

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского® 5.5 для
Linux и FreeBSD Mail Servers

РУКОВОДСТВО
АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ
LINUX И FREEBSD MAIL SERVERS

Руководство администратора

© ЗАО «Лаборатория Касперского»
Тел., факс: +7 (495) 797-87-00, +7 (495) 645-79-39,
+7 (495) 956-7000
<http://www.kaspersky.ru>

Дата редакции: июль 2007 года

Содержание

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ LINUX И FREEBSD MAIL SERVERS.....	6
1.1. Что нового в версии 5.5	7
1.2. Аппаратные и программные требования к системе	9
1.3. Комплект поставки.....	10
1.3.1. Лицензионное соглашение.....	10
1.3.2. Регистрационная карточка	11
1.4. Сервис для зарегистрированных пользователей.....	11
ГЛАВА 2. ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ.....	13
2.1. Внутренняя архитектура Антивируса Касперского	13
2.2. Работа на одном сервере с почтовой программой.....	15
2.3. Работа на выделенном сервере	17
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО.....	19
3.1. Установка приложения на сервер под управлением Linux.....	19
3.2. Установка приложения на сервер под управлением FreeBSD	20
3.3. Процесс установки	20
3.4. Конфигурация приложения	21
ГЛАВА 4. НАСТРОЙКА ПРИЛОЖЕНИЯ ПОСЛЕ УСТАНОВКИ.....	22
4.1. Настройка приложения по умолчанию	23
4.2. Установка / обновление баз Антивируса Касперского	24
4.3. Использование webmin-модуля для управления Антивирусом Касперского.....	25
4.4. Выполнение интеграции с почтовыми программами вручную	26
4.4.1. Интеграция с почтовой программой Sendmail	26
4.4.2. Интеграция с почтовой программой Qmail.....	27
4.4.3. Интеграция с почтовой программой Postfix	28
4.4.4. Интеграция с почтовой программой Exim	29
4.4.5. Настройка параметров Антивируса Касперского для интеграции с почтовой программой.....	30
ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО.....	32
5.1. Обновление баз Антивируса Касперского	32

5.1.1. Обновление баз Антивируса Касперского с серверов обновлений	33
5.1.2. Планирование обновлений баз Антивируса Касперского с помощью сервиса cron	34
5.1.3. Разовое обновление баз Антивируса Касперского	35
5.1.4. Создание и использование локального источника обновлений	35
5.1.5. Обновление баз Антивируса Касперского при использовании прокси-сервера	37
5.2. Антивирусная защита почтового трафика сервера	37
5.2.1. Доставка незараженных и вылеченных почтовых сообщений	38
5.2.2. Доставка всех сообщений	39
5.2.3. Доставка сообщений, содержащих защищенный паролем архив	41
5.2.4. Блокирование доставки сообщений	41
5.2.5. Дополнительная проверка писем по типу вложений	43
5.3. Антивирусная защита файловых систем	45
5.3.1. Проверка файлов по выбору	46
5.3.2. Планирование проверки каталога с помощью сервиса cron	46
5.3.3. Дополнительные возможности: использование скриптов	47
5.3.3.1. Лечение зараженных архивов	47
5.3.3.2. Отправка уведомлений администратору	48
5.3.4. Помещение объектов на карантин	49
5.3.5. Режим резервного копирования объектов	50
5.4. Управление ключами	51
5.4.1. Механизм лицензирования	51
5.4.2. Просмотр информации о ключе	52
5.4.3. Продление срока действия ключа	54
ГЛАВА 6. НАСТРОЙКА ДОПОЛНИТЕЛЬНЫХ ПАРАМЕТРОВ	56
6.1. Настройка параметров антивирусной защиты почтового трафика	56
6.1.1. Формирование групп пользователей	58
6.1.2. Режим проверки и лечения сообщений	59
6.1.3. Действия над объектами	60
6.1.4. Уведомление отправителей, получателей и администраторов	61
6.2. Настройка параметров антивирусной защиты файловых систем сервера	63
6.2.1. Область проверки	64
6.2.2. Режим проверки и лечения файлов	65
6.2.3. Действия над файлами	65

6.2.4. Режим резервного копирования	66
6.3. Оптимизация работы Антивируса Касперского	67
6.3.1. Использование базы данных iChecker	68
6.3.2. Ограничение нагрузки на сервер.....	68
6.4. Настройка параметров работы процесса <i>aveserver</i>	69
6.4.1. Перезагрузка <i>aveserver</i>	69
6.4.2. Принудительное завершение работы <i>aveserver</i>	70
6.5. Проверка почты, получаемой по POP3-протоколу	70
6.6. Дополнительные возможности для почтовой программы Postfix.....	72
6.6.1. Поддержка расширения DSN.....	73
6.6.2. Поддержка расширения 8bit-MIME.....	73
6.6.3. Поддержка расширения X-Forward	74
6.6.4. Использование SMTP-протокола компонентом <i>smtpscanner</i>	74
6.7. Локализация отображаемого формата даты и времени	74
6.8. Параметры формирования журнала событий Антивируса Касперского... 75	
6.8.1. Формат сообщений о проверке.....	77
6.8.2. Формат сообщений, выводящихся на консоль.....	79
6.8.3. Статистика вирусной активности.....	79
6.8.4. Дополнительные информационные поля в сообщениях.....	80
ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО	81
ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА	82
ГЛАВА 9. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	84
ПРИЛОЖЕНИЕ А. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО».....	91
А.1. Другие разработки «Лаборатории Касперского»	92
А.2. Наши координаты	104

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ LINUX И FREEBSD MAIL SERVERS

Антивирус Касперского® 5.5 для Linux и FreeBSD Mail Servers (далее также *Антивирус Касперского*) предназначен для антивирусной обработки почтового трафика и файловых систем серверов, работающих под управлением операционных систем Linux или FreeBSD и использующих любую из следующих почтовых программ: Sendmail, Postfix, Qmail, Exim.

Приложение позволяет:

- *проверять на наличие вирусов* входящий и исходящий поток почтовых сообщений SMTP-трафика сервера;
- *выявлять* зараженные, подозрительные, поврежденные и защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- *лечить* зараженные объекты файловых систем и почтовых сообщений;
- *переносить в карантинный каталог* зараженные, подозрительные и поврежденные объекты файловых систем сервера и его почтового трафика; также на карантин можно помещать защищенные паролем файлы и файлы, в результате проверки которых произошла ошибка;
- *обрабатывать почтовый трафик* в соответствии с правилами, заданными для групп отправителей и получателей;
- *организовывать дополнительную проверку почтового потока* сообщений по именам и типам вложенных файлов и применять к отфильтрованным объектам отдельные правила обработки;
- *уведомлять* отправителя, получателя и администратора группы о почтовом сообщении, содержащем зараженный, подозрительный и другие объекты;
- *обновлять базы Антивируса Касперского*. Источником для обновления баз являются серверы обновлений «Лаборатории Касперского»;

Базы используются в процессе поиска и лечения зараженных файлов. На основе записей, содержащихся в них, каждый файл во время проверки анализируется на присутствие вирусов: код файла сравнивается с кодом, характерным для того или иного вируса. В случае если файл заражен, приложение выполняет его лечение.

Необходимо помнить, что каждый день появляются новые вирусы, поэтому для поддержания приложения в актуальном состоянии специалисты «Лаборатории Касперского» рекомендуют обновлять базы Антивируса Касперского каждый час.

- *проверять на наличие вирусов* все примонтированные файловые системы;
- *настраивать параметры работы Антивируса Касперского* через веб-интерфейс программы Webmin и конфигурационный файл приложения.

1.1. Что нового в версии 5.5

В версии 5.5 Антивируса Касперского для Linux и FreeBSD Mail Servers по сравнению с версией 5.0 произведены следующие изменения:

- Внедрены новые технологии получения обновлений баз Антивируса Касперского и модулей приложения, в том числе проверка целостности скачиваемых баз. Это позволяет существенно экономить сетевой трафик (параметры добавлены в состав компонента *keepup2date*).
- Появилась возможность создания резервного хранилища (backup-хранилища) для сохранения копий подозрительных или зараженных объектов перед их лечением или удалением. Это позволяет избежать потери исходных данных в случае возникновения внештатных ситуаций в процессе лечения объекта.
- Для снижения нагрузок при антивирусной проверке объектов файловой системы внедрены технология iChecker и двухуровневое кеширование проверенных объектов.
- С помощью программы Webmin стало возможным просматривать статистику вирусной активности за определенное время, а также данные о типах вирусов, которые были выявлены при антивирусной проверке.
- Добавлена возможность ограничения количества одновременно проверяемых в фоновом режиме объектов, что позволяет оптимизировать загрузку сервера.
- Добавлена возможность генерации списка обнаруживаемых вирусов.

- Добавлена возможность выбора протокола работы (SMTP или LMTP) компонента *smtpscanner*.
- При использовании протокола SMTP реализована возможность уведомления отправителя почтового сообщения о доставке письма.
- Добавлена возможность сохранения для каждого письма имен вирусов и идентификационного кода письма в журнале событий компонента *smtpscanner*.
- Изменена политика лицензирования приложения. В частности, нет больше необходимости создавать и поддерживать в актуальном состоянии список пользователей, чья почта защищается. Теперь список формируется и ведется автоматически.
- Добавлена возможность выбора варианта баз Антивируса Касперского (стандартный набор баз, расширенный или избыточный). При этом для каждого компонента приложения можно отдельно задать используемый набор баз.
- Добавлен новый макрос (для использования в уведомлениях), позволяющий вставлять все заголовки исходного письма.
- Существенно упрощена процедура установки и удаления приложения. В частности, в процессе удаления приложение корректирует конфигурационные файлы, убирая из них информацию о себе.
- При установке приложения стал возможен импорт параметров предыдущих версий Антивируса (версии 4.0 или 5.0). Это позволяет существенно ускорить процесс получения работоспособной конфигурации.
- При установке приложение корректно распознает наличие установленного Kaspersky Anti-Spam и интегрируется с ним, восстанавливая при удалении предыдущую конфигурацию.
- Добавлена поддержка расширений DSN, 8bit-MIME, X-Forward и протокола SMTP в качестве входящего протокола.
- Реализована возможность добавления в заголовки проверяемого почтового сообщения дополнительной информации о результатах антивирусной проверки и обработки.

1.2. Аппаратные и программные требования к системе

Для работы Антивируса Касперского система должна соответствовать следующим требованиям:

- Аппаратные требования:
 - процессор класса Pentium;
 - 32 МБ оперативной памяти;
 - 100 МБ на жестком диске.
- Программные требования:
 - Одна из следующих операционных систем:
 - Red Hat Linux 9.0;
 - Red Hat Enterprise Linux Advanced Server 3;
 - Fedora Core 3;
 - SuSe Linux Enterprise Server 9.0;
 - SuSe Linux Professional 9.2;
 - Linux Mandrake 10.1;
 - Debian GNU/Linux 3.0 updated (r4);
 - FreeBSD 4.10 и 5.3.
 - Одна из почтовых программ:
 - sendmail 8.x;
 - qmail 1.03;
 - postfix 1.0 или выше;
 - exim 4.0.
 - Интерпретатор языка Perl версии 5.0 или выше (www.perl.org), утилита *which* – для установки приложения.
 - Программа Webmin (www.webmin.com) версии 1.070 или выше, если планируется удаленное администрирование приложения.

1.3. Комплект поставки

Антивирус Касперского вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, www.kaspersky.ru, раздел **Электронный магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы приложения;
- руководство пользователя;
- ключ, включенный в состав дистрибутива или записанный на специальную дискету;
- регистрационная карточка (с указанием серийного номера продукта);
- лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением.

При покупке Антивируса Касперского в интернет-магазине вы копируете продукт с веб-сайта «Лаборатории Касперского», в дистрибутив которого помимо самого продукта включено также данное руководство. Ключ либо включен в дистрибутив, либо отправляется вам по электронной почте по факту оплаты.

1.3.1. Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с Антивирусом Касперского дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с установочным компакт-диском должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском или устанавливая продукт на компьютер, вы тем самым принимаете все условия лицензионного соглашения.

1.3.2. Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели Антивирус Касперского.

Если впоследствии у вас изменится почтовый / электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока подписки. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского», высылается информация о выходе новых программных продуктов.

1.4. Сервис для зарегистрированных пользователей

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования Антивируса Касперского.

Приобретя подписку, вы становитесь зарегистрированным пользователем приложения и в течение срока действия подписки получаете следующие услуги:

- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта. Получить консультацию вы можете одним из следующих способов:
 - позвонить по телефону в Службу технической поддержки;
 - создать и отправить запрос на веб-сайте Службы технической поддержки (<http://www.kaspersky.ru/helpdesk>) или из своего персонального кабинета.

- оповещение о выходе новых продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского»).

Консультации по вопросам функционирования и использования операционных систем, а также работы различных технологий не проводятся.

ГЛАВА 2. ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ

В зависимости от исходной архитектуры почтового сервера мы предлагаем несколько вариантов развертывания Антивируса Касперского для Linux и FreeBSD Mail Servers:

- *на один сервер с почтовой программой*: такой вариант используется при наличии на сервере уже установленной и настроенной почтовой программы Sendmail, Qmail, Postfix или Exim (см. п. 2.2 на стр. 15).
- *на выделенный сервер в качестве дополнительного фильтра*: этот способ рекомендуется использовать при работе основного почтового сервера под управлением неподдерживаемых операционной и/или почтовой программы (см. п. 2.3 на стр. 17).
- *как фильтр для внешних почтовых сервисов*: такой способ организации полезно использовать, когда пользователи почтового сервера имеют почтовые ящики на внешних серверах и необходимо обеспечить антивирусную защиту скачиваемых почтовых сообщений (см. п. 6.5 на стр. 70).

Во всех перечисленных выше случаях помимо фильтрации почтового трафика Антивирус Касперского может также выполнять и проверку всех монтированных файловых систем.

Прежде чем приступить к подробному изучению перечисленных выше вариантов развертывания, рассмотрим внутреннюю архитектуру Антивируса Касперского для наиболее полного отражения алгоритма работы.

2.1. Внутренняя архитектура Антивируса Касперского

Важным аспектом в работе с Антивирусом Касперского является четкое понимание алгоритма его функционирования.

В данном разделе мы рассмотрим внутреннюю архитектуру приложения в контексте антивирусной проверки именно почтового трафика, поскольку

процесс проверки файловых систем сервера достаточно прост и не требует отдельного изучения.

Необходимо отметить, что Антивирус Касперского предназначен только для проверки почты на наличие вирусов и не представляет собой почтовый агент, способный принимать почтовый поток и выполнять его маршрутизацию. Для этого используется почтовая программа, установленная на сервере, с которой интегрируется Антивирус после установки.

Рассмотрим подробнее на примере почтовой программы Sendmail алгоритм внутренней работы Антивируса Касперского для Linux и FreeBSD Mail Servers после его интеграции с почтовой программой (см. рис. 1).

В процессе интеграции Антивируса Касперского с почтовой программой Sendmail создается дополнительный конфигурационный файл *sendmail.cf.listen*.

При запуске Sendmail с использованием этого конфигурационного файла почтовая программа осуществляет прием почтового трафика сервера и передачу его на обработку Антивирусу Касперского, а при запуске с исходным конфигурационным файлом (*sendmail.cf*) – доставку почтовых сообщений, переданных Антивирусом.

Проверка почтовых сообщений происходит по следующему алгоритму:

1. Почтовый трафик поступает по SMTP-протоколу почтовой программе Sendmail (конфигурационный файл *sendmail.cf.listen*). Sendmail создает очередь, где хранит поступающую почту, и передает ее по протоколу LMTP или SMTP компоненту *smtpscanner* на обработку.
2. Компонент *smtpscanner* обрабатывает почтовый поток в соответствии с заданными параметрами. Процесс проверки и лечения выполняется следующим образом:
 - a. *smtpscanner* передает имя файла почтового сообщения компоненту *aveserver* по локальному сокету;
 - b. *aveserver* выполняет проверку объекта, используя базы Антивируса Касперского;
 - c. *smtpscanner* получает от *aveserver* код возврата, определяющий статус файла;
 - d. в соответствии со статусом объекта *smtpscanner* выполняет действия над ним на основании параметров конфигурационного файла.
3. Обработанный почтовый поток с уведомлениями о результатах проверки и лечения передается по SMTP-протоколу почтовой программе Sendmail (с конфигурационным файлом *sendmail.cf*), которая выполняет доставку почтового потока локальным пользовате-

лям или осуществляет маршрутизацию на другие почтовые серверы.

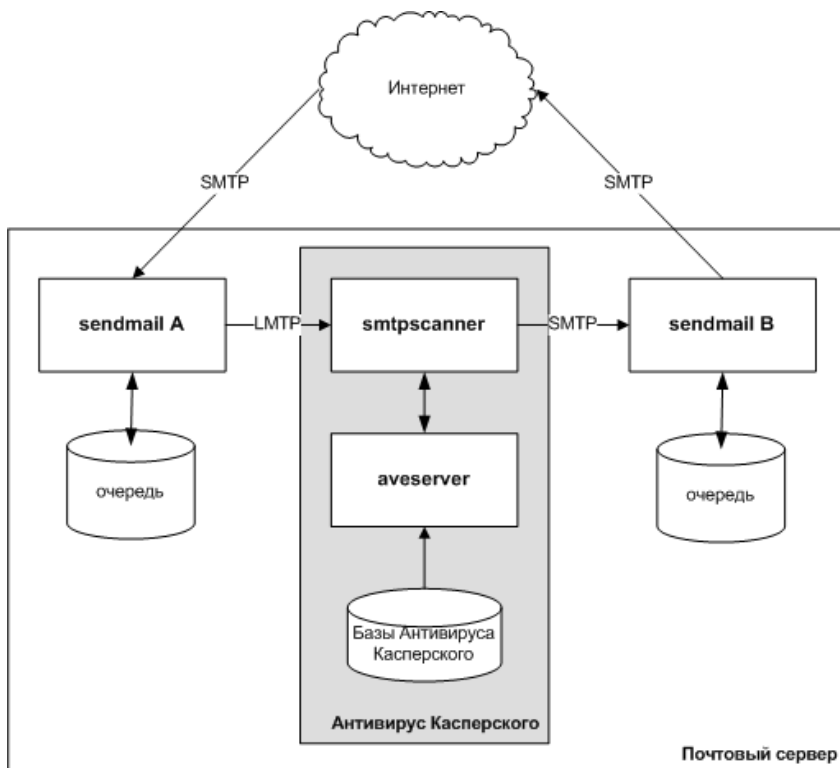


Рисунок 1. Внутренняя архитектура
Антивируса Касперского для Linux и FreeBSD Mail Servers

2.2. Работа на одном сервере с почтовой программой

Далее в этом документе рассматривая работу Антивируса Касперского и настройку его параметров, мы будем описывать именно такой вариант работы – на одном сервере с почтовой программой!

Установка и функционирование Антивируса на одном сервере с почтовой программой осуществляется только на поддерживаемых операционных системах (Linux или FreeBSD).

В качестве почтовой программы могут использоваться: Sendmail, Qmail, Postfix или Exim.

Такой вариант работы рекомендуется при средней загрузке почтового сервера.

Рассмотрим подробнее схему работы Антивируса Касперского и любой из приведенных почтовых программ на одном сервере (см. рис. 2). Порядок работы с входящей и исходящей почтой идентичен и состоит из следующих этапов:

1. Поток почтовых сообщений поступает с других серверов либо из локальной сети по SMTP-протоколу.
2. Почтовая программа принимает поток сообщений и передает его на обработку Антивирусу Касперского.
3. Антивирус обрабатывает почтовый трафик в соответствии с заданными параметрами и возвращает его почтовой программе с дополнительным набором уведомлений.
4. Почтовая программа осуществляет его дальнейшую маршрутизацию.

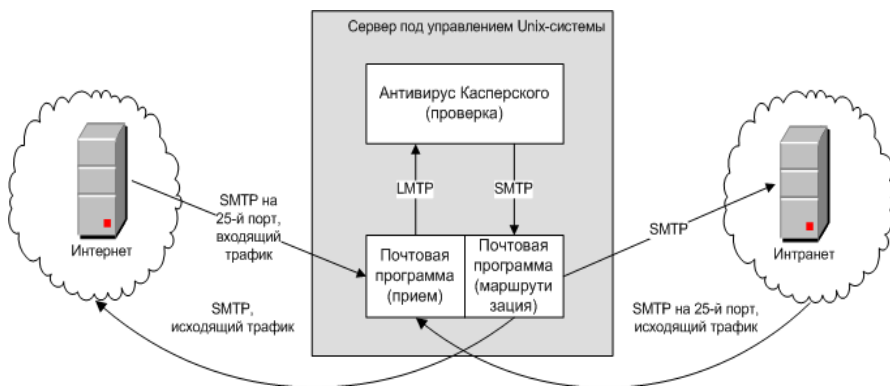


Рисунок 2. Схема работы Антивируса Касперского на одном сервере с почтовой программой

Исходя из приведенной схемы работы при установке Антивируса Касперского, вам необходимо выполнить следующую настройку параметров (в процессе установки либо сразу после нее):

- Определить порт, на котором будет работать Антивирус Касперского.
- Определить порт почтовой программы, на который она будет принимать почту от Антивируса Касперского после фильтрации.

2.3. Работа на выделенном сервере

Проверку и антивирусную обработку почтового трафика с помощью Антивируса Касперского для Linux и FreeBSD Mail Servers можно выполнять и в том случае, если ваш почтовый сервер работает под управлением другой операционной системы, например, Microsoft Windows Server 2003.

В такой ситуации Антивирус Касперского устанавливается на отдельный сервер под управлением операционной системы Linux и FreeBSD.

Для обеспечения приема трафика и его пересылки почтовому Windows-серверу на выделенный сервер устанавливается одна из почтовых программ – Sendmail, Qmail, Postfix или Exim. Затем устанавливается Антивирус Касперского и выполняется интеграция с ним почтовой программы (см. п. 4.4 на стр. 26).

При такой схеме имеет место следующая последовательность работы (см. рис. 3):

- Почтовый трафик поступает на сервер под управлением операционной системы семейства Unix.
- Почтовая программа (например, Postfix) направляет его на обработку Антивирусу Касперского по протоколу LMTP или SMTP.
- Проверенная почта с уведомлениями, сформированными Антивирусом, передается обратно почтовой программе, которая в свою очередь направляет ее на основной почтовый сервер для доставки или дальнейшей маршрутизации.

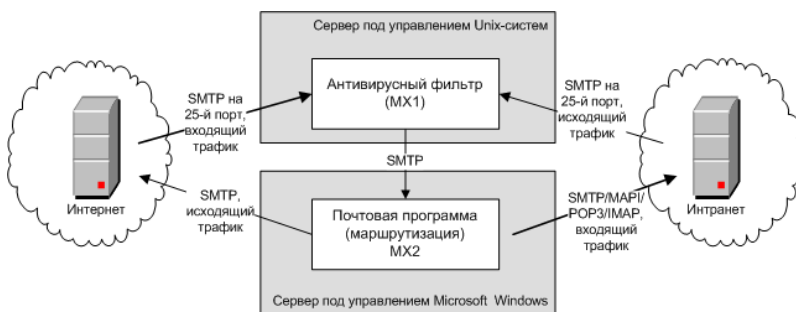


Рисунок 3. Схема работы Антивируса Касперского на выделенном сервере

В приведенной схеме сервер с Антивирусом Касперского является основным сервером, поскольку осуществляет прием потока почтовых сообщений и его пересылку, а сервер с Microsoft Exchange Server – дополнительным, выполняющим только доставку.

Если же до установки Антивируса Касперского ваш почтовый сервер выполнял проверку писем по IP-адресу отправителя, то сервер с Антивирусом Касперского необходимо использовать в качестве дополнительного. Причина состоит в следующем: если сервер с Антивирусом сделать основным, то все почтовые сообщения на дополнительный сервер (с проверкой по IP-адресу) будут поступать с одного IP-адреса, соответственно, проверка станет невозможной.

Если внутри вашей локальной сети есть почтовые серверы, то MX-записи или параметры пересылки должны указывать на основной сервер, а не на дополнительный.

- Настройка основного фильтра (MX1):
 - Имя сервера, на котором установлен фильтр: mx1.yourhost.domain.
 - Имя сервера для пересылки почты: mx2.yourhost.domain:25.
- Настройка дополнительного фильтра (MX2):
 - Имя сервера, на котором установлен фильтр: mx2.yourhost.domain.
 - Имя сервера, от которого принимается почта: mx1.yourhost.domain.

ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

Прежде чем приступить к установке Антивируса Касперского для Linux и FreeBSD Mail Servers, рекомендуется выполнить подготовку вашей системы:

- Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. п. 1.2 на стр. 9). Если не установлены какие-либо из приложений, следует установить их, иначе часть функциональности приложения будет недействительна.
- Сделать резервные копии конфигурационных файлов почтовой программы, установленной на вашем сервере.
- Настроить интернет-соединение.
- **Остановить работу почтового сервера**, с которым планируется интеграция Антивируса Касперского.
- Войти в систему с правами пользователя **root**.

Установку приложения рекомендуется выполнять в то время, когда поток почтовых сообщений наименьший!

3.1. Установка приложения на сервер под управлением Linux

Антивирус Касперского распространяется в двух вариантах пакетов установки: `rpm` или `deb`.

Для запуска установки Антивируса Касперского из `rpm`-пакета в командной строке введите:

```
# rpm -i <имя_файла_дистрибутива>
```

Для запуска установки Антивируса Касперского из `deb`-пакета в командной строке введите:

```
# dpkg -i <имя_файла_дистрибутива>
```

3.2. Установка приложения на сервер под управлением FreeBSD

Для серверов, работающих под управлением операционной системы FreeBSD, дистрибутив Антивируса Касперского поставляется в `pkg`-пакете.

Для запуска установки Антивируса Касперского из `pkg`-пакета в командной строке введите:

```
# pkg_add <имя_пакета>
```

3.3. Процесс установки

По ряду причин установка может завершиться с ошибкой. В этом случае убедитесь, что ваш компьютер соответствует аппаратным и программным требованиям (см. п. 1.2 на стр. 9), и что вход в систему выполнен с правами пользователя **root**.

Установка приложения на сервер включает в себя несколько этапов:

1. Копирование файлов дистрибутива на сервер.
2. Установка ключа.

Если ключ не установлен, работа с приложением невозможна. Если ключ временно отсутствует (например, приложение приобретено через интернет, и ключ еще не получен по электронной почте), можно установить его не в процессе установки, а позже, непосредственно перед началом использования приложения.

3. Конфигурация компонента *keepup2date*.
4. Обновление баз Антивируса Касперского.

Не забудьте обновить базы Антивируса Касперского после установки приложения. Базы содержат описание всех известных на настоящий момент вирусов и способов лечения зараженных ими объектов. Без баз Антивируса Касперского проверка и обработка файлов невозможна.

В случае если базы Антивируса Касперского не будут установлены, автоматическая конфигурация приложения не будет выполнена.

5. Установка модуля Webmin.

Модуль удаленного управления к пакету Webmin будет установлен при условии, что Webmin расположен в стандартном каталоге. После установки модуля будут даны соответствующие рекомендации по настройке его совместной работы с приложением.

3.4. Конфигурация приложения

Сразу по завершении копирования файлов дистрибутива на сервер выполняется конфигурация системы. В зависимости от используемого менеджера пакетов этап конфигурации будет запущен автоматически либо (в случае если менеджер пакетов не допускает использование интерактивных скриптов, как, например, rpm) потребует от администратора некоторых дополнительных действий. В таком случае на экран будет выведено соответствующее сообщение.

Процесс конфигурации приложения включает в себя:

- Поиск установленного почтового сервера и проверка его версии на соответствие программным требованиям.
- Поиск и изменение конфигурационного файла почтового сервера.

Если при конфигурации системы возникнет необходимость запроса каких-либо дополнительных сведений (например, пути к конфигурационному файлу почтового сервера), то на консоль сервера будут выведены соответствующие запросы. В случае ввода некорректных ответов процесс конфигурации будет прерван.

Если все описанные выше шаги конфигурации завершились успешно, приложение готово к работе, и дополнительное оповещение не производится. Конфигурационный файл, входящий в поставку приложения, содержит все необходимые для начала работы параметры.

Перезагрузите почтовый сервер перед началом работы.

ГЛАВА 4. НАСТРОЙКА ПРИЛОЖЕНИЯ ПОСЛЕ УСТАНОВКИ

В процессе установки выполняется анализ системы, на которую устанавливается Антивирус Касперского, в результате чего некоторые параметры его конфигурации определяются автоматически. Ряд параметров конфигурационного файла приложения определен по умолчанию как наиболее удобный для работы с Антивирусом (см. п. 4.1 на стр. 23).

Прежде чем приступить к работе с приложением, следует обновить базы Антивируса Касперского, если это не было сделано во время установки приложения. Также следует проверить на наличие вирусов файловые системы сервера.

Для начала работы с приложением необходимо:

- выполнить интеграцию Антивируса Касперского с почтовой программой, установленной на вашем сервере (см. п. 4.4.5 на стр. 30);
- сформировать список защищаемых доменов, почтовые сообщения которых будут подвергаться проверке на наличие вирусов и, при необходимости, дальнейшему лечению (см. п. 5.4.1 на стр. 51).

Также рекомендуется настроить совместную работу Антивируса Касперского с пакетом Webmin.

В данной главе рассмотрены параметры Антивируса Касперского, принятые по умолчанию, а также описана необходимая для работы с приложением конфигурация.

В приведенных ниже примерах пути к файлам указаны для дистрибутивов Linux.

4.1. Настройка приложения по умолчанию

Все параметры функционирования Антивируса Касперского для Linux и FreeBSD Mail Servers хранятся в конфигурационном файле, который по умолчанию имеет имя *kav4mailservers.conf*.

Вы можете создавать и использовать собственные конфигурационные файлы.

Ниже перечислены параметры конфигурационного файла, принятые по умолчанию. Информация о дополнительных параметрах, которые могут понадобиться для работы с приложением, представлена в другом разделе (см. Глава 6 на стр. 56).

По умолчанию лечение зараженных файлов не выполняется: зараженные файлы удаляются без лечения.

АНТИВИРУСНАЯ ЗАЩИТА ПОЧТОВОГО ТРАФИКА СЕРВЕРА

До интеграции Антивируса Касперского с почтовой программой антивирусная защита почтового трафика невозможна. Рассмотренные далее параметры определяют работу Антивируса Касперского по умолчанию при условии выполненной интеграции.

Секция **[smtpscan.group:default]** конфигурационного файла *kav4mailservers.conf* определяет наличие группы **default**, справедливой для всех защищаемых пользователей почтового сервера, для которых не определены особые правила проверки. В группе зафиксированы следующие правила антивирусной проверки и обработки почтового трафика:

- Проверяются входящие и исходящие почтовые сообщения.
- При обнаружении зараженных почтовых сообщений выполняется их лечение.

Вылеченные почтовые сообщения доставляются получателям и администратору группы (по умолчанию на адрес *postmaster@localhost*) и сопровождаются уведомлениями о том, что сообщения были заражены вирусами и успешно вылечены. Аналогичные уведомления отправляются и отправителям сообщений.

Если сообщение вылечить не удалось, оно удаляется, а отправителю, администратору группы и получателю направляется соответствующее уведомление.

Все уведомления, имеющие отношение к проверке почтовых сообщений, их лечению и другим действиям с почтой (удалению, отправке на карантин и т. д.), по умолчанию отправляются с адреса `MAILER-DAEMON@localhost`.

- Если в процессе антивирусной проверки почтового трафика обнаруживаются подозрительные и/или поврежденные файлы, а также почтовые сообщения, в результате проверки которых произошла ошибка, они удаляются. Отправителю, получателю и администратору группы отправляются соответствующие уведомления.
- Все действия приложения фиксируются в журнале событий.

Для антивирусной проверки почтового трафика должен быть запущен процесс `aveserver`. В случае если процесс не запущен, вся поступающая почта сохраняется в очереди на проверку и обработку. Информация об этом фиксируется в журнале событий приложения. Подробнее о работе процесса `aveserver` см. п. 6.4 на стр. 69.

АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВЫХ СИСТЕМ СЕРВЕРА

По умолчанию конфигурация Антивируса Касперского выполнена таким образом, что при запуске компонента антивирусной защиты (`kavscanner`) без дополнительных ключей командной строки осуществляется *антивирусная проверка* файловых систем сервера рекурсивно, начиная с текущего каталога.

При обнаружении зараженных, подозрительных или поврежденных файлов на консоль и в журнал событий заносятся соответствующие сообщения.

4.2. Установка / обновление баз Антивируса Касперского

Сразу после установки приложения на сервер необходимо установить базы Антивируса Касперского или обновить их, если они были установлены.

Для этого запустите компонент `keepup2date`:

```
# /opt/kav/5.5/kav4mailservers/bin/keepup2date
```

Базы будут скопированы с серверов обновлений «Лаборатории Касперского» и размещены в специальном каталоге, указанном в конфигурационном файле.

Специалисты «Лаборатории Касперского» рекомендуют обновлять базы каждый час, поскольку для эффективной работы приложения, необходимо поддерживать его в актуальном состоянии (подробнее об обновлении приложения см. в пп. 5.1.2 - 5.1.3 на стр. 32 - 35).

4.3. Использование webmin-модуля для управления Антивирусом Касперского

Если предполагается удаленное управление Антивирусом Касперского, то необходимо настроить его совместную работу с утилитой Webmin.

Например, средствами Webmin можно ограничить доступ к работе с приложением, организовав систему паролей для пользователей (подробнее о настройке параметров утилиты Webmin см. документацию по данному продукту).

Настройка параметров Антивируса, выполненная удаленно посредством утилиты Webmin, сохраняется в конфигурационном файле приложения, используемом по умолчанию.

Если вы хотите создать альтернативный конфигурационный файл с помощью утилиты Webmin, вам необходимо:

- Скопировать данные из существующего конфигурационного файла в новый, который необходимо сохранить под другим именем. После этого необходимо провести корректировку нового (альтернативного) конфигурационного файла в соответствии с поставленными задачами.
- Указать имя альтернативного конфигурационного файла на закладке **Config edit** в поле **Full path to KAV config**.

4.4. Выполнение интеграции с почтовыми программами вручную

Если интеграция не была выполнена при установке Антивируса Касперского (см. п. 3.4 на стр. 21), вы можете выполнить ее вручную.

Процесс интеграции заключается в настройке совместной работы почтовой программы с Антивирусом Касперского (см. п. 4.4.1-4.4.4 на стр. 26-29), настройке параметров приложения для работы с почтовой программой (см. п. 4.4.5 на стр. 30) и запуске почтовой программы с новой конфигурацией.

Пользователь, с правами которого запускается и работает почтовая программа, должен обладать правами на чтение конфигурационных файлов соответствующей почтовой программы.

Рассмотрим подробнее интеграцию Антивируса Касперского с почтовыми программами, выполненную вручную.

4.4.1. Интеграция с почтовой программой Sendmail

Чтобы настроить совместную работу Антивируса Касперского с почтовой программой *Sendmail*, необходимо:

1. Скопировать файл *sendmail.cf* в файл *sendmail.cf.listen*.
2. Создать в файле *sendmail.cf.listen* правило:

```
SParseLocal=98
R$*[символ_табуляции] $#smtpscanner $@$1 $:$1
```

3. Добавить в файл описание *smtpscanner*.

```
Msmtpscanner,
P= /opt/kav/5.5/kav4mailservers/bin/smtpscanner,
F=PCXmnz9, S=EnvFromSMTP, R=EnvToSMTP,
E=\r\n, L=2040,
T=SMTP,
A=smtpscanner
```

4. Настроить необходимые для интеграции параметры Антивируса Касперского (см. п. 4.4.5 на стр. 30).
5. Добавить в скрипты автоматического запуска процессов (start-up) два процесса:

```
/usr/sbin/sendmail -bd -q10m -C \  
/etc/mail/sendmail.cf.listen  
/usr/sbin/sendmail -C /etc/mail/sendmail.cf
```

При использовании почтовой программы Sendmail версии 8.12 или выше в конфигурации с *submit.cf* следует добавить в скрипты автоматического запуска следующие процессы:

```
/usr/sbin/sendmail -bd -q10m \  
-C /etc/mail/sendmail.cf.listen  
/usr/sbin/sendmail \  
-C /etc/mail/sendmail.cf  
/usr/sbin/sendmail -C /etc/mail/submit.cf
```

- После интеграции Антивируса Касперского с почтовой программой Sendmail используйте для запуска почтовой системы и антивирусной проверки почтовых сообщений скрипт *kavsendmail.sh*, входящий в поставку приложения.

4.4.2. Интеграция с почтовой программой Qmail

Компонент *smtpscanner* Антивируса Касперского при интеграции с почтовой программой **Qmail** заменяет собой программу *qmail-queue*. Для отправки сообщений и помещения их в очередь компонент *smtpscanner* вызывает оригинальную программу *qmail-queue*.

Чтобы настроить совместную работу Антивируса Касперского с почтовой программой **Qmail**, необходимо:

1. Переименовать файл *qmail-queue* в *queue.kav55* в каталоге */var/qmail/bin/*.
2. Скопировать файл *qmail-queue* из каталога */opt/kav/5.5/kav4mailservers/bin/* в каталог */var/qmail/bin* или создать на этот файл ссылку.
3. Задать для файлов *qmail-queue* и *queue.kav55* следующие права доступа:

```
16 -rws-x-x    1 qmailq    qmail          12688 Mar 24
13:56 queue.kav55
316 -rwx-x-x    1 qmailq    qmail          315612 Apr 14
11:29 qmail-queue
```

4. Настроить необходимые для интеграции параметры Антивируса Касперского (см. п. 4.4.5 на стр. 30).
5. Перезапустить почтовую программу.

Если в почтовой программе Qmail используется утилита *softlimit*, следует увеличить в ней размер доступной памяти (либо отключить ограничение размера), иначе возможны затруднения при проверке почтовых сообщений большого размера.

4.4.3. Интеграция с почтовой программой Postfix

Чтобы настроить совместную работу Антивируса Касперского с почтовой программой Postfix, необходимо:

1. Добавить в конфигурационный файл почтовой программы Postfix *main.cf* следующую строку:
`content_filter = lmtp:localhost:10025`
2. Добавить в конфигурационный файл почтовой программы Postfix *master.cf* следующие строки:

```
localhost:10025    inet    n        n        n        -
                  10      spawn  user=kluser
                  argv=/opt/kav/bin/smtpscanner
localhost:10026    inet    n        -        n        -
                  10      smtpd  -o content_filter=-o
myhostname=localhost
```
3. Создать каталог **/var/spool/filter**.
4. Создать пользователя **kluser**, включить его в группу **filter** с домашним каталогом **/var/spool/filter**.
5. Изменить права на каталог **/var/spool/filter** (*smtpscanner* будет работать с правами пользователя **kluser**):

```
mkdir /var/spool/filter
groupadd filter
useradd kluser -s /bin/false -d /var/spool\
/filter -g filter
chown kluser.filter /var/spool/filter
```

6. Настроить необходимые для интеграции параметры Антивируса Касперского (см. п. 4.4.5 на стр. 30).
7. Перезапустить почтовую программу.

4.4.4. Интеграция с почтовой программой Exim

Чтобы настроить совместную работу Антивируса Касперского с почтовой программой Exim, необходимо:

1. Скопировать конфигурационный файл, обычно *exim.conf*, в файл *exim.conf.listen*.
2. Отредактировать файл *exim.conf.listen*:
 - в секцию TRANSPORT CONFIGURATION добавить следующие строки:

```
kav_lmtp_transport:  
driver=lmtp  
command=/opt/kav/bin/smtpscanner
```
 - в секции ROUTERS CONFIGURATION определить параметры локальной доставки почты:

```
localuser:  
driver=accept  
transport=kav_lmtp_transport
```

задать параметры удаленной доставки почты:

```
lookuphost:  
driver=dnslookup  
transport=kav_lmtp_transport
```
3. Настроить необходимые для интеграции параметры Антивируса Касперского (см. п. 4.4.5 на стр. 30).
4. Добавить в скрипты автоматического запуска процессов (start-up) два процесса:

```
exim -q10m -bd -C /etc/exim/exim.conf.listen  
exim -C /etc/exim/exim.conf
```

При необходимости запуска компонента *smtpscanner* с правами другого пользователя следует скомпилировать почтовую программу Exim с определенными переменными EXIM_GID и EXIM_UID (подробнее см. документацию по почтовой программе Exim).

После интеграции Антивируса Касперского с почтовой программой Exim используйте для запуска почтовой системы и антивирусной проверки почтовых сообщений скрипт *kavexim.sh*, входящий в поставку приложения.

4.4.5. Настройка параметров Антивируса Касперского для интеграции с почтовой программой

Для того чтобы выполнить интеграцию Антивируса Касперского с почтовой программой, необходимо также настроить его собственные параметры.

Настройка параметров производится непосредственно в конфигурационном файле приложения.

Чтобы настроить Антивирус Касперского для работы с почтовой программой, необходимо:

- Указать адрес, с которого буду отправляться уведомления:

`NotifyFromAddress=<почтовый_адрес>`

- Задать параметры получения и отправки почты в секции **[smtpscan.general]**. Параметры задаются в следующем виде: **протокол:хост:порт**, где:
 - **протокол** – название протокола, по которому будет осуществляться доставка почтовых сообщений для антивирусной проверки (**LMTP**, **SMTP** или **qmail**);
 - **сервер** – имя хоста или его IP-адрес, с которого будет отправляться почта, или имя почтовой программы;
 - **порт** – номер порта (по умолчанию – 25).

Например, строка может иметь следующий вид: **smtp:localhost:25** или **lmtp:(local.mail -l)**

- Для Sendmail:

`ForwardMailer=smtp: (/usr/sbin/sendmail -bs \`
`-C /etc/mail/sendmail.cf)`

- Для Qmail:
`ForwardMailer=qmail: (/var/qmail/bin/qmail-queue)`
- Для Postfix:
`ForwardMailer=smtp:localhost:10026`
- Для Exim:
`ForwardMailer=smtp: (exim -bs \`
`-C/etc/exim/exim.conf)`
- Указать для группы пользователей в секции конфигурационного файла **[smtpscan.group:default]** следующие параметры:
`AdminAddress=<почтовый_адрес>`
`AdminNotify=yes`
- Задать максимальное время проверки объекта (в секундах) в секции **[smtpscan.limits]**. Например:
`MaxCheckTime=60`

ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

Посредством Антивируса Касперского вы можете организовать полную антивирусную защиту вашего сервера: от отдельного файла, хранящегося на сервере, до входящего и исходящего почтового трафика, включая почту с внешних почтовых сервисов.

Антивирус Касперского позволяет создавать задачи, с помощью которых администратор может управлять работой приложения. Все задачи можно разделить на три группы:

1. Обновление баз Антивируса Касперского, используемых для поиска вирусов и лечения зараженных объектов.
2. Антивирусная защита почтового потока сообщений сервера.
3. Антивирусная защита файловых систем сервера.

Каждая такая группа включает более конкретные задачи, реализующие ту или иную функциональность приложения. Далее будут рассмотрены наиболее актуальные задачи: настройка параметров задач и их запуск из командной строки.

Прежде чем запускать задачи, связанные с антивирусной проверкой почты, необходимо запустить процесс *aveserver*, если он не был запущен при старте операционной системы.

5.1. Обновление баз Антивируса Касперского

Неотъемлемой частью антивирусной защиты является обновление баз Антивируса Касперского, проводимое компонентом *keepup2date*. Источником обновлений баз, используемых Антивирусом Касперского в процессе поиска и лечения зараженных объектов, являются серверы обновлений «Лаборатории Касперского». Например:

<http://downloads1.kaspersky-labs.com/updates/>

<http://downloads2.kaspersky-labs.com/updates/>

<http://downloads1.kaspersky-labs.com/updates/> и другие.

Список серверов, с которых можно копировать обновления, приведен в файле *updcfg.xml*, включенном в поставку приложения. Этот список периодически обновляется в автоматическом режиме.

Самостоятельное редактирование файла *updcfg.xml* запрещено!

В процессе обновления компонент *keepup2date* обращается к данному списку, выбирает сервер и пытается скачать с него базы Антивируса. Если выполнить обновление с выбранного сервера невозможно, то компонент обращается по следующему адресу сервера и вновь пытается обновить базы. После успешного обновления по умолчанию происходит автоматическая перезагрузка приложения (параметр **PostUpdateCmd** секции **[updater.options]**).

Все параметры компонента *keepup2date* сгруппированы в секциях **[updater.*]** конфигурационного файла.

Если структура локальной сети достаточно сложная, рекомендуется скачивать обновления с серверов обновлений, размещать их в некотором сетевом каталоге, а для локальных компьютеров сети настроить копирование баз из этого каталога.

Настоятельно рекомендуется обновлять базы Антивируса Касперского каждый час!

Обновление может быть организовано по расписанию с помощью сервиса **cron** (см. п. 5.1.2 на стр. 34) или же выполняться по требованию администратора из командной строки (см. п. 5.1.3 на стр. 35).

5.1.1. Обновление баз Антивируса Касперского с серверов обновлений

Обновление баз Антивируса Касперского может проводиться из нескольких источников обновлений.

Для того чтобы настроить обновление баз с одного из серверов обновлений «Лаборатории Касперского», список которых содержится в отдельном файле, необходимо:

Присвоить параметру **UseUpdateServerUrl** секции **[updater.options]** значение **no**.

Для того чтобы настроить обновление баз Антивируса Касперского с сервера, указанного пользователем, а в случае невозможности – прервать процесс обновления, необходимо:

Присвоить параметрам **UseUpdateServerUri** и **UseUpdateServerUriOnly** секции **[updater.options]** значение **yes**. Параметр **UpdateServerUri** должен содержать адрес сервера обновлений.

Для того чтобы настроить обновление баз Антивируса Касперского с сервера, указанного пользователем, а в случае невозможности – обновить базы с сервера, указанного в списке серверов обновлений компонента keepip2date, необходимо:

Присвоить параметру **UseUpdateServerUri** секции **[updater.options]** значение **yes**, а параметру **UseUpdateServerUriOnly** значение **no**. Параметр **UpdateServerUri** должен содержать адрес сервера обновлений.

5.1.2. Планирование обновлений баз Антивируса Касперского с помощью сервиса cron

Вы можете спланировать регулярное автоматическое обновление баз Антивируса Касперского при помощи сервиса **cron**.

Пример:

Необходимо задать автоматическое обновление баз Антивируса Касперского каждые три часа. Установить случайный выбор сервера обновлений. В системном журнале фиксировать только ошибки при обновлении. Вести общий журнал по всем запускам задачи, на консоль информацию не выводить.

Для реализации поставленной задачи следует:

1. Задать следующие значения для параметров в конфигурационном файле приложения:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=1
```

2. Выполнить команду:

```
# crontab -e
```

и отредактировать список инструкций демона **cron**, добавив следующую строку:

```
0 */3 * * * /opt/kav/5.5/kav4mailservers/bin/keepup2date
```

5.1.3. Разовое обновление баз Антивируса Касперского

Обновление баз Антивируса Касперского можно запустить в любой момент из командной строки.

Пример:

Необходимо запустить обновление баз Антивируса Касперского, сохранив результаты работы в файле */tmp/updatesreport.log*.

Для реализации поставленной задачи в командной строке необходимо запустить компонент *keepup2date* следующим образом:

```
# keepup2date -l /tmp/updatesreport.log
```

5.1.4. Создание и использование локального источника обновлений

Так как сайты-источники обновлений баз «Лаборатории Касперского» имеют сложную структуру, то при настройке обновления локальных компьютеров вашей сети из некоторого сетевого каталога необходимо в нем создать аналогичную файловую структуру.

Пример:

Необходимо снизить сетевой трафик при обновлении баз Антивируса Касперского.

Для реализации поставленной задачи следует создать сетевой каталог, откуда базы будут копироваться на локальные компьютеры сети. Для этого необходимо:

1. Создать локальный каталог.
2. Запустить компонент *keepup2date*:

```
# keepup2date -u rdir
```

где *rdir* – полный путь к созданному каталогу.
3. Предоставить для локальных компьютеров сетевой доступ к данному каталогу.

Возможность копировать обновления из сетевого каталога доступна для приложений «Лаборатории Касперского» только версий 5.0 и 5.5.

В случае если необходимо обновить базы Антивируса Касперского на нескольких компьютерах, можно настроить получение обновлений из сетевого каталога. Такая организация удобна тем, что вместо многократного получения баз через интернет, можно скачать их один раз и поместить в каталог общего доступа, из которого обновления будут доступны для всех остальных компьютеров.

Пример:

Необходимо организовать обновление баз из локального каталога **/mnt/bases**, а если этот каталог недоступен или пуст, то обновлять базы с серверов «Лаборатории Касперского». Результаты работы вывести в журнал событий.

Для реализации поставленной задачи следует:

1. Задать следующие значения для параметров в конфигурационном файле:

```
[updater.options]  
UpdateServerUrl=/mnt/bases  
UseUpdateServerUrl=yes  
UseUpdateServerUrlOnly=no
```

(либо воспользуйтесь ключом `-g /mnt/bases`)
2. Запустить компонент *keepup2date* следующим образом:

```
# keepup2date -l /tmp/report.txt
```

5.1.5. Обновление баз Антивируса Касперского при использовании прокси-сервера

Пример:

Необходимо настроить обновление баз, если выход в интернет производится через прокси-сервер.

Для реализации поставленной задачи следует:

1. Присвоить параметру **UseProxy** значение **yes** в секции **[updater.options]** конфигурационного файла.
2. Убедиться, что параметр **ProxyAddress** в секции **[updater.options]** конфигурационного файла содержит корректный адрес прокси-сервера. Адрес должен быть задан в формате: **http://username:password@ip_address:port**. При этом значения **ip_address** и **port** являются обязательными, а **username** и **password** задаются только в случае, если необходима аутентификация на прокси-сервере.

или:

1. Присвоить параметру **UseProxy** значение **yes** в секции **[updater.options]** конфигурационного файла.
2. Задать переменную окружения **http_proxy** в формате **http://username:password@ip_address:port**. Переменная будет учитываться только в том случае, если параметр **UseProxy** секции **[updater.options]** отсутствует или имеет значение **yes**.

5.2. Антивирусная защита почтового трафика сервера

Антивирусная фильтрация почтового трафика, будь то входящий или исходящий поток сообщений, является основной задачей Антивируса Касперского, реализуемой при помощи компонента *smtpscanner*.

Компонент *smtpscanner* обеспечивает защиту пользователей от зараженных писем, организует доставку незараженных и вылеченных сообщений с уведомлениями о результатах проверки каждого сообщения.

Реализация дополнительной проверки по типам вложенных файлов позволяет снизить нагрузку на сервер в процессе антивирусной обработки почтового потока.

Все параметры компонента *smtpscanner* сгруппированы в секциях **[smtpscan.*]** конфигурационного файла *kav4mailservers.conf*.

Далее мы рассмотрим наиболее распространенные задачи, реализующие антивирусную защиту почтового трафика.

Для антивирусной проверки почтового трафика должен быть запущен процесс *aveserver!*

5.2.1. Доставка незараженных и вылеченных почтовых сообщений

Такой способ конфигурации Антивируса Касперского осуществляется в том случае, если не предполагается разделения пользователей на группы отправителей-получателей. Это удобно, например, в ситуации, когда необходимо настроить доставку всем получателям исключительно незараженных и вылеченных почтовых сообщений.

Пример:

Необходимо:

- проверять весь почтовый трафик сервера на наличие вирусов и лечить все зараженные почтовые сообщения;
- удалять зараженные почтовые сообщения, которые не удалось вылечить;
- доставлять вылеченные сообщения получателям;
- уведомлять отправителей, получателей и администраторов о вылеченных, удаленных, подозрительных и поврежденных почтовых сообщениях, а также об объектах, в результате проверки которых произошла ошибка; к уведомлениям администратора прикреплять зараженные объекты без изменений;
- фиксировать результаты работы в файле */tmp/report.log*.

Для реализации поставленной задачи следует:

1. Задать следующие параметры конфигурации для группы **default**:

```
[smtpscan.group:default]
Check=yes
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Подробнее о действиях над сообщениями см. п. 6.1.3 на стр. 60.

Параметры **Sender***, **Recipient*** и **Admin*** определяют правила работы с объектами всех типов, кроме **Clean**. Любое задание правил для конкретного объекта является более приоритетным. Например, в данном примере все типы объектов будут удаляться из письма получателя (**RecipientAction=remove**) кроме объекта **Cured** (**CuredRecipientAction=cured**).

2. Настроить запись отчета о результатах работы компонента в файл `/tmp/report.log`:

```
[smtpscan.report]
ShowOk=yes
ReportFileName=/tmp/report.log
ReportFilePermission=0660
```

5.2.2. Доставка всех сообщений

Возможно возникновение таких ситуаций, когда определенной группе получателей необходимо доставлять любые сообщения, в том числе и зараженные.

Пример:

Необходимо:

- проверять весь почтовый поток сообщений на присутствие вирусов;

- для всех получателей, кроме входящих в группу **urgent**, лечить все зараженные сообщения;
- почтовые сообщения, которые не удалось вылечить, а также подозрительные и поврежденные письма переносить в карантинный каталог для всех получателей, кроме входящих в группу **urgent**;
- отправлять уведомления отправителям, получателям и администраторам о заблокированных, вылеченных, удаленных, подозрительных и поврежденных почтовых сообщениях, а также об объектах, в результате проверки которых произошла ошибка; к уведомлениям администратора прикреплять зараженные объекты без изменений;
- получателям группы **urgent** доставлять все письма, в том числе и зараженные, с обязательным уведомлением о возможности их заражения вирусом.

Для реализации поставленной задачи следует:

1. Задать следующие параметры конфигурации для группы **default**:

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Подробнее о действиях над сообщениями см. п. 6.1.3 на стр. 60.

2. Настроить параметры группы **urgent** следующим образом:

```
[smtpscan.group:urgent]
Check=yes
Quarantine=no
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=unchanged
```

5.2.3. Доставка сообщений, содержащих защищенный паролем архив

Довольно часто возникает ситуация, когда почтовое сообщение содержит вложение в виде защищенного паролем архива. Антивирус Касперского не лечит зараженные файлы из архива, защищенного паролем (подробнее об этом см. п. 5.3.3.1 на стр. 47). Поэтому по умолчанию приложение доставляет письма, содержащие защищенные паролем архивы, без проверки. При этом формируется письмо-уведомление о том, что данный архив не был проверен. По умолчанию уведомление направляется получателю письма и администратору.

Для отключения отправления уведомлений о доставке непроверенного архива необходимо:

- Присвоить параметру **ProtectedRecipientAttachReport** значение **no** (в секции **[smtpscan.group:default]** конфигурационного файла приложения). Отправление уведомлений о сообщениях, содержащих защищенный паролем архив, получателю будет отключено.
- Присвоить параметру **ProtectedAdminNotify** значение **no** (в секции **[smtpscan.group:default]** конфигурационного файла приложения). Отправление уведомлений о сообщениях, содержащих защищенный паролем архив, администратору группы будет отключено.

5.2.4. Блокирование доставки сообщений

Зачастую администратору необходимо блокировать поступление некоторых почтовых сообщений получателям.

Например, почтовое сообщение подозревается на заражение вирусом, но содержит важные данные, которые необходимо сохранить. В процессе лечения данные могут быть потеряны. В такой ситуации лучше изолировать почтовое сообщение и, например, отправить его на исследование специалистам «Лаборатории Касперского».

Пример:

Необходимо:

- проверять весь почтовый трафик сервера на присутствие вирусов и лечить все зараженные почтовые сообщения;
- блокировать доставку зараженных, подозрительных, поврежденных и защищенных паролем почтовых сообщений, а также сообщений, в результате проверки которых произошла ошибка; помещать объекты на карантин;
- доставлять адресатам только вылеченные сообщения;
- уведомлять отправителей, получателей и администраторов о заблокированных, вылеченных, удаленных, подозрительных и поврежденных почтовых сообщениях, а также об объектах, в результате проверки которых произошла ошибка; к уведомлениям администратора прикреплять зараженные объекты без изменений.

Для реализации поставленной задачи следует:

Задать в конфигурационном файле *kav4mailservers.conf* следующие параметры:

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
```

```
RecipientAction=remove  
CuredRecipientNotify=yes  
CuredRecipientAttachReport=yes  
CuredRecipientAction=cured
```

Подробнее о действиях над сообщениями см. п. 6.1.3 на стр. 60.

5.2.5. Дополнительная проверка писем по типу вложений

Зачастую почтовые сообщения содержат файлы, которые имеют большую вероятность наличия вируса (например, ехе-файлы). Во избежание заражения специалисты «Лаборатории Касперского» рекомендуют организовать фильтрацию почтового трафика по имени и/или типу таких объектов, и помещать их в отдельный каталог для дальнейшего изучения.

Пример:

- для группы пользователей **users**:
 - проверять почтовые сообщения группы на присутствие вирусов;
 - фильтровать почту по вложенным ехе-файлам; выбранные сообщения помещать на карантин;
 - лечить зараженные почтовые сообщения; если попытка лечения объекта не удалась – удалять его из письма получателя, но доставлять в неизменном виде администратору группы;
 - уведомлять о помещенных на карантин объектах администратора группы и получателей;
 - отправлять администратору, получателям и отправителям уведомления об удаленных, зараженных, поврежденных, защищенных паролем объектах, а также почтовых сообщениях, в результате проверки которых произошла ошибка.
- для всех остальных получателей:
 - проверять весь почтовый трафик сервера на присутствие вирусов и лечить все зараженные почтовые сообщения;
 - помещать на карантин зараженные объекты, которые не удалось вылечить, а также подозрительные, поврежденные

письма и объекты, в результате проверки которых произошла ошибка;

- доставлять вылеченные сообщения получателям;
- доставлять получателю защищенные паролем файлы с уведомлением о возможности их заражения вирусом;
- уведомлять отправителей, получателей и администратора об удаленных, зараженных, поврежденных, помещенных на карантин, а также почтовых сообщениях, в результате проверки которых произошла ошибка; к уведомлениям администратора прикреплять все виды объектов без изменений.

Для выполнения поставленной задачи следует:

1. Настроить параметры группы **users**:

```
[smtpscan.group:users]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
FilterByName=.*\.exe$
FilteredQuarantine=yes
FilteredRecipientNotify=yes
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
ProtectedRecipientNotify=yes
ProtectedRecipientAction=unchanged
ProtectedRecipientAttachReport=no
ProtectedSenderNotify=no
ProtectedAdminNotify=no
```

Подробнее о действиях над объектами см. п. 6.1.3 на стр. 60.

2. Настроить параметры группы **default**:

```
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
AdminAddress=<почтовый_адрес>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=no
RecipientAction=remove
ProtectedRecipientNotify=yes
ProtectedRecipientAttachReport=yes
ProtectedRecipientAction=unchanged
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Подробнее о создании списка групп пользователей см. п. 6.1.1 на стр. 58.

5.3. Антивирусная защита файловых систем

Антивирусная защита файловых систем сервера выполняется при помощи компонента *kavscanner*, который проверяет файлы сервера на присутствие вирусов и выполняет обработку зараженных и подозрительных объектов в соответствии с заданными параметрами работы. Обработка объектов может носить как сугубо информационный характер (вывод информации в журнал событий и на консоль сервера, уведомления администратора), так и приводить к изменению объекта (лечение, помещение на карантин, удаление).

Все параметры компонента *kavscanner* сгруппированы в секциях **[scanner.*]** конфигурационного файла *kav4mailservers.conf*.

Проверка файловых систем сервера может быть запущена один раз по выбору из командной строки, либо по расписанию с помощью сервиса **cron**. Вы можете задавать проверку как всех файловых систем сервера, так и отдельного каталога или файла.

Проверка всего сервера на присутствие вирусов – очень ресурсоемкая процедура. При ее запуске скорость работы будет замедлена, следовательно, не рекомендуется параллельно запускать какие-либо процессы. Во избежание таких проблем рекомендуется проверять отдельные каталоги.

5.3.1. Проверка файлов по выбору

Одной из задач, решаемых Антивирусом Касперского, является проверка на присутствие вирусов и лечение файлов отдельного каталога сервера.

Пример:

Необходимо запустить рекурсивную проверку каталога **/tmp** с лечением всех зараженных объектов. Объекты, вылечить которые не удалось, удалить.

Результаты работы компонента (дату запуска, информацию обо всех файлах, кроме незараженных, с детализацией) выводить только в журнал событий *kavscanner-текущая_дата.log*, который сохранять в том же каталоге.

Чтобы реализовать поставленную задачу в командной строке, следует запустить компонент *kavscanner* следующим образом:

```
# kavscanner -Rlq -okavscanner-`date +%F`.log -i3\ -ePASBME -j3 -mCn /tmp
```

Если в результате проверки архива внутри него будет обнаружен зараженный объект, будет удален весь архив!

5.3.2. Планирование проверки каталога с помощью сервиса cron

Проверка каталога по расписанию выполняется с помощью сервиса **cron**.

Пример:

Необходимо каждый день в 0 часов 00 минут запускать проверку на присутствие вирусов в каталоге **/home**; использовать параметры

проверки, заданные в конфигурационном файле `/etc/kav/kavscanner.conf`

Для реализации поставленной задачи следует:

1. Создать конфигурационный файл `/etc/kav/kavscanner.conf` со всеми необходимыми параметрами проверки.
2. Выполнить команду:

```
# crontab -e
```

и отредактировать список инструкций демона **cron**, добавив следующую строку:

```
0 0 * * */opt/kav/5.5/kav4mailservers/bin\  
/kavscanner -c /etc/kav/kavscanner.conf /home
```

5.3.3. Дополнительные возможности: использование скриптов

Антивирус Касперского предоставляет возможность дополнительной обработки объектов, прошедших антивирусный анализ, путем использования различных стандартных команд Unix, а также скриптов. При помощи таких средств опытные администраторы могут самостоятельно определять действия над объектами различных статусов и, таким образом, расширять функциональность Антивируса Касперского.

5.3.3.1. Лечение зараженных архивов

Для лечения зараженных архивов необходимо, чтобы на сервере были установлены утилиты для работы с соответствующими типами архивов.

Антивирус Касперского не лечит зараженные файлы, запакованные в архивы, он лишь обнаруживает в архивах подозрительные и зараженные объекты. Однако возможность лечения может быть реализована посредством дополнительного скрипта. Ниже приводится пример лечения архивов типа *tar*, *rar*, *tgz* и *zip* с помощью скрипта *vox.sh*. Данный скрипт включен в поставку Антивируса Касперского.

Пример:

Необходимо проверить все доступные на сервере архивы типа *tar* и *zip* и с помощью скрипта *vox.sh* попытаться вылечить все обнаруженные внутри архива зараженные объекты. В качестве конфигурационного файла использовать `/etc/kav/kavscanner.conf.in`, где

предварительно указать использование скрипта для лечения архивов.

Список всех зараженных объектов с полными путями к ним привести в файле `/tmp/infected_archive.lst`. Отчет о работе компонента вывести в файл `/tmp/logfile.log`.

Для реализации поставленной задачи следует:

1. Создать альтернативный файл `kavscanner.conf.in`.
2. Задать правила обработки зараженных объектов в секции **[scanner.container]**:

```
OnInfected=exec /opt/kav/5.5/kav4mailservers\
/ contrib/vox.sh %FULLPATH%/%FILENAME%
```

3. Запустить компонент `kavscanner` следующим образом:

```
# kavscanner -c kavscanner.conf.in -ePASE -qR\
-o /tmp/logfile.log -j3\
-pi/tmp/infected_archive.lst /
```

5.3.3.2. Отправка уведомлений администратору

Используя стандартные средства Unix, можно настроить отправку писем-уведомлений администратору сервера об обнаружении в файловых системах зараженных, подозрительных и поврежденных файлов.

Пример:

Необходимо настроить уведомление администратора об обнаружении в файловых системах сервера зараженных файлов и архивов при каждой проверке сервера, выполняемой в соответствии с параметрами конфигурационного файла приложения.

Для реализации поставленной задачи следует задать правила обработки простых объектов и объектов-контейнеров в конфигурационном файле приложения:

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is\
infected by %VIRUSNAME% | mail -s kavscanner\
admin@<почтовый_адрес>

[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME%\
is infected, viruses list is in the attached file\
```

```
%LIST% | mail -s kavscanner -a %LIST% \  
admin@<почтовый_адрес>
```

5.3.4. Помещение объектов на карантин

Работу Антивируса Касперского можно организовать так, что он будет помещать все зараженные объекты файловой системы сервера на карантин.

Например, такая возможность может быть использована, когда в процессе антивирусной проверки каталога был обнаружен зараженный файл, содержащий важные данные. При лечении часть данных может быть потеряна. Решением в такой ситуации может быть помещение зараженного объекта на карантин для, например, последующей его отправки в «Лабораторию Касперского» на экспертизу. Возможно, экспертам удастся вылечить файл и сохранить целостность содержащихся в нем данных. Также на карантин следует помещать подозрительные объекты.

Если каталог с изолированными объектами (карантин) предполагается хранить в структуре файловой системы сервера, рекомендуем исключить его из области проверки для последующих проверок, указав полный путь к нему в качестве значения параметра **ExcludeDir** конфигурационного файла. Объекты на карантине хранятся в зашифрованном виде и не могут повредить файловую систему компьютера.

Пример:

Необходимо проверить на присутствие вирусов все объекты, перечисленные в файле */tmp/download.lst*, и переместить обнаруженные зараженные объекты с полными путями к ним в каталог */tmp/infected*. Использовать эвристический анализатор кода; рекурсию отключить. Информацию о зараженных, а также подозрительных и поврежденных объектах вывести в журнал событий.

Для реализации поставленной задачи следует:

1. Задать в качестве действий над зараженными объектами в секциях **[scanner.object]** и **[scanner.container]** конфигурационного файла:

```
OnInfected=movePath /tmp/infected
```

2. Отключить режим лечения (**Cure=no**), если он был включен.
3. Запустить компонент *kavscanner* следующим образом:

```
# kavscanner -@/tmp/download.lst -ePASBME -rq\  
-i0 -o /tmp/report.log -j3 -mCn
```

Подробнее о действиях над файлами см. п. 6.2.3 на стр. 65.

Если необходимо задать в правиле обработки зараженных объектов несколько действий, перечислите их через символ «;» (см. пример ниже).

Пример:

Необходимо ограничить доступ к файлам каталога `/tmp/infected`, разрешив только их чтение и запись.

Для реализации поставленной задачи следует использовать стандартные инструменты Unix (команды **chown**, **chmod**). В качестве правила обработки зараженных объектов в секциях **[scanner.object]** и **[scanner.container]** (см. выше) конфигурационного файла измените описание действия следующим образом:

```
OnInfected=exec mv %FULLPATH%/%FILENAME%\
/tmp/infected/%FILENAME%; chmod -x\
/tmp/infected/%FILENAME%
```

5.3.5. Режим резервного копирования объектов

В случае если файлы оказались заражены, а в качестве действия над зараженными объектами определено их удаление, существует риск потери ряда важных данных. Чтобы избежать этого, в Антивирусе Касперского предусмотрена возможность копирования файлов в резервное хранилище.

Перед лечением или удалением файла его копия создается в резервном хранилище (секция **[scanner.path]**, параметр **BackupPath**). Это позволяет сохранить резервную копию (и, при необходимости, восстановить первоначальный файл) в случае, если сам файл будет поврежден в процессе лечения. Файлы хранятся в зашифрованном виде. При повторной записи в резервное хранилище ранняя копия файла автоматически заменяется более поздней.

По умолчанию режим сохранения в резервное хранилище не включен и, соответственно, путь к каталогу, в котором предполагается хранить резервные копии, не определен. Для использования данной возможности вам необходимо задать этот путь самостоятельно.

В случае удаления объекта его копия будет храниться в резервном хранилище до тех пор, пока ее не удалит администратор.

5.4. Управление ключами

Ключ дает вам право на использование приложения и содержит всю необходимую информацию, связанную с покупкой, такую как: тип ключа, дата окончания действия ключа, количество защищаемых пользователей или объем защищаемого трафика (зависит от типа ключа), информацию о дистрибьюторах и т. д.

Помимо прав на использование приложения в течение срока действия ключа вы приобретаете следующие возможности:

- круглосуточную техническую поддержку;
- ежечасное обновление баз Антивируса Касперского;
- обновление приложения (patch);
- получение новых версий приложения (upgrade);
- своевременное информирование о новых вирусах.

По окончании срока действия ключа вы автоматически лишаетесь приведенных выше возможностей. Антивирус Касперского по-прежнему будет осуществлять антивирусную обработку файловых систем сервера и почтового трафика, но только с использованием баз Антивируса Касперского, актуальных на дату окончания срока действия ключа. Администратору сервера будут направляться уведомления об окончании действия ключа. Функция обновления баз будет не доступна.

Поэтому крайне важно регулярно просматривать информацию, приведенную в ключе и отслеживать дату истечения срока его действия.

5.4.1. Механизм лицензирования

В Антивирусе Касперского версии 5.5 внедрена новая технология лицензирования. В процессе установки приложения на сервер администратору требуется задать список доменов, почта для которых будет защищаться. Лицензирование может производиться:

- по объему проверяемого трафика;
- по количеству защищаемых пользователей.

В первом случае лицензированным трафиком будет считаться суммарный размер принятых приложением сообщений, которые были проверены с помощью антивирусного ядра и получили статус **Clean** (то есть не содержали вирусов).

Во втором случае лицензированным пользователем считается любой отправитель и/или получатель сообщения, которое было проверено приложением.

За 14 дней до истечения срока действия ключа автоматически будет сформировано уведомление администратору об этом. Информирование производится с периодичностью раз в сутки, а также при каждом повторном запуске приложения.

Аналогичный механизм оповещений предусмотрен по окончании срока действия ключа, а также при исчерпании объема лицензированного трафика.

Однако если объем трафика будет превышать размер лицензируемого более чем на 10 процентов, уведомление об этом будет направляться администратору каждый раз при обнаружении сообщения со статусом, отличным от **Clean**.

Для корректной настройки механизма лицензирования необходимо:

Задать значение параметра **LicenseDomains** секции **[smtpscan.license]**. Этот параметр определяет маски защищаемых доменов. Необходимо указать в качестве значения данного параметра все почтовые домены, защищаемые Антивирусом Касперского. Домены должны быть заданы в формате POSIX regexr, и быть перечислены в одной строке через запятую.

Обратите внимание, что символ «.» имеет свое значение в формате POSIX regexr, поэтому его нужно экранировать символом «\».

5.4.2. Просмотр информации о ключе

Вы можете просматривать информацию об установленных ключах в отчетах о работе компонентов *kavscanner*, *keepup2date* и *aveserver*, поскольку при старте каждый из этих компонентов загружает информацию о ключах в журнал событий.

Помимо этого в Антивирусе Касперского предусмотрен специальный компонент *licensemanager*, позволяющий вам просматривать не только более полную информацию о ключах, но и получать некоторые дополнительные данные.

Так, если вы приобрели Антивирус Касперского с типом лицензирования **ПО ОБЪЕМУ ПОЧТОВОГО ТРАФИКА**, то компонент *licensemanager* позволяет отслеживать, какой объем трафика уже исчерпан, сколько МБ лицензированного почтового трафика осталось на текущую дату.

Вы можете также просматривать информацию об объеме обработанного в течение суток (по часам) трафика, и, таким образом, оценивать пики на-

грузки. Данная информация может пригодиться, например, для отправки в Службу технической поддержки, если возникнут проблемы с работой приложения.

В случае приобретения Антивируса с типом лицензирования **ПО КОЛИЧЕСТВУ ПОЛЬЗОВАТЕЛЕЙ** вы можете просматривать общее количество лицензированных пользователей, соответствующее количеству приобретенных ключей.

Вся перечисленная выше информация может быть выведена на консоль сервера.

Чтобы просмотреть информацию обо всех ключах, в командной строке запустите компонент `licensemanager`:

```
# licensemanager -s
```

Будет выведена информация следующего вида:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1998-2006.
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix Mail
Server", expires 04-07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Unix Mail Server
(licence per e-mail address)", expires 25-01-2004 in
234 days
```

Чтобы просмотреть информацию о конкретном ключе, в командной строке необходимо запустить компонент `licensemanager` с указанием имени файла ключа, например, следующим образом:

```
# licensemanager -k 0003D3EA.key
```

Будет выведена информация следующего вида:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1998-2006.
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Unix Mail Server", expires 04-07-2003 in 28 days
```

Для получения информации по лицензированному почтовому трафику или количеству защищаемых пользователей, в командной строке необходимо запустить компонент `licensemanager` с ключом `-i`:

```
# licensemanager -i
```

Будет выведена информация следующего вида:

- при типе лицензирования по количеству пользователей:

```
Kaspersky license manager for Linux. Version  
5.5.0/RELEASE #68  
Copyright (C) Kaspersky Lab, 1997-2006.  
Portions Copyright (C) Lan Crypto
```

```
License users units: 5  
Users units used: 0  
Users units left: 5
```

- при типе лицензирования по объему почтового трафика:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1998-2006.  
Daily traffic statistic(Bytes):  
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0  
License traffic units: 10 (MB)  
Traffic units used: 0 (MB)  
Traffic units left: 10 (MB)
```

5.4.3. Продление срока действия ключа

Продление срока действия ключа на использование Антивируса Касперского дает право на восстановление полной функциональности приложения. Также возобновляются и дополнительные услуги, приведенные в п. 5.3.5 на стр. 50.

Чтобы продлить срок действия ключа на использование Антивируса Касперского для Unix Mail Servers, необходимо:

связаться с компанией, у которой вы купили приложение, и продлить срок действия ключа на использование Антивируса Касперского.

или:

продлить срок действия ключа непосредственно в «Лаборатории Касперского», написав в Отдел продаж (sales@kaspersky.com) или заполнив соответствующую форму на нашем сайте (www.kaspersky.ru) в разделе **Продукты → Продлить лицензию**. По факту оплаты вам будет отправлен ключ по электронной почте, адрес которой был указан вами в форме заказа.

Регулярно «Лаборатория Касперского» проводит акции, позволяющие продлить срок действия ключа на использование наших приложений со значительными скидками. Следите за акциями на сайте «Лаборатории

Касперского» в разделе **Продукты → Акции и спецпредложения**.

Приобретенный ключ необходимо установить. Для этого скопируйте его в каталог хранения ключей (параметр **LicensePath** конфигурационного файла) и перезапустите сервер.

После этого рекомендуется обновить базы Антивируса Касперского (см. п. 5.1 на стр. 32).

ГЛАВА 6. НАСТРОЙКА ДОПОЛНИТЕЛЬНЫХ ПАРАМЕТРОВ

В данном разделе описана настройка дополнительных параметров Антивируса Касперского. В отличие от настройки необходимых параметров (см. Глава 4 на стр. 22), без выполнения которой использование приложения невозможно, настройка дополнительных параметров осуществляется по усмотрению администратора. Она направлена на расширение функциональности приложения и его адаптации под условия использования в рамках конкретного предприятия.

Антивирус Касперского выполняет антивирусную проверку на наличие вирусов в соответствии с параметрами конфигурационного файла `kav4mailservers.conf`. Этот файл можно редактировать.

6.1. Настройка параметров антивирусной защиты почтового трафика

При проверке почтового трафика на наличие вирусов основным критерием при выборе правил обработки сообщений являются адреса отправителя и получателя и параметры группы, в состав которой они входят. Поэтому крайне важно отнести адреса в нужную группу.

Почтовое сообщение считается принадлежащим к конкретной группе, если адреса и отправителя и получателя сообщения принадлежат этой группе. Приложение просматривает список адресов группы на предмет содержания в нем нужных адресов. Как только обнаруживается искомая комбинация адресов «отправитель-получатель», к сообщению применяются правила, определенные параметрами группы.

Проверка наличия строки с адресом сообщения в группе происходит в соответствии с **POSIX regex**.

По умолчанию конфигурационный файл содержит группу `[smtpscan.group:default]`, в которой описаны правила обработки почтовых сообщений. Поскольку в группе изначально нет адресов отправителей и

получателей, то правила, описанные в группе, применяются ко всем сообщениям. Вы можете изменить параметры группы **default**, а также создать новые группы.

Если в конфигурационный файл были добавлены другие группы (см. п. 6.1.1 на стр. 58), то последовательность обработки почтового сообщения будет следующая (см. рис. 4):

- Приложение проверяет наличие адресов отправителя и получателя сообщения в группах, введенных администратором. Если адреса входят в какую-либо группу, то к сообщению будут применены правила обработки, определенные параметрами этой группы.
- Если адреса отправителя и получателя обрабатываемого сообщения попадают в список адресов нескольких групп, приложение будет использовать параметры первой из них.
- Если адреса не входят ни в одну из групп адресов, введенных администратором, то к сообщению будут применены действия приложения, описанные в группе **default**.

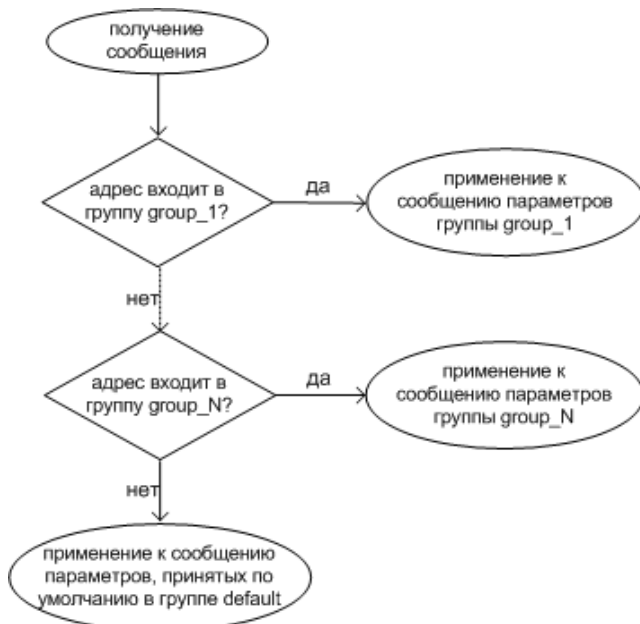


Рисунок 4. Обработка почтового сообщения

6.1.1. Формирование групп пользователей

По умолчанию в конфигурационном файле Антивируса Касперского есть группа **[smtpscan.group:default]**, в которую включены все отправители и получатели сообщений почтового трафика сервера. Для нее справедливы следующие правила обработки почтовых сообщений:

- Проверять все почтовые сообщения.
- Лечить обнаруженные зараженные письма.
- Доставлять получателям только незараженные и вылеченные почтовые сообщения.
- Почтовые сообщения, которые вылечить не удалось, а также подозрительные, поврежденные, защищенные паролем письма, а также почтовые сообщения, в результате проверки которых произошла ошибка, доставлять только администратору группы.
- Отправителей, получателей и администратора группы уведомлять о зараженных, вылеченных, подозрительных, поврежденных, защищенных паролем письмах и почтовых сообщениях, в результате проверки которых произошла ошибка.

Для того чтобы для различных отправителей и получателей Антивирус Касперского обрабатывал почтовые сообщения по отдельным правилам, необходимо создать для них группы.

Чтобы создать новую группу адресов, следует:

1. Создать секцию **[smtpscan.group:<имя_группы>]** в конфигурационном файле.
2. Задать адреса (маски адресов) отправителей и получателей группы, перечислив их через запятую в качестве значений параметров **Senders** и **Recipients**.

При вводе масок используется стандарт **POSIX regexp**.

Если не указать значение параметра **Recipients** или **Senders**, то оно будет определено как **'.*@.*'** (все адреса).

В версии 5.5 Антивируса Касперского в состав конфигурационного файла добавлена группа **kavadministrators**. В процессе установки приложения в данную группу автоматически будут включены все адреса администраторов, перечисленные в каталоге `/var/qmail/alias/postmaster`.

Если адрес администратора изменился (например, параметр **AdminAddress** группы **[smtpscan.group:default]**), необходимо добавить этот адрес (а также все прочие адреса, для которых новый адрес администратора является псевдонимом) в список значений параметра **Recipients** группы **[smtpscan.group:kavadministrators]**.

Это важно сделать в том случае, если администратору будут пересылаться зараженные почтовые сообщения.

6.1.2. Режим проверки и лечения сообщений

Для того чтобы выполнялась антивирусная проверка почтового трафика конкретной группы отправителей и получателей, администратору сервера необходимо в параметрах группы включить соответствующий режим.

Для этого в конфигурационном файле `kav4mailservers.conf` для группы следует задать параметр **Check=yes**.

При включенном режиме проверки все почтовые сообщения данной группы, проверяются Антивирусом Касперского на наличие вирусов. Однако лечение обнаруженных зараженных почтовых сообщений не выполняется.

Для **ВКЛЮЧЕНИЯ РЕЖИМА ЛЕЧЕНИЯ** зараженных писем необходимо в группе указать хотя бы один параметр для вылеченных (**Cured**) объектов. Например, если задать:

```
[smtpscan.group:account]
Check=yes
CuredRecipientNotify=yes
```

это будет означать, что:

- все почтовые сообщения для отправителей и получателей группы **account** будут проверяться на наличие вирусов;
- обнаруженные зараженные объекты будут подвергаться лечению;
- получателям будет доставляться соответствующие уведомления о вылеченных объектах.

6.1.3. Действия над объектами

Действия, выполняемые над объектами почтовых сообщений, определяются:

- статусом объекта, присвоенным после проверки (см. п. 6.2.2 на стр. 65);
- действием для конкретного статуса объекта, указанным в конфигурационном файле.

Статус объекту присваивается процессом *aveserver* сразу после проверки его на содержание вирусов; действие, выполняемое над объектом после проверки, определяется администратором сервера.

Антивирус Касперского позволяет определить действия над объектами почтовых сообщений, которые будут доставляться получателю и администратору группы. Для отправителей почтовых сообщений можно настроить **ТОЛЬКО** отправку уведомлений.

Для объектов почтовых сообщений можно задать одно из следующих действий:

- **Remove** – удалять объект из почтового сообщения.
- **Unchanged** – не изменять объект. В данном случае объект не будет подвергаться лечению и будет доставляться в исходном виде.
- **Cured** – доставлять только вылеченный объект (только для объекта типа **Cured**).

Над всеми типами объектов можно определить *единые действия* или задать для каждого типа свое действие.

Чтобы задать для всех типов объектов единые действия, следует

установить соответствующие значения для параметров **AdminAction** и **RecipientAction**. Эти параметры определяют действия для всех типов объектов. Например:

```
AdminAction=unchanged
RecipientAction=remove
```

Все почтовые сообщения группы будут доставлены администратору неизменными; для получателей объекты из сообщений будут удалены.

Чтобы для каждого типа объектов задать свое действие, следует

указать соответствующие значения для параметров **<тип_объекта>AdminAction** и **<тип_объекта>RecipientAction**. Например,

```
AdminAction=unchanged
RecipientAction=remove
CuredRecipientAction=cured
```

В данном случае все почтовые сообщения, независимо от типа объектов, будут доставлены без изменений администратору группы; получателю будут доставлены только вылеченные сообщения, а все остальные будут удалены.

Дополнительно к перечисленным выше действиям над объектами предусмотрено **помещение объекта на карантин**.

Чтобы поместить объект почтового сообщения на карантин, следует

задать в конфигурационном файле для группы следующие параметры:

```
QuarantinePath=/var/db/Quarantine
Quarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
```

6.1.4. Уведомление отправителей, получателей и администраторов

Антивирус Касперского позволяет отправлять уведомления для отправителей, получателей и администраторов групп об объектах почтовых сообщений с любым из возможных статусов (подозрительные, зараженные, вылеченные, поврежденные и т. д.). Отправка уведомлений определяется следующими параметрами:

- **RecipientNotify** – уведомление для получателя почтового сообщения.
- **SenderNotify** – уведомление для отправителя почтового сообщения.
- **AdminNotify** – уведомление для администратора группы.

Перечисленные параметры определяют отправку уведомлений для объектов всех статусов. Чтобы назначить отправку уведомлений для объектов конкретных статусов, следует задать следующие параметры:

- **<статус_объекта>RecipientNotify;**
- **<статус_объекта>SenderNotify;**
- **<статус_объекта>AdminNotify.**

В таком случае уведомление будет отправлено только при обнаружении объекта указанного статуса.

Например, если необходимо, чтобы уведомления администратору и отправителю поступали по объектам всех статусов, а получателю – только по зараженным, вылеченным и поврежденным объектам, следует задать в группе следующие параметры:

```
InfectedRecipientNotify=yes
CuredRecipientNotify=yes
CorruptedRecipientNotify=yes
SenderNotify=yes
AdminNotify=yes
```

Также необходимо указать адрес, с которого будут отправляться уведомления (параметр **NotifyFromAddress** секции **[smtpscan.general]**).

Уведомления содержат универсальный текст, основанный на шаблоне */etc/kav/5.5/template_notify_main*, который включен в поставку приложения и используется по умолчанию.

Если необходимо изменить текст уведомления, следует:

- Отредактировать текст шаблона, используемого по умолчанию.
- Либо создать новый файл шаблона и указать полный путь к нему в качестве значения параметра **Template** секции **[smtpscan.notify]**.

Текст уведомления изменяется с помощью макросов, включаемых в шаблон уведомления, которые автоматически заменяются приложением на соответствующее значение на основании статусов, присвоенных объектам по результатам антивирусной проверки:

- **%VERSION%** – версия Антивируса Касперского.
- **%SENDER%** – почтовый адрес отправителя сообщения.
- **%RECIPIENT%** – список всех получателей сообщения, разделенных символом перевода строки.
- **%MSGID%** – идентификационный номер письма.

- **%VIRUSNAME%** – текстовое описание проблемы (данный текст может быть локализован на любой язык, для чего необходимо добавить соответствующие строки для объекта каждого статуса в секции [locale]).
- **%SUBJECT%** – тема (поле **Subject**) исходного почтового сообщения.
- **%DATETIME%** – дата и время обработки почтового сообщения. Формат даты и времени можно редактировать (см. п. 6.5 на стр. 70).
- **%HEADERS%** – заголовки исходного письма.
- **%ACTION%** – действия, произведенные над вложенными объектами письма. Данный макрос используется во всех шаблонах, кроме уведомлений для отправителя письма. Возможны следующие действия:
 - *attachement not modified* – вложение не изменилось.
 - *attachement cured* – вложение успешно вылечено.
 - *attachment removed* – вложение удалено.
 - *attachments cured and removed* – часть вложений вылечена и доставлена получателю, часть – удалена.

Также эти макросы можно использовать и при формировании темы письма.

Параметры формирования уведомлений (MIME-тип, тема письма, кодировка и т. д.) сгруппированы в секции **[smtpscan.notify]** конфигурационного файла.

6.2. Настройка параметров антивирусной защиты файловых систем сервера

Весь набор параметров антивирусной защиты файловых систем сервера можно разделить на группы, определяющие:

- Область проверки (см. п. 6.2.1 на стр. 64).
- Режим проверки и лечения файлов (см. п. 6.2.2 на стр. 65).
- Действия над файлами (см. п. 6.2.3 на стр. 65).
- Параметры формирования журнала событий о результатах работы (см. п. 6.8 на стр. 75).

Рассмотрим подробнее настройку каждой из этих групп.

6.2.1. Область проверки

Область проверки можно условно разделить на:

- список каталогов и файлов, которые необходимо проверить;
- список типов файлов, которые будут проверяться на наличие вирусов (архивы, почтовые сообщения и т. д.).

По умолчанию проверяются все объекты доступных файловых систем, начиная с текущего каталога.

Для проверки всех файловых систем сервера необходимо перейти в корневой каталог или в командной строке указать область проверки.

Список каталогов и файлов, которые необходимо проверить, можно задать следующими способами:

- Перечислить через пробел каталоги и файлы (с указанием абсолютного или относительного пути к ним) непосредственно в командной строке при запуске компонента.
- Задать список каталогов и файлов в текстовом файле и указать его использование в командной строке с помощью ключа **-@<имя_файла>** (каждый объект в таком списке приводится с новой строки с указанием абсолютного пути к нему).

Если в командной строке будет указан как просто список, так и текстовый файл со списком объектов проверки, то будет проверяться область, указанная в файле.

- Ограничить список каталогов и файлов (как перечисленных в командной строке, так и содержащихся в текстовом файле) можно путем ввода в конфигурационном файле *kav4mailservers.conf* масок файлов и каталогов, которые будут исключены из области проверки (секция **[scanner.options]**, параметры **ExcludeMask** и **ExcludeDirs**).
- Существует возможность отключить *рекурсивную проверку каталогов* (секция **[scanner.options]**, параметр **Recursion** или ключ **-r**).
- После создания альтернативного конфигурационного файла указать его использование можно с помощью ключа **-с <имя_файла>** при запуске компонента.

Список типов файлов по умолчанию также задается в конфигурационном файле *kav4mailservers.conf* (секция **[scanner.options]**) и может быть переопределен:

- с помощью ключей командной строки при запуске компонента;

- путем использования альтернативного конфигурационного файла.

6.2.2. Режим проверки и лечения файлов

Лечение зараженных файлов, обнаруженных в результате проверки, является важным параметром антивирусной защиты.

По умолчанию возможность лечения зараженных объектов отключена, что предполагает только проверку файлов и информирование об обнаружении вирусов и других подозрительных или поврежденных файлов путем вывода сообщений на консоль и записи в журнал событий (см. п. 6.5 на стр. 70).

В результате проверки на наличие вирусов каждому файлу присваивается один из следующих статусов:

- **Clean** – вирусов в файле не обнаружено.
- **Infected** – файл заражен.
- **Warning** – код файла похож на код известного вируса.
- **Suspicious** – код файла похож на код неизвестного вируса.
- **Corrupted** – файл поврежден.
- **Protected** – файл защищен паролем.

При включенном режиме лечения (секция **[scanner.options]**, параметр **Cure=yes**) на антивирусную обработку отправляются только файлы со статусом **Infected**. В результате лечения файлу присваивается один из следующих статусов:

- **Cured** – файл успешно вылечен.
- **CureFailed** – файл вылечить не удалось (файл с таким статусом будет обрабатываться по правилам, заданным для зараженных объектов).

6.2.3. Действия над файлами

В зависимости от статуса, присвоенного по результатам антивирусной проверки, (см. п. 6.2.2 на стр. 65) к файлу могут применяться те или иные действия. По умолчанию осуществляется только следующее: о том, что были обнаружены файлы с определенным статусом, на консоль выводится сообщение и производится запись в журнал событий.

Для файлов со статусами **Infected**, **Suspicious**, **Warning** и **Corrupted** можно настроить выполнение набора действий:

- *перемещение в некоторый каталог* – перенос файлов определенного статуса в некоторый каталог; возможен *простой* и *рекурсивный перенос*;
- *удаление* файла из файловой системы;
- *выполнение некоторой команды* – обработка файлов посредством стандартных команд Unix, скриптов и т. д.

Для файлов со статусами **Protected** и **Cured** создается только уведомление, выводимое на консоль, и запись в журнал событий.

Следует отметить, что Антивирус Касперского различает простой объект (файл) и объект-контейнер (состоящий из нескольких объектов, например архив). Действия, выполняемые над такими объектами, также различаются; в конфигурационном файле они разнесены по отдельным секциям. Для простого объекта – секция **[scanner.object]**, для контейнера – **[scanner.container]**.

Действия над самораспаковывающимися архивами неоднозначны: если заражен сам архив, то он рассматривается как простой объект, а если заражены объекты внутри архива – как контейнер. Соответственно, и действия над архивом в таких случаях определяются параметрами из разных секций конфигурационного файла!

Выбрать действие над тем или иным файлом можно несколькими способами:

- Задать действия в конфигурационном файле приложения, если предполагается использовать их как действия по умолчанию (секции **[scanner.object]** и **[scanner.container]**).
- Указать действия в альтернативном конфигурационном файле и использовать его при запуске компонента.
- Задать действия на текущий сеанс работы с помощью ключей командной строки при запуске компонента *kavscanner*.

Синтаксис действий, как для простых объектов, так и для объектов-контейнеров одинаков.

6.2.4. Режим резервного копирования

Рассмотрим подробнее на примере конкретной задачи настройку параметров режима резервного копирования.

Пример:

Необходимо проверить на присутствие вирусов все объекты в каталогах и файлах, перечисленных в файле `/tmp/download.lst`, и проинформировать их лечение. В случае неудачного лечения перенести обнаруженные зараженные объекты (с полными путями к ним) в каталог `/tmp/infected`, подозрительные в `/tmp/suspicious`, предупреждения в `/tmp/warning`.

Для реализации поставленной задачи следует:

1. Создать альтернативный конфигурационный файл `scan_sample.conf`.
2. Включить режим лечения зараженных объектов, если он был отключен (**Cure=yes** в секции **[scanner.options]**).
3. Задать правила обработки зараженных объектов. Для этого в секциях **[scanner.object]** и **[scanner.container]** конфигурационного файла `scan_sample.conf` указать следующее:

```
OnInfected=MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```

4. Запустить в командной строке компонент `kavscanner` следующим образом:

```
# kavscanner -@ /tmp/downloads.lst -c \
scan_sample.conf
```

6.3. Оптимизация работы Антивируса Касперского

Для снижения нагрузок на сервер в Антивирусе Касперского предусмотрены возможности эффективной оптимизации его работы.

Данные технологии используются только при проверке объектов файловой системы сервера. Их применение регулируется соответствующими параметрами в секции **[scanner.options]** конфигурационного файла приложения.

6.3.1. Использование базы данных iChecker

Приложение использует ряд технологий, позволяющих не проводить анти-вирусную проверку файла каждый раз при обращении к нему, а по возможности ограничиваться операцией сравнения с уже существующими о нем данными. Алгоритм проверки объекта (файла) на наличие вирусов заключается в следующем:

- После первой проверки любого файла информация о нем (имя, контрольная сумма) фиксируется в базе данных iChecker – общей базе, включающей информацию о проверенных **незараженных** файлах определенных форматов. Такая база содержит информацию по объектам, проверенным компонентом *kavscanner*.
- При каждом последующем обращении пользователя к файлу производится его поиск сначала в базе iChecker. Критерием поиска является имя файла. Если такой файл будет обнаружен в базе iChecker, информация о файле сравнивается с указанной в базе. При условии полной идентичности текущего состояния объекта и его описания в базе файл считается неизменным и не проверяется на наличие вирусов.
- Если информации о запрашиваемом файле не обнаружено производится полная антивирусная проверка файла.

6.3.2. Ограничение нагрузки на сервер

Проверка файловых систем сервера при большом объеме данных может занять значительное время. Если при этом выполнять еще и текущие задачи, нагрузка на сервер возрастет. Чтобы оптимизировать загрузженность сервера необходимо приостанавливать антивирусную проверку при превышении порога нагрузки.

Для решения данной задачи в конфигурационный файл приложения в секцию **[scanner.options]** добавлен параметр **MaxLoadAvg**. В случае когда значение этого параметра определено, *kavscanner* перед проверкой каждого нового файла проверяет текущее значение степени загрузженности сервера (*load average*), и, в случае его превышения над указанным в конфигурационном файле значением, *kavscanner* приостанавливает работу до момента, когда значение параметра **load average** не снизится до указанного значения.

6.4. Настройка параметров работы процесса *aveserver*

Антивирусная обработка почтового трафика осуществляется за счет работы двух компонентов: процесса *aveserver* и *smtpscanner*.

Aveserver запускается при старте операционной системы. Установка соединения с *aveserver* выполняется непосредственно при обращении к нему *smtpscanner*.

Параметры работы процесса *aveserver* можно настроить в конфигурационном файле *kav4mailservers.conf* (секция **[aveserver.options]**):

- **DetachFromTerminal** – отсоединение процесса от терминала сразу после запуска. Включение такого режима необходимо, поскольку, пока процесс не отсоединится, загрузка системы не продолжится. По умолчанию режим включен (значение **yes**). Отключение режима (значение **no**) должно использоваться только в случае управления процессом программами типа **svc**.
- **StartupMode** – переход процесса в фоновый режим работы при условии, что **DetachFromTerminal=yes**. Значение **fast** определяет переход демона в фоновый режим сразу после загрузки конфигурационного файла, возвращая при этом код **0**. Значение **normal** осуществляет переход процесса в фоновый режим только после загрузки в память баз Антивируса Касперского и ключей.

В режиме **fast** время, затраченное на запуск процесса, меньше, но есть вероятность, что демон не будет запущен из-за какой-либо фатальной ошибки, при этом на консоль не будет выведена соответствующая информация!

- **LocalSocketPermission** – права, с которыми создается сокет (в восьмеричном виде). По умолчанию **LocalSocketPermission=0666**.

6.4.1. Перезагрузка *aveserver*

Перезапуск процесса *aveserver* выполняется автоматически сразу после обновления баз Антивируса Касперского, при условии включения соответствующего параметра конфигурации.

Перезагрузка выполняется командой:

```
# kill -HUP <PID_процесса>
```

В результате ее выполнения процесс получает сигнал **SIGHUP**. При таком сигнале родительский процесс заново загружает конфигурационный файл, ключи и базы или завершает работу с соответствующим сообщением в журнале событий, если путь к файлу задан некорректно. Все открытые соединения копий процесса с клиентскими программами остаются активными до их закрытия.

Такая перезагрузка процесса *aveserver* также необходима, например, в случае, если был изменен конфигурационный файл, установлен новый ключ или базы были обновлены вручную.

6.4.2. Принудительное завершение работы *aveserver*

Чтобы принудительно завершить работу процесса *aveserver*, воспользуйтесь командой:

```
# kill <PID_процесса>
```

Команда отправит процессу сигнал **SIGTERM**, по которому завершается работа *aveserver* с закрытием функционирования всех порожденных им копий.

Для завершения работы с процессом *aveserver* не рекомендуется использовать команду `kill -9`. В результате выполнения данной команды работа процесса будет завершена, однако в системе сохранится ряд временных и рабочих файлов, которые удаляются только вручную. Некоторые приложения (например, Webmin) по наличию в системе таких файлов определяют процесс как запущенный.

6.5. Проверка почты, получаемой по POP3-протоколу

В настоящее время широкое распространение имеют внешние почтовые сервисы. Зачастую почта с таких сервисов доставляется при помощи клиентов, использующих протокол POP3, тогда как Антивирус Касперского проверяет только почтовый трафик по SMTP-протоколу. Вместе с этим, необходимо предотвратить заражение и при скачивании зараженных почтовых сообщений с внешних почтовых сервисов.

Для обеспечения защиты в таком случае необходимо:

1. Отключить порт 110 и организовать работу шлюза как прокси-сервера для POP3 посредством пакета **fetchmail**. Этот пакет получает почтовые сообщения с внешних серверов и передает их почтовой программе по протоколу SMTP. Далее их обрабатывает Антивирус Касперского.

Для фильтрации почты внешних почтовых ящиков требуется наличие локального SMTP-сервера и учетной записи локального пользователя на компьютере, где установлен пакет **fetchmail**!

Настройка **fetchmail**, как правило, следующая: у каждого пользователя в каталоге \$HOME есть файл *.fetchmailrc*, как минимум содержащий следующие строки:

```
set postmaster "user"
set bouncemail
set no spambounce
set properties ""
poll mail.that.is.free.ru with proto POP3
    user 'remote_user' there with password
    'pass12345' is 'user' here
poll mail2.that.is.free.ru with proto POP3
    user 'remote_user2' there with password
    'pass123452' is 'user' here
```

где:

- **user** – имя пользователя в локальной сети;
- **mail.that.is.free.ru** и **mail2.that.is.free.ru** – имена хостов, с которых должна быть получена почта;
- **remote_user** и **remote_user2** – имена учетных записей на хостах *mail.that.is.free.ru* и *mail2.that.is.free.ru*, соответственно;
- **pass12345** и **pass123452** – пароли для учетных записей *remote_user* и *remote_user2*.

При такой настройке параметров программа **fetchmail** будет получать почтовые сообщения с хостов *mail.that.is.free.ru* и *mail2.that.is.free.ru* и отправлять их на локальный SMTP-порт пользователю *user*.

При этом поля почтовых сообщений (*From*, *To* и другие) не изменятся, появится только дополнительный заголовок *Received*, осл-
авленный **fetchmail**. Пользователь будет получать письма в том же виде, что и при получении обычным образом.

2. Внести команду **fetchmail** в crontab пользователя на запуск, например, каждые 10-15 минут.

Для автоматизации процесса настройки параметров программы **fetchmail** остальным пользователям, использующим внешние почтовые ящики, понадобятся следующие данные:

- имя внешнего хоста, с которого **fetchmail** будет получать почту;
- имя учетной записи на внешнем хосте;
- пароль учетной записи.

Также в домашнем каталоге каждого пользователя должен быть файл *.fetchmailrc* следующего вида:

```
set postmaster "user"
set bouncemail
set no spambounce
set properties ""
```

Для добавления в него записей о почтовых ящиках можно использовать скрипт-файл:

```
#!/bin/bash
echo "poll $1 with proto POP3 " >>$HOME/.fetchmailrc
echo "user '$2' with password '$3' is '$4' \
here">>$HOME/.fetchmailrc
```

Если запустить данный скрипт-файл со следующими параметрами:

```
pop.mail.ru dan secret admin
```

то письма для получателя *dan@mail.ru* будут пересылаться на адрес *admin@your_host_your_domain*.

6.6. Дополнительные возможности для почтовой программы Postfix

При использовании почтовой программы Postfix Антивирус Касперского предоставляет ряд дополнительных возможностей:

- Поддержка расширения DSN протокола SMTP (RFC 3461, RFC 3885) (см. п. 6.6.1 на стр. 73);

- Поддержка расширения 8bit-MIME протокола SMTP (RFC 1652) (см. п. 6.6.2 на стр. 73);
- Поддержка расширения X-Forward протокола SMTP (см. п. 6.6.3 на стр. 74).

Настройка параметров данных расширений протокола осуществляется по усмотрению администратора.

6.6.1. Поддержка расширения DSN

Компонент *smtpscanner* поддерживает расширение DSN протокола SMTP. Поддержка данного расширения позволяет сохранить параметры почтового сообщения, присвоенного ему входящей почтовой программой. Компонент *smtpscanner* в этом случае не анализирует их, а передает данные о сообщении внешней почтовой программе без изменений.

Чтобы включить поддержку расширения DSN, следует

задать в секции **[smtpscan.general]** конфигурационного файла параметр:

```
EHLOsupportDSN=yes
```

Прежде чем включать данный параметр, необходимо проверить, что внешняя почтовая программа поддерживает расширение DSN.

6.6.2. Поддержка расширения 8bit-MIME

При работе с национальными языками по протоколу SMTP часто используется расширение 8bit-MIME, поскольку в базовом протоколе SMTP не предусмотрена передача сообщений на языках, использующих не только ASCII-символы. Поэтому в Антивирус Касперского 5.5 добавлена возможность поддержки данного расширения.

Если внешняя почтовая программа не поддерживает расширение 8bit-MIME, следует внести соответствующие изменения и в настройки параметров Антивируса Касперского.

Чтобы включить поддержку расширения 8bit-MIME, следует

задать в секции **[smtpscan.general]** конфигурационного файла параметр:

```
EHLOsupport8BITMIME=yes
```

Поддержка расширения 8bit-MIME не влияет на работу Антивируса Касперского.

6.6.3. Поддержка расширения X-Forward

В Антивирусе Касперского реализована возможность поддержки расширения X-Forward, реализованного в почтовой программе Postfix.

Чтобы включить поддержку расширения X-Forward, следует:

- Использовать протокол SMTP при интеграции с почтовой программой Postfix (подробнее об этом см. п. 4.4.5 на стр. 32).
- Задать в секции **[smtpscan.general]** конфигурационного файла параметры:

```
EHLOsupportXFORWARD=yes
EHLOattrsXFORWARD=NAME ADDR PROTO HELO
```

6.6.4. Использование SMTP-протокола компонентом smtpscanner

Компонент антивирусной проверки почтового трафика *smtpscanner* может использовать для приема входящего почтового трафика как протокол LMTP, так и SMTP.

Для того чтобы переключить компонент smtpscanner на протокол SMTP необходимо:

- Присвоить параметру **Protocol** в секции **[smtpscan.general]** конфигурационного файла значение **smtp**.
- Изменить значение протокола с **lmtp** на **smtp** в конфигурационном файле почтовой программы Postfix (файл *master.cf*) в сервисе **smtp**.
- Перезапустить почтовую программу.

6.7. Локализация отображаемого формата даты и времени

Во время работы Антивируса Касперского формируются отчеты по каждому из компонентов, а также различные уведомления для пользователей и администраторов. Такая информация всегда сопровождается датой и временем ее формирования.

По умолчанию Антивирус Касперского использует форматы даты и времени, соответствующие стандарту `strftime`:

- **%H:%M:%S** – отображаемый формат времени.
- **%d/%m/%y** – отображаемый формат даты.

Администратору предоставляется возможность изменения формата даты и времени. Локализация форматов выполняется в секции **[locale]** конфигурационного файла *kav4mailservers.conf*. Например, вы можете задать следующие форматы:

- **%I:%M:%S %P** – для отображения времени в двенадцатичасовом формате (параметр **TimeFormat**).
- **%y/%m/%d** и **%m/%d/%y** – для отображения даты (параметр **DateFormat**) (*гг/мм/дд* и *мм/дд/гг*, соответственно).

6.8. Параметры формирования журнала событий Антивируса Касперского

Результаты работы всех компонентов Антивируса Касперского фиксируются в журнале событий.

Результаты проверки на наличие вирусов файловых систем сервера выводятся на консоль. По умолчанию информация, выводимая в журнал событий и на экран, дублирует друг друга. Для того чтобы на консоль выводилась отличная от журнала событий информация, необходимо выполнить дополнительную настройку параметров (подробнее см. п. 6.8.2 на стр. 79).

Объем выводимой информации можно редактировать путем изменения *уровня детализации* журнала событий.

Уровень детализации представляет собой число, определяющее степень конкретизации информации о работе компонентов в журнале событий. Каждый последующий уровень включает в себя информацию предыдущего и некоторую дополнительную.

В таблице, приведенной ниже, перечислены все возможные уровни детализации журнала событий.

Уровни	Название уровня	Значение
	Критические ошибки	Информация о критических ошибках (ошибках, которые приводят к завершению работы приложения из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при проверке, загрузке баз или ключей.
1	Errors	Информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов; например, информация об ошибке проверки файла.
2	Warning	Информация об ошибках, которые могут привести к завершению работы продукта (например, информация об отсутствии свободного места на диске).
3	Info, Notice	Информация о том, запущен ли компонент, путь к конфигурационному файлу, область проверки, информация о базах Антивируса Касперского, о ключах, результирующая статистика.
4	Activity	Сообщения о проверке файлов в соответствии с уровнем детализации журнала событий (см. п. 6.8.1 на стр. 77).
10	Debug	Все сообщения отладочного характера; например, содержание конфигурационного файла.

Информация о критических ошибках в работе компонента выводится всегда вне зависимости от установленного уровня детализации. Оптимальным уровнем является уровень **4**, который задан по умолчанию.

Общий формат вывода информации для любого из перечисленных уровней детализации имеет следующий вид:

[дата время уровень_детализации] STRING

где:

- [дата время уровень_детализации] – параметр, формирующийся системно и содержащий дату и время (в формате, указанном

администратором) и уровень детализации журнала событий (первая буква, соответствующая названию уровня детализации).

Формат представления даты и времени можно изменить в секции **[locale]** конфигурационного файла *kav4mailservers.conf* (см. п. 6.5 на стр. 70).

- **STRING** – строка журнала событий; в зависимости от вида сообщения имеет разный формат. Предусмотрены следующие виды сообщений:
 - Сообщения о проверке (см. п. 6.8.1 на стр. 77).
 - Прочие сообщения (о старте компонента, о загрузке баз, коды возврата и т. д.).
 - Сообщения, выводящиеся на консоль (см. п. 6.8.2 на стр. 79).

Виды сообщений и соответствующий им формат рассмотрены подробнее ниже.

6.8.1. Формат сообщений о проверке

Сообщения о проверке формируются только для компонентов *kavscanner* и *aveserver*.

Формат отчета о проверке каждого файла зависит от того, к какому типу объектов (простому или контейнеру) он относится.

Для простого объекта сообщения о проверке имеют следующий формат:

- Расширенный формат сообщений (**ShowObjectResultOnly=no**):

"имя_файла" результат [имя_вируса]

- Краткий формат сообщений (**ShowObjectResultOnly=yes**):

"имя_файла" результат

где:

- **имя_вируса** – имя вируса для событий CURED, INFECTED, CUREFAILED, WARNING, SUSPICIOUS. Для остальных событий это поле пустое.
- **результат** – статус, который присваивается файлу в результате проверки и лечения. Полный перечень возможных результатов приведен в таблице ниже.

Для контейнеров формат сообщений о проверке также может быть расширенным или кратким:

- Расширенный формат сообщений (**ShowContainerResultOnly=no**):

"имя_архива"

"имя_файла" результат [имя_вируса]

"имя_файла" результат [имя_вируса]

- Краткий формат сообщений (**ShowContainerResultOnly=yes**):

"имя_файла" результат

Событие/Результат	Значение
OK	Файл не заражен.
CURED (только при включенном режиме лечения)	Файл был заражен и успешно вылечен.
INFECTED	Файл заражен одним или несколькими вирусами; запрос на лечение отсутствует.
CUREFAILED (только при включенном режиме лечения)	Файл заражен одним или несколькими вирусами; запрос на лечение присутствует, но лечение файла невозможно.
WARNING	Код файла похож на код известного вируса.
SUSPICIOUS	Файл подозревается на заражение неизвестным вирусом.
ERROR	Файл проверить невозможно из-за возникающей ошибки (например, в результате обработки поврежденного архива).
PROTECTED	Файл проверить невозможно из-за того, что он защищен паролем.
CORRUPTED	Файл поврежден.

6.8.2. Формат сообщений, выводящихся на консоль

Вывод сообщений на консоль производится компонентами *kavscanner* и *keepup2date*!

Вывод информации компонента *kavscanner* на консоль регулируется наличием или отсутствием в командной строке при запуске компонента ключа **-q**. Если ключ указан, то информация на консоль не выводится. Наличие сообщений о работе компонента *keepup2date* на консоли обеспечивается параметром конфигурационного файла **KeepSilent=no**.

По умолчанию формат и объем информации, выводимой на экран, полностью соответствует включаемой в журнал событий.

Состав выводимой на консоль информации для компонента *kavscanner* можно изменить. Для этого необходимо в конфигурационный файл (*kav4mailservers.conf* или альтернативный) включить секцию **[scanner.display]**.

В этой секции можно задать возможность вывода на экран информации о проверке объектов внутри архива (**ShowContainerResultOnly**), о незараженных файлах (**ShowOK**), а также результатов текущей работы компонента (**ShowProgress**).

Детализация журнала событий о проверке при наличии секции **[scanner.display]** регулируется ключом **-x <параметр>**.

6.8.3. Статистика вирусной активности

В Антивирусе Касперского предусмотрена возможность сбора и просмотра статистики по вирусной активности за определенный период времени. Такая функциональность доступна через веб-интерфейс программы Webmin.

Чтобы настроить автоматический сбор антивирусной статистики, следует:

- Присвоить параметру **AVStatistics** в секции **[smtpscan.report]** конфигурационного файла следующее значение:

```
AVStatistics=\n/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- Настроить необходимую периодичность запуска скрипта, собирающего информацию из файла статистики:

```
perl /usr/libexec/webmin/kavms5.5/parse_avstat.pl\
```

```
-sd=/var/db/kav/5.5/kav4mailservers/proc_avstat\  
/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- С обновленными статистическими данными (с помощью программы Webmin) можно ознакомиться только после запуска этого скрипта.

Если программа Webmin установлена не по стандартному пути, то путь `/usr/libexec/webmin/kavms5.5/parse_avstat.pl` также будет другим!

6.8.4. Дополнительные информационные поля в сообщениях

В приложении реализована возможность добавления в заголовок почтового сообщения некоторую дополнительную информацию. Это могут быть сведения о версии приложения, дате последнего обновления баз Антивируса Касперского, времени и результате антивирусной проверки данного письма.

Добавление этой информации в заголовок почтового сообщения задается параметром `AddXHeaders` секции `[smtpscan.group:default]` конфигурационного файла.

Формат заголовка:

```
X-Anti-Virus: <имя приложения и его версия>, bases:  
<дата обновления баз в формате YYYYMMDD> #<количество  
записей в АВ-базах>, check: <дата проверки в формате  
YYYYMMDD> <статус проверки или not_checked>
```

Пример:

```
X-Anti-Virus:Kaspersky Anti-Virus for Unix Mail  
Servers version 5.5/RELEASE, bases: 20041101 #102746,  
check: 20041210 clean
```

ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Для того чтобы удалить Антивирус Касперского необходимо:

- Обладать правами привилегированного пользователя (**root**).
- Иметь в наличии журнал событий о процессе установки. Имена и размеры установленных файлов Антивируса Касперского должны полностью соответствовать приведенным в журнале событий установки.
- Остановить процесс *aveserver*.
- Остановить почтовую службу.

Если при установке использовался rpm-пакет Антивируса Касперского, для запуска процедуры удаления в командной строке введите:

```
# rpm -e <имя_пакета>
```

Если при установке использовался deb-пакет Антивируса Касперского, для запуска процедуры удаления в командной строке введите:

```
# dpkg -r <имя_пакета>
```

Если при установке использовался pkg-пакет Антивируса Касперского, для запуска процедуры удаления в командной строке введите:

```
# pkg_delete <имя_пакета>
```

Удаление приложения будет выполнено автоматически. В случае успешного завершения удаления дополнительных оповещений не производится.

ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА

После установки и настройки параметров Антивируса Касперского можно проверить корректность его работы с помощью тестового «вируса» и его модификаций.

Тестовый «вирус» был специально разработан организацией  (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.

Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!

Загрузить тестовый «вирус» можно с официального веб-сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Файл, который вы загрузили с веб-сайта компании **EICAR** содержит тело стандартного тестового «вируса». Антивирус обнаруживает его, присваивает тип **Infected**, не подвергающийся лечению, и выполняет действие, установленное администратором для объекта с таким типом.

Для того чтобы проверить реакцию Антивируса при обнаружении объектов других типов, вы можете модифицировать содержание стандартного тестового «вируса», добавив к нему один из префиксов (см. таблицу).

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый «вирус»	Зараженный. Объект не может быть вылечен.
CORR–	Поврежденный.

Префикс	Тип объекта
SUSP-	Подозрительный (код неизвестного вируса).
WARN-	Подозрительный (модифицированный код известного вируса).
ERRO-	Вызывающий ошибку проверки, соответствующую обнаружению поврежденного объекта.
CURE-	Зараженный. Объект подвергается лечению, при этом текст тела «вируса» изменяется на CURE.
DELE-	Зараженный. Объект автоматически удаляется.

В первом столбце таблицы приведены префиксы, которые нужно добавить в начало строки стандартного тестового «вируса».

Во втором столбце описаны типы объектов, идентифицируемые антивирусной программой в результате добавления префиксов. Действия над каждым из объектов определяются параметрами Антивируса, настроенными администратором.

ГЛАВА 9. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В данной главе мы осветим наиболее распространенные вопросы пользователей по установке, настройке параметров и работе Антивируса Касперского и постараемся ответить на них наиболее подробно.

Постоянно пополняемая База знаний, содержащая ответы на часто задаваемые вопросы, расположена на сайте «Лаборатории Касперского» по адресу http://support.kaspersky.ru/unix_mail_server. Здесь вы можете найти ответы на вопросы, которые не перечислены ниже. Также вы можете написать запрос в Службу технической поддержки через web-форму Help-Desk (<http://www.kaspersky.com/helpdesk>).

***Вопрос:** возможно ли использование Антивируса Касперского с антивирусными продуктами других производителей?*

Во избежание конфликтов мы рекомендуем удалять антивирусные продукты сторонних производителей до установки Антивируса Касперского.

***Вопрос:** Антивирус Касперского не проверяет файл повторно. Почему?*

Действительно Антивирус Касперского не проверяет повторно файлы, которые не изменились с момента последней проверки.

Это возможно благодаря применению новой технологии iChecker. Для реализации технологии используется база контрольных сумм объектов.

***Вопрос:** почему Антивирус Касперского вызывает определенное снижение производительности компьютера и ощутимо нагружает процессор?*

Детектирование вирусов является вычислительной (математической) задачей, связанной с анализом структур, подсчетом контрольных сумм и математическими преобразованиями данных. Поэтому основным ресурсом, который потребляется Антивирусом в процессе работы, является процессорное время. При этом каждый новый вирус, добавленный в базу Антивируса Касперского, увеличивает общее время проверки.

В отличие от других антивирусов, сокращающих время проверки путем исключения из баз более сложных в обнаружении или более редких (например, в географическом отношении) вирусов, а также более сложных в анализе форматов файлов (например, pdf), «Лаборатория Касперского» считает, что задача Антивируса – обеспечивать реальную антивирусную безопасность пользователей.

Антивирус Касперского позволяет опытному пользователю ускорить антивирусную проверку путем отключения антивирусной проверки различных типов файлов. Однако не стоит забывать, что это приводит к снижению уровня безопасности.

Антивирус Касперского распознает более семисот форматов архивированных и сжатых файлов. Это очень важно для антивирусной безопасности, поскольку каждый из распознаваемых форматов может содержать исполняемый вредоносный код. Тем не менее, новая версия продукта работает быстрее, чем предыдущая, несмотря на ежедневное увеличение общего количества обнаруживаемых Антивирусом Касперского вирусов (около 30 новых вирусов в день), а также постоянное увеличение количества распознаваемых форматов. Это следствие использования новых уникальных технологий, разработанных в «Лаборатории Касперского», таких как iChecker™.

Вопрос: *зачем нужен ключ? Может ли мой Антивирус работать без него?*

Без ключа Антивирус Касперского не работает.

Если вы еще не решились на приобретение Антивируса Касперского, мы можем предоставить вам пробный ключ (Trial), который будет работать в течение двух недель или месяца. По истечении данного срока ключ будет заблокирован.

Вопрос: *что произойдет, когда истечет срок действия ключа на использование продукта?*

По истечении срока действия ключа на использование Антивируса Касперского продукт будет продолжать работу, но использование новых баз Антивируса станет невозможным. Антивирус по-прежнему будет выполнять лечение зараженных объектов, но с использованием старых баз.

При возникновении данной ситуации проинформируйте вашего системного администратора или обратитесь за продлением срока

действия ключа в компанию, где был приобретен Антивирус Касперского или непосредственно в ЗАО «Лаборатория Касперского».

***Вопрос:** мой Антивирус не работает.*

Что мне делать?

Прежде всего, убедитесь, что **запущена работа компонента `aveserver`**, а также что метод решения вашей проблемы не описан в данной документации, в частности в этом разделе, или на сайте «Лаборатории Касперского» в Базе знаний (http://support.kaspersky.ru/unix_mail_server).

Также мы рекомендуем обратиться к фирме, где вы приобрели Антивирус Касперского или написать запрос в Службу технической поддержки (<http://www.kaspersky.com/helpdesk>).

Чтобы ваш запрос был обработан как можно скорее:

1. В заголовке сообщения укажите операционную систему вашего компьютера, название продукта «Лаборатории Касперского», который вы используете, и проблему. Например:
Linux, Webmin, нет доступа к настройкам списка лицензированных пользователей.
2. В запросе обязательно укажите точные версии операционной системы и Антивируса Касперского.
3. Кратко, но наиболее понятно опишите проблему. Помните, что Служба поддержки на момент чтения вашего письма ещё ничего не знает о вашей проблеме и сможет помочь вам, только полностью поняв и воспроизведя ее.
4. Отправьте в Службу технической поддержки следующие данные, предварительно запаковав их в один архив:
 - все файлы конфигурации вашего почтового агента (MTA);
 - файлы каталога `/etc/kav/`;
 - журнал событий почтовой программы;
 - журнал событий компонента Антивируса, например, `/var/log/aveserver.log`;

- информацию, которая выводится на консоль по команде **ps -ax**;
 - ключевой файл.
5. Обязательно укажите в запросе о наличии:
- SCSI-контроллера;
 - очень старого или нового процессора, нескольких процессоров;
 - размер памяти – если меньше, чем 64 МБ или больше 2 ГБ.
6. Укажите примерный размер дневного трафика и бывают ли пики нагрузки.

Вопрос: *Зачем нужны ежечасные обновления?*

Еще несколько лет назад вирусы передавались на дискетах, и для защиты компьютера достаточно было установить антивирусную программу и изредка обновлять базы. Но последние вирусные эпидемии распространялись по миру всего за несколько часов, и установленный Антивирус со старыми базами может оказаться бессильным перед новой угрозой. Для того чтобы не стать жертвой новых вирусов, необходимо обновлять базы ежедневно.

«Лаборатория Касперского» с каждым годом увеличивает частоту обновления баз Антивируса Касперского. Сейчас они обновляются каждый час.

Дополнительной функцией является задача обновления модулей Антивируса, в которых исправляются обнаруженные уязвимости или предоставляются новые функциональные возможности.

Вопрос: *Что изменилось в сервисе обновления, начиная с версии 5.0?*

В продуктовой линейке, начиная версии с 5.0, «Лаборатории Касперского» представлен новый сервис обновления. Разработка велась в соответствии с пожеланиями пользователей и маркетинговыми требованиями. Кроме того, стояла задача повысить технологичность всей процедуры обновлений, начиная с их подготовки в «Лаборатории Касперского» и заканчивая обновлением файлов у пользователей.

Преимущества нового сервиса обновления:

- *Дозагрузка файлов при разрыве соединения.* Теперь не нужно повторно скачивать уже полученные обновления после восстановления соединения.
- *Двукратное уменьшение размера кумулятивного обновления.* Кумулятивное обновление содержит в себе всю базу Антивируса Касперского, поэтому размер кумулятивного обновления значительно превышает размер обычного обновления. В новом сервисе применена специальная технология, позволяющая использовать уже имеющиеся базы для кумулятивного обновления.
- *Ускорение загрузки из интернета.* Антивирус Касперского выбирает сервер обновления «Лаборатории Касперского», расположенный в вашем регионе. Кроме того, нагрузка на серверы распределяется в соответствии с их производительностью, то есть вы не попадете на перегруженный сервер, в то время как другой сервер будет простаивать.
- *Применение «черных» списков ключей.* Это позволяют исключить обновление для пользователей, не имеющих ключа на использование Антивируса Касперского. В результате защищаемые пользователи не страдают от перегруженности серверов обновлений.
- *Для корпоративных продуктов реализована возможность создания локального сервера обновлений.* Такая функция востребована для организаций, где в одной локальной сети объединены компьютеры, защищенные приложениями «Лаборатории Касперского». В этом случае любой компьютер может быть превращен в сервер обновлений, который будет получать обновления из интернета, помещать их в локальный каталог и предоставлять к ним доступ другим компьютерам сети.

Вопрос: может ли злоумышленник подменить базы Антивируса Касперского?

Все базы имеют уникальную подпись, и при обращении к базам Антивирус Касперского проверяет ее. Если подпись не соответствует присвоенной в «Лаборатории Касперского», и дата баз – более поздняя, чем день окончания срока действия ключа на использова-

ние продукта, Антивирус Касперского не будет использовать такие базы.

Вопрос: *будет ли Антивирус Касперского для Unix Mail Servers работать на моем дистрибутиве операционной системы Linux?*

Тестирование Антивируса Касперского для Unix Mail Servers версии 5.5 производилось на дистрибутивах RedHat, Debian и SuSE и именно для них собирались дистрибутивы Антивируса Касперского.

О версиях поддерживаемых операционных систем см. п. 1.2 на стр. 9.

Если ваш дистрибутив совместим с поддерживаемым на сто процентов (например, ASPLinux совместим с Red Hat Linux), то вероятность возникновения проблем критического характера очень низка.

На дистрибутивах, не входящих в список поддерживаемых «Лабораторией Касперского», возможна некорректная работа приложения. Это, прежде всего, связано со спецификой операционной системы. Например, дистрибутив вашей системы использует другую версию библиотеки или имеет место нестандартное расположение скриптов инициализации системы. В таком случае Служба Технической Поддержки «Лаборатории Касперского» не сможет вам помочь.

Вопрос: *все работало хорошо, пока я не установил Антивирус Касперского для Linux Mail Servers и не выполнил его интеграцию с почтовой программой Postfix. После этого почтовые сообщения перестали проходить, и в maillog была зафиксирована следующая ошибка:*

```
Sep 23 15:17:03 server postfix/lmtp[1678]:  
8238C38987: to=<user@server.org  
<mailto:user@server.org>>, relay=none, delay=1,  
status=bounced (localhost: host not found)
```

Что мне делать?

Возникновение такой проблемы может быть в следующих случаях:

- в вашем DNS нет зоны localhost, наличие которой требуется по RFC 2606. Настройте ваш DNS так, как рекомендовано в RFC. Для более подробной информации смотрите <http://www.ietf.org/rfc/rfc2606.txt>.

- в файле `/etc/hosts` не определен IP-адрес для `localhost`. Добавьте в файл `/etc/hosts` строку:

```
127.0.0.1      localhost
```

Вопрос: возможно ли контролировать Антивирус Касперского посредством Network Control Centre для Windows?

Использование Network Control Centre для Windows при работе с Антивирусом Касперского для Unix Mail Servers невозможно. В данной версии приложения мы предусмотрели возможность удаленной конфигурации при помощи специального модуля к пакету Webmin.

Вопрос: как сохранить в файле то, что программа выводит на консоль?

Чтобы сохранить информацию, выводимую в процессе работы Антивирусом Касперского на консоль, нужно выполнить соответствующую настройку в конфигурационном файле, либо в командной строке ввести:

```
$ some_app > ./text_file 2>&1
```

где:

- **some_app** – приложение, строки стандартного вывода и вывода сообщений об ошибках в работе которого вы хотите сохранить в файле;
- **text_file** – полный путь к файлу, в котором будет храниться информация.

Пример:

```
$keepup2date > ./updater.log 2>&1
```

В данном случае в файл `updater.log` текущего каталога будут выведены стандартные сообщения вывода и сообщения об ошибках компонента `keepup2date`.

ПРИЛОЖЕНИЕ А. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ЗАО «Лаборатория Касперского» была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более четырехсот пятидесяти высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основным продуктом компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G

Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

А.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

Программа Новостной Агент предназначена для оперативной доставки новостей «Лаборатории Касперского», оповещения о «вирусной погоде» и появлении свежих новостей. С заданной периодичностью программа считывает с новостного сервера «Лаборатории Касперского» список доступных новостных каналов и содержащуюся в них информацию.

Новостной Агент также позволяет:

- визуализировать в системной панели состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антиви-

русную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в браузере. Таким образом, пользователи могут максимально оперативно получать ответ на вопросы, связанные с заражением вредоносными программами. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется непосредственно в браузере. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Антивирус Касперского® 7.0

Антивирус Касперского 7.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP – для исходящих) независимо от используемой почтовой программы, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно запустить анализ на присутствие вирусов только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе.* Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.
- *Наблюдение за процессами в оперативной памяти.* Антивирус Касперского 7.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.
- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.
- *Контроль скрытых процессов* позволяет бороться с сокрытием вредоносного кода в операционной системе с использованием технологий rootkit.
- *Эвристический анализатор.* При проверке какой-либо программы анализатор эмулирует ее исполнение и протоколирует все ее подозрительные действия, например, открытие или запись в файл, перехват векторов прерываний и т.д. На основе этого протокола принимается решение о возможном заражении программы вирусом. Эмуляция происходит в искусственной изолированной среде, что исключает возможность заражения компьютера.
- *Восстановление системы* после вредоносного воздействия программ-шпионов за счет фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;
- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы:* антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также воз-

можно проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;

- *проактивную защиту*: программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных скриптов на веб-страницах, всплывающих окон и рекламных баннеров). Функция *блокирования автоматического дозвола на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и блокировать их работу. Модуль *Защита конфиденциальных данных* обеспечивает защиту от несанкционированного доступа и передачи информации личного характера. Компонент *Родительский контроль* обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам.

Kaspersky Internet Security 7.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На основе *заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим *невидимости предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Sym-

bian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- *проверку по требованию* памяти мобильного устройства, карт памяти, отдельной папки либо конкретного файла. При обнаружении зараженного объекта он помещается на карантин или удаляется;
- *постоянную защиту*: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;
- *защиту от sms- и mms-спама*.

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare, Linux и Samba от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux File Server.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени*: все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- предотвращение вирусных эпидемий;
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- восстановление системы после заражения;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- соблюдение баланса загрузки системы;

- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- хранение резервных копий зараженных и удаленных объектов на тот случай, если потребуется их восстановление;
- изоляция подозрительных объектов в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;
- ведение детальных отчетов;
- автоматическое обновление баз программного продукта.

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Программный продукт включает в себя четыре продукта:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это продукт для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама;*
- *проактивная защита* от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;

- *отмена вредоносных изменений в системе;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *проверка электронной почты и интернет-трафика в режиме реального времени;*
- *блокирование всплывающих окон и рекламных баннеров при работе в интернете;*
- *безопасная работа в сетях любого типа, включая Wi-Fi;*
- *средства для создания диска аварийного восстановления, позволяющего восстановить систему после вирусной атаки;*
- *развитая система отчетов о состоянии защиты;*
- *автоматическое обновление баз;*
- *полноценная поддержка 64-битных операционных систем;*
- *оптимизация работы программного продукта на ноутбуках (технология Intel® Centrino® Duo для мобильных ПК);*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™).*

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз;*

- *использование технологии iSwift для исключения повторных проверок в рамках сети;*
- *распределение нагрузки между процессорами сервера;*
- *изоляция подозрительных объектов рабочих станций в специальном хранилище;*
- *отмена вредоносных изменений в системе;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *проверка электронной почты и интернет-трафика в режиме реального времени;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *защита при работе в беспроводных сетях Wi-Fi;*
- *технология самозащиты антивируса от вредоносных программ;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *автоматическое обновление баз.*

Kaspersky Enterprise Space Security

Программный продукт включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *защита рабочих станций и серверов от вирусов, троянских программ и червей;*
- *защита почтовых серверов Sendmail, Qmail, Postfix и Exim;*
- *проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *обработка сообщений, баз данных и других объектов серверов Lotus Domino;*

- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *предотвращение массовых рассылок и вирусных эпидемий;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа в беспроводных сетях Wi-Fi;*
- *проверка интернет-трафика в режиме реального времени;*
- *отмена вредоносных изменений в системе;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *система отчетов о состоянии системы защиты;*
- *автоматическое обновление баз.*

Kaspersky Total Space Security

Решение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;*

- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *защита почтовых серверов и серверов совместной работы*;
- *проверка интернет-трафика* (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *блокирование доступа с зараженных рабочих станций*;
- *предотвращение вирусных эпидемий*;
- *централизованные отчеты о состоянии защиты*;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *поддержка аппаратных прокси-серверов*;
- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- *использование технологии iSwift* для исключения повторных проверок в рамках сети;
- *динамическое перераспределение ресурсов* при полной проверке системы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *безопасная работа пользователей в сетях любого типа*, включая WiFi;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™);
- *отмена вредоносных изменений в системе*;
- *технология самозащиты антивируса от вредоносных программ*;
- *полноценная поддержка 64-битных операционных систем*;
- *автоматическое обновление баз*.

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Антивирус Касперского для Lotus Notes/Domino.
- Антивирус Касперского для Microsoft Exchange.
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- надежная защита от вредоносных и потенциально опасных программ;
- фильтрация нежелательной почтовой корреспонденции;
- проверка входящих и исходящих почтовых сообщений и вложений;
- антивирусная проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;
- проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino;
- *фильтрация сообщений* по типам вложений;
- изоляция подозрительных объектов в специальном хранилище;
- удобная система управления программным продуктом;
- предотвращение вирусных эпидемий;
- мониторинг состояния системы защиты с помощью уведомлений;
- *система отчетов* о работе приложения;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- автоматическое обновление баз.

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и

потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- Kaspersky Administration Kit.
- Антивирус Касперского для Proxy Server.
- Антивирус Касперского для Microsoft ISA Server.
- Антивирус Касперского для Check Point FireWall-1.

Среди его возможностей:

- надежная защита от вредоносных и потенциально опасных программ;
- *проверка интернет-трафика* (HTTP/FTP) в режиме реального времени;
- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- изоляция подозрительных объектов в специальном хранилище;
- удобная система управления;
- система отчетов о работе приложения;
- поддержка аппаратных прокси-серверов;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- автоматическое обновление баз.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая списки DNS Black List и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознать и уничтожить до девяноста пяти процентов нежелательного трафика.

Kaspersky® Anti-Spam представляет собой фильтр, который устанавливается на «входе» в сеть предприятия и проверяет входящий поток писем на предмет обнаружения спама. Продукт совместим с любой почтовой системой, используемой в сети заказчика, и может быть установлен как на уже существующий почтовый сервер, так и на выделенный.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации об-

разцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

Антивирус Касперского® для MIMESweeper обеспечивает высокоскоростную антивирусную проверку трафика на серверах, использующих Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

A.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-8707, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей персональных и бизнес-продуктов:	+7 (495) 797-8707, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-8700, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700, +7 (495) 645-79-39 +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru