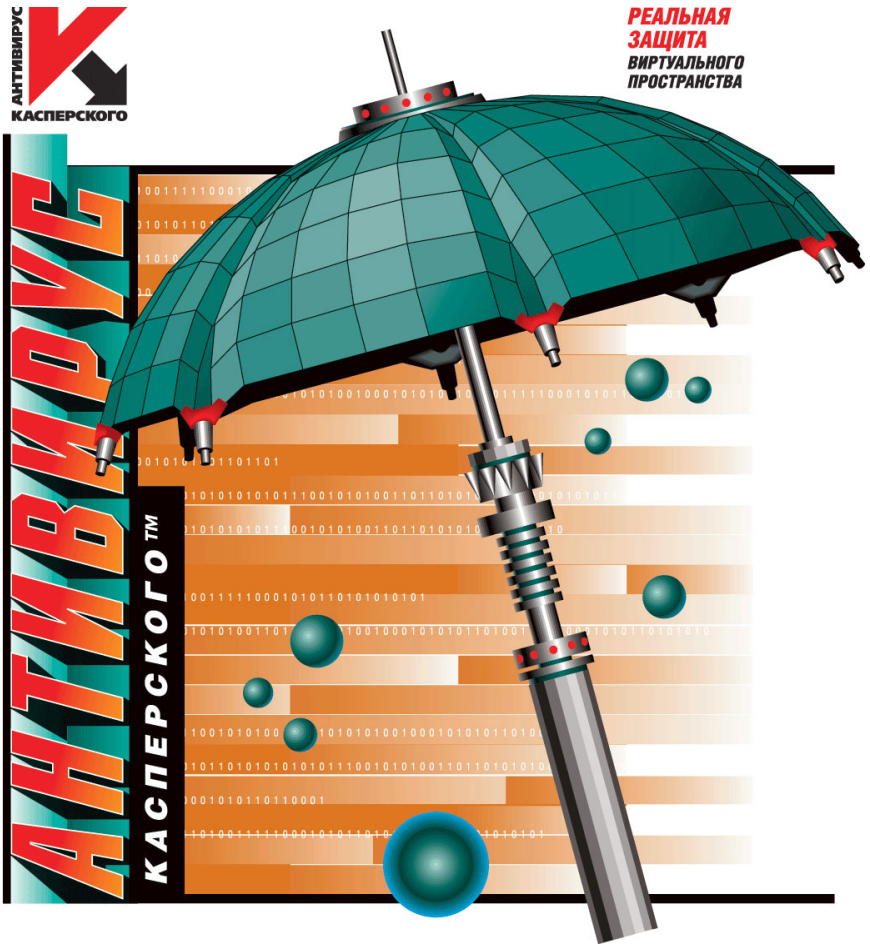
ЛАБОРАТОРИЯ КАСПЕРСКОГО



Антивирус Касперского® 5.0 для Sendmail с Milter API

Руководство администратора

АНТИВИРУС КАСПЕРСКОГО® 5.0
ДЛЯ SENDMAIL С MILTER API

Руководство администратора

Тел., факс: +7 (095) 797-87-00
http://www.kaspersky.ru

Дата редакции: сентябрь 2004 года

Содержание

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ SENDMAIL С MILTER API

Антивирус Касперского® для Sendmail с Milter API (далее также *Антивирус Касперского*) предназначен для антивирусной защиты почтового трафика Linux\Unix-сервера, использующего в качестве почтовой системы Sendmail с Milter API.

Приложение Антивирус Касперского для Sendmail с Milter API обеспечивает на почтовом сервере следующую функциональность:

- *Перехват входящих и исходящих почтовых сообщений сервера*.
- *Проверка потока сообщений на присутствие вирусов* с использованием антивирусного ядра. Проверяется как все письмо целиком, так и все его части: заголовок, тело, вложение (в зависимости от выбранной *политики антивирусной проверки*).
- *Резервное копирование почты* перед любой операцией, меняющей что-либо в сообщении, или перед его блокировкой и отклонением. Такая возможность позволяет в любой момент времени восстановить исходное письмо.
- *Антивирусная обработка зараженных элементов почтовых сообщений*, обнаруженных в результате проверки.
- *Фильтрация почтовых сообщений*. В настоящей версии предусмотрена MIME-фильтрация и фильтрация по имени и размеру вложенных файлов.
- *Уведомление отправителей, получателей и администраторов* о результатах антивирусной обработки или фильтрации почтовых сообщений. Предусмотрено также расширенное уведомление при помощи внешнего почтового агента.
- *Ведение общей статистики и отчетов* о результатах работы приложения.

Подробнее каждая из функций приложения будет рассмотрена в соответствующем разделе данного Руководства.

Антивирус Касперского для Sendmail с поддержкой Milter API также предоставляет дополнительные возможности:

- *Удаленная конфигурация Антивируса Касперского* через веб-интерфейс программы Webmin.
- *Создание собственных шаблонов уведомлений* отправителей, получателей и администраторов с использованием специального языка.

1.1. Аппаратные и программные требования к системе

Для нормального функционирования Антивирус Касперского для Sendmail с Milter API почтовый сервер должен удовлетворять следующим аппаратным и программным требованиям:

- Для почтового сервера с 250-300 почтовыми ящиками (адресами):
  - процессор 2xPentium Xeon с частотой 1,8 ГГц.
  - 1 ГБ оперативной памяти.
  - 100 МБ свободного места на диске (для работы приложения).
- Для почтового сервера с 100-150 почтовыми ящиками (адресами):
  - процесс Pentium III с частотой 900 МГц.
  - 512 МБ оперативной памяти.
- Одна из следующих операционных систем:
  - Linux RedHat (версия 8 или 9), Linux SuSE (версия 8.2, 9.0 или 9.1) или Linux Debian (версия 3.0).
  - FreeBSD версии 4.9, 4.10 или 5.2.1.
  - OpenBSD версии 3.4.
- Установленная почтовая система Sendmail версии 8.11.x или выше с Milter API.
- Установленная программа Webmin (www.webmin.com) для удаленного администрирования Антивируса Касперского.

1.2. Схемы лицензирования

Для приложения Антивирус Касперского 5.0 для Sendmail с Milter API предусмотрены следующие схемы лицензирования:

- Лицензирование по трафику.
- Лицензирование по почтовым адресам.

Какая именно из схем лицензирования будет активизирована, определяется лицензионным ключом.

Лицензирование по трафику подразумевает объем обрабатываемого приложением почтового трафика в день. Данная информация указывается в лицензионном ключе.

Лицензирование по почтовым адресам распространяется на почтовые адреса доменов, перечисленных в конфигурационном файле приложения, а также на почтовые адреса сервера, где установлен Антивирус Касперского, не входящих в доменную структуру.

Каждая из приведенных систем также подразумевает ограничение по времени использования приложения (как правило, один-два года, определяется ключом).

1.3. Комплект поставки

Программный продукт 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 программного продукта входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;
- руководство пользователя;
- лицензионный ключ, записанный на установочный компакт-диск или на отдельную 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 продукта в интернет-магазине вы копируете продукт с веб-сайта Лаборатории Касперского, в дистрибутив которого помимо самого продукта включено также данное руководство. Лицензионный 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 программный продукт.

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 программы 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, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных 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.

1.5. Принятые обозначения

Текст документации выделяется различными элементами оформления в зависимости от его смыслового назначения. В расположенной ниже таблице приведены используемые условные обозначения.

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.

Оформление	Смысловое назначение
 Примечание.	Дополнительная информация, примечания.
 Внимание!	Информация, на которую следует обратить особое внимание.
 *Чтобы выполнить действие,* 1. Шаг 1. 2. …	Описание последовательности выполняемых пользователем шагов и возможных действий.
 Задача, пример	Постановка задачи, примера для реализации возможностей программного продукта
 Решение	Реализация поставленной задачи
[ключ] – назначение ключа.	Ключи командной строки.
`Текст информационных сообщений и командной строки`	Текст конфигурационных фай, информационных сообщений программы и командной строки.

ГЛАВА 2. ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ

В зависимости от конфигурации почтового сервера и ваших нужд мы предлагаем следующие варианты развертывания Антивируса Касперского для Sendmail с Milter API:

- *на один сервер с почтовой системой*: этот базовый вариант используется при наличии на сервере уже установленной и настроенной почтовой системы Sendmail (см. п. 2.1 на стр. 12).
- *на выделенный сервер*: этот способ рекомендуется использовать при достаточно большой нагрузке на почтовый сервер (см. п. 2.2 на стр. 14).

В результате всех приведенных выше вариантов развертывания приложение будет функционировать совершенно идентично, отличие будет состоять лишь в обмене данными между Антивирусом Касперского и Sendmail.

Отдельным фактором, влияющим на эксплуатацию Антивируса, является наличие других Milter-фильтров в почтовой системе. При этом возможны следующие варианты установки Антивируса:

- *в качестве единственного Milter-фильтра*.
- *в сочетании с другими Milter-фильтрами*: этот вариант организации актуален в том случае, если на почтовом сервере уже установлен некоторый почтовый фильтр, например, Kaspersky Anti-Spam (см. п. 2.3 на стр. 15).

Рассмотрим подробнее каждую из схем развертывания.

2.1. Работа на одном сервере с почтовой системой

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

Порядок работы Антивируса Касперского для Sendmail с Milter API со входящей и исходящей почтой состоит из следующих этапов:

1. Почтовый поток сообщений поступает с других серверов либо от пользователей на вход Sendmail.
2. Почтовая система принимает поток сообщений и передает его на обработку Антивирусу Касперского через Milter API.
3. Антивирус Касперского обрабатывает почтовые сообщения в соответствии с настройками и возвращает их при помощи Milter API почтовой системе. Также Антивирус способен генерировать дополнительные почтовые сообщения и осуществлять их рассылку, используя внешний почтовый агент.
4. Почтовая система осуществляет маршрутизацию почтового трафика либо на внешние сервера, либо в почтовые ящики локальной сети.

Исходя из приведенной схемы работы при установке Антивируса Касперского вам необходимо внести изменения в конфигурацию Sendmail и Антивируса Касперского, касаемые сокета. При работе на одном сервере с почтовой системой рекомендуется использовать локальный сокет, поскольку он будет обеспечивать более быстрый обмен данными, нежели при использовании сетевого сокета. Итак, в конфигурацию Sendmail внесите следующие изменения:

1. если вы используете файл *sendmail.cf*:

   ```
   XKAVMilter, S=unix:socket_file_path,
   F=T,T=S:10m;R:15m;E:15m
   ```

   или

   ```
   XKAVMilter, S=local:socket_file_path,
   F=T,T=S:10m;R:15m;E:15m
   ```

2. если вы используете фай *sendmail.mc*:

   ```
   INPUT_MAIL_FILTER(`KAVMilter',
   `S=local:socket_file_path,
   F=T,T=S:10m;R:15m;E:15m')
   ```

   или

   ```
   INPUT_MAIL_FILTER(`KAVMilter',
   `S=unix:socket_file_path,
   F=T,T=S:10m;R:15m;E:15m')
   ```

3. В секцию **[kavmilter.global]** конфигурации Антивируса Касперского внесите следующие изменения:

```
ServiceSocket=unix:socket_file_path
```

или

```
ServiceSocket=local:socket_file_path
```

2.2. Работа на выделенном сервере

Если ваш почтовый сервер имеет достаточно большую нагрузку, имеет смысл установить Антивирус Касперского и осуществлять фильтрацию на выделенном сервере, дабы избежать перегрузок. Антивирусная проверка почтового трафика – достаточно ресурсоемкая процедура.

В данном случае имеет место следующая последовательность работы:

1. Почтовый трафик поступает на почтовый сервер с установленной системой Sendmail.
2. Sendmail направляет его на обработку Антивирусу Касперского, используя сетевой сокет.
3. Проверенная почта с уведомлениями, сформированными Антивирусом, передается обратно почтовой системе для доставки или дальнейшей маршрутизации.

В случае установки Антивируса на выделенный сервер для обеспечения приема трафика от Sendmail и его пересылки необходимо использовать сетевой сокет.

Итак, в конфигурацию Sendmail внесите следующие изменения:

1. если вы используете файл *sendmail.cf*:

   ```
   XKAVMilter, S= inet:1052@ip_address,
   F=T,T=S:10m;R:15m;E:15m
   ```

2. если вы используете фай *sendmail.mc*:

   ```
   INPUT_MAIL_FILTER(`KAVMilter',
   `S= inet:1052@ip_address,
   F=T,T=S:10m;R:15m;E:15m')
   ```

3. В секцию **[kavmilter.global]** конфигурации Антивируса Касперского внесите следующие изменения:

   ```
   ServiceSocket= inet:ip_address
   ```

2.3. Работа в качестве единственного или дополнительного фильтра

Антивирус Касперского может использоваться как в качестве единственного, так и дополнительного фильтра. Если на момент инсталляции приложения на вашем почтовом сервере уже были установлены некоторые фильтры почтового трафика, то вам необходимо определить их последовательность. Критерием выбора являются особенности фильтрации.

Если вы устанавливаете Антивирус Касперского перед некоторым фильтром, не забывайте о том, что после антивирусной обработки почтовые сообщения могут быть изменены (заголовки, тело и т.д.), почтовый поток может быть дополнен уведомлениями, часть трафика может быть удалена, или не принята к дальнейшей обработке. Соответственно, следующему после Антивируса Касперского фильтру поступит на вход измененный поток сообщений. Учитывайте это при организации процесса фильтрации следующих за Антивирусом фильтров. Например, можно исключить из фильтрации уведомления, формируемые Антивирусом Касперского.

Если вы устанавливаете Антивирус Касперского после некоторого фильтра, не забудьте настроить передачу потока сообщений от предыдущего фильтра к Антивирусу Касперского по сокету.

Также имейте в виду, что полученный Антивирусом почтовый трафик будет изменен предыдущим фильтром.

Итак, необходимо выполнить следующие настройки для установленных на почтовом сервере Milter-фильтров:

1. Внести изменения в конфигурацию Sendmail и Антивируса Касперского, касаемые сокета, аналогично приведенному описанию в п. 2.1 на стр. 12.
2. В конфигурации других установленных на почтовом сервере фильтров, которые будут использоваться до или после антивирусной фильтрации, выполните настройку передачи и приема данных от Антивируса через сокету.

ГЛАВА 3. УСТАНОВКА И УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Прежде чем приступить к установке Антивируса Касперского, мы рекомендуем вам:

1. Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. п. 1.1 на стр. 7).
2. Войти в систему под пользователем **root**.

3.1. Установка приложения на сервер под управлением Linux

Антивирус Касперского распространяется в трех вариантах инсталляции в зависимости от дистрибутива.

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 или OpenBSD

Для серверов, работающих под управлением операционной системы FreeBSD или OpenBSD, 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

Установка Антивируса Касперского производится в неинтерактивном режиме. В случае если какой-либо из шагов инсталляции не может быть выполнен, по завершении процедуры администратору необходимо выполнить его самостоятельно.

В процессе установки выполняются следующие шаги:

1. Создание группы и пользователя **kav**, под которым будет запускаться и работать Антивирус Касперского.
2. Добавление настроек приложения в файл */var/db/kav/applications.setup*, используемый для обновления антивирусных баз и модулей ядра.
3. Регистрация лицензионного ключа.

   Если на момент установки приложения лицензионный ключ отсутствует в поставке (например, вы приобрели Антивирус Касперского в интернет-магазине, и лицензионный ключ еще не доставлен вам по электронной почте), на консоль будет выведена соответствующая информация.

   Сразу после установки приложения вам необходимо будет произвести инсталляцию ключа самостоятельно, скопировав его в специальный каталог продукта.
4. Определение списка доменов, почта адресов которых будет защищаться от вирусов. В качестве домена по умолчанию используется домен системы, включая все поддомены, если они есть. Например, если ваш домен *domains.of.example.com*, то будет осуществляться антивирусная защита адресов следующих доменов: *example.com*, *of.example.com* и *domains.of.example.com*.
5. Регистрация сервиса *kavmilterd* в системе автоматического запуска на указанном уровне (в зависимости от системы, на которую выполняется установка приложения).
6. Поиск и автоматическое редактирование конфигурации почтовой системы Sendmail для использования антивирусного фильтра.

На данном шаге обязательно создается резервная копия исходной конфигурации Sendmail, которая восстанавливается в случае деинсталляции Антивируса Касперского.

После внесения изменений почтовая система перегружается для использования обновленной конфигурации. Если выполнить перезагрузку в процессе установки приложения не удалось, изменения конфигурации Sendmail не будут учтены. На консоль будет выведена соответствующая информация. Вам необходимо будет самостоятельно выполнить необходимые изменения конфигурации почтовой системы сразу после установки Антивируса Касперского, иначе антивирусная фильтрация почтового трафика сервера не будет осуществляться.

7. Запуск сервиса *kavmilter*, инициирующего антивирусную фильтрацию почтового трафика.
8. Регистрация cron-задачи автоматического обновления антивирусных баз и модулей ядра. Первое обновление будет выполнено через две минуты после завершения установки приложения. Последующие обновления будут выполняться каждый час.

Пожалуйста, проверьте, корректно ли настроены параметры прокси-сервера (см. п. А.1 на стр. 83, секция **[updater.options]**).

Также убедитесь, что запущен сервис cron, поскольку это необходимо для автоматического обновления приложения

9. Регистрация cron-задачи ежечасной проверки размера резервного хранилища (backup). При превышении ограничения в 128 МБ выполняется очищение хранилища на 20 процентов.
10. Формирование ссылок на справочную информацию по работе Антивируса Касперского, которая будет доступна по ключу командной строки **man**.

Обратите внимание на то, что модуль к программе Webmin не устанавливается в процессе инсталляции приложения.

Если вы хотите удаленно управлять приложением, установите модуль к Webmin вручную (подробнее см. п. 6.2 на стр. 40).

3.4. Постинсталляционная настройка

Во время установки Антивируса Касперского для Sendmail с Milter API выполняется необходимая конфигурация приложения и почтовой системы.

Возможно, понадобится выполнить дополнительные действия:

1. Установить лицензионный ключ, если он не был инсталлирован. Для этого скопируйте ключ в специальный каталог приложения, определенный параметром конфигурации **LicensePath**, и выполните перезагрузку приложения (подробнее о перезагрузке см. п. 6.15 на стр. 65).
2. Выполнить конфигурацию почтовой системы Sendmail для использования антивирусного фильтра, если это не удалось при установки приложения (см. п. 6.1 на стр. 38), а затем перезагрузить Sendmail.
3. Настроить в конфигурации Антивируса Касперского параметры прокси-сервера, если вы используете его для выхода в интернет (см. Приложение А на стр. 83). Это необходимо сделать для обновления антивирусных баз и модулей ядра.
4. Выполнить другую настройку приложения, если это необходимо (подробнее см. Глава 6 на стр. 38).
5. Установить модуль Антивируса Касперского к программе Webmin для удаленного управления продуктом (см. п. 6.2 на стр. 40).

3.5. Схема расположения файлов по каталогам

Если Антивирус Касперского установлен на сервер под управлением операционной системы Linux, имеет место следующее расположение каталогов:

/etc/kav/5.0/kavmilter/ – каталог, включающий конфигурацию приложения:

kavmilter.conf – конфигурационный файл приложения;

kavmilter.setup – конфигурационный файл, добавляемый в *applications.setup* для выполнения обновлений;

init.d/kavmilterd – сервис-скрипт, контролирующий работу исполняемого файла *kavmilter*.

profiles/ – каталог, содержащий конфигурацию предустановленных уровней.

/opt/kav/5.0/kavmilter/man – каталог расположения manual pages.

/opt/kav/5.0/kavmilter/bin – каталог исполняемых файлов приложения, таких как *kavmilter*, *keepup2date*, *licensemanager*.

/opt/kav/5.0/kavmilter/doc – каталог хранения документации по приложению.

/opt/kav/5.0/kavmilter/web – каталог хранения модуля удаленного управления *kavmilter.wbm* к программе Webmin.

/var/db/kav/5.0/kavmilter/ – каталог приложения, включающий:

backup/ – каталог хранения резервных копий почтовых сообщений;

bases/ – каталог, содержащий антивирусные базы и модули ядра;

bases/backup/ – каталог хранения резервной копии антивирусных баз и модулей ядра, создаваемой перед обновлением;

licenses/ – каталог, содержащий лицензионные ключи приложения;

patches/ – каталог для размещения обновлений модулей антивирусного ядра;

run/ – каталог для хранения файла, содержащего ID приложения;

templates/ – каталог, содержащий шаблоны уведомлений;

tmp/ – каталог хранения временных файлов.

/var/log/kav/5.0/kavmilter – каталог хранения файла отчета, если не выбран режим записи в системный журнал.

Если Антивирус Касперского установлен на сервер под управлением операционной системы xBSD, наблюдается следующее отличие в расположении каталогов приложения:

/etc/kav/5.0/kavmilter/ – каталог конфигурации приложения для OpenBSD.

/usr/local/etc/kav/5.0/kavmilter/ – каталог конфигурации приложения для FreeBSD.

/usr/local/share/kav/5.0/kavmilter/bin – каталог исполняемых файлов приложения.

/usr/local/share/kav/5.0/kavmilter/doc – каталог хранения документации.

/usr/local/share/kav/5.0/kavmilter/web – каталог хранения модуля удаленного управления *kavmilter.wbm* к программе Webmin.

/usr/local/man – каталог расположения manual pages.

При установке Антивируса Касперского на сервер под управлением операционной системы FreeBSD сервис-скрипт *kavmilterd*, контролирующий работу исполняемого файла *kavmilter*, должен быть размещен в каталоге */usr/local/etc/kav/5.0/kavmilter/rc.d/*

3.6. Удаление приложения с сервера под управлением Linux

В зависимости от дистрибутива, выбранного при установке приложения, для удаления Антивируса Касперского с сервера под управлением операционной системы Linux необходимо выполнить одну из приведенных ниже операций.

Для удвления Антивируса Касперского, установленного из rpm-пакета, в командной строке введите:

```
rpm –e <имя_файла_дистрибутива>
```

Для удаления Антивируса Касперского, установленного из deb-пакета в командной строке введите:

```
dpkg –r <имя_файла_дистрибутива>
```

3.7. Удаление приложения с сервера под управлением FreeBSD или OpenBSD

Для удаления Антивируса Касперского, установленного из pkg-пакета в командной строке введите:

```
pkg_delete <имя_пакета>
```

3.8. Процесс деинсталляции

Процедура удаления Антивируса Касперского включает последовательное выполнение следующих действий:

1. Удаление cron-задачи контроля резервного хранилища обработанных почтовых сообщений из списка задач пользователя **kav**.
2. Удаление cron-задачи обновления антивирусных баз и модулей ядра из списка задач пользователя **kav**.
3. Откат изменений конфигурации почтовой системы Sendmail, связанных с использованием антивирусного фильтра. Перезагрузка почтовой системы для использования обновленного файла конфигурации.
4. Остановка сервиса *kavmilter*. Начиная с данного момента, прекращается антивирусная фильтрация почтового трафика.
5. Откат регистрации сервиса *kavmilterd* в системе: в SySV-системах удаляются ссылки на каталог *rc.d*, в BSD-системах удаляются ссылки на соответствующий сервису скрипт, в OpenBSD – редактируется файл *rc.local*.
6. Откат регистрации приложения в системе: соответствующая секция удаляется из */var/db/kav/applications.setup*.
7. Удаление пользователя **kav** из системы.
8. Удаление ссылок на справочную информацию приложения.
9. Удаление временных файлов или каталогов, созданных в процессе работы Антивируса Касперского.
10. Удаление пакета Антивирус Касперского: удаляются все каталоги и файлы Антивируса, за исключением отчетов и конфигурационных файлов.

ГЛАВА 4. ПРЕДУСТАНОВЛЕННЫЕ УРОВНИ ЗАЩИТЫ

В поставку Антивируса Касперского для Sendmail с Milter API помимо *kavmilter.conf* входят дополнительные четыре конфигурационных файла, обеспечивающие защиту почтового сервера четырех видов:

kavmilter-high-security.conf – конфигурация приложения, обеспечивающая наиболее полную общую защиту почтового трафика сервера (см. п. 4.1 на стр. 24).

kavmilter-high-accuracy.conf – конфигурация, соответствующая максимальной антивирусной защите почтового трафика (см. п. 4.2 на стр. 24).

kavmilter-default.conf – конфигурация, оптимально сочетающая в себе защиту почтового трафика и нагрузку на сервер, которая при этом создается. Такая конфигурация позволяет комфортно работать с другими приложениями на сервере (см. п. 4.3 на стр. 25). Конфигурационный файл *kavmilter.conf*, используемый приложением по умолчанию, является точной копией данного файла.

kavmilter-high-scanspeed.conf – конфигурация, обеспечивающая высокую скорость проверки и обработки почтового трафика сервера за счет сокращения ряда функций приложения (см. п. 4.4 на стр. 26).

В зависимости от потребностей конкретного предприятия и для достижения наиболее эффективной работы приложения администратор может отредактировать любой из перечисленных файлов.

Все приведенные выше файлы после установки приложения хранятся в каталоге */etc/kav/5.0/kavmilter/profiles*.

Рассмотрим подробнее каждый из уровней.

4.1. Уровень наиболее полной защиты

Данный уровень обеспечивает полную защиту почтового трафика сервера и информирование получателей, отправителей и администраторов об антивирусной обработке почтовых сообщений. Реализация полной защиты выполняется за счет следующей конфигурации приложения:

1. Используется комбинированная политика проверки почтовых сообщений: каждое письмо проверяется на присутствие вирусов целиком, а затем каждая его часть отдельно, независимо от того, обнаружены зараженные объекты или нет.
2. Включена фильтрация почтовых сообщений по MIME-типу, имени и размеру вложенных файлов, а также по имени вируса.
3. Резервная копия создается для каждого письма, подвергаемого антивирусной обработке или фильтрации, и сопровождается информационным файлом.
4. Все зараженные почтовые сообщения или их части подвергаются антивирусной обработке. Если лечение не удалось – письмо или его часть удаляются.
5. Все поврежденные письма или их части заменяются соответствующими уведомлениями. Все защищенные объекты, проверить которые на вирусы невозможно, удаляются.
6. Уведомления о выполненных действиях над письмом или его частью отправляются получателю, отправителю и администратору.
7. В отчет выводятся все сообщения и события о работе приложения.

4.2. Уровень максимальной надежности

На данном уровне защиты по сравнению с предыдущим сокращается объем фиксируемой в отчете информации. Однако повышается уровень антивирусной защиты за счет удаления и поврежденных и защищенных объектов. Такие объекты проверить на присутствие вирусов невозможно, следовательно, нет гарантии избежать заражения:

1. Используется комбинированная политика проверки почтовых сообщений: каждое письмо проверяется на присутствие вирусов

целиком, а затем каждая его часть отдельно, независимо от того, обнаружены зараженные объекты или нет.

2. Включена фильтрация почтовых сообщений по MIME-типу и имени вложенных файлов.
3. Резервная копия создается для каждого письма, подвергаемого антивирусной обработке, и сопровождается информационным файлом.
4. Все зараженные почтовые сообщения или их части подвергаются антивирусной обработке. Если лечение не удалось – письмо или его часть удаляются.
5. Все защищенные и поврежденные письма или их части удаляются, заменяясь при этом соответствующими уведомлениями.
6. Уведомления о выполненных действиях над письмом или его частью отправляются получателю, отправителю и администратору.
7. В отчет выводятся все сообщения и события о работе приложения, за исключением отладочной информации.

4.3. Оптимальный уровень защиты

Защита данного уровня обеспечивает оптимальное соотношение антивирусной проверки и обработки почтового трафика и скорости ее выполнения:

1. Проверяются почтовые сообщения целиком, анализ отдельных частей выполняется только в том случае, если письмо идентифицировано как зараженное.
2. Включена фильтрация почтовых сообщений по MIME-типу и имени вложенных файлов.
3. Резервная копия создается для каждого письма, подвергаемого антивирусной обработке; информационный файл не формируется.
4. Все зараженные почтовые сообщения или их части подвергаются антивирусной обработке. Если лечение не удалось – письмо или его часть удаляются.
5. Все защищенные и поврежденные письма или их части удаляются, заменяясь при этом соответствующими уведомлениями.
6. Уведомления о выполненных действиях над письмом или его частью отправляются получателю и отправителю. Администратор не уведомляется.

7. В отчет выводятся все сообщения и события о работе приложения, за исключением отладочной информации.

4.4. Уровень максимального быстродействия

Данный режим ориентирован на обеспечение максимальной скорости работы приложения, однако в данном случае надежность антивирусной защиты несколько снижается.

1. Проверяются почтовые сообщения целиком, анализ отдельных частей выполняется только в том случае, если письмо идентифицировано как зараженное.
2. Фильтрация почтовых сообщений отключена.
3. Резервная копия создается для каждого письма, подвергаемого антивирусной обработке; информационный файл не формируется.
4. Все зараженные почтовые сообщения или их части подвергаются антивирусной обработке. Если лечение не удалось – письмо или его часть удаляются.
5. Все защищенные и поврежденные письма пропускаются без проверки на присутствие вирусов.
6. Уведомления о выполненных действиях над письмом или его частью отправляются только получателю. Администратор и отправитель не уведомляются.
7. В отчет выводятся сообщения и события только критического и информационного характера, а также сообщения об ошибках.

ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

Основной и главной функцией Антивируса Касперского для Sendmail с Milter API является антивирусная проверка и обработка почтового трафика сервера, на котором установлено приложение. Однако есть и другие функции, которые позволяют расширить применение приложения в рамках конкретной компании, например, фильтрация почтовых сообщений по вложениям, резервное копирование и т.д.

В данном разделе мы рассмотрим на наш взгляд наиболее часто используемые задачи, реализуемые посредством приложения. Для более детального изучения всех возможных функций Антивируса Касперского для Sendmail с Milter API рекомендуем вам прочесть Глава 6 на стр. 38.

Обращаем ваше внимание на то, что в приведенных далее примерах будет освещаться только та часть конфигурации приложения, которая относится непосредственно к реализации поставленных задач. Причем для каждой задачи приводится ее реализация только средствами редактирования конфигурационного файла. В документации не рассматривается удаленная настройка задач через Webmin.

Большинство приведенных далее примеров требуют изменения конфигурации приложения, а, следовательно, и последующей его перезагрузки. Это необходимо для того, чтобы все изменения вступили в силу (подробнее см. п. 6.14 на стр. 64).

5.1. Доставка адресатам вылеченных почтовых сообщений

Главной задачей Антивируса является проверка почтового трафика и лечение зараженных почтовых сообщений с использованием антивирусных баз.

Если в результате антивирусной проверки было выявлено, что почтовое сообщение или его часть заражены, и попытка лечения такого сообщения не удалась, рекомендуется отправлять получателю такого сообщения уведомление, комментирующее данную ситуацию.

Задача: проверять все входящие сообщения и их вложения на присутствие вирусов; пытаться лечить зараженные письма и их части; в случае если вылечить письмо невозможно, удалить зараженную его часть, заменив ее соответствующим уведомлением; отправить письмо с уведомлением получателю письма; в системный журнал выводить всю информацию по почтовым сообщениям; вести статистику по сообщениям, вирусам и ресурсам в xml-формате.

Для реализации данной задачи необходимо выполнить следующую конфигурацию приложения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.engine]
ScanArchives=yes
ScanPacked=yes
ScanCodeanalyzer=yes

[kavmilter.actions]
DefaultAction=cure

[kavmilter.notifications]
EnableNotifications=on
NotifyRecipients=infected
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject=”Anti-virus notification message”

[kavmilter.log]
LogFacility=syslog
```

```
LogOption=scan.all

[kavmilter.statistics]
TrackStatistics=all
DataFormat=xml
DataFile=/var/opt/kav/log/statistics.data
```

5.2. Блокирование доставки адресатам зараженных почтовых сообщений

Блокировка почтовых сообщений может осуществляться несколькими способами: администратор может принять решение удалить зараженное письмо без предварительного уведомления об этом получателя, а также вернуть отправителю такого сообщения код ошибки, якобы отправленный почтовым агентом.

Задача: блокировать доставку зараженных почтовых сообщений получателям, удаляя их; отправлять уведомление администратору.

Для выполнения поставленной задачи в конфигурационном файле приложения задайте следующие значения для параметров:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.engine]
ScanArchives=yes
ScanPacked=yes
ScanCodeanalyzer=yes

[kavmilter.actions]
DefaultAction=drop
```

```
[kavmilter.notifications]
EnableNotifications=on
SendmailPath=/usr/sbin/sendmail
NotifyAdmin=infected
AdminAddresses=admin@localhost
UseCustomTemplates=on
AdminSubject=”Anti-virus notification message”
```

Задача: не принимать зараженные сообщения; отправлять отправителю код ошибки; уведомлять администратора о выполненных действиях.

```
[kavmilter.global]
ScanPolicy=message

[kavmilter.actions]
DefaultAction=reject

[kavmilter.notifications]
EnableNotifications=on
SendmailPath=/usr/sbin/sendmail
NotifyAdmin=infected
AdminAddresses=admin@localhost
UseCustomTemplates=on
AdminSubject=”Anti-virus notification message”
```

5.3. Доставка защищенных почтовых сообщений

Возможно возникновение ситуации, когда проверить почтовое сообщение или его часть не представляется возможным, поскольку оно может быть защищено паролем или зашифровано. В данном случае администратор должен быть уверен, что получатель сможет самостоятельно обезвредить сообщение, если оно окажется зараженным

Задача: обеспечить доставку почтовых сообщений, даже если они заражены; уведомлять администратора о выполненных действиях.

Для реализации поставленной задачи в конфигурации приложения выполните следующие изменения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.actions]
ProtectedAction=skip

[kavmilter.notifications]
EnableNotifications=on
SendmailPath=/usr/sbin/sendmail
NotifyAdmin=all
AdminAddresses=admin@localhost
UseCustomTemplates=on
AdminSubject=”Anti-virus notification message”
```

5.4. Отправка уведомления отправителю, получателю и администратору

Антивирус Касперского предоставляет возможность уведомлений в случае обнаружения зараженного сообщения.

Адреса отправителя и получателя, на которые отправляются уведомления, наследуются из исходного почтового сообщения.

Адреса администраторов необходимо определить в качестве значения параметра **AdminAddresses** секции **[kavmilter.notifications]**.

Для отправки уведомления достаточно произвести следующую настройку конфигурации:

```
[kavmilter.notifications]
```

```
EnableNotifications=on
NotifySender=infected
NotifyRecipients=infected
NotifyAdmin=infected
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject="Anti-virus notification message"
```

Вы можете менять формат уведомлений. Подробнее об этом см. п. 6.9 на стр. 46.

Рассмотрим несколько примеров конфигурации уведомлений.

Задача: уведомлять получателя и администратора о том, что зараженное письмо не было принято к доставке (действие над зараженным объектом – *reject*). Отправителю сообщения отправить уведомление в виде кода ошибки якобы о невозможности почтовым агентом доставить почтовое сообщение адресату.

Для реализации поставленной задачи в конфигурации приложения выполните следующие изменения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.actions]
DefaultAction=reject

[kavmilter.notifications]
EnableNotifications=on
NotifySender=infected
NotifyRecipients=infected
NotifyAdmin=infected
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
```

```
RejectReply="Message rejected because it contains
malware"
```

Задача: уведомлять получателя и администратора о том, что почтовое сообщение, содержащее защищенные объекты, не было подвержено антивирусной обработке (действие над защищенным объектом – *skip*).

Для реализации поставленной задачи в конфигурации приложения выполните следующие изменения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.actions]
ProtectedAction=skip

[kavmilter.notifications]
EnableNotifications=on
NotifyRecipients=protected
NotifyAdmin=protected
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject="This message was NOT scanned by KAV!"
```

Задача: информировать получателя, отправителя и администратора о сообщении, подвергнутом фильтрации. В любое почтовое сообщение, проверяемое Антивирусом Касперского, вставлять дополнительный заголовок с информацией о приложении.

Для реализации поставленной задачи в конфигурации приложения выполните следующие изменения:

```
[kavmilter.global]
ScanPolicy=combined
AddxHeader=yes
```

```
[kavmilter.actions]
DefaultAction=cure

[kavmilter.filter]
IncludeSize=10
FilteredSizeAction=skip

[kavmilter.notifications]
EnableNotifications=on
NotifySender=filtered
NotifyRecipients=filtered
NotifyAdmin=filtered
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject="Anti-Virus notification message"
SendmailPath=/usr/sbin/sendmail
UseCustomTemplates=on
```

5.5. Фильтрация почты по вложениям

Фильтрация почтовых сообщений может производиться по трем критериям: по имени вложения, по MIME-типу вложения и по его размеру.

Задача: доставлять почтовые сообщения, вложения которых меньше 500 КБ, без дополнительной обработки; обязательной фильтрации подвергать почтовые сообщения, содержащие вложение с именем *loveletter*, удаляя их; отправлять получателю и администратору уведомление о выполненных действиях над объектом почтового сообщения.

Для выполнения поставленной задачи требуется внести следующие изменения в конфигурацию приложения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.engine]
ScanArchives=yes
ScanPacked=yes
ScanCodeanalyzer=yes

[kavmilter.actions]
DefaultAction=cure

[kavmilter.filter]
IncludeSize=500
FilteredSizeAction=skip
IncludeName=loveletter.*
FilteredNameAction=delete

[kavmilter.notifications]
EnableNotifications=on
NotifyRecipient=filtered
NotifyAdmin=all
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject=”Anti-virus notification message”
SendmailPath=/usr/sbin/sendmail
UseCustomTemplates=on
```

5.6. Обновление антивирусных баз и ядра приложения

В текущей версии приложения во время установки его на сервер регистрируется cron-задача обновления антивирусных баз и антивирусного ядра. Обновление выполняется каждые четыре часа с момента установки Антивируса Касперского для Sendmail с Milter API.

Если вам необходимо выполнить обновление самостоятельно, не дожидаясь запуска данной задачи по расписанию, воспользуйтесь специальным скриптом *keepup2date.sh*, входящим в поставку приложения. Для этого в командной строке введите:

```
keepup2date.sh –run
```

5.7. Резервное копирование почтовых сообщений (backup)

Перед выполнением каких-либо действий над почтовыми сообщениями или их частями полезно сохранять копии исходных объектов на случай, если в них возникнет необходимость.

Задача: проверять почтовый трафик на присутствие вирусов и лечить все зараженные объекты; все объекты, вылечить которые не удастся – удалять; каждый раз перед выполнением лечения или удаления создавать копию письма с полным его описанием; уведомлять получателя и администратора о выполненных действиях над почтой.

Для выполнения поставленной задачи в конфигурацию приложения необходимо внести следующие изменения:

```
[kavmilter.global]
ScanPolicy=combined

[kavmilter.engine]
ScanArchives=yes
ScanPacked=yes
```

```
ScanCodeanalyzer=yes

[kavmilter.actions]
DefaultAction=cure

[kavmilter.backup]
BackupPolicy=info
BackupOption=cured, deleted
BackupDir=/var/opt/kav/backup

[kavmilter.notifications]
EnableNotifications=on
NotifyRecipient=infected
NotifyAdmin=all
AdminAddresses=admin@localhost
MessageDir=/etc/kav/5.0/kavmilter/messages/
MessageSubject=”Anti-virus notification message”
SendmailPath=/usr/sbin/sendmail
UseCustomTemplates=on
```

ГЛАВА 6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА

В данном разделе мы подробно остановимся на дополнительных настройках функциональности Антивируса Касперского. В отличие от необходимых настроек, выполняемых в процессе инсталляции (см. Глава 2 на стр. 12), без которых использование приложения невозможно, дополнительные настройки осуществляются по усмотрению администратора. Они направлены на расширение возможностей приложения и его настройку для использования в рамках конкретного предприятия.

6.1. Интеграция с почтовой системой

Если в процессе установки интеграция с почтовой системой Sendmail не была выполнена, вы можете сделать это посредством специальной утилиты *kavmilter-setup.sh*. После внесения изменений в конфигурацию Sendmail необходимо перегрузить. Также возможно откатить выполненные изменения.

Вы можете использовать следующие ключи командной строки:

–add-filter – изменить конфигурационный файл Sendmail;

–del-filter – откатить изменения в конфигурации Sendmail, удалив дополнения;

–check-filter – проверить конфигурацию Sendmail на предмет добавления фильтра *kavmilter*. Если фильтр добавлен, на консоль будет выведено **yes**, если не добавлен – **no**.

–set-filter <действие> – выберите дальнейшие действия Sendmail в случае если фильтр *kavmilter* не доступен (в результате превышения установленных ограничений, холодной перезагрузки и т.д.). Эти действия прописываются в конфигурации почтовой системы в определении фильтра. Возможно использование следующих действий:

tempfail – отказ клиентского соединения с возвращением кода ошибки 451 (например, *451 4.7.1 Please try again later*);

reject – отклонение любых входящих сообщений в возвращением кода ошибки 554 (например, *554 not accepting messages*);

pass – пропускать почту (возможно, к другому фильтру), даже если фильтр *kavmilter* не проверил их. Данное действие подвергает риску получателей;

–add-service – зарегистрировать запуск *kavmilter* как сервиса (в формате SySV или запуск из *rc.local*);

–del-service – отменить регистрацию *kavmilter* как сервиса и откатить все изменения в измененных файлах;

–check-service – проверить, зарегистрирован ли *kavmilter* как сервис и запущен ли он при старте операционной системы. Если фильтр зарегистрирован и запущен, на консоль будет выведено **yes**, если не зарегистрирован – **no**;

–add-product – добавить файл конфигурации приложения *kavmilter.setup* в */var/d/kav/applications.setup*, который используется для обновлений;

–del-product – удалить файл конфигурации приложения *kavmilter.setup* из */var/d/kav/applications.setup*;

–check-product – проверить, добавлен ли файл конфигурации приложения *kavmilter.setup* в */var/d/kav/applications.setup*. Если файл добавлен, на консоль будет выведено **yes**, если не добавлен – **no**;

–default-domains – определить имя домена и добавить его и все поддомены в конфигурационный файл приложения в качестве значения параметра **LicensedUsersDomains**. Этот ключ используется только в случае использования *схемы лицензирования по почтовым адресам* (подробнее см. п. 1.2 на стр. 8).

Поскольку Sendmail может использовать в качестве конфигурационного файла сгенерированный *sendmail.cf* или mc-файл *sendmail.mc*, решение о том, в какой именно будет вноситься информация о фильтре kavmilter, принимается автоматически в соответствии со следующими условиями:

- Если файл *sendmail.mc* не существует или значением переменной окружения USE_SENDMAIL_CF является *sendmail.cf*, или бинарный m4-файл не найден в системе, тогда в качестве файла конфигурации почтовой системы используется */etc/mail/sendmail.cf*.

- Если значением переменной окружения USE_SENDMAIL_MC является *sendmail.mc*, тогда в качестве файла конфигурации почтовой системы используется *sendmail.mc* . В него добавляется директива INPUT_MAIL_FILTER, определяющая использование *kavmiter* в качестве фильтра.

- Если оба конфигурационных файла существуют, и переменная окружения строго не определяет использование одного из них, используется *sendmail.mc*.

При работе на сервере под управлением операционной системы OpenBSD Sendmail по умолчанию использует конфигурационный файл *localhost.cf*. Антивирус Касперского вносит изменения именно в данный файл конфигурации.

Помните, если вы работаете на сервере под управлением OpenBSD и запускаете Sendmail с использованием другого конфигурационного файла (ключ **–C**) или запускаете Sendmail с ключами командной строки или только с ключом **–bd**, Sendmail будет использовать в качестве конфигурационного файла *sendmail.cf*.

6.2. Установка и удаление модуля удаленного управления

Антивирус Касперского предоставляет возможность удаленно управлять своими настройками и запуском \ остановкой задач с помощью программы Webmin. Для этого необходимо установить программу Webmin, установить к ней Webmin-модуль Антивируса Касперского и произвести некоторую предварительную настройку.

Описание установки программы Webmin см. в документации к данному продукту.

Для установки Webmin-модуля Антивируса Касперского выполните следующие действия:

1. Откройте страницу вашего Webmin в браузере.
2. Выберите **Webmin Configuration** и перейдите к разделу конфигурации **Webmin Modules**.
3. В разделе **Install Module** выберите установку модуля из файла (**From local file**) и укажите полный путь к Webmin-модулю Антивируса Касперского *kavmilter.wbm* в соответствующем поле ввода.

   Для Linux по умолчанию модуль расположен в каталоге */opt/kav/5.0/kavmilter/web/kavmilter.wbm*, для FreeBSD и OpenBSD – */usr/local/share/kav/5.0/kavmilter/web/kavmilter.wbm*.
4. Нажмите на кнопку **Install Module From File**.

В результате модуль **KAV for Sendmail** будет добавлен на закладку **Others**.

После того, как модуль будет установлен, откройте его (**Others → KAV for Sendmail**), откройте закладку **Module Config** и проверьте, верно ли указаны пути к основным файлам и каталогам Антивируса Касперского.

Далее вы можете настроить совместную работу Антивируса с пакетом Webmin. Например, средствами Webmin можно ограничить доступ к работе с программой, организовав систему паролей для пользователей (подробнее о настройке программы Webmin см. документацию по данному продукту).

Обратите внимание на то, что все примеры в данном Руководстве приведены с использованием конфигурационного файла. Настройка и запуск задач удаленно не описывается, поскольку структура интерфейса модуля сходна с порядком секций и параметров в конфигурационном файле.

Чтобы получить справку по параметрам конфигурации в модуле Webmin, используйте справку. Открыть ее можно по кнопке **?** в правом верхнем углу раздела конфигурации.

Чтобы удалить модуль управления Антивирусом Касперского, выполните следующие действия:

1. Откройте программу Webmin.
2. Выберите **Webmin Configuration** и перейдите к разделу конфигурации **Webmin Modules**.
3. В разделе **Delete Module** выберите модуль **KAV for Sendmail** и нажмите на кнопку **Delete Selected Modules**.

Для того чтобы переустановить модуль удаленного управления, удалите его и установите заново.

При переустановке все пути к основным файлам и каталогам продукта, приведенные на закладке **Module Config**, сохранятся.

6.3. Определение политики проверки почтовых сообщений

Антивирус Касперского предоставляет возможность администратору почтового сервера самостоятельно регулировать степень антивирусной проверки входящих и исходящих почтовых сообщений. Осуществляется это с помощью выбора политики проверки.

Предусмотрены следующие два типа политики:

- **message** – проверка на присутствие вирусов путем анализа всего письма целиком, не обращая внимания на его отдельные части (заголовок, тело, вложение). Такая политика также позволяет обнаруживать вирусы, которые поражают почтовые сообщения MIME-формата, повреждая их при этом. Проверка незараженных почтовых сообщений выполняется быстрее, поскольку не проверяются

  Если в результате проверки письмо будет идентифицировано как незараженное, не выполняется анализ его частей, оно передается почтовой системе для доставки адресату. Это обеспечивает более быструю проверку незараженных писем, нежели при комбинированной политике (см. далее).

  Если окажется, что письмо заражено вирусом, и в качестве его обработки выбрано действие **cure** или **delete**, то выполняется последовательный анализ всех его частей.

- **combined** – антивирусная проверка всего письма целиком, а затем, независимо от результатов анализа всего письма, проверка каждой его части (заголовка, тела, вложения).

В каждой из приведенных политик для анализа почтового сообщения по частям выполняется его разделение на составляющие компоненты, затем проверка на присутствие вирусов каждой из них и восстановление целостности письма.

Как видно из определений, политика **message** менее строгая в проверке почты на вирусы, следовательно, требует для выполнения меньше времени и ресурсов. Политика **combined** же напротив достаточно детальная и обеспечивает максимально полный анализ почтовых сообщений.

Тип используемой политики определяется в конфигурации приложения с помощью параметра **ScanPolicy** секции **[kavmilter.global]**.

6.4. Детализация антивирусной проверки

Администратор почтового сервера также может контролировать детализацию антивирусной проверки, а именно:

- Использовать ли *эвристический анализатор кода* при проверке почтовых сообщений.

Эвристика позволяет анализировать почтовые сообщения на присутствие *модифицированного вредоносного кода* (похож на код известного вируса) и возможно вредоносного кода (код похож на вирусную сигнатуру), то есть находить новые вирусы, записей о которых еще нет в антивирусных базах. Использование данной технологии регулируется параметром **ScanCodeAnalyser** секции **[kavmilter.engine]**.

- Как долго проверять почтовое письмо или его часть на присутствие вирусов.

  Количество секунд, в течение которых выполняется поиск вирусов в почтовом сообщении или его части, определяется посредством параметра **MaxScanTime** и по умолчанию равно десяти секундам. Если за это время не удастся проверить объект целиком, он пропускается.

- Сколько объектов проверять на присутствие вирусов.

  Администратор может ограничить количество запросов на антивирусную проверку почтовых сообщений посредством параметра **MaxScanRequests**. По умолчанию количество запросов не ограничено. Вводить данное ограничение рекомендуется в том случае, если антивирусная проверка приводит к большой нагрузке на сервер.

6.5. Выбор объектов проверки

В процессе антивирусной проверки почтового трафика сервера выполняется поиск вирусов и во вложениях сообщений.

Поскольку проверка архивов и упакованных исполняемых файлов требует достаточного количества времени и ресурсов сервера, администратор может самостоятельно определить необходимость их анализа на присутствие вирусов.

Проверка таких вложений почтовых сообщений на вирусы регулируется параметрами **ScanArchives** и **ScanPacked** секции **[kavmilter.engine]**. По умолчанию проверка архивов и упакованных исполняемых файлов выполняется.

Внимание! Проверка архивов, защищенных паролем, не выполняется! Такому вложению при анализе присваивается статус **Protected**, и дальнейшие действия Антивируса Касперского в отношении данного объекта определяются параметром **ProtectedAction** секции **[kavmilter.actions]**.

6.6. Статусы почтовых сообщений по результатам проверки

Результатом антивирусной проверки почтовых сообщений антивирусным ядром является код (не выводится на консоль, является внутренним кодом приложения), который определяет статус проанализированного объекта:

Clean – в почтовом сообщении или его части не обнаружено вирусов.

Error – почтовое сообщение или его часть повреждены или в результате их проверки возникла ошибка.

Protected – почтовое сообщение или его часть защищены паролем или другими средствами защиты, и выполнить их анализ на присутствие вирусов не удалось.

Infected – почтовое сообщение или его часть содержит вредоносный код (информация о нем имеется в антивирусных базах или он обнаружен в результате эвристического анализа кода).

В результате неудавшейся попытки лечения зараженным почтовым сообщениям присваивается статус **CureFailed**.

На основании приведенных выше статусов выполняется дальнейшая обработка почтовых сообщений.

6.7. Настройка способа обработки объектов

Следующим за проверкой этапом антивирусной защиты является обработка почтовых сообщений или их частей в соответствии с присвоенным им статусом (см. п. 6.6 на стр. 44).

В качестве действия над зараженным почтовым сообщением вы можете выбрать одно из приведенных ниже:

warn – заменить зараженное письмо или объект уведомлением о том, что объект заражен;

cure – пытаться лечить зараженный объект письма; если лечение невозможно – удалить его, заменив соответствующим уведомлением;

drop – принять сообщение, но не отправлять его адресату, а удалить;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

skip – передать почтовое сообщение для доставки без обработки;

delete – удалить зараженный объект письма, заменив его соответствующим уведомлением.

В конфигурации приложения выполняемое над зараженным объектом действие определяется параметром **DefaultAction** секции **[kavmilter.action]**. По умолчанию все зараженные почтовые сообщения или их части подвергаются лечению.

В качестве действия над защищенным или зашифрованным почтовым сообщением вы можете выбрать **skip** или **delete**.

Для обработки почтовых сообщений, в результате проверки которых произошла ошибка, вы можете выбрать **warn**, **skip** или **delete**.

При выполнении действий **warn**, **cure** и **delete** формируется почтовое уведомление, которое заменяет зараженное письмо и содержит описание произведенных над объектом действий. По умолчанию исходное почтовое сообщение (для действий **warn** и **delete**) или обработанное (для действия **cure**) присоединяется к уведомлению и отправляется отправителю, получателю и администратору. Вы можете настраивать тексты уведомлений, редактируя соответствующие шаблоны (см. п. 6.11 на стр. 49).

6.8. Выбор объектов фильтрации и действий над ними

Дополнительно к антивирусной проверке и обработке почтовых сообщений вы можете использовать их антивирусную фильтрацию. Данная процедура выполняется на уровне объектов почтового сообщения и может осуществляться по MIME-типу вложений, по их имени и по размеру.

Следует отметить, что в данной версии приложения при выполнении фильтрации **выполняется анализ вложений только по заголовкам объектов**, содержание объектов не рассматривается.

Рассмотрим подробнее все критерии, влияющие на процедуру фильтрации почтовых сообщений:

- Если вы хотите включить возможность фильтрации почтовых сообщений, вам НЕОБХОДИМО ОПРЕДЕЛИТЬ ХОТЯ БЫ ОДИН ТИП ИЛИ РАЗМЕР ВЛОЖЕНИЯ, в соответствии с которым будет проходить фильтрация, в качестве значения параметров **IncludeMime**, **IncludeName** и **IncludeSize** секции **[kavmilter.filter]**.

- Типы объектов почтовых сообщений из множества объектов **IncludeMime**, **IncludeName** и **IncludeSize**, которые вы хотите исключить из процесса фильтрации (например, по вашему мнению, в них не может содержаться вирусов и других вредоносных программ), нужно указать в качестве значений параметров **ExcludeMime**, **ExcludeName** и **ExcludeSize**.

Для объектов, подверженных фильтрации, вы можете назначить следующие правила обработки (соответствующие значения задайте для параметров **FilteredMimeAction**, **FilteredNameAction** и **FilteredSizeAction**):

delete – удалить объект из письма, заменив его соответствующим уведомлением;

skip – передать почтовое сообщение с таким объектом почтовой системе для доставки без обработки; в данном случае соответствующая информация будет зафиксирована в отчете о работе приложения;

drop – принять сообщение, но не отправлять его адресату, а удалить;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

warn – заменить письмо или объект уведомлением;

rename – переименовать вложение с использованием следующего правила: последняя буква расширения вложения заменяется подчеркиванием "_", например, расширение *exe* будет заменено на *ex_*, *com* – на *co_* и так далее. Данное действие не применимо к MIME-типам вложений.

6.9. Настройка резервного копирования почтовых сообщений

Резервное копирование почтовых сообщений – дополнительная функция Антивируса Касперского, позволяющая сохранять копию каждого почтового сообщения в специальном хранилище перед любой его модификацией. Это дает возможность сохранять исходные письма на случай, если будет необходимость вернуться к ним.

Предусмотрены следующие политики создания резервных копий:

message – формируется только копия исходного почтового сообщения;

info – создается копия почтового сообщения и информационный файл (данная политика используется по умолчанию);

none – резервное копирование отключено.

Для определения политики задайте соответствующее значение параметра **BackupPolicy** секции **[kavmilter.backup]**.

Рассмотрим список видов почтовых сообщений, для которых предусмотрена возможность создания резервной копии:

cured – почтовые сообщения, подвергаемые лечению;

deleted – письма, хотя бы одна часть которых будет удалена;

dropped – письма, которые были приняты, но не будут отправлены;

rejected – не принятые почтовые сообщения;

warning – почтовые сообщения, любая часть которых будет заменена уведомлением;

renamed – почтовые сообщения, подвергаемые фильтрации (MIME-тип) или переименованию;

all – письма всех перечисленных выше типов.

Чтобы определить, для каких именно сообщений будет формироваться копия, задайте соответствующее значение для параметра **BackupOption**.

Все резервные копии хранятся в каталоге, определяемом параметром **BackupDir** и, как было отмечено выше, могут также содержать в себе сопроводительный информационный файл. Данный файл включает информацию об отправителе и получателе, действии над письмом, перед выполнением которого была создана данная копия и др.

В процессе работы Антивируса хранилище резервных копий писем достаточно быстро наполняется, следовательно, нуждается в периодическом очищении от устаревших или не представляющих особой ценности почтовых сообщений. Эту и другие операции с резервными копиями можно выполнить посредством специальной утилиты *backup-sweeper.sh*, входящей в состав приложения. Утилита регистрируется в системе как задача cron сразу после установки приложения и позволяет:

- распределять резервные копии писем в специально создаваемые каталоги хранилища, имена которых имеют следующий формат: *год-месяц-день*;
- проверять размер хранилища и уведомлять администратора, если размер приближается к критическому;
- удалять наиболее старые каталоги с копиями.

Поддерживаются следующие ключи командной строки для данной утилиты:

–install – сформировать задачу cron выполнения данной утилиты для пользователя по умолчанию;

–uninstall – удалить задачу cron выполнения утилиты для пользователя по умолчанию;

–size – определить максимальный размер хранилища резервных копий сообщений. По умолчанию размер составляет 10 МБ;

–warn-only – игнорировать заданный максимальный размер хранилища, отправлять уведомление администратору о текущем размере хранилища и о его превышении, если оно есть;

–delete-oldest – удалять каталоги с самой старой датой формирования, если наблюдается превышение максимального размера хранилища;

Ключи **–warn-only** и **–delete-oldest** не могут быть использованы одновременно, поскольку являются взаимоисключаемыми.

–path – изменить каталог хранения резервных копий почтовых сообщений, указав полный путь к каталогу.

6.10. Настройка обновления антивирусных баз и модулей ядра

Запуск обновления антивирусных баз и ядра выполняется автоматически каждые четыре часа после установки Антивируса Касперского на сервер. Это обуславливается созданной в процессе установки приложения cron-задачей.

В качестве ресурсов для обновления используется сервер обновлений Лаборатории Касперского, определенный параметром **UpdateServerUrl** конфигурации приложения.

Если для выхода в интернет вы используете прокси-сервер, не забудьте указать его IP-адрес в качестве значения параметра **ProxyAddress** секции **[updater.options]**.

Если в качестве источника обновления вы хотите использовать локальный каталог, задайте значение **no** для параметра **UseUpdateServerUrl** и укажите полный путь к каталогу хранения обновлений (параметр **UpdateServerUrl**).

Перед обновлением всегда выполняется резервное копирование баз и модулей ядра на случай неудачной попытки обновления для восстановления предыдущей версии. Каталог хранения резервной копии

определяется параметром **BackUpPath**. Таким образом, вы всегда можете вернуться к использованию предыдущей версии антивирусных баз, а также восстановить более ранние модули антивирусного ядра.

Если возникла необходимость настроить общие параметры, такие как, например имя пользователя, под которым запускается процесс обновления, или выполнить запуск обновления самостоятельно, воспользуйтесь утилитой *keepup2date.sh* и следующими ключами командной строки:

–install – сформировать задачу cron выполнения данной утилиты для пользователя по умолчанию;

–uninstall – удалить задачу cron выполнения утилиты для пользователя по умолчанию;

–run – запустить обновление антивирусных баз и ядра; в случае неудавшейся попытки обновления выполнится откат уже произведенных обновлений до состояния на момент начала обновления;

–user – задать отличное от используемого по умолчанию имя пользователя, под которым запускается и работает утилита на сервере.

6.11. Настройка уведомлений

Уведомление – это почтовое сообщение, содержащее описание обработанного письма и отправляемое получателю, отправителю и администратору сервера.

Помимо описания самого почтового сообщения уведомление содержит также описание объектов, которые были по тем или иным причинам удалены из сообщения.

Предусмотрена также возможность вставки исходного почтового сообщения в уведомление. Однако это возможно только для уведомления получателя. Для администратора и отправителя создаются новые почтовые сообщения, содержащие только текст уведомления.

Все уведомления, содержание и формирование которых администратор может настроить, можно разделить на следующие две группы:

- *Стандартное уведомление* – уведомление, которое может быть основано как на едином шаблоне, так и на разных шаблонах в зависимости от ситуации. Такое уведомление отправляется:
    - *Получателю сообщения* посредством Milter API. Новое сообщение не создается; текст уведомления встраивается в обработанное письмо.

- *Администратору и отправителю сообщения* с использованием внешнего почтового агента Sendmail. Формируются отдельные почтовые сообщения, в которые по необходимости можно вставить исходное письмо. Как правило, такой способ отправки уведомлений используется для администратора в случае выполнения действия **drop** или **reject**.

- *Специальное уведомление администратора* – уведомление, формируемое и отправляемое администратору в исключительных случаях, например, при возникновении критической ошибки в процессе работы Антивируса Касперского. Такое уведомление также отправляется с использованием внешнего почтового агента Sendmail.

Вы можете самостоятельно создавать шаблоны уведомлений (подробнее см. п. 6.11.2 на стр. 53).

Все параметры формирования уведомления содержатся в секции **[kavmilter.notifications]** конфигурационного файла приложения.

Уведомления могут быть сформированы при возникновении следующих событий:

Infected – уведомлять о почтовом сообщении, которому в результате антивирусной проверки был присвоен статус **Infected** и над ним было выполнено одно из следующих действий: **reject**, **drop**, **warn**, **cure** или **delete**.

Protected – уведомлять о почтовом сообщении, которое защищено, и проверить его на вирусы невозможно, в результате над почтовым сообщением было выполнено действие **delete** или **skip**.

Error – уведомлять о почтовом сообщении, в результате проверки которого возникла ошибка (или оно повреждено), над почтовым сообщением было выполнено одно из следующих действий: **warn**, **delete** или **skip**.

Filtered – уведомлять о почтовом сообщении, которое было подвержено фильтрации, над письмом было выполнено одно из следующих действий: **delete**, **skip** или **rename**.

All – уведомлять обо всех событиях, перечисленных выше.

None – не отправлять уведомление.

Если вы хотите отправлять уведомление об одном из приведенных выше событий, задайте соответствующее значение для параметров **NotifySender**, **NotifyRecipients** и **NotifyAdmin**.

Языковая версия уведомлений зависит от установленной в конфигурации приложения кодировки (параметр **Charset** секции **[kavmilter.notifications]**). Также можно настроить шифрование уведомлений посредством параметра **TransferEncoding**.

Например, для формирования русского текста уведомления необходимо

1. установить следующие значения для параметров:

```
[kavmilter.notifications]
Charset=koi8-r_1251
TransferEncoding=8bit
```

2. сформируйте шаблон уведомления на русском языке.

6.11.1. Шаблоны уведомлений

В процессе формирования уведомлений используются следующие шаблоны (хранятся в каталоге, определенном параметром **MessageDir** конфигурации приложения):

- **Шаблон уведомлений для описания удаленных объектов** – текст, который встраивается в исходное почтовое сообщение в том случае, если какая-либо его часть в результате антивирусной обработки или фильтрации была удалена. Данный текст может содержать макросы, детализирующие причины, по которым объект был удален. Предусмотрены следующие шаблоны:
    - *part_infected_deleted* – текст, заменяющий в исходном почтовом сообщении объект, который был удален в результате неудавшейся попытки его лечения;
    - *part_filtered_deleted* – текст, заменяющий в исходном почтовом сообщении MIME-объект, удаленный в результате фильтрации объектов MIME-типа;
    - *part_filtered_rename* – текст, заменяющий в исходном почтовом сообщении объект, который был переименован в результате фильтрации;
    - *part_protected_deleted* – текст, заменяющий в исходном почтовом сообщении защищенный объект, который не удалось проверить на вирусы, и, как следствие, он был удален;
    - *part_error_deleted* – текст, заменяющий в исходном почтовом сообщении объект, в результате проверки которого произошла ошибка, и его пришлось удалить.

- **Шаблон стандартного уведомления** – текст, единый для отправителя, получателя и администратора, для отправки которого используется Milter API. Текст шаблона может содержать макросы, детализирующие действия, которые были выполнены над исходным почтовым сообщением. Предусмотрены следующие шаблоны:
    - *message_default_notify* – текст, используемый по умолчанию для уведомлений получателя, отправителя и администраторов о выполненных над почтовым сообщением действиях;
    - *message_infected_warn* – текст, заменяющий зараженное почтовое сообщение;
    - *message_filtered_warn* – текст, заменяющий почтовое сообщение, подвергнутое фильтрации;
    - *message_error_warn* – текст, заменяющий письмо, в результате проверки которого произошла ошибка.
- **Шаблон расширенного уведомления** – текст, используемый для уведомления конкретного лица, заинтересованного в получении информации об антивирусной обработке исходного почтового сообщения. Разработан отдельный шаблон для уведомления отправителя, получателя и администратора. Для использования таких шаблонов необходимо задать для параметра **UseCustomTemplates** значение **on**. Предусмотрены следующие шаблоны:
    - *message_sender_notify* – текст уведомления отправителя почтового сообщения о выполненных над исходным письмом действиях;
    - *message_recipients_notify* – текст уведомления получателя почтового сообщения о выполненных над исходным письмом действиях;
    - *message_admin_notify* – текст уведомления администратора почтового сообщения о выполненных над исходным письмом действиях.
- **Шаблон специального уведомления администратора** – текст, используемый для формирования специальных уведомлений об исключительных событиях, требующих отдельного внимания администратора. Предусмотрены следующие шаблоны:
    - *message_admin_discard* – текст, используемый для уведомления администратора о том, что исходное почтовое сообщение не было принято для доставки (действие **reject** или **drop**);

- *message_admin_fault* – текст, используемый для уведомления администратора о том, что во время работы Антивируса возникла критическая ошибка;
- *Уведомление администратора об истечении срока действия лицензии* или о ее превышении формируется и отправляется приложением трижды (за неделю, за три дня и в день окончания лицензии). Редактирование текста уведомления или регулирование его отправки недоступно для администратора.

Во время запуска приложения выполняется проверка наличия всех перечисленных выше шаблонов. Если хотя бы одного их них не будет, приложение возвращает ошибку.

Также производится проверка размера каждого шаблона, который не должен превышать 8 КБ.

6.11.2. Создание собственных шаблонов уведомлений

Антивирус Касперского предоставляет возможность создавать собственные шаблоны уведомлений для администраторов, получателей и отправителей с использованием специального языка уведомлений.

Язык уведомлений представляет собой набор макросов и управляющих конструкций.

Рассмотрим подробнее все составляющие языка, его синтаксис и ряд примеров.

6.11.2.1. Макросы

Макрос – это элемент подстановки, используемый в шаблонах почтовых уведомлений. В формируемом на основе шаблона тексте макрос заменяется на некоторое значение.

Синтаксис макроса: %имя_макроса%

Если вы хотите включить символ % в имя макроса, такой символ должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57).

Макрос может иметь несколько значений. В этом случае при использовании %имя_макроса% будет использоваться последнее из указанных значений.

Для использования нескольких значений макроса необходимо использовать *итерационные конструкции*.

6.11.2.2. Итерационные конструкции

Итерационная конструкция – это основной элемент языка уведомлений, с использованием которого формируются шаблоны уведомлений

Синтаксис конструкции:

<FOR INAME **IOP** IVALUE**>**BODY**</FOR>**

где:

<FOR – начало определения конструкции. Символ <, не являющийся началом определения конструкции, должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57);

INAME – имя конструкции формата **1*(nchar)*(nchar)**; максимальная длина имени составляет 64 байта;

IOP – операция сравнения формата **==**, **|**, **!=**; длина 2 байта;

IVALUE – значение конструкции формата **1*(vchar)*(vchar)**, максимальная длина составляет 4096 байт. Значение итерационной конструкции обязательно должно быть выделено кавычками. В случае сравнения значения конструкции со значением, имеющим кавычку, необходимо использовать скрывающий (escape) символ (подробнее см. п. 6.11.2.5 на стр. 57). Например:

<FOR *_macro_name_parent_* == "\"_value_1\""**>**

> – конец определения итерационной конструкции, начало определения тела итератора. Символ >, не являющийся концом определения конструкции, должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57);

BODY – тело итератора формата ***(char)**;

</FOR> – конец определения тела итератора. Символ <, не являющийся концом определения тела итератора, должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57);

… – разделитель формата ***( )*(\t)**

nchar – символы из набора a-z, A-Z, 0-9, -, _

vchar – символы из набора nchar, *, ?

char – символы из набора значений 32 – 255

Пример итерационной конструкции:

<**FOR** _macro_name_ == "*">%_macro_name_%</**FOR**>

При выполнении данной конструкции препроцессор разделяет ее на следующие условные конструкции:

```
<FOR _macro_name_ == "_value_1">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_2">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_3">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_N">%_macro_name_%</FOR>
```

Эти условные конструкции выполняются последовательно.

Таким образом, итерационные конструкции позволяют выделять как конкретное значение макроса, так и группу значений.

Например, если макрос `%FILTERNAME%` имеет значения `KAVFilter1`, `KAVFilter2`, `KAVFilter3`, `SimpleFilter`, тогда:

конструкция:

```
<FOR FILTERNAME == "KAVFilter1">%FILTERNAME%</FOR>
```

будет преобразована в текст:

```
KAVFilter1
```

конструкция:

```
<FOR FILTERNAME `= "KAVFilter?">%FILTERNAME%, </FOR>
```

будет преобразована в текст:

```
KAVFilter1, KAVFilter2, KAVFilter3
```

конструкция:

```
<FOR FILTERNAME != "KAVFilter2">%FILTERNAME%, </FOR>
```

будет преобразована в текст:

```
KAVFilter1, KAVFilter3, SimpleFilter
```

конструкция:

```
<FOR FILTERNAME != "KAV*">%FILTERNAME%, </FOR>
```

будет преобразована в текст:

```
    SimpleFilter,
```

6.11.2.3. Границы видимости итерационной конструкции

Любая итерационная конструкция может иметь вложенные макросы, чье значение определено только в границе видимости данной конструкции. Итерационные конструкции могут использоваться не только для вывода конкретных значений макроса, но и для обозначения границ видимости вложенных макросов.

Границы видимости вложенного макроса задаются открывающим и закрывающим тегом условной конструкции:

```
<F0R _macro_name_parent_ ==
"_value_1">%_macro_name_child_%</F0R>
```

При этом область действия макроса %*_macro_*name*_parent_%* распространяется на все вложенные уровни (попадающие между указанными тегами), если значение макроса не перекрыто.

6.11.2.4. Переменные

Переменные используются для определения большей гибкости при составлении шаблонов.

Для определения переменной в заданной области видимости предусмотрена следующая конструкция:

```
<DEF _var_name_ = "_const_value_"/>
```

В дальнейшем эта переменная может быть использована как обычный макрос безо всяких ограничений.

Синтаксис определения переменной:

```
<DEF VNAME V0P VVALUE/>
```

где:

- `<DEF` – начало конструкции определения переменной. Символ <, не являющийся началом определения, должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57);
- `VNAME` – имя переменной формата **1*(nchar)*(nchar)**; максимальная длина составляет 64 байта;
- `VOP` – операция присваивания формата **=**, длина 1 байт;
- `VVALUE` – значение переменной формата **1*(vchar)*(vchar)**; максимальная длина составляет 4096 байт. Значение переменной обязательно должно быть выделено кавычками. В случае

сравнения со значением, имеющим кавычку, необходимо использовать скрывающий (escape) символ (подробнее см. п. 6.11.2.5 на стр. 57). Пример конструкции определения переменной:

<DEF _value_name_ = "\"_value_1\""/**>**

> – конец конструкции определения переменной. Символ >, не являющийся концом определения переменной, должен быть скрыт (подробнее см. п. 6.11.2.5 на стр. 57). Конструкция DEF не имеет тела, как конструкция FOR, поэтому закрывающая скобка её тега должна уведомлять парсер об отсутствии закрывающего тега.

… – разделитель формата ***( )*(\t)**

nchar – символы из набора a-z, A-Z, 0-9, -, _

vchar – символы из набора nchar, *, ?

В случае переопределения переменной в границах её области видимости подстановка нового значения будет производиться после каждого переопределения. Таким образом, конструкция:

```
<DEF __NAME__= "ИМЯ_1"/>Сейчас мы увидим первое
значение: %__NAME__%.
<DEF __NAME__= "ИМЯ_2"/>Сейчас мы увидим второе
значение: %__NAME__%.
```

будет преобразована в следующий текст:

```
Сейчас мы увидим первое значение: ИМЯ_1.
Сейчас мы увидим второе значение: ИМЯ_2.
```

Переменная может иметь макрос в качестве значения.

<DEF _var_name_ = "% macro_name %"/**>**

В этом случае препроцессор сначала заменит переменную на макрос, а затем – на его значение.

6.11.2.5. Синтаксис языка

Служебные символы

% признак макроса. Макрос располагается между двумя знаками "%". Пример: %VIRUSNAME%

< открывающая скобка тега.
Пример: <FOR FILTERNAME == "KAVFilter1">

> закрывающая скобка тега.
Пример: `<FOR FILTERNAME == "KAVFilter1">`

</ открывающая скобка закрывающего тега.
Пример: `</FOR>`

/> закрывающая скобка тега конструкции без тела.
Пример: `<DEF __NAME __= "ИМЯ_1"/>`

**** escape-символ. Отменяет действие следующей за ним лексемы.
Пример: `\%VIRUSNAME\%`

== сравнение: совпадение по маске или значению.
Пример: `<FOR FILTERNAME == "KAVFilter1">`
Пример: `<FOR FILTERNAME == "KAVFilter*">`

!= сравнение: несовпадение по маске или значению.
Пример: `<FOR FILTERNAME != "KAVFilter1">`
Пример: `<FOR FILTERNAME != "KAVFilter*">`

***** Все возможные значения неограниченного размера.
Используется только внутри тегов при сравнении с шаблонами.
Пример: `<FOR FILTERNAME == "KAV*">`

? Все возможные значения размером в один символ.
Используется только внутри тегов при сравнении с шаблонами.
Пример: `<FOR FILTERNAME == "KAVFilter?">`

Комментарий, парсер игнорирует все символы, начиная с # до конца строки.

Служебные слова

FOR Определение итерационной конструкции.
Пример: `<FOR FILTERNAME = "KAVFilter1">`

DEF Определение переменной (конструкция без закрывающего тега). Пример: `<DEF __NAME__= "ИМЯ_1"/>`

Предопределённые макросы

%CRLF% Макрос перевода строки (CR+LF)

%TAB% Макрос табулятора

Вся обработка ведется внутри глобальной секции, не определенной никакой конструкцией, либо внутри условной конструкции
`<FOR KAV_LANGUAGE == "5.0"> ... </FOR>`

Escape-последовательности

В языке уведомлений поддерживаются следующие последовательности:

- Для вывода в текст шаблона символа '\' необходимо использовать последовательность '\\'.
- Строка, оканчивающаяся escape-символом '\', продолжается на следующей строке. При этом escape-символ выводится на экран как символ перевода строки. При обработке, такая строка объединяется со следующей строкой перед тем, как разборщиком предприняты другие действия по обработке шаблона. Действие такого escape-символа сохраняется независимо от того, встретился ли он внутри или снаружи тега.

  При необходимости поместить символ '\' в конец строки так чтобы он не принимал значение продолжения строки, необходимо использовать последовательность '\\'.
- Для вывода в текст шаблона символа '%' необходимо использовать последовательность '\%'.
- Для вывода в текст шаблона символа '/' необходимо использовать последовательность '\/'.
- Для вывода в текст шаблона символа '<' необходимо использовать последовательность '\<'.
- Для вывода в текст шаблона символа '>' необходимо использовать последовательность '\>'.
- Для вывода в текст шаблона символа '#' необходимо использовать последовательность '\#'.

Язык отчетов чувствителен к регистру.

Количество пробелов или символов табуляции (а также их наличие либо отсутствие) между лексемами языка никак не оговаривается.

Служебные слова должны выделяться пробелами или символами табуляции либо служебными символами языка.

6.11.2.6. Макросы уведомлений в составе приложения

В поставку приложения входит ряд макросов, которые могут использоваться как в шаблонах уведомлений по почтовому сообщению в целом, так и в шаблонах по удаленным частям писем. Они позволяют наполнять текст уведомлений более подробной информацией об исходном письме или объекте, а также о действиях, выполненных над ними.

Администратор может использовать следующие макросы в уведомлениях по почтовому сообщению в целом:

%CLIENT_ADDR% – удаленный адрес почтового клиента.

%SENDER_ADDR% – адрес отправителя почтового сообщения.

%RECPT_ADDR% – адрес получателя.

%HEADERS% – заголовок сообщения.

%BK_ACTION% – действие над почтовым сообщением, в результате которого была создана резервная копия (если таковая была создана).

%BK_LOCATION% – полный путь к каталогу хранения резервной копии почтового сообщения (если таковая была создана).

%ACTION_LIST% – список, содержащий информацию о письме и его отдельных частях, а также набор действий, выполненных над почтовым сообщением. Информация представляется в виде **статус действие информация** для каждой обработанной части письма.

В уведомлениях по удаленным частям почтового сообщения могут использоваться следующие макросы:

%STATUS% – статус объекта, присвоенный в результате антивирусной проверки или фильтрации.

%ACTION% – действие, которое было выполнено над объектом на основании его статуса.

%INFO% – информация, имеющая отношение к выполненным действиям:

- список обнаруженных вредоносных программ – для зараженных объектов;
- поясняющая строка к коду ошибки – для объектов, в результате проверки которых возникла ошибка;

- MIME-тип или имя вложения – для объектов, подвергнутых фильтрации.

Макросы нужно указать непосредственно в тексте шаблонов уведомлений.

6.12. Настройка параметров формирования отчетов

Результаты работы Антивируса Касперского фиксируются в отчете о работе приложения. Причем, для хранения данной информации вы можете выбрать системный журнал или отдельный файл (определяется значением параметра **LogFacility** секции **[kavmilter.log]**).

В отчете фиксируются:

- *События, связанные с функционированием приложения* – все события, которые возникают в процессе работы приложения, и являются некоторыми результатами его функционирования. Например, результаты проверки почтовых сообщений.
- *События, не связанные с функционированием приложения* – все события, напрямую не связанные с работой Антивируса, однако несущие очень важную информацию. Например, размер хранилища резервных копий, ошибки в процессе работы программы, события, имеющие отношение к лицензионной политике и т.д.

Администратор может настраивать, какие именно категории информации он хочет видеть в отчете, а также определять детализацию каждой из выбранных категорий.

Итак, рассмотрим подробнее категории информации и ее детализацию.

Предусмотрены следующие категории информации, подлежащие фиксированию в отчете:

config – сообщения, относящиеся к конфигурации приложения;

scan – информация о статусах антивирусной проверки и о выполненных действиях;

backup – сообщения, относящиеся к резервному копированию почтовых сообщений;

internal – системные сообщения инициализации приложения, сигналы, процессы;

all – все перечисленные выше типы сообщений.

Каждая категория информации, фиксируемой в отчете, может подразделяться на уровни детализации:

critical – критические события, прерывающие работу приложения;

error – события, отражающие возникновение ошибок в работе приложения, которые могут как приводить, так и не приводить к остановке приложения;

warning – события, которые фиксируют возникновение необычной ситуации в ходе работы приложения; администратору полезно знать о таких событиях;

notice – события, связанные с бизнес-логикой приложения;

info – события общего характера, отражающие работу приложения;

debug – события отладочного характера;

all – все приведенные выше варианты событий.

Вы можете комбинировать категории информации и уровни ее детализации. Например, чтобы в отчет выводилась вся информация, относящаяся к резервному копированию, в конфигурационном файле задайте следующее значение:

```
LogOption=backup.all
```

Для вывода в отчет только сообщений об ошибках конфигурации приложения:

```
LogOption=config.error
```

Для того чтобы определить, какую информацию вы не хотите выводить в отчет, достаточно воспользоваться следующим правилом:

```
LogOption=-scan.debug
```

Префикс перед комбинацией обозначает отключение вывода информации такого рода в отчет, вся остальная информация выводится.

Файл отчета наполняется достаточно быстро, следовательно, его размер становится большим и влияет на скорость записи в него новых сообщений.

Для того чтобы избежать снижения скорости, необходимо воспользоваться функцией ротации файлов отчетов (параметр **LogRotate=on**).

Если данный режим используется, каждый раз при превышении заданного размера файла отчета (параметр **RotateSize**), он будет переименовываться в файл с именем *kavmilter.<число_ротации>.log*, а новая информация будет по-прежнему записываться в файл *kavmilter.log*.

В результате будут созданы файлы отчетов *kavmilter.1*.log, *kavmilter.2.log* и так далее. Общее количество ротаций определяется параметром **RotateRounds**. Как только число файлов отчетов превысит заданное этим параметром, для фиксирования сообщений будет использоваться самый старый файл отчетов.

6.13. Настройка параметров формирования отчета о результатах обновлений

Результаты выполнения обновлений антивирусных баз и модулей ядра Антивируса Касперского фиксируются в отчете, который выводится в файл или системный журнал (параметр **ReportFileName** секции **[updater.report]**).

Объем выводимой информации вы можете откорректировать путем изменения *уровня детализации отчета*.

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

В таблице, приведенной ниже, перечислены все возможные уровни детализации отчета.

Уровни	Название уровня	Значение
	Фатальные ошибки	информация только о критических ошибках (ошибках, которые приводят к завершению работы программы из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при загрузке баз.
1	Ошибки	информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов.
2	Информация	важные сообщения информационного характера; например: информация о том, запущен ли компонент, путь к конфигурационному файлу, информация об антивирусных базах, о лицензионных ключах, результирующая статистика.
3	Обновление	сообщения о процедуре обновления.

Уровни	Название уровня	Значение
10	Отладочная информация	все сообщения отладочного характера; например, содержание конфигурационного файла.

Информация о фатальных ошибках в процессе обновления выводится всегда вне зависимости от установленного уровня детализации. По умолчанию задан уровень **10**.

Для определения уровня детализации отчета задайте соответствующее значение для параметра **ReportLevel** секции **[updater.report]**.

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 отчета (первая буква, соответствующая названию уровня детализации).

Формат представления даты и времени вы можете изменить в секции **[locale]** конфигурационного файла.

`STRING` – строка отчета

6.14. Редактирование параметров статистики

Во время работы приложения формируется общая статистика результатов его функционирования:

- *Статистика по почтовым сообщениям* – общая информация по почтовым сообщениям, включающая количество входящих сообщений, проверенных Антивирусом сообщений, защищенных писем, поврежденных сообщений и общий размер всех писем.
- *Статистика по использованным ресурсам* – общая информация о затраченных ресурсах на проверку и обработку сообщений. Здесь

фиксируется общий объем почтового трафика, среднее время проверки одного почтового сообщения и т.д.

- *Статистика по обнаруженным вирусам* – информация по последним десяти обнаруженным вирусам и IP-адресам, с которых было отправлено наибольшее количество вирусов.

Для того чтобы определить, какого рода статистику вы хотите получать, задайте одно из следующий значений для параметра **TrackStatistics** секции **[kavmilter.statistics]**:

none – не формировать статистику работы приложения;

message – формировать статистику по почтовым сообщениям;

resources – формировать статистику по используемым ресурсам;

viruses – формировать статистику по вирусам;

all – формировать статистику по почтовым сообщениям, ресурсам и вирусам.

Статистика может быть представлена в текстовом или xml-формате (формат определяется значением параметра **DataFormat** секции **[kavmilter.statistics]**).

Полный путь к файлу, содержащему статистику, определяется параметром **DataFile**.

6.15. Перезагрузка Антивируса Касперского

Существует ряд событий, при возникновении которых необходима перезагрузка приложения. Перезагрузка выполняется различными способами в зависимости от ситуации:

- Изменение конфигурации приложения.

  Для того чтобы новые настройки приложения вступили в силу, требуется перезагрузка Антивируса Касперского с помощью скрипта *kavmilter*.

  Вы можете использовать следующие ключи командной строки для запуска/остановки/перезагрузки приложения:

  start – проверить, запущен или нет Антивирус Касперского (по ID процесса). Если приложение уже запущено, выполнение скрипта *kavmilter* останавливается. Если приложение не запущено, выполняется его запуск и проверяется, внесены ли необходимые изменения в конфигурацию почтовой системы

Sendmail для осуществления антивирусной фильтрации почты. Если изменения конфигурации выполнены, запускается антивирусный фильтр. Код возврата **0** сообщает об успешном старте.

stop – проверить, запущен или нет Антивирус Касперского (по ID процесса). Если приложение запущено, выполняется сигнал SIGTERM. Если по истечении трех секунд приложение не будет остановлено, выполняется сигнал SIGKILL. Результатом успешного выполнения является код возврата **0**.

restart – выполнить остановку и запуск приложения в соответствии с ключами **stop** и **start**.

reload – выполнить перезагрузку конфигурации приложения и антивирусных баз посредством сигнала SIGUSR1.

status – проверить, запущен или нет Антивирус Касперского (по ID процесса) с помощью сигнала **0** и вывести на консоль информацию о статусе приложения. Если приложение запущено, возвращается код **0**, если не запущено – код **1**.

check – проверить, запущен или нет Антивирус Касперского Проверка выполняется аналогично status- ключу, за исключением вывода на консоль статуса приложения. Коды возврата аналогичны status-ключу.

- Возникновение проблем в процессе работы приложения.

  Для перезагрузки приложения в случае возникновения проблем (например, ошибок ввода \ вывода, ошибок в работе библиотеки и т.д.) используется утилита *watchdog*, которая входит в состав дистрибутива и устанавливается в процессе инсталляции Антивируса Касперского.

  Утилита порождает от родительского процесса процесс-потомок, с которого наблюдает за приложением. Как только родительский процесс останавливается из-за возникновения какой-либо ошибки, утилита watchdog перезагружает его.

  Максимальное количество попыток перегрузки приложения утилитой watchdog определяется параметром **WatchdogMaxRetries** секции **[kavmilter.global]**. Для того чтобы снять ограничение, задайте для данного параметра значение **–1**.

  Использование утилиты *watchdog* регулируется ключом командной строки **–f**. Если приложение загружено с таким ключом, утилита *watchdog* не используется при работе Антивируса.

После обновления антивирусных баз автоматически выполняется их перезагрузка, не требует перезапуска приложения. Автоматический перезапуск регулируется параметром **PostUpdateCmd** секции **[updater.options]**.

6.16. Управление приложением из командной строки

Управление Антивирусом Касперского из командной строки осуществляется посредством скрипта *kavmilter.sh*.

Вы можете использовать следующие ключи командной строки:

–h – вывести на консоль справочную информацию по ключам командной строки;

–v – вывести на консоль версию приложения;

–t – проверить конфигурацию приложения; все ошибки конфигурации, сообщения выводить на консоль;

–f – запускать приложение и работать на текущей консоли; (не переходить после запуска в фоновый режим работы);

–s <socket> – определить сокет для передачи данных; формат параметра **<socket>** следующий:

inet:port@ip-addr – использовать сетевой сокет, работающий на порте **port** и адресе **ip-addr**.

local:/socket/file/path – использовать локальный сокет.

–u <user > – запускаться с правами пользователя **<user>** (например, с правами пользователя **root**). По умолчанию приложение запускается с правами пользователя **kav**;

–g <group> – запускаться с правами группы **<user>** (например, с правами группы **root**). По умолчанию приложение запускается с правами группы **kav**;

–c <file> - использовать в качестве конфигурационного файла **<file>** (по умолчанию используется */etc/kav/5.0/kavmilter/kavmilter.conf*);

–r <command> - выполнить одну их следующих команд:

reload – перезагрузить конфигурационный файл приложения и антивирусные базы; все изменения и обновления вступят в силу сразу после перезагрузки;

stats – записать статистическую информацию о работе приложения в файл, заданный параметром **DataFile**;

stop – остановить приложения (фильтрация).

6.17. 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 в соответствии со стандартной утилитой формирования дат:

%H:%M:%S – отображаемый формат времени (*чч.мм.сс.*).

%d/%m/%y – отображаемый формат даты (*дд.мм.гг.*).

Администратору предоставляется возможность изменения формата даты и времени. Локализация форматов выполняется в секции **[locale]** конфигурационного файла приложения. 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).

6.18. Контроль работы приложения

В поставку приложения включен скрипт *troubleshooter.sh*, посредством которого вы можете контролировать проблемы, возникающие в процессе работы приложения, а также отправлять информацию о них в Службу технической поддержки Лаборатории Касперского.

Информация почтового сообщения для Службы поддержки упаковывается, а также может быть зашифрована при помощи открытой части PGP-ключа, входящего в поставку приложения. Сама процедура шифрования может быть выполнена утилитами *pgp* или *gpg* (не поставляется).

Для этого используйте следующие ключи командной строки:

–h – вывести на экран все ключи командной строки скрипта *trouble-shooter.sh*.

–report – работать в неинтерактивном режиме (по умолчанию используется интерактивный режим). В случае возникновения вопросов к пользователю использовать значения по умолчанию и продолжать формировать отчет.

–check – автоматически проверить работу приложения, конфигурацию и смежные области, где могут возникнуть проблемы.

–to email – отправить информацию по проблемам работы приложения по адресу, отличному от адреса Службы технической поддержки Лаборатории Касперского.

–key id – определить PGP/GnuPG-ключ для шифрования архива с информацией, отправляемой в Службу технической поддержки.

ГЛАВА 7. УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

В Антивирусе Касперского предусмотрено ограничение работы с приложением по сроку его использования (как правило, это срок в один год со дня приобретения) в сочетании с ограничением по объему дневного почтового трафика, обрабатываемого приложением, или с ограничением по почтовым адресам. В последнем случае проверяется почта адресов доменов, указанных в конфигурации приложения, а также адресов сервера, на котором установлено приложение.

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

Лицензионный ключ дает вам право на использование приложения и содержит всю необходимую информацию, связанную с лицензией, которую вы приобрели, такую как: тип лицензии, дата окончания срока ее действия, информацию о дистрибьюторах и т.д.

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

- круглосуточную техническую поддержку;
- ежедневное обновление антивирусных баз *каждые три часа*;
- обновление приложения (патч);
- получение новых версий приложения (upgrade);
- своевременное информирование о новых вирусах.

По окончании срока действия лицензии вы автоматически лишаетесь приведенных выше возможностей. Антивирус Касперского по-прежнему будет осуществлять антивирусную обработку почтового трафика сервера, но только с использованием антивирусных баз, актуальных на дату окончания срока действия лицензии. Функция автоматического обновления антивирусных баз будет не доступна. В случае если будет произведена попытка ручного обновления антивирусных баз, приложение утратит работоспособность.

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

Если вы приобрели лицензию со *схемой лицензирования по трафику*, то лицензия распространяется только на дневной объем почтового трафика, указанный в лицензионном ключе. Если дневной почтовый трафик превышает определенный лицензией, администратору будут отправляться уведомления о том, что необходимо приобрести лицензию на недостающий трафик.

Если вы приобрели лицензию со *схемой лицензирования по почтовым адресам*, то лицензия распространяется на почтовые адреса доменов, перечисленных в конфигурационном файле приложения (параметр **LicensedUsersDomains**), а также на адреса сервера, где установлен Антивирус Касперского, не входящих в доменную структуру. Если количество почтовых адресов превышает определенное лицензией, администратору будут отправляться уведомления о том, что необходимо приобрести лицензию на почтовые ящики сверх текущей лицензии.

При определении параметра вам необходимо указать как ваш домен, так и все его поддомены. Для того чтобы определить несколько доменов и поддоменов, вы можете использовать регулярные выражения (regular expressions) с синтаксисом:

```
re: domain-regexp
```

где:

`re:` – префикс, определяющий регулярное выражение;

`domain-regexp` – регулярное выражение POSIX указывающее домен отправителя или получателя.

7.1. Просмотр информации

Вы можете просматривать информацию об установленных лицензионных ключах в отчетах о работе компонента *kavmilter*, поскольку при его старте данная информация загружается в отчет.

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.

Чтобы просмотреть информацию обо всех установленных лицензионных ключах,

в командной строке введите:

```
#./licensemanager -s
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2003.
Active key info:
Product name: Kaspersky Anti-Virus 5 Business Optimal
1 month
Key file 00053BC3.key
Type: Commercial
Expiration date: 17-11-2003, expires in 60 days
Serial: 02B1-000454-00053BC
Additional key info:
Product name: Kaspersky Anti-Virus 5 Business Optimal
1 month
Key file 00053E3D.key
Type: Commercial
Expiration date: expired
Serial: 02B1-000454-00053E3
```

Чтобы просмотреть информацию о лицензионном ключе,

в командной строке введите, например, такую строку:

```
#./licensemanager -k 00053E3D.key
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2003.
Product name: Kaspersky Anti-Virus 5 Business Optimal
1 month
Creation date:   23-07-2003
Expiration date: 21-11-2003
Serial 02B1-000454-00053E3
Type: Commercial
Lifespan: 30
```

7.2. Продление лицензии

Продление лицензии на использование Антивируса Касперского дает вам право на восстановление полной функциональности приложения. Кроме того, возобновляются дополнительные услуги, приведенные в Глава 7 на стр. 70.

Срок действия лицензии зависит от типа лицензирования, который вы выбрали, приобретая приложение (на Антивирус Касперского для Sendmail с Milter API срок составляет, как правило, один год).

Чтобы продлить лицензию на использование Антивируса Касперского, вам необходимо:

связаться с компанией, у которой вы купили приложение, и приобрести продление лицензии на использование Антивируса Касперского.

или:

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

Регулярно Лаборатория Касперского проводит акции, позволяющие продлить лицензии на использование наших продуктов со значительными скидками. Следите за акциями на веб-сайте Лаборатории Касперского в разделе **Продукты → Акции и спецпредложения**.

Приобретенный лицензионный ключ необходимо установить с помощью утилиты *licensemanager*.

Чтобы установить новый ключ вам необходимо:

в командной строке ввести, например, такую строку:

```
#./licensemanager -a 00053E3D.key
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2003.
Key file 00053E3D.key is successfully registered
```

После этого рекомендуем вам обновить антивирусные базы.

Если вы хотите установить новый лицензионный ключ до истечения срока действия актуального, вы можете поставить его в качестве резервного. Резервный ключ начинает свою работу после истечения срока действия подписки предыдущего. Срок действия резервного ключа начинает отсчитываться с момента его активации.

Установка резервного ключа проводиться стандартным способом, аналогичным установке основного. После этого при запросе информации о лицензионном ключе на консоль сервера будет выводиться информация как об актуальном, так и о резервном ключах.

7.3. Удаление лицензионного ключа

Чтобы удалить активный ключ,

в командной строке введите такую строку:

```
#./licensemanager -da
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2003.
Active key was successfully removed
```

Чтобы удалить резервный ключ,

в командной строке введите такую строку:

```
#./licensemanager -dr
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2003.
Additional key was successfully removed
```

ГЛАВА 8. РАБОТА С ДРУГИМИ ПРИЛОЖЕНИЯМИ ЛАБОРАТОРИИ КАСПЕРСКОГО

Антивирус Касперского 5.0 для Sendmail с Milter API корректно работает со следующими антивирусными приложениями для Unix\Linux-платформ, разработанными Лабораторией Касперского:

- Антивирус Касперского 5.0.1-0 для Samba Servers.
- Kaspersky SMTP Gateway 5.0.0.28.

При совместной работе с Антивирусом Касперского для Unix/Linux, в состав которого входит компонент постоянной защиты *kavmonitor*, следует учитывать, что очередь почтовых сообщений системы Sendmail до их отправки адресатам хранится на диске и в момент обращения системы к письму оно перехватывается компонентом *kavmonitor*. В случае если письмо заражено или содержит подозрительный код, оно будет заблокировано, и доставить его не удастся. Во избежание подобных проблем рекомендуем вам исключать каталог хранения очереди Sendmail из области проверки *kavmonitor*.

При инсталляции Касперского для Sendmail с Milter API на сервер, где установлен Антивирус Касперского для Unix/Linux, выполняется регистрация модуля *kavmilter* в модуле *kavmonitor* посредством специального кода. В результате этой регистрации модуль *kavmilter* получает разрешение от *kavmonitor* на проверку почтовых сообщений Sendmail.

Однако при проверке почтового сообщения Антивирусом Касперского для Sendmail с Milter API создается и размещается в каталоге на диске временный файл. При этом файл перехватывается на проверку модулем *kavmonitor*. Если файл окажется зараженным, он будет заблокирован, и Антивирус Касперского для Sendmail не сможет обработать письмо (сигнал **mlfi_abort**).

Дабы избежать этой проблемы, рекомендуем вам исключать из области проверки модуля *kavmonitor* каталог хранения временных файлов Антивируса Касперского для Sendmail с Milter API.

Каталог задается параметром конфигурации **TempDir** секции **[kavmilter.global]**.

ГЛАВА 9. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить правильность настроек и корректность работы программы с помощью тестового "вируса" и его модификаций.

Тестовый "вирус" был специально разработан организацией eicar (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. При отсутствии доступа к интернету вы можете самостоятельно создать тестовый "вирус". Для этого в любом текстовом редакторе наберите следующую строку, а затем сохраните в файле с именем **eicar.com**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Файл, который вы загрузили с веб-сайта компании **EICAR** или создали в текстовом редакторе описанным выше способом, содержит тело стандартного тестового "вируса". Антивирус обнаруживает его, присваивает тип **Инфицированный**, 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 ниже).

Вы можете проверять корректность работы Антивируса Касперского с помощью модифицированного "вируса" EICAR только при наличии антивирусных баз, датированных не ранее 24.10.2003 (кумулятивное обновление – Октябрь, 2003).

Таблица. Модификации тестового "вируса"

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый "вирус"	**Инфицированные**. Объект не подвергается лечению.
CORR–	**Нераспознанные**.
SUSP–	**Подозрительные** (код неизвестного вируса).
WARN–	**Подозрительные** (модифицированный код известного вируса).
ERRO–	**Не проверенные из-за сбоя**.
CURE–	**Вылеченные**. Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURED.
DELE–	Объект автоматически удаляется.

В первом столбце таблицы приведены префиксы, которые нужно добавить в начало строки стандартного тестового "вируса" (например, CORR–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*). Во втором столбце описаны типы объектов, идентифицируемые антивирусной программой в результате добавления префиксов. Действия над каждым из объектов определяются настройками Антивируса, выполненными администратором.

Рекомендуется произвести проверку работы Антивируса для входящей и исходящей почты, как в теле сообщения, так и во вложении. Для проверки обнаружения вирусов в теле сообщения, поместите текст стандартного или модифицированного "вируса" в тело сообщения.

ГЛАВА 10. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В данной главе мы осветим наиболее часто задаваемые пользователями вопросы по установке, настройке и работе Антивируса Касперского и постараемся ответить на них наиболее подробно.

Вопрос: почему Антивирус Касперского вызывает определенное снижение производительности сервера 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 антивирусную базу, увеличивает общее время проверки.

В отличие от других антивирусов, сокращающих время проверки путем исключения из антивирусных 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.

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

Без лицензионного ключа Антивирус Касперского не работает.

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

Вопрос: что произойдет, когда истечет лицензия на использование продукта?

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

Загрузка антивирусных баз с веб-сайта Лаборатории Касперского посредством с помощью Антивируса Касперского будет невозможна. Даже если вы скопируете антивирусные базы без его использования, Антивирус Касперского не будет их использовать.

Следовательно, мы не можем гарантировать вам защиту от заражения новыми вирусами.

Вопрос: мой Антивирус не работает.

Что мне делать?

Прежде всего, убедитесь, не описан ли метод решения вашей проблемы в данной документации, в частности в этом разделе, или на нашем веб-сайте.

Также мы рекомендуем обратиться к фирме, продавшей вам Антивирус Касперского или написать письмо в Службу технической поддержки (support@kaspersky.com).

Чтобы ваш запрос был обработан как можно скорее:

1. В заголовке сообщения укажите операционную систему вашего сервера, имя компонента, который вы не можете настроить, и проблему. Например:
   Linux, не работает обновление антивирусных баз.
2. Пишите сообщения в виде *plain text*. Сообщения HTML-формата труднее читать.
3. В начале сообщения укажите точную версию операционной системы, дистрибутива Антивируса Касперского и имени вашего лицензионного ключа.
4. Кратко, но наиболее понятно опишите проблему. Помните, что Служба технической поддержки на момент чтения вашего письма ещё ничего не знает о вашей проблеме и сможет помочь вам, только полностью поняв и воспроизведя её.
5. Отправьте в Службу технической поддержки следующие данные, предварительно запаковав их в один архив:
   - все файлы конфигурации вашего почтового агента (MTA);
   - файл отчета почтовой системы;

- файл отчета компонентов Антивируса;
- лицензионный ключ.

6. Обязательно укажите в письме о наличии:
   - SCSI-контроллера;
   - очень старого или нового процессора, нескольких процессоров;
   - памяти меньше, чем 64 МБ или больше 2 ГБ.
7. Укажите примерный размер дневного трафика и бывают ли пики нагрузки.

Вопрос: может ли злоумышленник подменить антивирусные базы?

Все антивирусные 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 лицензии на использование продукта, Антивирус Касперского не будет использовать такие базы.

Вопрос: поддерживаются ли процессоры архитектуры X (PowerPC, SPARC, Alpha, PA-RISC и др.)?

Данные виды процессоров в текущей версии приложения не поддерживаются.

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

Тестирование Антивируса Касперского для Sendmail с Milter API производилось на дистрибутивах RedHat, Debian и SuSE и именно для них собирались дистрибутивы Антивируса Касперского.

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: как распаковать архив .tgz или .tar.gz?

Архивы типа *.tgz* или *.tar.gz* распаковываются следующей командой:

```
tar zxvf <имя_архива>
```

ПРИЛОЖЕНИЕ А. СПРАВОЧНАЯ ИНФОРМАЦИЯ ПО ПРИЛОЖЕНИЮ

А.1. Конфигурационный файл приложения

В данном приложении мы подробно рассмотрим конфигурационный файл *kavmilter.conf*, который используется для работы Антивируса Касперского по умолчанию сразу после его установки на сервер.

Все значения параметров, приведенные здесь, установлены в качестве рекомендуемых специалистами Лаборатории Касперского.

Секция **[kavmilter.global]** содержит общие параметры, необходимые для запуска и работы приложения в целом:

RunAsUid=kav – идентификационный код пользователя, под которым (с правами которого) запускается приложение.

RunAsGid=kav – идентификационный код группы, под которой (с правами которой) запускается приложение.

ServiceSocket=inet:1052@127.0.0.1 – вид сокета (локальный или сетевой), через который осуществляется передача данных между Sendmail и Антивирусом Касперского. Параметр имеет следующий формат: *вид_сокета:путь_к_сокету*. Например:

inet:port@ip-address – использование сетевого сокета;

local:/path/to/socket – использование локального сокета.

WatchdogMaxRetries=10 – максимальное количество попыток перезагрузки Антивируса Касперского утилитой *watchdog*. Значение **–1** соответствует отсутствию ограничения.

ScanPolicy=message – политика проверки почтовых сообщений. В качестве значений параметра могут использоваться:

message – проверять на вирусы все письмо целиком, а в случае обнаружения вирусов – по частям (заголовок, тело, вложение).

combined – проверять на вирусы сначала все письмо целиком, а затем каждую его часть.

TempDir=/var/opt/kav/5.0/kavmilter/tmp/ – каталог хранения временных файлов.

LicensedUsersDomains=localhost – список доменов, почтовые адреса которых лицензированы на использование Антивируса Касперского. Данный параметр определяется только в случае использования схемы лицензирования по почтовым адресам.

AddXHeaders=yes – режим использования дополнительного заголовка в проверенном почтовом сообщении, содержащего информацию о приложении.

Секция **[kavmilter.engine]** содержит параметры, определяющие процедуру антивирусной проверки почтовых сообщений:

MaxScanRequests=0 – максимальное количество запросов на проверку почтовых сообщений. Значение 0 означает отсутствие ограничения.

MaxScanTime=10 – количество секунд, в течение которых выполняется проверка одного письма или его части. При превышении заданного ограничения приложение возвращает ошибку.

ScanArchives=yes – режим проверки объектов в архивах. Для отключения режима установите **no** в качестве значения параметра.

ScanPacked=yes – режим проверки упакованных исполняемых файлов. Для отключения режима установите **no** в качестве значения параметра.

ScanCodeanalyzer=yes – режим использования при проверке эвристического анализа кода для обнаружения вредоносных программ, модификаций известных вирусов и неизвестных вирусов. Для отключения режима установите **no** в качестве значения параметра.

Секция **[kavmilter.actions]** включает параметры, определяющие способ обработки зараженных объектов почтовых сообщений:

DefaultAction=cure – действие над зараженным объектом почтового сообщения, которое выполняется по умолчанию. Вы можете использовать любое из следующих действий:

warn – заменить зараженное письмо сообщением, содержащим уведомление о том, что данное письмо заражено;

drop – принять сообщение, но не отправлять его адресату;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

cure – пытаться лечить зараженный объект письма; если лечение невозможно – удалить письмо, заменив его уведомлением о том, что письмо было заражено;

delete – удалить зараженный объект письма, заменив его соответствующим уведомлением.

ProtectedAction=skip – действие над защищенным (например, паролем) объектом почтового сообщения, который не удалось проверить на присутствие вирусов. Вы можете использовать любое из следующих действий:

skip – не обрабатывать защищенный объект;

delete – удалить защищенный объект из почтового сообщения, заменив его соответствующим уведомлением.

ErrorAction=skip – действие над поврежденным объектом почтового сообщения или объектом, которое не удалось проверить из-за ошибки. Вы можете использовать любое из следующих действий:

warn – заменить письмо сообщением, содержащим соответствующее уведомление;

skip – не обрабатывать объект;

delete – удалить объект из почтового сообщения, заменив его соответствующим уведомлением.

VirusNameList – список названий вирусов, при обнаружении которых необходимо выполнить специфическое действие над почтовым сообщением или его объектом.

VirusNameAction=drop – действие над почтовым сообщением или его частью, если оно заражено вирусом, имя которого определено параметром **VirusNameList**.

warn – заменить зараженное письмо сообщением, содержащим уведомление о том, что данное письмо заражено;

drop – принять сообщение, но не отправлять его адресату;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

delete – удалить зараженный объект письма, заменив его соответствующим уведомлением.

UsePlaceholderNotice=yes – добавление в почтовое сообщение уведомления об удаленном объекте.

Секция **[kavmilter.backup]** содержит параметры, определяющие формирование резервных копий объектов почтовых сообщений перед любой их модификацией:

BackupPolicy=info – политика формирования резервных копий почтовых сообщений. Вы можете использовать одно из следующих значений:

none – не создавать резервную копию почтового сообщения;

message – создавать резервную копию почтового сообщения каждый раз перед его обработкой;

info – создавать резервную копию почтового сообщения и информационный файл, содержащий полное описание письма.

BackupOption=all – тип почтовых сообщений, для которых создаются резервные копии. Вы можете использовать одно из следующих значений:

filtered – почтовые сообщения, подвергаемые фильтрации хотя бы по одному из его частей;

infected – зараженные почтовые сообщения;

deleted – письма, хотя бы одна часть которых будет удалена;

warning – почтовые сообщения, любая часть которых будет заменена уведомлением;

dropped – письма, которые были приняты, но не будут отправлены;

rejected – не принятые почтовые сообщения;

error – почтовые сообщения, вызывающие появление ошибки при их проверке на вирусы;

all – письма всех перечисленных выше типов.

BackupDir=/var/opt/kav/backup – каталог хранения резервных копий почтовых сообщений, создаваемых приложением перед любой модификацией писем.

Секция **[kavmilter.filter]** содержит параметры, задающие правила фильтрации почтовых сообщений:

IncludeMime – MIME-тип вложений почтового сообщения, подвергающегося фильтрации.

ExcludeMime – MIME-тип вложений почтового сообщения, не подвергающегося антивирусной проверке.

IncludeName – имя вложения, подвергающегося фильтрации.

ExcludeName – имя вложения, которое не будет проверяться на вирусы.

IncludeSize – размер вложения почтового сообщения, подвергающегося фильтрации.

ExcludeSize – размер вложения письма, в соответствии с которым оно не будет проверяться на вирусы.

FilteredMimeAction=skip – действие над вложением типа **IncludeMime**. Вы можете выбрать одно из следующих действий:

skip – не обрабатывать объект данного типа;

delete – удалить объект данного MIME-типа из почтового сообщения, заменив его соответствующим уведомлением;

drop – принять сообщение с таким объектом, но не отправлять его адресату;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

warn – заменить письмо сообщением, содержащим соответствующее уведомление.

FilteredNameAction=skip – действие над именем вложения **IncludeName**. Вы можете выбрать одно из следующих действий:

skip – не обрабатывать объект с таким именем;

replace – переименовать объект;

delete – удалить объект с таким именем из почтового сообщения, заменив его соответствующим уведомлением;

drop – принять сообщение с таким объектом, но не отправлять его адресату;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

warn – заменить письмо сообщением, содержащим соответствующее уведомление.

FilteredSizeAction=skip – действие над вложением, размер которого соответствует указанному в качестве значения параметра **IncludeSize**. Вы можете выбрать одно из следующих значений:

skip – не обрабатывать объект такого объема, пропустить его для доставки получателю;

delete – удалить объект указанного размера из почтового сообщения, заменив его соответствующим уведомлением;

drop – принять сообщение с таким объектом, но не отправлять его адресату;

reject – отказать в доставке сообщения, возвратив отправителю соответствующий код ошибки;

warn – заменить письмо сообщением, содержащим соответствующее уведомление.

Секция **[kavmilter.notifications]** содержит параметры формирования стандартных уведомлений:

EnableNotifications=yes – режим формирования уведомлений. Для отключения режима установите **no** в качестве значения параметра.

NotifySender=none – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, о котором будет отправлено уведомление отправителю письма. Вы можете использовать одно из следующих значений:

filtered – почтовое сообщение или его часть было подвержено фильтрации;

infected – почтовое сообщение или его часть заражено вирусом;

protected – часть письма защищена и не может быть проверена на присутствие вирусов;

error – почтовое сообщение или его часть повреждена или в результате его проверки возникла ошибка;

all – письма всех перечисленных выше типов;

none – не отправлять уведомление.

NotifyRecipients=infected – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, о котором будет отправлено уведомление получателю письма. Виды статусов аналогичны приведенным для параметра **NotifySender**.

NotifyAdmin=none – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, о котором будет отправлено уведомление администратору сервера. Виды статусов аналогичны приведенным для параметра **NotifySender**.

AdminAddresses=postmaster@localhost – электронный адрес администратора почтового сервера. Вы можете указать несколько адресов через пробел.

MessageDir=/etc/opt/kav/messages/ – каталог хранения шаблонов уведомлений.

MessageSubject=Anti-virus notification message – заголовок стандартного уведомления, который добавляется в поле **Тема**.

RejectReply=Message rejected because it contains malware – заголовок уведомления об отказе доставки почтового сообщения.

Charset=us-ascii – имя кодировки, в которой формируется уведомление.

TransferEncoding=7bit – значение алгоритм шифрования уведомления.

SendmailPath=/usr/sbin/sendmail – полный путь к бинарному Sendmail, используемому для отправки дополнительных уведомлений.

UseCustomTemplates=off – режим использования пользовательских шаблонов для формирования уведомлений. Для включения режима задайте **on** в качестве значения параметра.

SenderSubject – заголовок уведомления для отправителя.

ReceiverSubject – заголовок уведомления для получателя.

AdminSubject – заголовок уведомления для администратора сервера.

Секция **[kavmilter.log]** включает параметры формирования отчетов о работе приложения:

LogFacility=syslog – файл, в который будут записываться результаты работы приложения. Вы можете выбрать одно из следующих значений:

syslog – записывать результаты работы приложения в системный журнал;

file – фиксировать результаты работы приложения в специальном файле. При выборе данного значения укажите полный путь к файлу отчета в качестве значения параметра **LogFilepath**.

LogFilepath=/var/opt/kav/log/kavmilter.log – путь к файлу отчета. Значение параметра игнорируется, если для хранения результатов работы приложения используется системный журнал.

LogOption=all – категория сообщений, фиксируемых в отчете. Вы можете выбрать одно из следующих значений:

internal – системные сообщения инициализации приложения, сигналы, процессы;

scan – информация о статусах антивирусной проверки и о выполненных действиях;

config – сообщения, относящиеся к конфигурации приложения;

backup – сообщения, относящиеся к резервному копированию почтовых сообщений;

all – все перечисленные выше типы сообщений.

Каждая категория сообщений, фиксируемых в отчете, может подразделяться на уровни детализации *debug*, *info*, *notice*, *warning*, *error*, *critical*, *all*.

Вы можете комбинировать как категории сообщений в отчете и уровни детализации. Например:

```
LogOption=backup.all
LogOption=config.error
LogOption=scan.all
LogOption=-scan.debug
```

Префикс перед комбинацией обозначает отключение вывода информации такого рода в отчет, вся остальная информация выводится.

LogRotate=on – режим ротации файла отчета. Данный режим не распространяется на системный журнал. Для отключения ротации отчетов задайте **off** в качестве значения параметра.

RotateSize=1MB – максимальный размер файла отчета, при достижении которого формируется новый файл отчета.

RotateRounds=10 – максимальное количество формируемых в результате ротации отчетов. При превышении этого числа выполняется перезапись самого старого файла отчета.

Секция **[kavmilter.statistics]** содержит параметры формирования статистики работы приложения:

TrackStatistics=none – категория информации для ведения статистики. Вы можете выбрать одно из следующих значений:

none – не формировать статистику работы приложения;

message – формировать статистику, связанную с почтовыми сообщениями (общее количество проверенных сообщений, количество входящих сообщений и т.д.);

resources – формировать статистику, связанную с ресурсами, затраченными на работу приложения (общий объем почтового трафика, время проверки одного сообщения и т.д.);

viruses – фиксировать статистику по обнаруженным вирусам (десять последних вирусов, обнаруженных в почтовых сообщениях и т.д.);

all – фиксировать статистику по всем перечисленным выше категориям информации.

DataFormat=text – формат, в котором выводится статистика. Вы можете выбрать одно из следующих значений:

text – текстовый вид в формате category.field=value;

xml – root element is statistic, children elements are category and field, and value is body element.

DataFile=/var/opt/kav/log/statistics.data – полный путь к файлу, хранящему статистику.

Секция **[path]** содержит параметры, определяющие пути к важнейшим каталогам для работы приложения:

BasesPath=/var/opt/kav/5.0/kavmilter/bases/ – полный путь к каталогу хранения антивирусных баз приложения.

LicensePath=/var/opt/kav/5.0/kavmilter/licenses/ – полный путь к каталогу хранения лицензионных ключей приложения.

Секция **[locale]** включает параметры, определяющие формат отображения даты и времени в отчетах и статистике работы приложения:

DateFormat=%d-%m-%Y – формат отображения даты в отчете о работе приложения.

TimeFormat=%H:%M:%S – формат отображения времени в отчете.

Секция **[updater.path]** содержит параметры, определяющие пути к важнейшим каталогам, используемым в процессе обновления:

UploadPatchPath=/var/db/kav/5.0/kavmilter/patches/ – полный путь к каталогу хранения обновлений антивирусного ядра.

BackUpPath=/var/db/kav/5.0/kavmilter/bases/backup/ – полный путь к каталогу хранения резервной копии обновлений антивирусных баз и модулей ядра.

Секция **[updater.options]** включает параметры, определяющие процесс обновления антивирусных баз и модулей ядра:

UseUpdateServerUrl=yes – использовать в качестве ресурса обновлений сервер Лаборатории Касперского, определяемый параметром **UpdateServerUrl**.

UpdateServerUrl=ftp://downloads1.kaspersky-labs.com – адрес сервера Лаборатории Касперского, используемого в качестве ресурса для обновлений антивирусных баз и модулей ядра.

PostUpdateCmd=/etc/kav/5.0/kavmilter/init.d/kavmilter reload – строка перезагрузки приложения сразу после обновления антивирусных баз и модулей ядра.

RegionSettings=Russia – имя региона.

ConnectTimeout=30 – количество секунд, в течение которого выполняется соединение с источником обновления.

ProxyAddress – IP-адрес прокси-сервера, если таковой используется для выхода в интернет. По умолчанию значение не задано.

PassiveFtp – режим использования пассивного режима работы FTP-сервера при загрузке обновлений по FTP. По умолчанию значение не задано. Для использования данного режима задайте для параметра значение **yes**, для отключения – значение **no**.

Секция **[updater.report]** содержит параметры формирования отчета о результатах обновления:

Append=no – режим формирования отчета, при котором в отчете хранятся данные только о последней процедуре обновления (каждый раз при старте компонента *keepup2date* прежний файл отчета удаляется, и создается новый). Если вы хотите добавлять в существующий отчет новую информацию, установите для параметра значение **yes**.

ReportFileName=/var/log/kav/5.0/kavmilter/keepup2date.log – полный путь к файлу, в котором будет храниться отчет о результатах обновления.

ReportLevel=10 – уровень детализации информации в отчете.

A.2. Коды возврата приложения

В процессе работы с приложением возможно возникновение ошибок. Ниже приведены их коды возврата.

Внутренние ошибки:

1 – неверный параметр формирования отчета;

2 – попытка запуска приложения в качестве UNIX-демона при помощи утилиты daemonize не удалась;

3 – недостаточно прав для изменения uid;

4 – недостаточно прав для изменения gid;

5 – нельзя создать child-процесс для фильтра;

6 – не удалось перезагрузить приложение, максимальное количество попыток перезапуска превышено;

7 – файл уже существует и не является сокетом;

8 – не удалось зарегистрировать приложение в качестве фильтра *kavmilter*;

9 – не удалось инициализировать ядро Антивируса Касперского;

10 – не удалось запустить главный цикл *kavmilter*;

255 – неустановленная ошибка.

Ошибки ядра:

51 – ошибка инициализации менеджера базы данных;

52 – ошибка загрузки базы данных;

54 – не удалось запустить менеджер локальной проверки (local scan manager);

63 – ошибка выделения памяти для ядра.

Ошибки конфигурации:

100 – параметр не найден;

101 – неизвестный параметр;

102 – неверный тип параметра;

103 – параметр уже существует;

104 – конец массива значений параметра;

105 – секция не найдена;

106 – неизвестная секция;

107 – ошибка чтения конфигурационного файла;

108 – параметры не заданы.

ПРИЛОЖЕНИЕ В. ВРЕДОНОСНЫЕ ПРОГРАММЫ В UNIX-СРЕДЕ

В среде Unix-систем вирусы распространены значительно меньше, чем, например, в среде Windows ввиду особенности данных платформ. Большее распространение имеют троянцы и сетевые черви.

Распространение вредоносных программ производится по сети, в том числе и через "дырки" в программном обеспечении. Рассмотрим подробнее виды вредоносных программ для Unix и способы заражения ими.

B.1. Вирусы

Вирус – это программа (некоторая совокупность исполняемого кода и/или инструкций), которая способна создавать свои копии (необязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты и/или ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Если исследовать среду обитания вирусов, то вирусы под Unix-системы, как правило, файловые, которые записывают свой код в исполняемые файлы, либо создают файлы-двойники.

По особенности алгоритма работы можно выделить:

- *резидентный вирус* – вирус, оставляющий при заражении в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.
- *нерезидентный вирус* – вирус, который не заражает память компьютера и сохраняет активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус.

Как правило, вирусы под Unix-системы неопасные – влияние ограничивается уменьшением свободной памяти на диске, графическими,

звуковыми и прочими эффектами. Некоторые из них и вовсе безобидны, поскольку никак не влияют на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения.

Приведем примеры некоторых вирусов под Unix-системы:

ELF_SNOOPY – вирус, инфицирующий исполняемые Unix-файлы.

Алгоритм работы вируса: он находит на рабочей станции все исполняемые файлы, переименовывает их на файлы с расширением .X23 и помещает в созданную директорию /E. Затем вирус копирует свой код в оригинальные файлы и изменяет их атрибуты на **777**. Параллельно в основном списке паролей на зараженной рабочей станции создается пользователь **snoopy** также с правами 777.

Linux.Bliss – группа нерезидентных вирусов, заражающих исполняемые файлы Linux; эти вирусы написаны на GNU C и имеют формат ELF.

Алгоритм работы вируса: при запуске вирус ищет на рабочей станции исполняемые файлы и заражает их, сдвигая содержимое файла вниз, записывая свой код в освободившееся место и добавляя в конец файла строку-идентификатор. Действие вируса ограничивается правами пользователя, запустившего его (заражаются только файлы, к которым есть доступ). Если же пользователь имеет системные привилегии, то вирус может распространиться по всему компьютеру.

Linux.Diesel – неопасный нерезидентный Linux-вирус, инфицирующий исполняемые файлы Linux.

Алгоритм работы вируса: после запуска вирус считывает свой бинарный код из файла-носителя, ищет исполняемые Linux-файлы в системных подкаталогах и записывает свой код в середину кода каждого файла, увеличивая таким образом размер последней секции.

Linux.Siilov – неопасный Linux-вирус, заражающий исполняемые файлы; имеет формат ELF.

Алгоритм работы вируса: использует два способа заражения файлов: резидентный и нерезидентный. Резидентный способ: вирус остается в системной памяти и заражает файлы в фоновом режиме. Нерезидентный способ: вирус ищет исполняемые файлы на диске и поражает их.

Linux.Winter – безобидный нерезидентный Linux-вирус. Имеет очень небольшой размер – всего 341 байт.

Алгоритм работы вируса: при запуске вирус получает управление, ищет ELF-файлы (исполняемые файлы Linux) в текущем каталоге и заражает их.

В.2. Троянские программы

Троянская программа – программа, которая выполняет несанкционированные пользователем действия. При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Компьютер открыт для удаленного управления.

Распространение троянских программ осуществляется по сети.

Ярким представителем семейства троянских программ для Unix-систем является **TROJ_IRCKILL** – троянец, представляющий собой набор программных инструментов для отключения пользователей от каналов IRC. Этот набор объединяет четыре утилиты для нападения: FLOOD (flood – наводнение, потоп), MCB (Multiple Collide BOTs), SUMO BOTs и FLASH – особый тип "потопа" для использования в среде UNIX.

Тип атаки FLASH используется для непосредственного разъединения модема путем отправки на определенный IP-адрес **ping**-команды с "неправильными" данными, указанными в определенной последовательности. Эти данные будут интерпретированы пользовательским модемом как команда разъединения, и он будет отключен от интернета. Однако этот вид атаки может быть применим не для всех типов модемов.

Атака MCB выполняется через IRC-каналы. В момент, когда IRC-серверы будут не в состоянии синхронизировать друг друга (net split) троянская программа дублирует пользовательское имя (nickname). После налаживания синхронизации IRC-серверов данное имя становится ошибочным, и пользователь отключается от IRC-канала.

Атака FLOOD BOTS/SUMO BOTS также используется в IRC-сети, "порождая" многочисленных пользователей со случайными именами (nick-name). С помощью этой атаки "затопляется" IRC-канал или пользователь, посылающий или получающий сообщения в чате, до тех пор, пока пользовательская машина не достигнет определенного лимита пропускной способности. Затем этот пользователь также отключается от IRC-канала.

Root kit – это пакет программ, используемый взломщиком для получения root-доступа к удалённому компьютеру. Он использует стандартные программы Unix – ps и ls. Единственный эффективный метод восстановления после его взлома с помощью Root kit – восстановление важных данных с резервной копии, которые желательно регулярно создавать, , полная очистка жёсткого диска и переустановка системы.

B.3. Сетевые черви

Данная категория вредоносных программ не дописывается к исполняемым объектам, а копирует себя на сетевые ресурсы. Название этой категории было дано именно исходя из способности червей "ползать" по сетям и другим информационным каналам.

Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

Представители этого класса иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Worm.Linux.Ramen – первый известный червь, заражающий системы RedHat Linux. Он заражает удаленные Linux-системы (RedHat Linux) при помощи проблемы буферного переполнения. Эта "дыра" в программном обеспечении позволяет отправлять на удаленный компьютер исполняемый код и выполнять его там без вмешательства администратора (пользователя).

Источник распространения: по сети в виде архива **tgz**.

Алгоритм работы: используя проблемы буферного переполнения червь отправляет на удаленные компьютеры короткий кусок своего кода. При старте основного компонента червя (файл *start.sh*) поочередно вызываются прочие компоненты, которые определяют адреса атакуемых систем, посредством атаки "переполнение буфера" засылают туда "загрузчик" червя, который затем докачивает и запускает основной код червя. Главная страница веб-сервера подменяется HTML-файлом с текстом: "RameN Crew – Hackers looooooooooooove noodles". Наконец, червь отправляет сообщение e-mail по двум адресам, перезагружает систему и начинает сканировать интернет заново.
Червь также добавляет команду запуска своего основного файла к файлу инициализации системы */etc/rc.d/rc.sysinit*. В результате, червь запускается каждый раз при последующих запусках зараженной системы.

Worm.Linux.Lion – интернет-червь, атакующий Linux-сервера. Для проникновения на компьютеры червь использует "дыру" в безопасности BIND DNS-сервиса.

Алгоритм работы: червь сканирует интернет в поиске систем, имеющих уязвимость в безопасности root-доступа. Найдя подобную систему, червь инфицирует ее, собирает информацию о ней (ip-адрес,

логины, пароли) в файл с именем *mail.log* и затем отсылает его на электронный адрес *1i0nsniffer@china.com*.

Помимо этого червь предпринимает попытки связаться через интернет с сайтом www.51.net (домен 51.net зарегистрирован в Китае) и скачать оттуда файл *crew.tgz*. На зараженной машине архив распаковывается и инсталлируются процедуры, при выполнении которых уже вновь инфицированный компьютер также начинает сканировать ресурсы глобальной сети для поиска следующих жертв.

mIRC.Acoragil и **mIRC.Simpsalapim** – первые известные mIRC-черви. Свои названия они получили по кодовым словам, которые используются червями: если в тексте, переданном в канал каким-либо пользователем, присутствует строка *Acoragil*, то все пользователи, зараженные червем **mIRC.Acoragil**, автоматически отключаются от канала. То же самое происходит с червем **mIRC.Simpsalapim** – он аналогично реагирует на строку *Simpsalapim*.

Источник распространения: по сети командами mIRC черви пересылают свой код в файле *SCRIPT.INI* каждому новому пользователю, который подключается к каналу.

Алгоритм работы: черви включают троянскую часть. **mIRC.Simpsalapim** содержит код захвата канала IRC: если mIRC владельца канала заражен, то по вводу кодового слова *ananas*, злоумышленник перехватывает управление каналом.

mIRC.Acoragil по кодовым словам пересылает системные файлы DOC, Windows или UNIX. Некоторые кодовые слова выбраны таким образом, чтобы не привлекать внимания жертвы – *hi* или *the*. Одна из модификаций этого червя пересылает злоумышленнику файл паролей UNIX.

Worm.Linux.Adm – интернет-червь, заражающий Linux-системы. Червь отправляет на удаленные компьютеры короткий кусок своего кода, выполняет его там, докачивает свой основной код и исполняет его.

Источник распространения: по сети; распространяет свои копии (заражает удаленные Linux-системы) при помощи "дыры" в системе защиты Linux (так называемая дыра "переполнение буфера"). Эта дыра позволяет засылать исполняемый код на удаленный компьютер и выполнять его там без ведома администратора (пользователя).

ПРИЛОЖЕНИЕ С. 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, Бенилюксе, 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 двухсот пятидесяти высококвалифицированных специалистов, девять из которых имеют дипломы MBA, пятнадцать – степени кандидатов наук и двое являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками 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. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, межсетевых 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. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

С.1. Другие разработки Лаборатории Касперского

Антивирус Касперского® Personal

Антивирус Касперского® Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное ПО. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

- **Постоянная защита компьютера** – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
- **Проверка компьютера по требованию** – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Антивирус Касперского® Personal теперь не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию. Такая организация работы **заметно повышает скорость работы программы**.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского® Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах.

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их

содержимого, а также удаление вредоносного кода из архивных файлов формата **ZIP**, **CAB**, **RAR**, **AFJ**.

Простота настройки программы осуществляется за счет возможности выбора одного из трех предопределенных уровней: **Максимальная защита**, **Рекомендуемая защита** и **Максимальная скорость**.

Обновления антивирусных баз осуществляется каждые три часа, при этом обеспечивается их гарантированная доставка при разрыве или смене соединений с интернетом.

Антивирус Касперского® Personal Pro

Пакет разработан специально для полномасштабной антивирусной защиты домашних компьютеров, работающих под управлением операционных систем Windows 98/ME, Windows 2000/NT, Windows XP с бизнес-приложениями из состава MS Office 2000. Антивирус Касперского® Personal Pro включает программу загрузки ежедневных обновлений антивирусной базы и программных модулей. Уникальная система эвристического анализа данных второго поколения эффективно нейтрализует неизвестные вирусы. Простой и удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского® Personal Pro обеспечивает:

- **антивирусную проверку по требованию пользователя** локальных дисков;
- **автоматическую проверку в масштабе реального времени** на присутствие вирусов всех используемых файлов;
- **почтовый фильтр**, осуществляющий проверку входящих и исходящих почтовых сообщений в фоновом режиме.
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов.

Kaspersky® Anti-Hacker

Программа Kaspersky® Anti-Hacker представляет собой персональный межсетевой экран, обеспечивающий полномасштабную защиту компьютера, работающего под управлением операционной системы Windows, от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети и интернета.

Kaspersky® Anti-Hacker отслеживает сетевую активность по протоколу TCP/IP для всех приложений на вашем компьютере. При обнаружении подозрительных действий какого-либо приложения программа информирует вас об этом, и, при необходимости, блокирует сетевой доступ этому приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере.

Благодаря технологии SmartStealth™ значительно затрудняется обнаружение компьютера извне: режим невидимости вашего компьютера обеспечивает защиту от хакерских атак, не оказывая никакого негативного влияния на вашу работу в интернете. Программа обеспечивает стандартную прозрачность и доступность информации.

Kaspersky® Anti-Hacker также блокирует наиболее распространенные сетевые хакерские атаки, отслеживает попытки сканирования портов.

Программа поддерживает упрощенное администрирование по пяти режимам безопасности. По умолчанию используется режим самообучения, который позволяет настроить систему безопасности в зависимости от вашей реакции на различные события. Данный режим позволяет сконфигурировать межсетевой экран под конкретного пользователя и конкретный компьютер.

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на КПК, работающих под управлением Palm OS или Windows CE, а также информации, переносимой с PC или любой карты расширения, ROM файлы и базы данных, В состав программы входит оптимальный набор средств антивирусной защиты:

- **антивирусный сканер**, обеспечивающий проверку информации (хранимой как на PDA, так и на картах расширения любого типа) по требованию пользователя;
- **антивирусный монитор**, осуществляющий перехват вирусных программ, передаваемых в процессе синхронизации с использованием технологии HotSync™ или с другими КПК.

Программа также обеспечивает защиту данных, хранящихся на карманном компьютере, от несанкционированного доступа путем шифрования доступа к самому устройству и ко всей информации, хранящейся на портативном компьютере и картах расширения.

Антивирус Касперского® Business Optimal

Программный комплекс представляет собой уникальное конфигурируемое решение антивирусной защиты для предприятий малого и среднего бизнеса.

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту[1]:

А.1.1. [1] В зависимости от типа поставки

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *почтовых систем* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.

Антивирус Касперского® Business Optimal также включает систему централизованной установки и управления – Kaspersky® Administration Kit. Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite – это интегрированная система, обеспечивающая информационную безопасность вашей корпоративной сети независимо от ее сложности и размера. Программные компоненты, входящие в состав комплекса, предназначены для защиты всех узлов сети компании. Они совместимы с большинством используемых сегодня операционных систем и программных приложений, объединены системой централизованного управления и обладают единым пользовательским интерфейсом. Программный комплекс обеспечивает создание системы защиты, полностью совместимой с системными требованиями вашей сети.

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.
- *карманных компьютеров*, работающих под управлением Windows CE и Palm OS.

Kaspersky® Corporate Suite также включает *систему централизованной установки и управления* – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

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 RBL-списки 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 базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal предназначен для защиты пользователей почтовых клиентов Microsoft Outlook и Microsoft Outlook Express от нежелательных писем (спама).

Программный пакет Kaspersky Anti-Spam Personal представляет собой мощный инструмент для обнаружения спама в потоке входящей электронной почты, поступающей по протоколам POP3 и IMAP4 (только для Microsoft Outlook).

Во время фильтрации проверяются все возможные атрибуты письма: адреса отправителя и получателя, его заголовки. Также используется *контентная фильтрация*, то есть анализируется содержание самого письма (включая заголовок *Subject*) и файлов вложений. Применяются уникальные лингвистические и эвристические алгоритмы.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

C.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, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700	
Экстренная круглосуточная помощь	+7 (095) 797-8707 support@kaspersky.com	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	
Антивирусная лаборатория	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)	
Департамент продаж	+7 (095) 797-8700	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (095) 797-8700	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.com	