kaspersky

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Использование утилиты Info Collector

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать архив с данными о работе программы с помощью утилиты InfoCollector и отправить его в Службу технической поддержки.

Ознакомиться с описанием утилиты Info Collector и скачать утилиту вы можете на странице Kaspersky Security в Базе знаний (https://support.kaspersky.ru/kse9) в разделе "Устранение сбоев в работе".

kaspersky

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

kaspersky

Глоссарий

D

Domain Name System Block List (DNSBL)

Общедоступные списки IP-адресов, уличенных в рассылке спама.

E

Enforced Anti-Spam Updates Service

Служба быстрых обновлений баз Анти-Спама, позволяющий увеличить скорость реагирования Анти-Спама на появление новых рассылок. Для работы Enforced Anti-Spam Updates Service требуется постоянное соединение с интернетом.

K

Kaspersky CompanyAccount

Портал, предназначенный для отправки электронных запросов в "Лабораторию Касперского" и отслеживания их обработки специалистами "Лаборатории Касперского".

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

P

PCL-оценка

Phishing Confidence Level, специальная метка сообщения, которая используется почтовыми серверами Microsoft Exchange для определения вероятности того, что сообщение содержит фишинг. PCL-оценка может принимать значения от 0 до 8. Сообщение, PCL-оценка которого не превышает 3, расценивается почтовым сервером как не содержащее фишинга. Сообщение, у которого этот параметр имеет значение 4 и более, расцениваются как фишинг-сообщение. Значение PCL-оценки сообщения может быть изменено программой Kaspersky Security в соответствии с результатами проверки сообщения.

kaspersky

S

SCL-оценка

Spam Confidence Level, специальная метка сообщения, которая используется почтовыми серверами Microsoft Exchange для определения вероятности того, что сообщение является спам-сообщением. SCL-оценка может принимать значения от 0 (вероятность спама минимальна) до 9 (сообщение, скорее всего, является спам-сообщением). Значение SCL-оценки сообщения может быть изменено программой Kaspersky Security в соответствии с результатами проверки сообщения.

Spam URI Realtime Block Lists (SURBL)

Общедоступные списки ссылок, которые ведут на рекламируемые отправителями спама ресурсы.

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

B

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Возможно зараженный объект

Объект, код которого содержит модифицированный участок кода известной программы, представляющей угрозу, или объект, напоминающий такую программу по своему поведению.

Возможный спам

Сообщение, которое нельзя однозначно классифицировать как спам, но которое обладает некоторыми признаками спама (например, некоторые виды рассылок и рекламных сообщений).

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

З

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

К

Консоль управления

Компонент приложения Kaspersky Security. Предоставляет пользовательский интерфейс к административным средствам и позволяет осуществлять настройку и управление серверной частью. Модуль управления выполнен в виде компонента расширения к Microsoft® Management Console.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

М

Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

Массовая рассылка

Санкционированная получателями массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

Н

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора. Таким объектам присваивается статус возможно зараженных.

kaspersky

О

Обновление

Функция программы "Лаборатории Касперского", позволяющая поддерживать защиту компьютера в актуальном состоянии. Во время обновления программа копирует обновления баз и модулей программы с серверов обновлений "Лаборатории Касперского" на компьютер и автоматически устанавливает и применяет их.

Объект-контейнер

Объект, состоящий из нескольких объектов, например, архив, сообщение с любым вложенным сообщением. См. также простой объект.

П

Персональные данные

Информация, на основании которой можно прямо или косвенно идентифицировать человека.

Проверка хранилищ

Антивирусная проверка хранящихся на почтовом сервере сообщений и содержимого общих папок с использованием последней версии баз. Проверка осуществляется в фоновом режиме и может запускаться как по расписанию, так и вручную. Проверяются все общие папки и почтовые хранилища (mailbox storage). При проверке могут быть обнаружены новые вирусы, информация о которых отсутствовала в базах на момент предыдущих проверок.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Простой объект

Содержимое сообщения или простое вложение, например, в виде исполняемого файла. См. также объект-контейнер.

Профиль

Набор параметров, применяемых одновременно к нескольким Серверам безопасности.

kaspersky

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов перед лечением, удалением или заменой. Представляет собой служебную папку и создается в папке хранения данных программы при установке компонента Сервер безопасности.

Резервный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

С

Сервер безопасности

Серверный компонент Kaspersky Security. Обеспечивает проверку почтового трафика на вирусы и спам, осуществляет обновление баз, поддерживает свою целостность, хранит статистическую информацию, а также предоставляет административные средства для удаленного управления и настройки.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

У

Удаление объекта

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

Удаление сообщения

Способ обработки сообщения электронной почты, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам или вредоносный объект. Перед удалением сообщения его копия сохраняется в резервном хранилище (если данная функциональность не отключена).

Управляемое устройство

Устройство с установленной программой для обеспечения безопасности, подключенное к Kaspersky Security.

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Фоновая проверка

Режим работы Антивируса для роли Почтовый ящик, при котором Антивирус проверяет на вирусы и наличие других угроз сообщения, хранящиеся на сервере Microsoft Exchange, и другие объекты Microsoft Exchange с использованием последней версии антивирусных баз. Фоновая проверка может быть запущена вручную или согласно заданному расписанию.

Формальное сообщение

Сообщение, автоматически генерируемое и рассылаемое почтовыми клиентами, роботами (например, о невозможности доставки сообщения или о подтверждении регистрации пользователя на каком-нибудь интернет-ресурсе).

Ч

Черный список ключей

База данных, содержащая информацию о заблокированных "Лабораторией Касперского" ключах. Содержимое файла с черным списком обновляется вместе с базами.

kaspersky

Информация о стороннем коде

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

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, Access, Microsoft, Outlook, SharePoint, SQL Server, Win32, Windows, Windows Server и Windows PowerShell – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

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

kaspersky

Предметный указатель

E

K

A

Б

B

Д

Ж

З

И

К

Л

М

О

П

Р

С

Т

У

Ф