

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 5.6 для
Linux Mail Server

РУКОВОДСТВО
АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО 5.6 ДЛЯ LINUX MAIL
SERVER

Руководство администратора

© ЗАО «Лаборатория Касперского»
Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939, +7 (495) 956-7000
<http://www.kaspersky.ru>

Дата редакции: октябрь 2008 г.

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	7
1.1. Что нового.....	8
1.2. Аппаратные и программные требования к системе.....	9
1.3. Сервис для зарегистрированных пользователей.....	10
ГЛАВА 2. СОСТАВ И АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ.....	12
ГЛАВА 3. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ.....	15
3.1. Установка приложения на сервер под управлением Linux.....	15
3.2. Установка приложения на сервер под управлением FreeBSD.....	16
3.3. Схема расположения файлов приложения.....	17
3.3.1. Схема расположения файлов на сервере под управлением Linux.....	17
3.3.2. Схема расположения файлов на сервере под управлением FreeBSD.....	19
3.4. Постинсталляционная настройка.....	21
3.5. Настройка разрешающих правил в системах SELinux и AppArmor.....	24
3.6. Установка webmin-модуля для управления Антивирусом Касперского.....	26
3.7. Удаление приложения.....	28
ГЛАВА 4. ИНТЕГРАЦИЯ С ПОЧТОВОЙ СИСТЕМОЙ.....	30
4.1. Интеграция с почтовой системой Exim.....	31
4.1.1. Post-queue интеграция методом изменения маршрутов.....	31
4.1.2. Pre-queue интеграция с использованием динамически подгружаемой библиотеки.....	34
4.2. Интеграция с почтовой системой Postfix.....	37
4.2.1. Post-queue интеграция.....	37
4.2.2. Pre-queue интеграция.....	39
4.2.3. Интеграция с помощью функций Milter.....	42
4.3. Интеграция с почтовой системой qmail.....	43
4.4. Интеграция с почтовой системой Sendmail.....	45
4.4.1. Интеграция с помощью файла <i>.cf</i>	45
4.4.2. Интеграция с помощью файла <i>.mc</i>	47

ГЛАВА 5. АНТИВИРУСНАЯ ЗАЩИТА ПОЧТЫ	48
5.1. Формирование групп	48
5.2. Определение политики проверки почтовых сообщений.....	50
5.3. Режим проверки сообщений.....	51
5.3.1. Антивирусная проверка	51
5.3.2. Фильтрация почты	53
5.4. Действия над объектами	54
5.5. Предустановленные профили защиты	56
5.5.1. Рекомендуемый профиль защиты	56
5.5.2. Профиль максимальной защиты.....	57
5.5.3. Профиль максимальной скорости.....	58
5.6. Резервное копирование сообщений.....	59
5.7. Уведомления.....	60
5.7.1. Настройка уведомлений	60
5.7.2. Шаблоны уведомлений.....	62
5.7.3. Создание собственных шаблонов уведомлений	65
5.7.3.1. Макросы	66
5.7.3.2. Итерационные конструкции.....	66
5.7.3.3. Границы видимости итерационной конструкции	68
5.7.3.4. Переменные	69
5.7.3.5. Синтаксис языка.....	70
5.7.3.6. Макросы уведомлений в составе приложения	72
ГЛАВА 6. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВЫХ СИСТЕМ.....	74
6.1. Область проверки.....	75
6.2. Режим проверки и лечения объектов	76
6.3. Действия над объектами	77
6.4. Проверка директории по требованию	78
6.5. Проверка по расписанию.....	79
6.6. Отправка уведомлений администратору.....	79
ГЛАВА 7. ОБНОВЛЕНИЕ БАЗ АНТИВИРУСА.....	81
7.1. Автоматическое обновление	82
7.2. Обновление по требованию	83
7.3. Обновление из сетевой директории.....	84

ГЛАВА 8. УПРАВЛЕНИЕ КЛЮЧАМИ	86
8.1. Просмотр лицензионной информации	87
8.2. Продление срока действия ключа	89
ГЛАВА 9. ОТЧЕТЫ И СТАТИСТИКА РАБОТЫ ПРИЛОЖЕНИЯ.....	91
9.1. Формирование отчетов.....	91
9.2. Статистика работы приложения.....	94
ГЛАВА 10. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ	98
10.1. Контроль состояния защиты с помощью протокола SNMP	98
10.2. Использование скрипта настройки приложения	103
10.3. Управление приложением из командной строки	105
10.4. Дополнительные информационные поля в сообщениях	107
10.5. Локализация формата отображаемых дат и времени	108
ГЛАВА 11. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ ПРИЛОЖЕНИЯ	109
ПРИЛОЖЕНИЕ А. СПРАВОЧНАЯ ИНФОРМАЦИЯ	111
А.1. Конфигурационный файл приложения <i>kav4lms.conf</i>	111
А.1.1. Секция [<i>kav4lms:server.settings</i>]	111
А.1.2. Секция [<i>kav4lms:server.log</i>].....	114
А.1.3. Секция [<i>kav4lms:server.statistics</i>].....	115
А.1.4. Секция [<i>kav4lms:server.snmp</i>]	116
А.1.5. Секция [<i>kav4lms:server.notifications</i>]	119
А.1.6. Секция [<i>kav4lms:filter.settings</i>]	120
А.1.7. Секция [<i>kav4lms:filter.log</i>]	123
А.1.8. Секция [<i>kav4lms:groups</i>]	125
А.1.9. Секция [<i>path</i>]	125
А.1.10. Секция [<i>locale</i>]	126
А.1.11. Секция [<i>options</i>].....	126
А.1.12. Секция [<i>updater.path</i>].....	127
А.1.13. Секция [<i>updater.options</i>].....	127
А.1.14. Секция [<i>updater.report</i>]	129
А.1.15. Секция [<i>updater.actions</i>]	129
А.1.16. Секция [<i>scanner.display</i>].....	131
А.1.17. Секция [<i>scanner.options</i>]	132
А.1.18. Секция [<i>scanner.report</i>].....	134
А.1.19. Секция [<i>scanner.container</i>].....	135

A.1.20. Секция <i>[scanner.object]</i>	137
A.1.21. Секция <i>[scanner.path]</i>	138
A.2. Конфигурационный файл группы	138
A.2.1. Секция <i>[kav4lms:groups.<имя_группы>.definition]</i>	139
A.2.2. Секция <i>[kav4lms:groups.<имя_группы>.settings]</i>	140
A.2.3. Секция <i>[kav4lms:groups.<имя_группы>.actions]</i>	142
A.2.4. Секция <i>[kav4lms:groups.<имя_группы>.contentfiltering]</i>	143
A.2.5. Секция <i>[kav4lms:groups.<имя_группы>.notifications]</i>	147
A.2.6. Секция <i>[kav4lms:groups.<имя_группы>.backup]</i>	149
A.3. Параметры командной строки компонента <i>kav4lms-licensemanager</i>	150
A.4. Коды возврата компонента <i>kav4lms-licensemanager</i>	151
A.5. Параметры командной строки компонента <i>kav4lms-keepup2date</i>	152
A.6. Коды возврата компонента <i>kav4lms-keepup2date</i>	153
ПРИЛОЖЕНИЕ В. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	155
В.1. Другие разработки «Лаборатории Касперского»	156
В.2. Наши координаты	168
ПРИЛОЖЕНИЕ С. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СТОРОННИХ ПРОИЗВОДИТЕЛЕЙ	170
С.1. Библиотека <i>Pcre</i>	170
С.2. Библиотека <i>Expat</i>	171
С.3. Библиотека <i>AgentX++v1.4.16</i>	172
С.4. Библиотека <i>Agent++v3.5.28a</i>	178
С.5. Библиотека <i>Boost v 1.0</i>	179
С.6. Библиотека <i>Milter</i>	180
С.7. Библиотека <i>libkavexim.so</i>	182

ГЛАВА 1. ВВЕДЕНИЕ

Антивирус Касперского® 5.6 для Linux Mail Server (далее называемый *Антивирус Касперского* или *приложение*) обеспечивает антивирусную защиту почтового трафика и файловых систем серверов, работающих под управлением операционных систем Linux или FreeBSD и использующих почтовые системы Sendmail, Postfix, qmail или Exim.

Приложение позволяет:

- Проверять файловые системы сервера, входящие и исходящие почтовые сообщения на наличие угроз.
- Обнаруживать зараженные, подозрительные, защищенные паролем и недоступные для проверки объекты.
- Обезвреживать обнаруженные в файлах и почтовых сообщениях угрозы. Лечить зараженные объекты.
- Сохранять резервные копии сообщений перед их антивирусной обработкой и фильтрацией; восстанавливать сообщения из резервных копий.
- Обработать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей.
- Выполнять фильтрацию почтовых сообщений по имени, типу и размеру вложений.
- Уведомлять отправителя, получателей и администратора об обнаружении сообщений, содержащих зараженные, подозрительные, защищенные паролем и недоступные для проверки объекты.
- Формировать статистику и отчеты о результатах работы.
- Обновлять базы антивируса с серверов обновлений «Лаборатории Касперского» по расписанию и по требованию.

Базы используются в процессе поиска и лечения зараженных файлов. На основе записей, содержащихся в них, каждый файл во время проверки анализируется на присутствие угроз: код файла сравнивается с кодом, характерным для той или иной угрозы.

- Настраивать параметры и управлять работой приложения как локально (стандартными средствами операционной системы с помощью параметров командной строки, сигналов и модификацией конфигурационного файла приложения), так и удаленно через веб-интерфейс программы Webmin.

- Получать конфигурационную информацию и статистику работы приложения по протоколу SNMP, а также настроить приложение на отправку SNMP-ловушек при наступлении определенных событий.

1.1. Что нового

Антивирус Касперского 5.6 для Linux Mail Server объединяет функциональность двух приложений: Антивируса Касперского 5.5 для Linux и FreeBSD Mail Server и Антивируса Касперского 5.6 для Sendmail с Milter API, а также обладает следующими дополнительными возможностями:

- Для почтовой системы Exim поддерживается как pre-queue, так и post-queue интеграция. При pre-queue интеграции сообщения передаются на проверку перед размещением в очереди почтовой системы, при post-queue интеграции – после размещения в очереди почтовой системы. Реализован процесс автоматической интеграции с помощью скрипта настройки приложения. Подробное описание процесса интеграции содержит Глава 4 на стр. 30.
- Расширены возможности по настройке проверки сообщений – доступны два способа проверки: сообщение может проверяться как единый объект и комбинированно – как единый объект, затем «по частям». Способы отличаются уровнем предоставляемой защиты. Подробная информация содержится в п. 5.2 на стр. 50.
- Изменился процесс настройки приложения – появилась возможность настройки для отдельных групп отправителей и получателей. Подробная информация о настройке групп содержится в п. 5.1 на стр. 48.
- Расширен список действий, выполняемых над сообщениями – добавлено действие в зависимости от обнаруженной в объекте угрозы. Подробная информация о действиях приложения содержится в п. 5.4 на стр. 54.
- Расширены возможности по фильтрации сообщений – добавлен критерий фильтрации по размеру вложения. Подробная информация о настройке фильтрации сообщений содержится в п. 5.3.2 на стр. 53.
- Расширена библиотека шаблонов уведомлений – добавлены шаблоны уведомления администратора. Шаблоны уведомлений вынесены в отдельную директорию.
- Не поддерживается возможность помещения зараженных объектов на карантин.
- Расширены возможности резервного копирования сообщений – для каждой копии теперь возможно создание информационного файла.

Подробная информация о настройке резервного копирования сообщений содержится в п. 5.6 на стр. 59.

- Расширены возможности настройки детализации отчетов приложения. Подробная информация о настройке отчетов приложения содержится в п. 9.1 на стр. 91.
- Добавился новый тип статистической информации – детализированная статистика по каждому сообщению. Подробная информация по настройке статистики о работе приложения содержится в п. 9.2 на стр. 94.
- Появилась возможность опроса статуса, конфигурации и других аспектов работы приложения с помощью SNMP-запросов и SNMP-ловушек. Подробная информация содержится в п. 10.1 на стр. 98.
- В поставку приложения добавлен инструмент для управления приложением из командной строки. Подробная информация об этом инструменте содержится в п. 10.3 на стр. 105.

1.2. Аппаратные и программные требования к системе

Системные требования Антивируса Касперского следующие:

- Аппаратные требования для почтового сервера, поддерживающего около 200 МБ трафика в день:
 - процессор Intel Pentium IV, 3 ГГц или выше;
 - 1 ГБ оперативной памяти;
 - 200 МБ свободного места на жестком диске (в это количество не входит пространство, необходимое для хранения резервных копий сообщений).
- Программные требования:
 - для 32-битной платформы одна из следующих операционных систем:
 - Red Hat Enterprise Linux Server 5.2;
 - Fedora 9;
 - SUSE Linux Enterprise Server 10 SP2;
 - openSUSE 11.0;

- Debian GNU/Linux 4.0 r4;
- Mandriva Corporate Server 4.0;
- Ubuntu 8.04.1 Server Edition;
- FreeBSD 6.3, 7.0.
- для 64-битной платформы одна из следующих операционных систем:
 - Red Hat Enterprise Linux Server 5.2;
 - Fedora 9;
 - SUSE Linux Enterprise Server 10 SP2;
 - openSUSE Linux 11.0.
- Одна из перечисленных почтовых систем: Sendmail 8.12.x или выше, qmail 1.03, Postfix 2.x, Exim 4.x.
- Программа Webmin (www.webmin.com), если планируется удаленное управление Антивирусом Касперского.
- Perl версии 5.0 или выше (www.perl.org).

1.3. Сервис для зарегистрированных пользователей

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

Приобретая ключ, вы становитесь зарегистрированным пользователем программы и в течение срока действия ключа можете получать 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»).

Примечание

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

ГЛАВА 2. СОСТАВ И АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ

В состав Антивируса Касперского входят следующие компоненты:

- фильтр – сервис связи с почтовой системой, отдельная программа, обеспечивающая взаимодействие Антивируса Касперского с почтовой системой; в состав дистрибутива приложения включены модули для каждой из поддерживаемых почтовых систем:
 - *kav4lms-milter* – Milter-сервис связи с почтовыми системами Sendmail и Postfix через Milter API;
 - *kav4lms-filter* – SMTP-сервис связи с почтовыми системами Postfix и Exim;
 - *kav4lms-qmail* – обработчик очереди почтовых сообщений для почтовой системы qmail;
- *kavmd* – центральная служба приложения, принимает запросы от фильтра и обеспечивает антивирусную защиту почтового трафика;
- *kav4lms-kavscanner* – обеспечивает антивирусную защиту файловых систем сервера;
- *kav4lms-keepup2date* – обеспечивает обновление баз антивируса путем их скачивания с серверов обновлений «Лаборатории Касперского» или из локального каталога;
- *kav4lms-licensemanager* – компонент, предназначенный для работы с ключами: установки, удаления, просмотра статистической информации;
- *kav4lms.wbm* – webmin-модуль для удаленного управления приложением при помощи веб-интерфейса (устанавливается опционально), позволяет настраивать и организовывать обновления баз антивируса, просматривать статистическую информацию, задавать действия над объектами в зависимости от их статуса, контролировать результаты работы приложения;
- *kav4lms-cmd* – утилита управления Антивирусом из командной строки.

Предусмотрен следующий алгоритм проверки сообщений:

1. Фильтр получает сообщение от почтовой системы. Если фильтр и центральная служба работают на одном компьютере, то вместо сообщений передаются имена файлов сообщений.
2. Фильтр определяет, каким группам принадлежит сообщение, выбирает группу с наивысшим приоритетом (см. п. 5.1 на стр 48) и передает сообщение на проверку центральной службе приложения. Если такой группы не обнаружено, сообщение обрабатывается по правилам группы **Default**, входящей в состав дистрибутива приложения.

Центральная служба выполняет проверку сообщения в соответствии с параметрами, заданными в конфигурационном файле группы. В зависимости от способа, заданного **политикой**, сообщение может проверяться как единый объект и комбинированно – как единый объект, затем «по частям» (см. п. 5.2 на стр. 50).

Комбинированная проверка является более тщательной и обеспечивает более высокий уровень защиты, хотя быстродействие при этом несколько снижается.

3. Если задана антивирусная проверка сообщений (см. п. 5.3 на стр. 51), центральная служба проверяет сообщение как единый объект. Согласно статусу, присвоенному по результатам проверки (см. п. 5.3.1 на стр. 51), центральная служба: блокирует доставку, отклоняет или пропускает сообщение, заменяет его предупреждением, изменяет заголовки (см. п. 5.4 на стр. 54). Если для определенных угроз задана специальная обработка (параметр **VirusNameList**), в случае их обнаружения будут выполнены указанные действия (параметр **VirusNameAction**). Порядок обработки сообщения задается в конфигурационном файле группы.

Перед обработкой, если определено в параметрах группы, создается резервная копия сообщения.

4. После антивирусной проверки сообщения, выполняется фильтрация, если она задана в параметрах группы.

Фильтрация осуществляется по имени, типу и размеру вложения (см. п. 5.3.2 на стр. 53). По результатам проверки выполняются действия, заданные параметрами фильтрации в конфигурационном файле группы. Обработанные, а также удовлетворяющие параметрам фильтрации объекты передаются на проверку «по частям», если в параметрах группы задан комбинированный способ проверки.

5. При проверке сообщения «по частям» выполняется разбор MIME-структуры и обработка составных частей сообщения.

Объекты сообщения обрабатываются согласно статусу, присвоенному конкретному объекту, несмотря на статус, присвоенный сообщению в целом.

В случае если при проверке сообщения как единого объекта оно было признано зараженным, а при проверке «по частям» угроза не обнаружена, будет применено действие ко всему сообщению, заданное для зараженных сообщений (параметр **InfectedAction**). Также, если уровень вложенности прикрепленного к незараженному сообщению объекта превышает установленное в параметрах группы ограничение (параметр **MaxScanDepth**), будет применено действие ко всему сообщению, назначенное для сообщений, проверка которых завершена с ошибкой (параметр **ErrorAction**).

При обработке объектов сообщения центральная служба переименовывает, удаляет или заменяет объект предупреждающим сообщением, добавляет информационные заголовки, либо пропускает сообщение (см. п. 5.4 на стр. 54). Зараженные объекты подвергаются лечению. Перед обработкой объекта, если определено в параметрах группы, создается резервная копия всего сообщения (если она не была создана ранее).

6. После проверки и обработки центральная служба передает сообщение фильтру. Обработанное сообщение с уведомлениями о результатах проверки и лечения передается почтовой системе, которая выполняет доставку почтового потока локальным пользователям или осуществляет маршрутизацию на другие почтовые сервера.

ГЛАВА 3. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Рекомендуется выполнить следующие действия, прежде чем приступить к установке Антивируса Касперского:

- Убедиться, что система соответствует аппаратным и программным требованиям, перечисленным в п. 1.2 на стр. 9.
- Создайте резервные копии конфигурационных файлов почтовой системы, установленной на вашем сервере.
- Настройте соединение с интернетом.
- Зарегистрируйтесь в системе с правами учетной записи **root** или любым другим, имеющим права привилегированного пользователя.

Внимание!

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

3.1. Установка приложения на сервер под управлением Linux

Для серверов, работающих под управлением операционной системы Linux, Антивирус Касперского распространяется в *двух вариантах* установки, в зависимости от дистрибутива операционной системы Linux.

Для дистрибутивов Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise Server, openSUSE и Mandriva Linux предусмотрена установка приложения из rpm-пакета.

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

```
# rpm -i <имя_пакета>
```

Внимание!

Если для установки вы использовали *rpm*-пакет, после копирования файлов дистрибутива на сервер вам необходимо самостоятельно запустить скрипт *postinstall.pl*, выполняющий настройку приложения после установки. Скрипт *postinstall.pl* устанавливается по умолчанию в каталог */opt/kaspersky/kav4lms/lib/bin/setup/* (для Linux) и в каталог */usr/local/libexec/kaspersky/kav4lms/setup/* (для FreeBSD).

Для дистрибутивов Debian GNU/Linux и Ubuntu установка осуществляется с помощью *deb*-пакета приложения.

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

```
# dpkg -i <имя_пакета>
```

После запуска команды дальнейший процесс установки будет выполнен автоматически. После его завершения на экран будет выведена информация о постинсталляционной настройке приложения (см. п. 3.4 на стр. 21).

Внимание!

Существуют особенности установки приложения для дистрибутива Mandriva.

Для корректного запуска Антивируса Касперского после установки убедитесь, что для хранения временных файлов в операционной системе используется директория */root/tmp/* и пользователь, под которым работает приложение (по умолчанию – *kluser*), имеет права на запись в этой директории.

Возможно, вам потребуется изменить права на эту директорию, либо переопределить или удалить переменные окружения **TMP**, **TEMP** с тем, чтобы использовалась другая директория (например, */tmp/*) с необходимыми для работы приложения правами.

3.2. Установка приложения на сервер под управлением FreeBSD

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

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

```
# pkg_add <имя_пакета>
```

После запуска команды дальнейший процесс установки будет выполнен автоматически. После его завершения на экран будет выведена информация о постинсталляционной настройке приложения (см. п. 3.4 на стр. 21).

3.3. Схема расположения файлов приложения

При установке Антивируса Касперского файлы приложения копируются в рабочие директории на сервере.

Внимание!

Для того чтобы *man*-страницы к приложению были доступны по команде *man* <имя_*man*-страницы>, необходимо:

- для дистрибутивов Debian Linux, Ubuntu Linux, SUSE Linux в файл */etc/manpath.config* добавить строку:

```
MANDATORY_MANPATH /opt/kaspersky/kav4lms/share/man
```
- для дистрибутивов Red Hat Linux и Mandriva Linux в файл */etc/man.config* добавить строку:

```
MANPATH /opt/kaspersky/kav4lms/share/man
```
- для дистрибутивов FreeBSD в файл */etc/manpath.config* добавить строку:

```
MANDATORY_MANPATH /usr/local/man
```

Если в системе используется переменная **MANPATH**, добавьте в список ее значений путь к каталогу *man*-страниц приложения, выполнив следующую команду:

```
# export MANPATH=$MANPATH:<путь к каталогу man-страниц>
```

3.3.1. Схема расположения файлов на сервере под управлением Linux

После установки Антивируса Касперского на сервер под управлением операционной системы Linux файлы дистрибутива будут расположены следующим образом:

- /etc/opt/kaspersky/kav4lms.conf* – основной конфигурационный файл приложения;
- /etc/opt/kaspersky/kav4lms* – директория, содержащая конфигурационные файлы Антивируса Касперского:
 - groups.d/* – директория, содержащая конфигурационные файлы групп приложения;
 - default.conf* – конфигурационный файл, содержащий параметры группы по умолчанию;
 - locale.d/strings.en* – файл, содержащий строковые константы, используемые приложением;
 - profiles/* – директория, содержащая профили параметров по умолчанию;
 - default_recommended/* – директория, содержащая конфигурационные файлы рекомендуемого профиля;
 - high_overall_security/* – директория, содержащая конфигурационные файлы профиля максимальной защиты;
 - high_scan_speed/* – директория, содержащая конфигурационные файлы профиля максимальной скорости проверки;
 - templates/* – директория, содержащая шаблоны уведомлений;
 - templates-admin/* – директория, содержащая шаблоны уведомлений администратора;
- /opt/kaspersky/kav4lms/* – основная директория приложения, содержащая:
 - bin/* – директория, содержащая исполняемые файлы компонентов Антивируса Касперского:
 - kav4lms-cmd* – исполняемый файл инструмента управления приложением с помощью командной строки;
 - kav4lms-setup.sh* – скрипт настройки приложения;
 - kav4lms-kavscanner* – исполняемый файл компонента проверки файловых систем;
 - kav4lms-licensemanager* – исполняемый файл компонента управления ключами приложения;
 - kav4lms-keepup2date* – исполняемый файл компонента обновления баз антивируса;
 - sbin/* – директория, содержащая исполняемые файлы сервисов приложения;
 - lib/* – директория, содержащая файлы библиотек Антивируса Касперского;
 - bin/avbasestest* – утилита проверки корректности обновлений баз антивируса, используемая компонентом *kav4lms-keepup2date*;
 - share/doc/* – директория, содержащая лицензионное соглашение и документацию по развертыванию приложения;

share/man/ – директория, содержащая man-файлы приложения;

share/scripts/ – директория, содержащая скрипты, необходимые для работы приложения;

share/snmp-mibs/ – директория, содержащая MIB Антивируса Касперского;

share/webmin/ – директория, содержащая модуль к программе Webmin;

/etc/init.d/ – директория, содержащая скрипты управления сервисами приложения;

kav4lms – скрипт управления центральной службой приложения;

kav4lms-filters – скрипт управления фильтром Антивируса Касперского;

/var/opt/kaspersky/kav4lms/ – директория, содержащая переменные данные приложения;

backup/ – директория, содержащая резервные копии сообщений и информационные файлы;

bases/ – директория, содержащая базы антивируса;

bases.backup/ – директория, содержащая резервную копию баз антивируса;

licenses/ – директория, содержащая файлы ключей;

patches/ – директория, содержащая обновления программных модулей приложения;

stats/ – директория, содержащая файлы статистики работы приложения;

updater/ – директория, содержащая файл с информацией о последнем обновлении;

nqueue/ – директория, содержащая файлы очереди почтовых сообщений.

Внимание!

Далее в этом руководстве по умолчанию используются пути для Linux!

3.3.2. Схема расположения файлов на сервере под управлением FreeBSD

После установки Антивируса Касперского на сервер под управлением операционной системы FreeBSD файлы дистрибутива будут расположены следующим образом:

/usr/local/etc/kaspersky/kav4lms.conf – основной конфигурационный файл приложения;

- /usr/local/etc/kaspersky/kav4lms/* – директория, содержащая конфигурационные файлы Антивируса Касперского:
- groups.d/* – директория, содержащая конфигурационные файлы групп приложения;
 - default.conf* – конфигурационный файл, содержащий параметры группы по умолчанию;
 - locale.d/strings.en* – файл, содержащий строковые константы, используемые приложением;
 - profiles/* – директория, содержащая профили параметров по умолчанию:
 - default_recommended/* – директория, содержащая конфигурационные файлы рекомендуемого профиля;
 - high_overall_security/* – директория, содержащая конфигурационные файлы профиля максимальной защиты;
 - high_scan_speed/* – директория, содержащая конфигурационные файлы профиля максимальной скорости проверки;
 - templates/* – директория, содержащая шаблоны уведомлений;
 - templates-admin/* – директория, содержащая шаблоны уведомлений администратора;
- /usr/local/bin/* – директория, содержащая исполняемые файлы компонентов Антивируса Касперского:
- kav4lms-cmd* – исполняемый файл инструмента управления приложением с помощью командной строки;
 - kav4lms-setup.sh* – скрипт настройки приложения;
 - kav4lms-kavscanner* – исполняемый файл компонента проверки файловых систем;
 - kav4lms-licensemanager* – исполняемый файл компонента управления ключами приложения;
 - kav4lms-keepup2date* – исполняемый файл компонента обновления баз антивируса;
- /usr/local/sbin/* – директория, содержащая исполняемые файлы сервисов приложения;
- /usr/local/etc/rc.d/* – директория, содержащая скрипты управления сервисами приложения:
- kav4lms.sh* – скрипт управления центральной службой приложения;
 - kav4lms-filters.sh* – скрипт управления фильтром Антивируса Касперского;
- /usr/local/lib/kaspersky/kav4lms/* – директория, содержащая файлы библиотек Антивируса Касперского;

- /usr/local/libexec/kaspersky/kav4lms/avbasestest* – утилита проверки корректности обновлений баз антивируса, используемая компонентом *kav4lms-keepup2date*;
- /usr/local/share/doc/kav4lms/* – директория, содержащая лицензионное соглашение и документацию по разворачиванию приложения;
- /usr/local/man/* – директория, содержащая man-файлы приложения;
- /usr/local/share/kav4lms/scripts/* – директория, содержащая скрипты, необходимые для работы приложения;
- /usr/local/share/kav4lms/snmp-mibs/* – директория, содержащая MIB Антивируса Касперского;
- /usr/local/share/kav4lms/webmin/* – директория, содержащая модуль к программе Webmin;
- /var/db/kaspersky/kav4lms/* – директория, содержащая переменные данные приложения:
 - backup/* – директория, содержащая резервные копии сообщений и информационные файлы;
 - bases/* – директория, содержащая базы антивируса;
 - bases.backup/* – директория, содержащая резервную копию баз антивируса;
 - licenses/* – директория, содержащая файлы ключей;
 - patches/* – директория, содержащая обновления программных модулей приложения;
 - stats/* – директория, содержащая файлы статистики работы приложения;
 - updater/* – директория, содержащая файл с информацией о последнем обновлении;
 - nqueue/* – директория, содержащая файлы очереди почтовых сообщений.

3.4. Постинсталляционная настройка

При установке Антивируса Касперского после завершения копирования файлов дистрибутива на сервер выполняется настройка системы. В зависимости от менеджера пакета этап конфигурации будет запущен автоматически либо (в случае, если менеджер пакета не допускает использование интерактивных скриптов, как, например, *rpm*) его потребуется запустить вручную.

Для запуска процесса настройки приложения вручную в командной строке введите:

для Linux:

```
# /opt/kaspersky/kav4lms/lib/bin/setup/postinstall.pl
```

для FreeBSD:

```
# /usr/local/libexec/kaspersky/kav4lms/setup/postinstall.pl
```

В результате вам будет предложено выполнить следующие действия:

1. Если приложение обнаружит на компьютере конфигурационные файлы Антивируса Касперского 5.5 для Linux Mail Server или Антивируса Касперского 5.6 для Sendmail с Milter API, на этом шаге будет предложено выбрать, какой из файлов преобразовать и сохранить в формате текущей версии приложения, и, в случае выбора одного из файлов будет предложено заменить входящий в состав дистрибутива конфигурационный файл приложения восстановленным и преобразованным файлом.

Для того чтобы заменить входящий в состав дистрибутива конфигурационный файл приложения восстановленным файлом, введите в качестве ответа **yes**. Чтобы отказаться от замены, введите **no**.

По умолчанию преобразованные конфигурационные файлы сохраняются в следующих директориях:

```
kav4mailservers -  
/etc/opt/kaspersky/kav4lms/profiles/kav4mailservers5.  
5-converted
```

```
kavmilter -  
/etc/opt/kaspersky/kav4lms/profiles/kavmilter5.6-  
converted
```

2. Указать путь к файлу ключа.

Обратите внимание, что если ключ не установлен, обновление баз антивируса и формирование списка защищаемых доменов в рамках процесса установки не выполняется. В этом случае необходимо выполнить эти действия самостоятельно после установки ключа.

3. Указать параметры прокси-сервера, используемого для подключения к интернету в формате:

```
http://<IP-адрес_прокси_сервера>:<порт>
```

или

```
http://<имя_пользователя>:<пароль>@<IP-адрес_прокси_  
сервера>:<порт>
```

если на прокси-сервере используется авторизация.

Если для подключения к интернету прокси-сервер не используется, введите в качестве ответа **no**.

Заданное значение будет использоваться компонентом обновления *kav4lms-keepup2date* для подключения к источнику обновлений.

4. Выполнить обновление баз антивируса. Для этого введите в качестве ответа **yes**. Если вы хотите отказаться от копирования обновлений сейчас, введите **no**. Вы сможете выполнить обновление позже с помощью компонента *kav4lms-keepup2date* (подробнее см. п. 7.2 на стр. 83).

Примечание

Обновление баз антивируса возможно только при установленном ключе.

5. Настроить автоматическое обновление баз антивируса. Для этого введите в качестве ответа **yes**. Чтобы отказаться от настройки автоматического обновления сейчас, введите **no**. Вы сможете выполнить эту настройку позже с помощью компонента *kav4lms-keepup2date* (подробнее см. п. 7.1 на стр. 82) или с помощью скрипта настройки приложения (подробнее см. п. 10.2 на стр. 103).

Внимание!

При интеграции с *qmail*, настройку автоматического обновления необходимо произвести следующим образом:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-cron=updater --user=root
```

6. Установить *webmin*-модуль для управления Антивирусом Касперского через веб-интерфейс программы *Webmin*.

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

Введите в качестве ответа **yes** для установки *webmin*-модуля или **no**, чтобы отказаться от установки.

7. Определить список доменов, почтовый трафик которых будет защищаться от вирусов. Значение, предусмотренное по умолчанию – **localhost, localhost.localdomain**. Чтобы использовать его, нажмите на клавишу **Enter**.

Чтобы задать список доменов вручную, перечислите их в командной строке. Вы можете указать несколько значений, разделенных запятой, допускается использование масок и регулярных выраже-

ний. Точки в именах доменов должны быть «экранированы» с помощью символа «\».

Например:

```
re:.*\example\.com
```

8. Интегрировать Антивирус Касперского в почтовую систему. Вы можете принять предлагаемый по умолчанию вариант интеграции с обнаруженной на компьютере почтовой системой или отказаться от интеграции и выполнить ее позже. Подробное описание интеграции с почтовой системой содержит Глава 4 на стр. 30.

По умолчанию для почтовых систем Exim и Postfix используется post-queue интеграция (см. п. 4.1.1 на стр. 31 и п. 4.2.1 на стр. 37).

Внимание!

При автоматической интеграции с Sendmail скрипт всегда пытается внести изменения в *.mc*-файл, потому что любое последующее обновление сохранит сделанные изменения. Если *.mc*-файл содержит include-директивы, ссылающиеся на несуществующие *.mc*-файлы, то такой файл не может быть использован для интеграции Антивируса Касперского. В таком случае установите пакет **sendmail-cf** для интеграции с использованием *.cf*-файла.

Если *.mc*-файл не может быть использован для интеграции приложения, то будет использован *.cf*-файл.

3.5. Настройка разрешающих правил в системах SELinux и AppArmor

Для создания модуля SELinux с правилами, необходимыми для работы Антивируса Касперского, после установки приложения и его интеграции с почтовой системой выполните следующие шаги:

1. Переведите SELinux в разрешающий режим:

```
# setenforce Permissive
```
2. Отправьте одно или несколько тестовых сообщений и убедитесь, что они прошли антивирусную проверку и доставлены получателям.
3. Создайте модуль правил на основе блокирующих записей:

Для Fedora:

```
# audit2allow -l -M kav4lms -i /var/log/messages
```

Для RHEL:

```
# audit2allow -l -M kav4lms -i \  
/var/log/audit/audit.log
```

4. Загрузите полученный модуль правил:

```
# semodule -i kav4lms.pp
```

5. Переведите SELinux в принудительный режим:

```
# setenforce Enforcing
```

В случае появления новых audit-сообщений, связанных с Антивирусом Касперского, следует обновлять файл модуля правил:

Для Fedora:

```
# audit2allow -l -M kav4lms -i /var/log/messages  
# semodule -u kav4lms.pp
```

Для RHEL:

```
# audit2allow -l -M kav4lms -i /var/log/audit/audit.log  
# semodule -u kav4lms.pp
```

Для дополнительной информации смотрите:

- **RedHat Enterprise Linux:** руководство «Red Hat Enterprise Linux Deployment Guide», глава «44. Security and SELinux».
- **Fedora:** Fedora SELinux Project Pages.
- **Debian GNU/Linux:** руководство «Configuring the SELinux Policy» из пакета selinux-doc «Documentation for Security-Enhanced Linux».

Для обновления профилей AppArmor, необходимых для работы Антивируса Касперского, после установки приложения и его интеграции с почтовой системой выполните следующие шаги:

1. Переведите все правила для приложений в «щадящий» режим:

```
# aa-complain /etc/apparmor.d/*  
# /etc/init.d/apparmor reload
```

2. Перезапустите почтовую систему:

```
# /etc/init.d/postfix restart
```

3. Перезапустите kav4lms и kav4lms-filters:

```
# /etc/init.d/kav4lms restart  
# /etc/init.d/kav4lms-filters restart
```

4. Отправьте одно или несколько тестовых сообщений и убедитесь, что они прошли антивирусную проверку и доставлены получателям.
5. Запустите утилиту обновления профилей:

```
# aa-logprof
```
6. Перезагрузите правила AppArmor:

```
# /etc/init.d/apparmor reload
```
7. Переведите все правила для приложений в «принудительный» режим:

```
# aa-enforce /etc/apparmor.d/*  
# /etc/init.d/apparmor reload
```

В случае появления новых audit-сообщений, связанных с Антивирусом Касперского, следует повторить шаги, описанные в п. 5 и 6.

Для дополнительной информации смотрите:

- **openSUSE** и **SUSE Linux Enterprise Server**: «Novell AppArmor Quick Start», «Novell AppArmor Administration Guide».
- **Ubuntu**: руководство «Ubuntu Server Guide», глава «8. Security».

3.6. Установка webmin-модуля для управления Антивирусом Касперского

Работой Антивируса Касперского можно также управлять удаленно через веб-браузер, используя программу Webmin.

Webmin – это программа, упрощающая процесс управления Linux/Unix-системой. Программа использует модульную структуру с возможностью подключения новых и разработки собственных модулей. Получить дополнительную информацию о программе и ее установке, а также скачать документацию и дистрибутив Webmin можно на официальном сайте программы: www.webmin.com.

В дистрибутив Антивируса Касперского включен webmin-модуль, который можно либо установить в процессе постинсталляционной настройки приложения (см. п. 3.4 на стр. 21), если в системе уже установлена программа Webmin, либо в любой другой момент времени после установки программы Webmin.

Далее подробно рассматривается процесс подключения webmin-модуля для управления Антивирусом Касперского.

Если при установке Webmin были использованы настройки по умолчанию, то по завершении установки доступ к программе можно получить с помощью браузера, подключившись через протокол HTTP/HTTPS на порт 10000.

Для того чтобы установить webmin-модуль управления Антивирусом Касперского необходимо:

Получить доступ через веб-браузер к программе Webmin с правами администратора данной программы.

1. В меню Webmin выбрать закладку **Webmin Configuration** и затем раздел **Webmin Modules**.
2. В разделе **Install Module** выбрать пункт **From Local File** и нажать на кнопку (см. рис. 1).

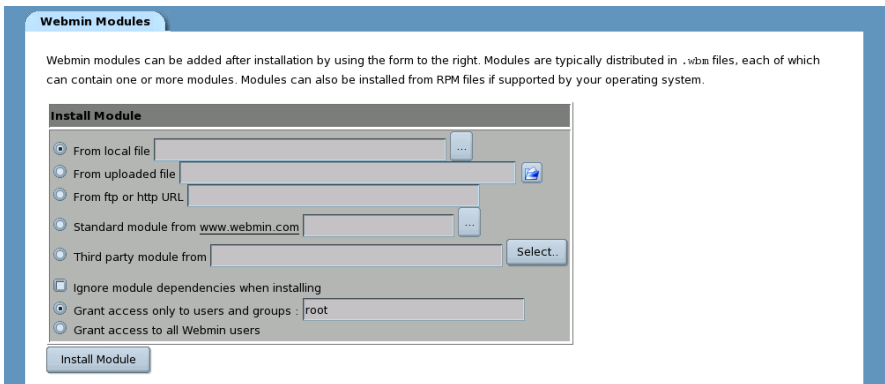


Рисунок 1. Раздел **Install Module**

3. Указать путь к webmin-модулю приложения и нажать на кнопку **OK**.

Примечание

Webmin-модуль представляет собой файл *mailgw.wbm* и устанавливается по умолчанию в каталог */opt/kaspersky/kav4lms/share/webmin/* (для дистрибутивов Linux) или */usr/local/share/kav4lms/webmin/* (для дистрибутивов FreeBSD).

В случае успешной установки webmin-модуля на экран будет выведено соответствующее сообщение.

Доступ к настройкам Антивируса Касперского можно получить, перейдя на закладку **Others** и затем щелкнув по значку Антивируса Касперского (см. рис. 2).

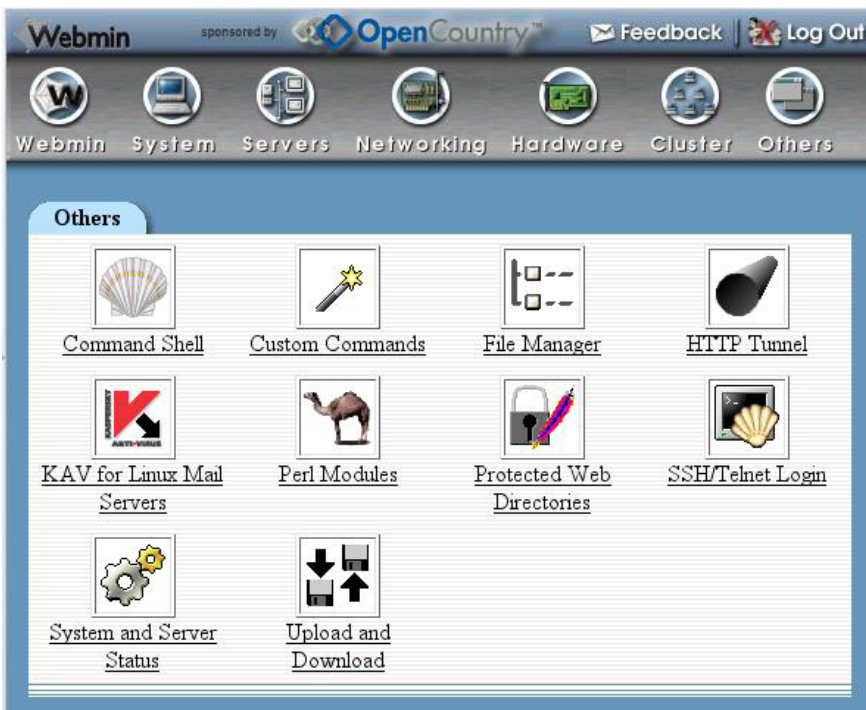


Рисунок 2. Значок Антивируса Касперского в закладке **Others**

3.7. Удаление приложения

Для удаления Антивируса Касперского с сервера требуется наличие прав привилегированного пользователя (**root**). Если на момент удаления вы не обладаете такими правами, то вам необходимо войти в систему под пользователем **root**.

Внимание!

Процесс удаления самостоятельно остановит работу приложения!

При удалении производится остановка приложения, удаление созданных при установке файлов и каталогов. Однако каталоги и файлы, созданные или измененные администратором (конфигурационный файл приложения,

конфигурационные файлы групп, файлы шаблонов уведомлений, каталоги карантинного хранения, файл ключа), сохраняются.

Запуск процедуры удаления приложения происходит различными способами в зависимости от используемого менеджера пакетов. Рассмотрим эти варианты подробнее.

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

```
# rpm -e <имя_пакета>
```

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

```
# dpkg -P <имя_пакета>
```

если вы хотите удалить приложение вместе с его конфигурационными файлами, или

```
# dpkg -r <имя_пакета>
```

если вы хотите удалить приложение, не удаляя при этом его конфигурационных файлов.

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

```
# pkg_delete <имя_пакета>
```

В случае успешного завершения процедуры удаления будет выведено соответствующее сообщение.

Если для управления Антивирусом Касперского был установлен модуль удаленного управления приложением (webmin-модуль), его удаление выполняется вручную, стандартными для программы Webmin средствами.

ГЛАВА 4. ИНТЕГРАЦИЯ С ПОЧТОВОЙ СИСТЕМОЙ

После установки Антивирус должен быть интегрирован с почтовой системой. Для этого следует изменить параметры конфигурационных файлов приложения и почтовой системы. Вы можете выполнить интеграцию с помощью скрипта настройки приложения, входящего в комплект поставки (см. п. 3.4 на стр. 21 и п. 10.2 на стр. 103), либо вручную настроить параметры конфигурационных файлов Антивируса Касперского и почтовой системы.

Для почтовых систем Exim и Postfix Антивирус поддерживает как pre-queue, так и post-queue интеграцию. При pre-queue интеграции сообщения передаются на проверку перед размещением в очереди почтовой системы, при post-queue интеграции – после размещения в очереди почтовой системы.

Примечание

При post-queue интеграции почтовая система не позволяет отклонять сообщения. Однако если в параметрах Антивируса Касперского в качестве действия над объектами будет выбрано **reject**, отправителю будет доставляться уведомление об отклонении сообщения. Текст уведомления задается параметром **RejectReply** в секции **[kav4lms: groups.<имя_группы>.settings]** конфигурационного файла группы.

Сокеты, используемые для обмена информацией между почтовой системой, фильтром и центральной службой Антивируса Касперского назначаются по следующим правилам:

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

Внимание!

При использовании сокета необходимо соблюдать 2 правила:

- при определении сетевого сокета номер порта должен быть больше 1024;
- при определении локального сокета фильтр и центральная служба приложения должны иметь права для доступа к указанному сокету.

4.1. Интеграция с почтовой системой Exim

Для интеграции с почтовой системой Exim в Антивирусе предусмотрено два метода:

- **post-queue интеграция методом изменения маршрутов:** весь почтовый трафик, проходящий через защищаемый сервер, передается на проверку после размещения в очереди почтовой системы (post-queue фильтрация);
- **pre-queue интеграция с использованием динамически подгружаемой библиотеки:** сообщения передаются на проверку до размещения в очереди почтовой системы (pre-queue фильтрация).

4.1.1. Post-queue интеграция методом изменения маршрутов

Интеграция методом изменения маршрутов подразумевает, что сообщения направляются на проверку от всех почтовых маршрутизаторов. Для этого для каждого маршрутизатора Exim в качестве значения параметра **pass_router** следует задать **kav4lms_filter**.

При post-queue интеграции для корректной передачи сообщений на проверку Антивирусу и возвращения их почтовой системе необходимо соблюдение следующих условий:

1. Фильтр должен быть настроен для перехвата сообщений от почтовой системы. Конечной точкой соединения «фильтр - почтовая система» является сокет, заданный параметром **FilterSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.
2. Фильтр должен передавать сообщения для проверки центральной службе приложения. Конечной точкой соединения «фильтр - центральная служба» является сокет, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла приложения.

Внимание!

При post-queue интеграции с Exim параметры **FilterSocket**, **ServiceSocket** и **ForwardSocket** должны указывать на сетевой сокет.

3. Фильтр должен возвращать сообщения почтовой системе. Конечной точкой соединения «приложение – почтовая система» является сокет, заданный параметром **ForwardSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.

Для интеграции Антивируса Касперского с Exim при помощи скрипта настройки приложения, запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh --install-filter=exim
```

Для интеграции приложения с Exim вручную:

1. Сделайте резервную копию конфигурационных файлов Exim.
2. Добавьте следующие строки в секцию **main configuration settings** конфигурационного файла Exim:

```
#kav4lms-filter-begin-1
local_interfaces=0.0.0.0.25:<forward_socket_ip>.\
<forward_socket_port_number>
#kav4lms-filter-end-1
```

где `<forward_socket_ip>.<forward_socket_port_number>` – IP-адрес и номер порта, на который почта направляется после проверки.

3. Добавьте следующие строки в секцию **routers** конфигурационного файла Exim:

```
#kav4lms-filter-begin-2
kav4lms_dnslookup:
    driver = dnslookup
    domains = ! +local_domains
    ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
    verify_only
    pass_router = kav4lms_filter
    no_more

kav4lms_system_aliases:
    driver = redirect
```

```
allow_fail
allow_defer
data = ${lookup{$local_part}lsearch{/etc/aliases}}
verify_only
pass_router = kav4lms_filter

kav4lms_localuser:
driver = accept
check_local_user
verify_only
pass_router = kav4lms_filter

failed_address_router:
driver = redirect
verify_only
condition = "{0}"
allow_fail
data = :fail: Failed to deliver to address
no_more

kav4lms_filter:
driver = manualroute
condition = "${if or {{eq {$interface_port}\
{<forward_socket_port_number>}} \
{eq {$received_protocol}{spam-scanned}} \
}{0}{1}}"
transport = kav4lms_filter
route_list = "* localhost byname"
self = send
#kav4lms-filter-end-2
```

где `<forward_socket_port_number>` – номер порта сокета, на который передается почта после проверки.

4. Добавьте следующие строки в секцию **transports** конфигурационного файла Exim:

```
#kav4lms-filter-begin-3
kav4lms_filter:
```

```

driver = smtp
port = <filter_socket_port_number>
delay_after_cutoff = false
allow_localhost
#kav4lms-filter-end-3

```

где <filter_socket_port_number> - номер порта для связи с фильтром Антивируса Касперского.

5. Присвойте параметру **ForwardSocket** из секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения значение <forward_socket_ip>.<forward_socket_port_number> из пункта 2.
6. Остановите службу *kav4lms-filter*.
7. Добавьте в секцию **[1043]** файла */var/opt/kaspersky/applications.setup* (для Linux) */var/db/kaspersky/applications.setup* (для FreeBSD) следующие строки:

```

FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter

```
8. Запустите службу *kav4lms-filter*.
9. Перезапустите почтовую систему.

4.1.2. Pre-queue интеграция с использованием динамически подгружаемой библиотеки

Фильтр должен передавать сообщения для проверки центральной службе приложения. Конечной точкой соединения «фильтр - центральная служба» является сокет, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла приложения.

Для интеграции Антивируса Касперского с Exim при помощи скрипта настройки приложения запустите команду:

для Linux:

```

# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim-dlfunc

```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \  
--install-filter=exim-dlfunc
```

Для интеграции Антивируса Касперского с Exim вручную:

1. Убедитесь, что почтовая система Exim поддерживает функцию контентной фильтрации `dlfunc`. Для этого запустите команду:

```
exim -bV
```

Положительным ответом будет результат:

```
Expand_dlfunc
```

2. Сделайте резервную копию конфигурационных файлов Exim.
3. Добавьте следующие строки в секцию **main configuration settings** конфигурационного файла Exim:

```
#kav4lms-filter-begin  
acl_smtp_data = acl_check_data  
#kav4lms-filter-end
```

4. Добавьте следующие строки в секцию **ACL** конфигурационного файла Exim:

```
acl_check_data:  
#kav4lms-dlfunc-begin  
warn set acl_m0 = \  
${dlfunc{<libkavexim.so>}{kav}{<socket>}\  
{/var/tmp//.kav4lms-exim}}  
accept condition = ${if match{$acl_m0}{\N^kav4lms:\  
continue\N}{yes}{no}}  
logwrite = kav4lms returned continue  
deny condition = ${if match{$acl_m0}{\N^kav4lms: \  
reject.*\N}{yes}{no}}  
logwrite = kav4lms returned reject  
message = Kaspersky Anti-Virus rejected the mail  
discard condition = ${if match{$acl_m0}\  
{\N^kav4lms: drop.*\N}{yes}{no}}  
logwrite = kav4lms returned drop  
message = Kaspersky Anti-Virus dropped the mail  
defer condition = ${if match{$acl_m0}\  
{\N^kav4lms: temporary failure.*\N}{yes}{no}}  
logwrite = kav4lms returned temporary failure
```

```
message = Kaspersky Anti-Virus returned \  
temporary failure  
accept  
#kav4lms-dlfunc-end
```

где `<socket>` - сокет связи фильтра и центральной службы Антивируса Касперского, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла Антивируса Касперского; `<libkavexim.so>` - путь к библиотеке *libkavexim.so*:

для 32-битных дистрибутивов Linux:

```
/opt/kaspersky/kav4lms/lib/libkavexim.so
```

для 64-битных дистрибутивов Linux:

```
/opt/kaspersky/kav4lms/lib64/libkavexim.so
```

для FreeBSD:

```
/usr/local/lib/kaspersky/kav4lms/libkavexim.so
```

5. Остановите службу *kav4lms-filter*.
6. Добавьте в секцию **[1043]** файла */var/opt/kaspersky/applications.setup* (для Linux) */var/db/kaspersky/applications.setup* (для FreeBSD) следующие строки:

для Linux:

```
FILTER_SERVICE=false  
FILTER_PROGRAM=/opt/kaspersky/kav4lms/lib/  
libkavexim.so
```

для FreeBSD:

```
FILTER_SERVICE=false  
FILTER_PROGRAM=/usr/local/lib/kaspersky/kav4lms/  
libkavexim.so
```

7. Перезапустите почтовую систему.

4.2. Интеграция с почтовой системой Postfix

Для интеграции с почтовой системой Postfix в Антивирусе предусмотрено три метода:

- **post-queue интеграция:** весь почтовый трафик, проходящий через защищаемый сервер, передается на проверку после размещения в очереди почтовой системы;
- **pre-queue интеграция:** сообщения передаются на проверку до размещения в очереди почтовой системы;
- **интеграция с использованием функций Milter:** сообщения передаются на проверку с помощью функций программного интерфейса Milter.

4.2.1. Post-queue интеграция

Для корректной передачи сообщений на проверку Антивирусу и возвращения их почтовой системе необходимо соблюдение следующих условий:

1. Фильтр должен быть настроен для перехвата сообщений от почтовой системы. Конечной точкой соединения «фильтр - почтовая система» является сокет, заданный параметром **FilterSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.
2. Фильтр должен передавать сообщения для проверки центральной службе приложения. Конечной точкой соединения «фильтр - центральная служба» является сокет, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла приложения.

Внимание!

При интеграции с Postfix параметры **FilterSocket**, **ServiceSocket** и **ForwardSocket** могут указывать как на сетевой, так и на локальный сокет.

3. Фильтр должен возвращать сообщения почтовой системе. Конечной точкой соединения «приложение – почтовая система» является параметром **ForwardSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.

Примечание

При переносе строк из руководства в конфигурационный файл Postfix удалите символы «\» и следующие за ними символы перевода строки.

Для интеграции Антивируса Касперского с Postfix: при помощи скрипта настройки приложения запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix
```

Для интеграции приложения с Postfix вручную:

1. Добавьте следующие строки в файл *master.cf*:

```
#kav4lms-filter-begin
kav4lms_filter      unix      -      -      n\
-      10      smtp
-o smtp_send_xforward_command=yes
<forward_socket_ip_address>:<forward_socket_port>\
inet      n      -      n      -      10\
smtpd
-o content_filter=
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

Примечание

Если для интеграции с Postfix 2.3 или выше используется локальный сокет, добавьте параметр «no_milters» в строку выше, то есть:

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters

-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=\
permit_mynetworks,reject
```

```
-o mynetworks=127.0.0.0/8,[::1]/128
-o smtpd_authorized_xforward_hosts=\
127.0.0.0/8,[::1]/128
#kav4lms-filter-end
```

где `<forward_socket_ip_address>`:`<forward_socket_port>`
– IP-адрес и номер порта сокета, на который передается почта после проверки.

2. Добавьте следующие строки в файл *main.cf*.

```
#kav4lms-filter-begin
content_filter = \
kav4lms_filter:<filter_socket_ip_address>:\
<filter_socket_port>
#kav4lms-filter-end
```

где `<filter_socket_ip_address>`:`<filter_socket_port>` – IP-адрес и номер порта сокета, который служит для связи фильтра с почтовой системой.

3. Остановите службу *kav4lms-filter*.
4. Добавьте в секцию **[1043]** файла */var/opt/kaspersky/applications.setup* (для Linux) */var/db/kaspersky/applications.setup* (для FreeBSD) следующие строки:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

5. Запустите службу *kav4lms-filter*.
6. Перезапустите почтовую систему.

4.2.2. Pre-queue интеграция

Для корректной передачи сообщений на проверку Антивирусу и возвращения их почтовой системе необходимо соблюдение следующих условий:

1. Фильтр должен быть настроен для перехвата сообщений от почтовой системы. Конечной точкой соединения «фильтр - почтовая система» является сокет, заданный параметром **FilterSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.
2. Фильтр должен передавать сообщения для проверки центральной службе приложения. Конечной точкой соединения «фильтр - цен-

тральная служба» является сокет, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла приложения.

Внимание!

При интеграции с Postfix параметры **FilterSocket**, **ServiceSocket** и **ForwardSocket** могут указывать как на сетевой, так и на локальный сокет.

3. Фильтр должен возвращать сообщения почтовой системе. Конечной точкой соединения «приложение – почтовая система» является сокет, заданный параметром **ForwardSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.

Примечание

При переносе строк из руководства в конфигурационный файл Postfix удалите символы «\» и следующие за ними символы перевода строки.

Для интеграции Антивируса Касперского с Postfix: при помощи скрипта настройки приложения запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix-prequeuee
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix-prequeuee
```

Для интеграции приложения с Postfix вручную:

1. Добавьте следующие строки в файл *master.cf*:

```
#kav4lms-prequeuee-begin
kav4lms_filter      unix      -      -      n\
-      10      smtp
-o smtp_send_xforward_command=yes
<forward_socket_ip_address>:<forward_socket_port>\
inet      n      -      n      -      10\
smtpd
-o content_filter=
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

Примечание

Если для интеграции с Postfix 2.3 или выше используется локальный сокет, добавьте параметр «no_milters» в строку выше, то есть:

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters
```

```
-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=\
permit_mynetworks,reject
-o mynetworks=127.0.0.0/8,[::1]/128
-o smtpd_authorized_xforward_hosts=\
127.0.0.0/8,[::1]/128
#kav4lms-prequeue-end
```

где <forward_socket_ip_address>:<forward_socket_port> – IP-адрес и номер порта сокета, на который передается почта после проверки.

2. Необходимо к существующему правилу в *master.cf* вида:

```
smtp inet n - n - 20 smtpd
```

добавить параметр

```
#kav4lms-prequeue-begin
-o smtpd_proxy_filter=:<filter_socket_port>
#kav4lms-prequeue-end
```

3. Остановите службу *kav4lms-filter*.

4. Добавьте в секцию **[1043]** файла */var/opt/kaspersky/applications.setup* (для Linux) */var/db/kaspersky/applications.setup* (для FreeBSD) следующие строки:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

5. Запустите службу *kav4lms-filter*.
6. Перезапустите почтовую систему.

4.2.3. Интеграция с помощью функций Milter

Для корректной передачи сообщений на проверку Антивирусу и возвращения их почтовой системе необходимо соблюдение следующих условий:

1. Фильтр должен быть настроен для перехвата сообщений от почтовой системы. Конечной точкой соединения «фильтр - почтовая система» является сокет, заданный параметром **FilterSocket** в секции **[kav4lms:filter.settings]** главного конфигурационного файла приложения.
2. Фильтр должен передавать сообщения для проверки центральной службе приложения. Конечной точкой соединения «фильтр - центральная служба» является сокет, заданный параметром **ServiceSocket** в секции **[kav4lms:server.settings]** главного конфигурационного файла приложения.

Внимание!

При интеграции с Postfix параметры **FilterSocket** и **ServiceSocket** могут указывать как на сетевой, так и на локальный сокет.

Примечание

При переносе строк из руководства в конфигурационный файл Postfix удалите символы «\» и следующие за ними символы перевода строки.

Для интеграции Антивируса Касперского с Postfix: при помощи скрипта настройки приложения запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-filter=postfix-milter
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \  
--install-filter=postfix-milter
```

Для интеграции приложения с Postfix вручную:

1. Добавьте следующие строки в файл *main.cf*.

```
smtpd_milters = inet:127.0.0.1:10025,  
#kav4lms-milter-begin  
milter_connect_macros = j _ {daemon_name} {if_name} \  
{if_addr}
```

```

milter_helo_macros = {tls_version} {cipher} \
{cipher_bits} {cert_subject} {cert_issuer}
milter_mail_macros = i {auth_type} {auth_authen} \
{auth_ssf} {auth_author} {mail_mailer} {mail_host} \
{mail_addr}
milter_rcpt_macros = {rcpt_mailer} {rcpt_host} \
{rcpt_addr}
milter_default_action = tempfail
milter_protocol = 3
milter_connect_timeout=180
milter_command_timeout=180
milter_content_timeout=600
#kav4lms-milter-end

```

2. Остановите службу *kav4lms-milter*.

3. Добавьте в секцию **[1043]** файла */var/opt/kaspersky/applications.setup* (для Linux) */var/db/kaspersky/applications.setup* (для FreeBSD) следующие строки:

```

FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-milter

```

4. Запустите службу *kav4lms-milter*.

5. Перезапустите почтовую систему.

4.3. Интеграция с почтовой системой qmail

Почтовая система на основе qmail не предоставляет средств для интеграции расширений. Процесс интеграции заключается в замене оригинального исполняемого файла *qmail-queue* файлом */opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail* (*/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail* для FreeBSD), входящим в поставку приложения. Данный файл обеспечивает фильтрацию сообщений и передает почтовый трафик оригинальному файлу *qmail-queue* для дальнейшей доставки. Сообщения передаются на проверку до размещения в очереди почтовой системы (pre-queuee фильтрация).

Внимание!

При интеграции с `qmail` параметр **ServiceSocket** может указывать как на сетевой, так и на локальный сокет.

Для интеграции Антивируса Касперского с `qmail` при помощи скрипта настройки приложения запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh --install-filter=qmail
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh --install-filter=qmail
```

Для интеграции приложения с `qmail` вручную:

1. Переименуйте файл `qmail-queue`, находящийся в директории `/var/qmail/bin`, в `qmail-queue-real`.
2. Скопируйте файл `/opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail` (`/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail` для FreeBSD) в директорию `/var/qmail/bin` и переименуйте его в `qmail-queue`.
3. Установите следующие права доступа для файлов `qmail-queue` и `qmail-queue-real`:

```
-rws--x--x 1 qmailq qmail
```

4. Остановите службу `kav4lms-filter`.
5. Измените владельца и группу на `qmailq:qmail` с помощью следующих команд:

- для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--switch-credentials=qmailq,qmail
```

- для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \
--switch-credentials=qmailq,qmail
```

6. Добавьте в секцию **[1043]** файла `/var/opt/kaspersky/applications.setup` (для Linux) `/var/db/kaspersky/applications.setup` (для FreeBSD) следующие строки:

для Linux:

```
FILTER_SERVICE=false
```

```
FILTER_PROGRAM=/opt/kaspersky/kav4lms/lib/bin\  
/kav4lms-qmail
```

для FreeBSD:

```
FILTER_SERVICE=false
```

```
FILTER_PROGRAM=/usr/local/libexec/kaspersky/kav4lms\  
/kav4lms-qmail
```

7. Перезапустите почтовую систему.

4.4. Интеграция с почтовой системой Sendmail

Sendmail предоставляет программный интерфейс Milter для интеграции с фильтрами сторонних производителей. Почтовый трафик передается от Sendmail Антивирусу и обратно с помощью вызовов функций Milter. Сообщения передаются на проверку до размещения в очереди почтовой системы (pre-queue интеграция).

Как правило, при интеграции с Sendmail изменения вносятся в конфигурационный файл почтовой системы формата *mc*, файл *cf* изменяется автоматически. Если такая возможность не поддерживается, после изменения *mc*-файла следует внести изменения в *cf*-файл.

Примечание

Если вы внесете изменения только в *cf*-файл, при следующем запуске генерации *cf*-файла из *mc* все изменения будут утеряны.

Внимание!

При интеграции с Sendmail параметры **FilterSocket** и **ServiceSocket** могут указывать как на сетевой, так и на локальный сокет.

4.4.1. Интеграция с помощью файла *.cf*

Для интеграции Антивируса Касперского с Sendmail при помощи скрипта настройки приложения запустите команду:

для Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-filter=sendmail-milter
```

для FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=sendmail-milter
```

Для интеграции приложения с *Sendmail* вручную:

1. Создайте резервную копию файла *sendmail.cf*.
2. Добавьте следующие строки в файл *sendmail.cf*:

```
#kav4lms-milter-begin-filter
O InputMailFilters=kav4lms_filter
O Milter.macros.connect=j, _, {daemon_name}, \
{if_name}, {if_addr}
O Milter.macros.helo={tls_version}, {cipher}, \
{cipher_bits}, {cert_subject}, {cert_issuer}
O Milter.macros.envfrom=i, {auth_type}, \
{auth_authen}, {auth_ssf}, {auth_author}, \
{mail_mailer}, {mail_host}, {mail_addr}
O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, \
{rcpt_addr}
#kav4lms-milter-end-filter
```

3. Добавьте в файл *sendmail.cf* следующие строки:

- a) при использовании сетевого сокета:

```
#kav4lms-milter-begin-socket
Xkav4lms_filter,
S=inet:<filter_port>@<filter_address>,F=T,\
T=S:3m;R:5m;E:10m
#kav4lms-milter-end-socket
```

где *<filter_port>* – номер порта сетевого сокета, соединяющего почтовую систему с фильтром, *<filter_address>* – IP-адрес компьютера, на котором запущен фильтр.

- b) при использовании локального сокета:

```
#kav4lms-milter-begin-socket
Xkav4lms_filter,
S=unix:<filter_socket_file_path>,F=T,T=S:3m;\
R:5m;E:10m
#kav4lms-milter-end-socket
```

где *<socket_file_path>* – путь к локальному сокету.

4. Остановите службу *kav4lms-milter*.

5. Добавьте в секцию **[1043]** файла `/var/opt/kaspersky/applications.setup` (для Linux) `/var/db/kaspersky/applications.setup` (для FreeBSD) следующие строки:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-milter
```

6. Запустите службу `kav4lms-milter`.
7. Перезапустите почтовую систему.

4.4.2. Интеграция с помощью файла `.mc`

Для интеграции приложения с Sendmail с помощью файла `.mc`:

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

```
dnl kav4lms-milter-begin dnl
define(`_FFR_MILTER', `true')dnl
INPUT_MAIL_FILTER(`kav4lms_filter',\
`S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
dnl kav4lms-milter-end dnl
```
3. Скомпилируйте конфигурационный файл `.cf` согласно настройкам вашей операционной системы.
4. Остановите службу `kav4lms-filter`.
5. Добавьте в секцию **[1043]** файла `/var/opt/kaspersky/applications.setup` (для Linux) `/var/db/kaspersky/applications.setup` (для FreeBSD) следующие строки:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-milter
```

6. Запустите службу `kav4lms-filter`.
7. Перезапустите почтовую систему.

ГЛАВА 5. АНТИВИРУСНАЯ ЗАЩИТА ПОЧТЫ

5.1. Формирование групп

Группа – заданные множества адресов отправителей и получателей, почтовые сообщения которых обрабатываются с одинаковыми значениями параметров Антивируса Касперского.

Для каждой группы могут быть установлены собственные параметры проверки сообщений, определяющие, например:

- способ проверки сообщений (см. п. 5.2 на стр. 50);
- режим проверки сообщений (см. п. 5.3 на стр. 51);
- действия над сообщениями и объектами сообщений (см. п. 5.4 на стр. 54);
- резервное копирование сообщений перед обработкой (см. п. 5.6 на стр. 59);
- уведомления об обнаруженных объектах (см. п. 5.7 на стр. 60).

Параметры каждой группы хранятся в отдельном конфигурационном файле (см. п. А.2 на стр. 138). Все конфигурационные файлы групп должны быть прописаны в секции **[kav4lms:groups]** главного конфигурационного файла приложения *kav4lms.conf* с помощью директивы `_include`. Данная директива поддерживает подключение с помощью указания имени конфигурационного файла или имени директории, хранящей конфигурационные файлы групп.

По умолчанию конфигурационные файлы групп должны размещаться в директории */etc/opt/kaspersky/kav4lms/groups.d/*.

В состав дистрибутива приложения включен конфигурационный файл группы **Default** – *default.conf*. После установки приложения он размещается в директории */etc/opt/kaspersky/kav4lms/groups.d/*. Значения, заданные в этом файле, используются в качестве значений параметров по умолчанию, если они не определены в конфигурационном файле группы. С параметрами конфигурационного файла группы **Default** обрабатываются сообщения, если ни одной группы не сформировано.

Антивирус проверяет сообщение согласно параметрам той группы, в которой обнаружены его отправитель или получатель (из команд MAIL FROM и RCPT TO). Если отправитель и все получатели принадлежат к разным группам, то выбирается группа с наибольшим *приоритетом*. Если группы не обнаружено, сообщение обрабатывается в соответствии с параметрами, заданными в конфигурационном файле группы **Default**, она имеет наименьший приоритет равный **0**. В связи с этим, рекомендуется для групп с более высоким приоритетом задавать более высокий уровень защиты.

Приоритет является уникальным идентификатором группы. Он задается параметром **Priority** в секции **[kav4lms:groups.<имя_группы>.definition]** конфигурационного файла группы.

Отправители и получатели задаются параметрами **Senders** и **Recipients** в секции **[kav4lms:groups.<имя_группы>.definition]** конфигурационного файла группы.

Чтобы создать новую группу,

1. Создайте конфигурационный файл группы в директории, заданной в секции **[kav4lms:groups]** главного конфигурационного файла приложения. По умолчанию, это директория **/etc/opt/kaspersky/kav4lms/groups.d/**

Примечание

При создании конфигурационного файла группы рекомендуется использовать файл *default.conf*. Для быстрой замены имени группы выполните следующие команды:

```
# cd /etc/opt/kaspersky/kav4lms/groups.d
# sed 's|groups.default|groups.<имя_группы>|'
default.conf > <имя_группы>.conf
```

2. Задайте приоритет группы в конфигурационном файле группы: параметр **Priority** в секции **[kav4lms:groups.<имя_группы>.definition]**. В качестве значения параметра может быть указано любое натуральное число. Не допускается создание групп с одинаковым приоритетом и приоритетом **0**.
3. Определите адреса отправителей и получателей в конфигурационном файле группы: параметры **Senders** и **Recipients** в секции **[kav4lms:groups.<имя_группы>.definition]**.

Вы можете использовать символы «*» и «?» для создания масок и регулярные выражения, начинающиеся с префикса «г:». Чтобы задать несколько адресов (масок адресов), необходимо каждую новую запись начинать с новой строки:

```
Senders=reporter@*.mydomain.com  
Recipients=re:office\d+@central\mydomain.com
```

Если в описании группы отсутствует параметр **Recipients** или **Senders**, то приложение будет использовать для данного параметра значение, заданное в конфигурационном файле *default.conf*. Если значения параметров **Senders** и **Receivers** не заданы в описании группы, то групповые правила не применяются ни к одному сообщению.

Внимание!

Регулярные выражения нечувствительны к регистру.

4. Если это требуется, укажите значения параметров проверки сообщений в секциях конфигурационного файла группы (подробнее см. п. А.2 на стр. 138). Если значение параметра в конфигурационном файле группы не определено, используется значение этого параметра, заданное в конфигурационном файле группы **Default** – *default.conf*.

5.2. Определение политики проверки почтовых сообщений

Антивирус предоставляет возможность проверять сообщения одним из следующих способов:

- как единый объект – заголовок и тело сообщения проверяются целиком;
- комбинированно – сообщение сначала проверяется как единый объект, затем производится разбор сообщения на объекты: тело сообщения, вложения и прочее, каждый из них проверяется отдельно. Этот способ обеспечивает более высокое качество проверки и уровень защиты.

Примечание

Если в качестве действия над сообщением выбрано действие, применимое к части сообщения (см. п. 5.4 на стр. 54), то сообщение проверяется по частям независимо от выбранного способа проверки.

Способ проверки сообщений определяется политикой и задается в конфигурационном файле группы параметром **ScanPolicy** в секции **[kav4lms:groups.<имя_группы>.settings]**.

Чтобы сообщения проверялись как единый объект,

присвойте параметру **ScanPolicy** значение **message**.

Чтобы сообщения проверялись комбинированно,

присвойте параметру **ScanPolicy** значение **combined**.

5.3. Режим проверки сообщений

Следующий шаг настройки группы – выбор режима проверки сообщений. Антивирус осуществляет проверку почтовых сообщений в следующих режимах:

- проверка на наличие угроз;
- фильтрация вложений.

Режим проверки сообщений для группы задается параметром **Check** в секции **[kav4lms:groups.<имя_группы>.settings]** конфигурационного файла группы и может принимать следующие значения:

- **anti-virus** – выполнять антивирусную проверку сообщений;
- **content-filter** – выполнять фильтрацию по имени, типу и размеру вложений;
- **all** – выполнять и антивирусную проверку, и фильтрацию вложений;
- **none** – отключить проверку сообщений.

Если включена и проверка сообщений на наличие угроз, и фильтрация, то проверка выполняется в следующей последовательности:

1. антивирусная проверка сообщения как единого объекта;
2. фильтрация вложений;
3. проверка сообщения «по частям» (если выбран комбинированный способ проверки сообщений **ScanPolicy=combined**).

5.3.1. Антивирусная проверка

Антивирусная проверка сообщений выполняется, если для параметра **Check** задано значение **anti-virus** или **all** (конфигурационный файл группы, секция **[kav4lms:groups.<имя_группы>.settings]**).

По результатам антивирусной проверки приложение присваивает сообщению или входящему в его состав объекту статус:

- **clean** – сообщение не содержит угроз;
- **infected** – сообщение (или его часть) содержит вредоносные объекты;
- **suspicious** – сообщение (или его часть) содержит подозрительный объект (такой статус присваивается только если включен эвристический анализатор);
- **protected** – сообщение (или его часть) защищено паролем или зашифровано;
- **error** – сообщение (или его часть) повреждено или процесс проверки завершился с ошибкой.

На основании присвоенного при проверке статуса выполняется дальнейшая обработка сообщений и их объектов (см. п. 5.4 на стр. 54).

Для зараженных сообщений (**infected**), в случае обнаружения угрозы из заданного набора, может быть настроен отдельный порядок обработки (параметр **VirusNameAction**, конфигурационный файл группы, секция **[kav4lms:groups.<имя_группы>.actions]**). Имя обнаруженной угрозы возвращается Антивирусом в формате, принятом «Лабораторией Касперского». Данный формат представлен на сайте www.viruslist.com. Список угроз, подлежащих особой обработке, задается параметром **VirusNameList** в секции **[kav4lms:groups.<имя_группы>.contentfiltering]**. Данный параметр позволяет задавать имена угроз в строковом формате или в формате регулярных выражений (стандарта POSIX).

Параметры антивирусной проверки могут быть изменены с целью повышения качества или скорости проверки. Параметры антивирусной проверки находятся в секции **[kav4lms:group.<имя_группы>.settings]** конфигурационного файла группы. Эти параметры задают:

- необходимость проверки архивов (параметр **ScanArchives**);
- необходимость проверки упакованных файлов (параметр **ScanPacked**);
- необходимость применения эвристического анализатора (параметр **UseCodeAnalyzer**);

Примечание

Установка данного параметра в значение **yes** включает возможность присвоения сообщению статуса **suspicious**. В противном случае данный статус не присваивается.

- максимальное время проверки сообщения или части сообщения (параметр **MaxScanTime**). В случае превышения данного ограничения проверка завершается с присвоением сообщению статуса **error**;
- режим перекодирования MIME-объектов, не соответствующих RFC-стандартам, с использованием эвристических алгоритмов (параметр **MIMEEncodingHeuristics**);
- тип используемых приложением баз антивируса (параметр **UseAVBasesSet**).

5.3.2. Фильтрация почты

Фильтрация сообщений выполняется, если для параметра **Check** задано значение **content-filter** или **all** (конфигурационный файл группы, секция **[kav4lms:groups.<имя_группы>.settings]**).

В качестве критериев фильтрации в Антивирусе могут быть использованы:

- MIME-тип вложений (применяется к заголовкам “Content-Type”);

Внимание!

Существуют случаи, когда тип содержимого вложения отличается от указанного в заголовке сообщения. Антивирус Касперского не проверяет соответствие заголовка сообщения содержимому вложения.

- имя вложения (применяется к именам и расширениям вложений);
- размер вложения (применяется к размерам частей сообщения, размер учитывается после распаковки вложения).

Примечание

Если одновременно выбраны антивирусная проверка и фильтрация сообщений, то фильтрация выполняется до антивирусной проверки.

Критерии фильтрации задаются в конфигурационном файле группы в секции **[kav4lms:groups.<имя_группы>.contentfiltering]**.

Для каждого критерия фильтрации можно задать два правила:

- правило включения – указывает объекты, которые подлежат фильтрации, и задаются следующими параметрами:
 - **IncludeMime** – список MIME-типов;
 - **IncludeName** – список имен или расширений вложений;

- **IncludeSize** – список размеров объектов.
- правило исключения – указывает объекты, которые не подлежат фильтрации, и задаются следующими параметрами:
 - **ExcludeMime** – список MIME-типов;
 - **ExcludeName** – список имен или расширений вложений;
 - **ExcludeSize** – список размеров объектов.

Внимание!

Если задано правило исключения, а правило включения не задано, то все объекты, не попадающие под действие правила исключения, подлежат фильтрации.

Если оба правила не заданы, то фильтрация не производится, даже если параметру **Check** присвоено значение **content-filter** или **all**.

Правила для MIME-типов и имен вложений могут содержать:

- строки;
- выражения, содержащие символы обобщения (синтаксис UNIX);
- регулярные выражения (синтаксис POSIX).

Внимание!

Регулярные выражения нечувствительны к регистру и должны начинаться с префикса «ге:».

Правила для размера объектов могут задаваться в виде:

- количества байт;
- числа с указателем единиц измерения («KB» или «MB»);
- указанных выше типов со знаками сравнения.

5.4. Действия над объектами

По результатам антивирусной проверки и фильтрации Антивирус выполняет действия над сообщениями и входящими в их состав объектами. Часть действий может быть применена только ко всему сообщению как к единому объекту, а часть действий только к составным частям сообщения. Для параметров, определяющих действия Антивируса Касперского, могут быть установлены следующие значения:

- **warn**: сообщение полностью заменяется текстом, предупреждающим о наличии вредоносного объекта;
- **drop**: сообщение удаляется без передачи адресату;
- **reject**: сообщение не доставляется (если приложение интегрируется с Postfix (интеграция после передачи в очередь) или Exim, то вместо данного действия выполняется bounce). В результате применения данного действия отправитель получает сообщение, заданное параметром **RejectReply**.
- **skip**: сообщение или объект сообщения пропускается без изменений, результат проверки записывается в журнал приложения;
- **cure** (применяется только по результатам антивирусной проверки к объектам сообщения): приложение пытается вылечить зараженный объект. Если лечение невозможно, к объекту применяется действие **delete**.
- **rename** (применяется только по результатам фильтрации к объектам сообщения): к имени вложения добавляется значение параметра **RenameTo**. Если этот параметр задает расширение (например, `.vir`), то значение параметра добавляется к имени вложения. В противном случае значение параметра заменяет имя вложения.
- **delete**: объект сообщения удаляется и, если значение параметра **UsePlaceholderNotice** – **yes**, заменяется уведомлением. Текст уведомления берется из файла шаблона с именем `part_<action>`.

Внимание!

Вследствие того, что фильтрация происходит до антивирусной проверки, проверка сообщения по частям может не показать наличия угрозы, в то время как проверка сообщения как единого объекта завершается с присвоением статуса **infected**. Такой случай возможен, если к части сообщения было применено действие **delete** после фильтрации.

Действия, применяемые в результате антивирусной проверки, задаются параметрами **InfectedAction**, **SuspiciousAction**, **ProtectedAction**, **ErrorAction** и **VirusNameAction**. Действия, применяемые в результате фильтрации, задаются параметрами **FilteredMimeAction**, **FilteredNameAction** и **FilteredSizeAction**.

Данные параметры находятся в секции `[kav4lms:groups.<имя_группы>.actions]` конфигурационного файла группы.

5.5. Предустановленные профили защиты

В поставку Антивируса Касперского входят предустановленные конфигурационные профили, обеспечивающие различные уровни защиты почты:

- **рекомендуемый:** хранится в директории *default_recommended* (см. п. 5.5.1 на стр. 56);
- **максимальная защита:** хранится в директории *high_overall_security* (см. п. 5.5.2 на стр. 57);
- **максимальная скорость:** хранится в директории *high_scan_speed* (см. п. 5.5.3 на стр. 58).

Каждый профиль состоит из двух конфигурационных файлов: *kav4lms.conf* и *default.conf* (находящийся в поддиректории *groups.d*). Профили хранятся в поддиректориях, соответствующих названию профилей, директории */etc/opt/kaspersky/kav4lms/profiles*.

Вы можете выбрать один из предустановленных профилей либо выполнить настройку параметров защиты почты вручную, через конфигурационные файлы приложения.

Для использования предустановленного профиля:

1. Создайте резервную копию конфигурационных файлов приложения (*kav4lms.conf* и *groups.d/default.conf*).
2. Скопируйте содержимое нужной директории в директорию */etc/opt/kaspersky/kav4lms*.
3. Перезагрузите приложение с новыми параметрами работы с помощью следующей команды:

```
/etc/init.d/kav4lms reload
```

5.5.1. Рекомендуемый профиль защиты

Данный профиль содержит параметры, представляющие компромисс между уровнем антивирусной защиты и скоростью обработки почты. Характеристика профиля:

- К почтовым сообщениям применяется политика проверки **message**: каждое сообщение обрабатывается как единый объект.
- При проверке используется расширенный набор баз антивируса.

- Максимально допустимый уровень вложенности MIME-объектов равен 10.
- Для каждого сообщения, подвергающегося антивирусной проверке, создается резервная копия и информационный файл.
- Проводится лечение зараженных объектов.
- Включен режим фильтрации вложений по MIME-типам. Приложение удаляет из сообщений ссылки на внешние объекты (*message/external-body* type) и вложения с расширениями *.pif*, *.com*, *.bat* и *.exe*.
- Сообщения, которым были присвоены статусы *suspicious*, *protected*, *error*, а также отфильтрованные по имени и MIME-типу вложения, заменяются уведомлениями. В случае обнаружения угрозы из заданного набора, сообщения удаляются.
- В заголовок и тело почтового сообщения добавляется информация о результатах его обработки.
- Получателям доставляются уведомления о проверке сообщений. Уведомление отправителя и администратора не производится.
- В отчет о работе приложения записываются все сообщения, кроме отладочной информации.
- Статистика собирается по всем аспектам активности приложения.

5.5.2. Профиль максимальной защиты

Данный профиль содержит параметры, обеспечивающие максимальную защиту почтового трафика. Характеристика профиля:

- Приложение осуществляет антивирусную проверку в соответствии с политикой типа **combined**: каждое сообщение сначала проверяется как единый объект, а затем – по частям, не смотря на статус первоначальной проверки.
- Сообщения, не соответствующие RFC-стандартам разбираются с использованием эвристических алгоритмов, и в случае успешной перекодировки передаются на проверку.
- При проверке используется расширенный набор баз антивируса.
- Включен режим фильтрации вложений по MIME-типам. Приложение удаляет из сообщений ссылки на внешние объекты (*message/external-body* type) и вложения с расширениями *.pif*, *.com*, *.bat* и *.exe*.

- Максимально допустимый уровень вложенности сообщения неограничен.
- Для каждого сообщения, подвергающегося антивирусной проверке или фильтрации, создается информационный файл.
- Проводится лечение зараженных объектов.
- Сообщения, которым были присвоены статусы `suspicious`, `protected`, а также отфильтрованные по имени и MIME-типу вложения, удаляются. В случае обнаружения угрозы, из заданного списка, сообщения удаляются без доставки адресатам.
- Если при проверке сообщения возникает ошибка, то содержимое сообщения заменяется уведомлением.
- Получателям доставляются уведомления о проверке сообщений. Уведомление отправителя и администратора не производится.
- В отчет о работе приложения записываются все сообщения, кроме отладочной информации.
- Статистика не сохраняется.

5.5.3. Профиль максимальной скорости

Данный профиль обеспечивает максимальную скорость антивирусной проверки. Характеристика профиля:

- К почтовым сообщениям применяется политика проверки **message**: каждое сообщение обрабатывается как единый объект.
- Фильтрация сообщений отключена.
- При проверке используется расширенный набор баз антивируса.
- Резервная копия создается при совершении действий: `drop` и `warn`. Информационный файл не создается.
- Сообщения, которым были присвоены статусы `infected`, `suspicious`, `protected`, `error`, заменяются уведомлениями. В случае обнаружения угрозы из заданного списка, сообщения удаляются.
- В заголовок почтового сообщения добавляется информация о результатах его обработки.
- Получателям доставляются уведомления о проверке сообщений. Уведомление отправителя и администратора не производится.

- В отчет о работе приложения записывается информация обо всех аспектах функциональности приложения; уровень детализации: критические и прочие ошибки, а также важные сообщения информационного характера.
- Проводится сбор статистики об обнаруженных угрозах.
- Максимальное число запросов к центральной службе приложения удвоено по сравнению с рекомендуемым профилем и профилем максимальной защиты. Максимальное число одновременных запросов для проверки неограниченно.

5.6. Резервное копирование сообщений

Приложение позволяет сохранять резервную копию сообщения перед его обработкой. Параметры резервного копирования находятся в секции **[kav4!ms:groups.<имя_группы>.backup]** конфигурационного файла группы.

Режим резервного копирования задается параметром **Policy**, который может принимать следующие значения:

- **message** – создается только копия сообщения;
- **info** – вместе с копией сообщения создается информационный файл. Этот файл содержит следующую информацию:
 - IP-адрес или имя клиента почтовой системы;
 - IP-адрес или имя сервера почтовой системы;
 - отправитель сообщения;
 - адрес сервера, обработавшего сообщение;
 - название группы, правила которой применены для обработки сообщения;
 - список получателей сообщения;
 - причина создания резервной копии (лечение, удаление, отклонение, фильтрация сообщения);
 - путь к файлу резервной копии сообщения;
 - информация о приложении (идентификаторы процесса и потока).
- **none** – резервная копия не создается.

Параметр **Options** позволяет указать причину создания резервной копии:

- **cured** – в случае лечения части исходного сообщения;
- **deleted** – в случае удаления части сообщения;
- **rejected** – в случае отказа в доставке сообщения;
- **dropped** – в случае удаления сообщения без передачи адресату;
- **warning** – в случае замены сообщения уведомлением;
- **renamed** – в случае переименования хотя бы одного вложения;
- **all** – во всех вышеперечисленных случаях.

В качестве значения параметра **Options** может быть указано как одно значение, так и список значений, разделенных запятой.

Резервные копии сообщений и информационные файлы хранятся в директории, заданной параметром **Destination**.

5.7. Уведомления

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

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

Предусмотрена 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.

5.7.1. Настройка уведомлений

Параметры уведомлений находятся:

- в секции **[kav4lms:server.notifications]** конфигурационного файла приложения *kav4lms.conf*;
- в секции **[kav4lms:group.<имя_группы>.notifications]** конфигурационного файла группы.

Настройка уведомлений выполняется в два этапа.

Шаг 1. Выбор адресата уведомления

Уведомления могут быть отправлены:

- отправителю сообщения (задается параметром **NotifySender** конфигурационного файла группы);
- получателям сообщения (задается параметром **NotifyRecipients** конфигурационного файла группы);
- администраторам информационной безопасности (задается параметром **NotifyAdmin** в параметрах группы). Список почтовых адресов администраторов информационной безопасности задается параметром **AdminAddresses** в параметрах группы;
- администраторам Антивируса Касперского (задается параметром **ProductNotify** в файле *kav4lms.conf*). Список почтовых адресов администраторов приложения задается параметром **ProductAdmins** в файле *kav4lms.conf*.

Уведомления доставляются указанным категориям пользователей при установке перечисленных параметров в любое значение, кроме **none**.

Шаг 2. Выбор темы уведомления

Отправителей, получателей сообщений и администраторов информационной безопасности можно уведомлять:

- о выполнении над сообщением действия (см. п. 5.4 на стр. 54), заданного параметрами **InfectedAction**, **ProtectedAction**, **ErrorAction**. Отправка уведомления такого типа включается установкой параметра, определяющего адресата уведомления (см. шаг 1), в значения **infected**, **protected**, **error**;
- о выполнении правила фильтрации (см. п. 5.4 на стр. 54). Отправка уведомления такого типа включается установкой параметра, определяющего адресата уведомления (см. шаг 1), в значение **filtered**;
- обо всех вышеперечисленных событиях. Отправка уведомления такого типа включается установкой параметра, определяющего адресата уведомления (см. шаг 1), в значение **all**.

Администраторов приложения можно уведомлять:

- о получении обновления баз антивируса. Отправка уведомления такого типа включается установкой параметра **ProductNotify** в значение **update**;

- о критической ошибке в работе приложения. Отправка уведомления такого типа включается установкой параметра **ProductNotify** в значение **fault**;
- о событиях, связанных с ключом и лицензионным ограничением. Отправка уведомления такого типа включается установкой параметра **ProductNotify** в значение **license**;

Уведомления о лицензии бывают двух типов:

- истечение срока действия ключа. Первый раз отправляются за 14 дней до истечения срока действия ключа, затем ежедневно до истечения указанного периода. На следующий день после истечения срока действия ключа отправляется соответствующее уведомление;
- превышение лицензионного ограничения. Отправляются при превышении числа пользователей или объема трафика, указанных в условиях приобретения приложения.

Внимание!

Уведомления о превышении лицензионных ограничений - исключительно важный тип уведомлений. Если отправка уведомлений отключена, то такие уведомления будут записаны в журнал приложения.

- обо всех вышеперечисленных событиях. Отправка уведомления такого типа включается установкой параметра **ProductNotify** в значение **all**.

5.7.2. Шаблоны уведомлений

В процессе формирования уведомлений используются следующие шаблоны (хранятся в директории, определенном параметром **Templates** конфигурационного файла 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* – текст, заменяющий в исходном почтовом сообщении объект, который был удален в результате неудавшейся попытки его лечения;

- *part_filtered* – текст, заменяющий в исходном почтовом сообщении MIME-объект, удаленный в результате фильтрации объектов MIME-типа;
- *part_suspicious* – текст, заменяющий в исходном почтовом сообщении объект, который был опознан приложением как подозрительный и удален;
- *part_filtered* – текст, заменяющий в исходном почтовом сообщении объект, который был переименован в результате фильтрации;
- *part_protected* – текст, заменяющий в исходном почтовом сообщении защищенный объект, который не удалось проверить на вирусы, и, как следствие, он был удален;
- *part_error* – 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 фильтр или средства SMTP. Текст шаблона может содержать макросы, детализирующие действия, которые были выполнены над исходным почтовым сообщением. Предусмотрены следующие шаблоны:
 - *notify_common* – текст, используемый по умолчанию для уведомлений получателя, отправителя и администраторов о выполненных над почтовым сообщением действиях;
 - *notify_infected* – текст, заменяющий зараженное почтовое сообщение;
 - *notify_suspicious* – текст, заменяющий почтовое сообщение, содержащее подозрительные объекты;
 - *notify_filtered* – текст, заменяющий почтовое сообщение, подвергнутое фильтрации;
 - *notify_error* – текст, заменяющий письмо, в результате проверки которого произошла ошибка;
 - *notify_protected* – текст, заменяющий письмо, защищенное от проверки;
 - *disclaimer* – текст, добавляемый в любое проверяемое или создаваемое в процессе антивирусной обработки письмо. По умолчанию шаблон содержит уведомление о том, что письмо было проверено Антивирусом Касперского.
- **Шаблон расширенного уведомления** – текст, используемый для уведомления конкретного лица, заинтересованного в получении

информации об антивирусной обработке исходного почтового сообщения. Разработаны отдельные шаблоны для уведомления отправителя, получателя и администратора. Для использования таких шаблонов необходимо задать для параметра **UseCustomTemplates** значение **yes**. Предусмотрены следующие шаблоны:

- уведомления отправителя:
 - *notify_sender_common* – текст уведомления отправителя почтового сообщения о выполненных над исходным письмом действиях;
 - *notify_sender_infected* – текст, заменяющий зараженное почтовое сообщение;
 - *notify_sender_suspicious* – текст, заменяющий почтовое сообщение, содержащее подозрительные объекты;
 - *notify_sender_filtered* – текст, заменяющий почтовое сообщение, подвергнутое фильтрации;
 - *notify_sender_error* – текст, заменяющий письмо, в результате проверки которого произошла ошибка;
 - *notify_sender_protected* – текст, заменяющий письмо, защищенное от проверки.
- уведомления получателей:
 - *notify_recipients_common* – текст уведомления получателя почтового сообщения о выполненных над исходным письмом действиях;
 - *notify_recipients_infected* – текст, заменяющий зараженное почтовое сообщение;
 - *notify_recipients_suspicious* – текст, заменяющий почтовое сообщение, содержащее подозрительные объекты;
 - *notify_recipients_filtered* – текст, заменяющий почтовое сообщение, подвергнутое фильтрации;
 - *notify_recipients_error* – текст, заменяющий письмо, в результате проверки которого произошла ошибка;
 - *notify_recipient_protected* – текст, заменяющий письмо, защищенное от проверки.
- уведомления администратора:
 - *notify_admin_common* – текст уведомления администратора почтового сообщения о выполненных над исходным письмом действиях;

- *notify_admin_infected* – текст, заменяющий зараженное почтовое сообщение;
 - *notify_admin_suspicious* – текст, заменяющий почтовое сообщение, содержащее подозрительные объекты;
 - *notify_admin_filtered* – текст, заменяющий почтовое сообщение, подвергнутое фильтрации;
 - *notify_admin_error* – текст, заменяющий письмо, в результате проверки которого произошла ошибка;
 - *notify_admin_protected* – текст, заменяющий письмо, защищенное от проверки.
- **Шаблон специального уведомления администратора** – текст, используемый для формирования специальных уведомлений об исключительных событиях, требующих отдельного внимания администратора. Предусмотрены следующие шаблоны:
 - *product_update* – текст, используемый для уведомления администратора о получении обновлений баз антивируса приложения;
 - *product_fault* – текст, используемый для уведомления администратора о том, что во время работы Антивируса Касперского возникла критическая ошибка;
 - *product_license* – текст, используемый для уведомления администратора об истечении срока действия ключа или о нарушении лицензионного соглашения.

Внимание!

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

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

5.7.3. 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.

Внимание!

Первая строка шаблона не должна содержать символа «:», так как в таком случае она будет интерпретироваться как заголовок. Для избежания таких ситуаций следует начинать шаблон переводом строки (нажатием клавиши **Enter**).

5.7.3.1. 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 экранирован (подробнее см. п. 5.7.3.5 на стр. 70).

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*.

5.7.3.2. 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 экранирован (подробнее см. п. 5.7.3.5 на стр. 70).

`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 экранирующий (escape) символ (подробнее см. п. 5.7.3.5 на стр. 70). Например:

```
<FOR _macro_name_parent_ == "\" value 1\"">
```

> – конец определения итерационной конструкции, начало определения тела итератора. Символ >, не являющийся концом определения конструкции, должен быть экранирован (подробнее см. п. 5.7.3.5 на стр. 70).

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

</FOR> – конец определения тела итератора. Символ <, не являющийся концом определения тела итератора, должен быть экранирован (подробнее см. п. 5.7.3.5 на стр. 70).

... – 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,
```

5.7.3.3. 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:

```
<FOR _macro_name_parent_ ==  
" value 1">%_macro_name_child_</FOR>
```

При этом область действия макроса `%_macro_name_parent_` распространяется на все вложенные уровни (попадающие между указанными тегами), если значение макроса не перекрыто.

5.7.3.4. 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 VOP VVALUE/>
```

где:

<DEF – начало конструкции определения переменной. Символ <, не являющийся началом определения, должен быть экранирован (подробнее см. п. 5.7.3.5 на стр. 70);

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 экранирующий (escape) символ (подробнее см. п. 5.7.3.5 на стр. 70). Пример конструкции определения переменной:

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

> – конец конструкции определения переменной. Символ >, не являющийся концом определения переменной, должен быть экранирован (подробнее см. п. 5.7.3.5 на стр. 70). Конструкция DEF не имеет тега, как конструкция FOR, поэтому закрывающая скобка ее тега должна уведомлять парсер об отсутствии закрывающего тега.

... – разделитель формата ***()*(lt)**

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

vchar – символы из набора nchar, *, ?

В случае переопределения переменной в границах ее 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.

5.7.3.5. 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"/>

Предопределенные макросы

%CRLF% Макрос перевода строки

%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 «\» используйте 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 приняты другие действия по обработке шаблона. Действие такого escape-символа сохраняется независимо от того, встретился ли он внутри или снаружи тега.

Для того чтобы поместить символ «\» в конец строки так, чтобы он не принимал значение продолжения строки, используйте последовательность «\\».

- Для вывода в текст шаблона символа «%» используйте последовательность «\%».
- Для вывода в текст шаблона символа «/» используйте последовательность «\/».
- Для вывода в текст шаблона символа «<» используйте последовательность «\<».
- Для вывода в текст шаблона символа «>» используйте последовательность «\>».
- Для вывода в текст шаблона символа «#» используйте последовательность «\#».

Примечание

Язык макросов 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.

5.7.3.6. 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:

%VERSION% – номер установленной версии Антивируса Касперского, с помощью которого было проверено сообщение.

%PRODUCT% – полное имя Антивируса Касперского.

%CLIENT % – удаленный IP-адрес почтового клиента.

%SERVER% – имя сервера, где установлена центральная служба приложения.

%SENDER% – адрес отправителя почтового сообщения.

%RECIPIENTS% – адрес получателя.

%HEADERS% – заголовок сообщения.

%MSGID% – идентификационный номер почтового сообщения.

%SUBJECT% – тема (поле **Subject**) исходного почтового сообщения.

%DATE% – дата обработки почтового сообщения.

%TIME% – время обработки почтового 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. Для каждой обработанной части письма информация представляется в виде:

<статус> <действие> <информация>.

В уведомлениях по удаленным частям почтового сообщения может использоваться следующий макрос:

%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.

ГЛАВА 6. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВЫХ СИСТЕМ

Антивирусная защита файловых систем компьютера осуществляется с помощью компонента *kav4lms-kavscanner*, который выполняет проверку и производит обработку зараженных и подозрительных объектов в соответствии с настройками.

Примечание

Все параметры компонента *kav4lms-kavscanner* сгруппированы в секциях **[scanner.*]** конфигурационного файла приложения.

Внимание!

По умолчанию запуск проверки по требованию могут выполнять только пользователи **root** и **kluser**.

Вы можете задавать проверку, как всей файловой системы, так и отдельного каталога или объекта. Весь набор параметров защиты можно разделить на группы, определяющие:

- область проверки (см. п. 6.1 на стр. 75);
- режим проверки и лечения объектов (см. п. 6.2 на стр. 76);
- действия над объектами (см. п. 6.3 на стр. 77).

Процесс проверки файловых систем вашего компьютера может быть запущен:

- разово из командной строки (см. п. 6.4 на стр. 78);
- по расписанию при помощи программы **cron** (см. п. 6.5 на стр. 79).

Внимание!

Процесс проверки на присутствие вирусов всего компьютера – очень ресурсоемкая процедура. Следует помнить, что при ее запуске скорость работы будет замедлена, следовательно, не рекомендуется запускать какие-либо ресурсоемкие приложения параллельно с проверкой. Во избежание таких проблем рекомендуем вам проверять отдельные каталоги.

6.1. Область проверки

Область проверки можно условно разделить на две части:

- *путь проверки* – список каталогов и объектов, в которых производится поиск вирусов;
- *объекты проверки* – набор типов объектов, которые будут проверяться на предмет наличия вирусов (архивы и т.д.).

По умолчанию проверяются все объекты доступных файловых систем, начиная с текущей директории.

Примечание

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

Вы можете переопределить путь проверки следующими способами:

- Перечислить через пробел директории и файлы с абсолютными или относительными (относительно текущего каталога) путями к ним непосредственно в командной строке при запуске компонента.
- Задать пути проверки в текстовом файле и указать его использование в командной строке посредством ключа **-@ <имя_файла>**. Каждый объект в таком файле приводится с новой строки с абсолютным путем к нему.

Внимание!

Если в командной строке будет указан и путь проверки и текстовый файл со списком объектов проверки, то будет проверяться область, указанная в файле. Путь в командной строке будет проигнорирован.

- Отключить *рекурсивную проверку директорий* (секция **[scanner.options]**, параметр **Recursion** или ключ **-r**).
- Создать альтернативный конфигурационный файл и указать его использование посредством ключа **-с (-C) <имя_файла>** при запуске компонента.

Внимание!

Длина пути к проверяемому объекту не должна превышать 4096 байт. Объекты, расположенные на более глубоком уровне вложенности проверяться не будут.

Объекты проверки по умолчанию также задаются в конфигурационном файле `kav4lms.conf` (секция **[scanner.options]**) и могут быть переопределены:

- непосредственно в данном файле;
- ключами командной строки при запуске компонента;
- путем использования альтернативного конфигурационного файла.

6.2. Режим проверки и лечения объектов

Настройка данного режима является очень важным параметром проверки, поскольку определяет, будет ли выполняться лечение зараженных файлов, обнаруженных в результате проверки.

По умолчанию режим лечения отключен, что предполагает только проверку объектов и информирование об обнаружении вирусов и других подозрительных или поврежденных файлов путем вывода сообщений на консоль и в отчет.

В результате проверки на присутствие вирусов каждому объекту присваивается один из следующих статусов:

- **clean** – вирусов не обнаружено (объект не заражен);
- **infected** – объект заражен;
- **warning** – код объекта похож на код известного вируса;
- **suspicious** – объект подозревается на заражение неизвестным вирусом (не присваивается, если параметру **UseCodeAnalyzer** присвоено значение **no**);
- **corrupted** – объект поврежден;
- **protected** – объект проверить невозможно из-за того, что он зашифрован (защищен паролем);
- **error** – при проверке объекта произошла ошибка.

При включенном режиме лечения (секция **[scanner.options]**, параметр **Cure=yes**), на лечение отправляются объекты только со статусом **infected**. В результате лечения объекту присваивается один из следующих статусов:

- **cured** – объект был успешно вылечен;

- **curefailed** – объект вылечить не удалось. Файл с таким статусом будет обрабатываться по правилам, заданным для зараженных объектов.

6.3. Действия над объектами

В зависимости от статуса объекта к нему могут применяться те или иные действия. По умолчанию выполняется только уведомление об обнаружении объектов с определенным статусом. Однако для объектов со статусами **infected**, **suspicious**, **warning**, **error**, **protected** и **corrupted** можно настроить выполнение ряда действий, таких как:

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

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

Внимание!

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

Выбрать действие над тем или иным объектом можно следующими способами:

- Задать их в конфигурационном файле *kav4lms.conf*, если их предполагается использовать как действия по умолчанию (секции **[scanner.object]** и **[scanner.container]**).
- Указать действия в альтернативном конфигурационном файле и использовать его при запуске компонента.

Примечание

Если в командной строке при запуске компонента не указывается какой-либо конфигурационный файл, то параметры функционирования берутся из файла *kav4lms.conf*. Использование данного файла при запуске специально не указывается!

- Задать их на текущий сеанс работы посредством ключей командной строки при запуске компонента *kav4lms-kavscanner*.

Синтаксис действий как для простых объектов, так и для объектов-контейнеров одинаков (секции [**scanner.object**] и [**scanner.container**]).

6.4. Проверка директории по требованию

Одной из самых распространенных задач, решаемых посредством Антивируса Касперского, является антивирусная проверка и лечение отдельной директории.

Пример: выполнить проверку согласно следующим условиям:

1. Запустить проверку директории */tmp* с автоматическим лечением всех обнаруженных зараженных объектов. Все объекты, вылечить которые не удалось, – удалить.
2. В этой же директории создать файлы *infected.lst*, *suspicion.lst*, *corrupted.lst* и *warning.lst*, в которых сохранить имена всех обнаруженных в результате проверки зараженных, подозрительных или поврежденных объектов соответственно.
3. Результаты работы компонента (дату запуска, информацию обо всех файлах, кроме незараженных) выводить в файл-отчет *kav4lms-kavscanner-текущая_дата-pid.log*, который сохранить в той же директории:

Для выполнения задачи в командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-kavscanner -\
rlq -pi/tmp/infected.lst -ps/tmp/suspicion.lst -\
pc/tmp/corrupted.lst -pw/tmp/warning.lst -o /tmp/ \
kav4lms-kavscanner-`date "+%Y-%m-%d-$$"` .log -i3 \
-ePASBMe -j3 -mCn /tmp
```

6.5. Проверка по расписанию

Запуск программ по расписанию, в том числе и задач Антивируса Касперского, осуществляется с помощью программы **cron**.

Пример: каждый день в 0 часов 00 минут запускать проверку на присутствии вирусов директории /home; использовать параметры проверки, заданные в конфигурационном файле /etc/kav/scanhome.conf.

Для реализации поставленной задачи выполните следующие действия:

1. Создайте конфигурационный файл `/etc/kav/scanhome.conf`, где укажите все необходимые параметры проверки.
2. Отредактируйте файл, задающий правила работы процесса **cron** (**crontab -e**), введя следующую строку:

```
0 0 * * * /opt/kaspersky/kav4lms/bin/kav4lms-\  
kavscanner -c /etc/kav/scanhome.conf /home
```

6.6. Отправка уведомлений администратору

С использованием стандартных средств Unix вы можете настроить уведомление администратора об обнаружении в файловых системах компьютера зараженных, подозрительных и поврежденных объектов.

Пример: настроить уведомление администратора при обнаружении в файловых системах зараженных файлов и архивов при каждой проверке компьютера, выполняемой в соответствии с параметрами конфигурационного файла `kav4lms.conf`.

Внимание!

Приведен пример для Linux!

Для реализации поставленной задачи выполните следующие действия:

Задайте следующие правила обработки простых объектов и контейнеров в конфигурационном файле `kav4lms.conf`:

```
[scanner.object]  
OnInfected=exec echo %FULLPATH%/%FILENAME% is \  
infected by %VIRUSNAME% |  
mail -s kav4lms-kavscanner admin@localhost  
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/%FILENAME% \  
is infected, viruses list is in the attached file \  
%LIST% | mail -s kav4lms-kavscanner -a %LIST% \  
admin@localhost
```

Внимание!

Перед запуском примера пользователю необходимо убедиться, что утилита **mail** расположена по стандартному пути установки данной утилиты в операционной системе.

ГЛАВА 7. ОБНОВЛЕНИЕ БАЗ АНТИВИРУСА

Неотъемлемым фактором полноценной антивирусной защиты является обновление баз антивируса, проводимое компонентом *kav4lms-keepup2date* приложения. Источником обновлений баз, используемых Антивирусом Касперского в процессе поиска и лечения зараженных объектов, являются серверы обновлений «Лаборатории Касперского». Например, такие как:

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

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

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

Список адресов, с которых можно копировать обновления, приведен в файле */var/opt/kaspersky/kav4lms/bases/updcfg.xml*, включенном в дистрибутив приложения. Для просмотра списка серверов обновлений введите в командной строке:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -s
```

В процессе обновления компонент *kav4lms-keepup2date* обращается к данному списку, выбирает адрес и пытается скопировать с сервера базы антивируса. С помощью параметра **RegionSettings** в секции **[updater.options]** конфигурационного файла приложения можно задать текущее положение компьютера (в виде двухбуквенного кода в соответствии со стандартом ISO 3166-1). В этом случае компонент *kav4lms-keepup2date* начинает выбор серверов обновлений с серверов, помеченных в списке, как принадлежащих выбранному региону. Если выполнить обновление с выбранного адреса невозможно, компонент обращается по следующему адресу и вновь пытается обновить базы.

Примечание

Обновления для баз антивируса публикуются на серверах обновлений «Лаборатории Касперского» каждый час.

После успешного обновления выполняется команда, указанная в качестве значения параметра **PostUpdateCmd** секции **[updater.options]** конфигурационного файла. По умолчанию эта команда запустит автоматическую перезагрузку баз антивируса. Некорректное изменение данного параметра может привести к тому, что приложение либо не будет использовать обновленные базы, либо будет работать некорректно.

Примечание

Все параметры компонента *kav4lms-keepup2date* сгруппированы в опциях **[updater.*]** конфигурационного файла.

Если структура вашей локальной сети достаточно сложная, рекомендуется каждый час скачивать обновления баз антивируса с серверов обновлений, размещать их в некотором сетевом каталоге, а для локальных компьютеров сети настроить копирование баз из этого каталога. Подробнее о создании сетевого каталога см. п. 7.3 на стр. 84.

Обновление может быть организовано по расписанию с помощью программы **cron** (см. п. 7.1 на стр. 82) или же выполняться по требованию администратора, запускаясь вручную из командной строки (см. п. 7.2 на стр. 83).

7.1. Автоматическое обновление

Вы можете задать автоматическое обновление баз антивируса с помощью внесения изменений в конфигурационный файл.

Пример: задать автоматическое обновление баз антивируса каждый час. В системном журнале фиксировать только ошибки при работе приложения. Вести общий журнал по всем запускам задачи, на консоль никакой информации не выводить.

Для реализации поставленной задачи выполните следующие действия:

1. В конфигурационном файле приложения задайте соответствующие значения для параметров, например:

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

2. Отредактируйте файл, задающий правила работы процесса **cron** (**crontab -e**), введя следующую строку:

```
0 0-23/1 * * * /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -e
```

Пример: настроить получение обновлений баз антивируса с сайтов-источников обновлений «Лаборатории Касперского». Адрес сайта обновлений автоматически определить из списка, включенного в состав компонента kav4lms-keepup2date.

Для реализации поставленной задачи выполните следующие действия:

Присвойте параметру **UseUpdateServerUrl** секции **[updater.options]** значение **No**.

Пример: настроить получение обновлений баз антивируса с адреса, указанного администратором. Если проведение обновлений с данного адреса невозможно, прервать процесс обновления.

Для реализации поставленной задачи выполните следующие действия:

Присвойте параметрам **UseUpdateServerUrl** и **UseUpdateServerUrlOnly** секции **[updater.options]** значение **Yes**. Кроме того, параметр **UpdateServerUrl** должен содержать адрес сервера обновлений.

Пример: настроить получение обновлений баз антивируса с адреса, указанного администратором. Если проведение обновлений с данного адреса невозможно, обновить базы с адреса, указанного в списке встроенного в Антивирус Касперского списка обновлений.

Для реализации поставленной задачи выполните следующие действия:

Присвойте параметру **UseUpdateServerUrl** секции **[updater.options]** значение **Yes**, а параметру **UseUpdateServerUrlOnly** значение **No**. Кроме того, параметр **UpdateServerUrl** должен содержать адрес сервера обновлений.

7.2. Обновление по требованию

В любой момент времени вы можете запустить обновление баз антивируса из командной строки с помощью команды:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date
```

Пример: запустить обновление баз антивируса, сохранив результаты работы в файле /tmp/updatesreport.log.

Для реализации поставленной задачи в командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -l \  
/tmp/updatesreport.log
```

Если вам необходимо обновить базы антивируса на нескольких компьютерах, удобнее вместо многократного получения баз через интернет получить

базы с серверов обновлений один раз, записать их в некоторый сетевой каталог, а затем обновлять базы из этого каталога.

Пример: организовать обновление баз антивируса из сетевого каталога ftp://10.10.10.1/home/bases, а если этот каталог недоступен или пуст, проводить обновление баз с серверов «Лаборатории Касперского». Результаты работы вывести в файл отчета report.txt.

Для реализации поставленной задачи выполните следующие действия:

1. В конфигурационном файле приложения задайте соответствующие значения для параметров:

```
[updater.options]
UpdateServerUrl=ftp://10.10.10.1/home/bases
UseUpdateServerUrl=yes
UseUpdateServerUrlOnly=no
```

2. В командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -l \
/tmp/report.txt
```

7.3. Обновление из сетевой директории

Для того чтобы обновления баз антивируса из сетевого каталога проходили корректно, вам необходимо создать в этом каталоге файловую структуру, аналогичную структуре серверов обновлений «Лаборатории Касперского». Рассмотрим реализацию этой задачи подробнее.

Пример: создать сетевой каталог, откуда базы антивируса будут копироваться на локальные компьютеры сети.

Для реализации поставленной задачи выполните следующие действия:

1. Создайте локальный каталог.
2. Запустите компонент *kav4lms-keepup2date* следующим образом:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -u
<dir>
```

где *<dir>* - полный путь к созданному каталогу.

3. Предоставьте для локальных компьютеров сетевой доступ на чтение к данному каталогу.

Пример: настроить обновление баз антивируса через прокси-сервер.

Для реализации поставленной задачи выполните следующие действия:

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

или:

1. В секции **[updater.options]** конфигурационного файла присвойте параметру **UseProxy** значение **Yes**.
2. Задайте переменную окружения **http_proxy** в формате **http://username:password@ip_address:port**. Обратите внимание, что переменная будет учитываться только в том случае, если параметр **UseProxy** секции **[updater.options]** отсутствует или имеет значение **Yes**.

ГЛАВА 8. УПРАВЛЕНИЕ КЛЮЧАМИ

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 действия лицензии, информацию о дистрибьюторах и т.д.

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

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

По окончании срока действия ключа вы автоматически лишаетесь приведенных выше возможностей. Антивирус Касперского по-прежнему будет осуществлять обработку сообщений, но только с использованием баз антивируса, актуальных на дату окончания срока действия ключа. Функция обновления баз антивируса будет не доступна. При получении обновления баз антивируса без помощи функций приложения базы могут быть выпущены позже даты окончания срока действия ключа. В таком случае приложение прекращает обработку сообщений, о чем записывается соответствующее уведомление в файл отчета.

Поэтому крайне важно регулярно просматривать файлы отчета, в которых приведена информация о ключе, и отслеживать дату истечения срока его действия.

Приложение реализует следующие схемы лицензирования:

- **по трафику.**

Данный тип лицензирования обеспечивает защиту ежедневного трафика, в объеме, указанном в ключе. Учитывается только трафик, которому в результате проверки проверки были присвоены статусы **clean** или **notchecked**. В случае превышения лицензионного ограничения администратор получает уведомления о первом и последующих сообщениях, выходящих за ограничение.

- **по числу защищаемых адресов.**

Данный тип лицензирования предоставляет антивирусную защиту определенного числа почтовых адресов. Защищаемые адреса должны принадлежать доменам, заданным параметром **LicensedUsersDomains** в секции **[kav4lms:server.settings]** конфигурационного файла *kav4lms.conf*, и адресам, принадлежащим серверу, на котором запущено приложение.

Лицензируемые домены могут быть заданы:

- строкой;
- выражением, содержащим символы обобщения (синтаксис UNIX);
- регулярными выражениями (синтаксис POSIX).

Внимание!

Регулярные выражения нечувствительны к регистру.

Если число почтовых адресов в заданном домене превышает лицензионное ограничение, администратору будет предложено приобрести ключи для дополнительного числа адресов.

8.1. Просмотр лицензионной информации

В составе Антивируса Касперского предусмотрен специальный компонент *kav4lms-licensemanager*, позволяющий вам просматривать не только более полную информацию о ключах, но и получать некоторые аналитические данные.

Вся информация может быть выведена на экран терминала.

Чтобы просмотреть информацию обо всех ключах, в командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager -s
```

На экран будет выведена информация подобного рода:

```
Kaspersky license manager for Linux. Version  
5.6/RELEASE #68
```

```
Copyright (C) Kaspersky Lab, 1997–2007.
```

```
Portions Copyright (C) Lan Cryptot
```

```
License info:
```

```
Product name: Kaspersky Anti-Virus BO for SendMail /
Qmail / Postfix Milter API International Edition. 10-
14 MailAddress 1 month Beta Licence
Expiration date: 01-09-2007, expires in 28 days
```

Active key info:

```
Key file:          00BEA0DB.key
Install date:     02-08-2007
Product name:    Kaspersky Anti-Virus BO for SendMail
/ Qmail / Postfix Milter API International Edition.
10-14 MailAddress 1 month Beta Licence
Creation date:   02-02-2007
Expiration date: 03-03-2008
Serial:          0038-000413-00BEA0DB
Type:            Beta
Count:           10
Lifespan:        30
Objs:            7:10
```

Параметр `Objs` представляет собой число объектов лицензирования. Его значение состоит из частей `<тип_объектов>`: `<число_объектов>`. Часть `<тип_объектов>` может принимать следующие значения:

- 3 – схема лицензирования по трафику;
- 7 – схема лицензирования по числу адресов.

Часть `<число_объектов>` имеет то же значение, что и параметр `Count`.

Чтобы просмотреть информацию о конкретном ключе, в командной строке введите такую строку:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\
-k <key filename>
```

где `<имя_ключа>` - имя файла ключа, например, 0003D3EA.key.

На экран будет выведена информация подобного рода:

```
Kaspersky license manager for Linux. Version
5.6/RELEASE #68
Copyright (C) Kaspersky Lab, 1997-2007.
Portions Copyright (C) Ian Crypto
```

```
Product name:    Kaspersky Anti-Virus BO for SendMail
                 / Qmail / Postfix Milter API International Edition.
                 10-14 MailAddress 1 month Beta Licence
Creation date:   02-02-2007
Expiration date: 03-03-2008
Serial:          0038-000413-00BEA0DB
Type:            Beta
Count:           10
Lifespan:        30
Objs:            7:10
```

8.2. Продление срока действия ключа

Продление срока действия ключа на использование Антивируса Касперского дает вам право на восстановление полной функциональности приложения – обновления баз антивируса. Кроме того, возобновляются дополнительные услуги, приведенные в п. 1.3 на стр. 10.

Срок действия ключа зависит от схемы лицензирования, который вы выбрали, приобретая приложение.

Чтобы продлить срок действия ключа на использование Антивируса Касперского, вам необходимо:

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

или:

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

Примечание

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

Приобретенный ключ необходимо установить.

Чтобы установить новый ключ, в командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\  
-a <путь_к_файлу_ключа>
```

После этого рекомендуем вам обновить базы антивируса (см. Глава 7 на стр. 81).

Чтобы удалить ключ, в командной строке введите:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\  
-da
```

для удаления активного ключа,

или

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\  
-dr
```

для удаления резервного ключа.

ГЛАВА 9. ОТЧЕТЫ И СТАТИСТИКА РАБОТЫ ПРИЛОЖЕНИЯ

9.1. Формирование отчетов

Примечание

Параметры отчетов о работе приложения содержатся в секциях `[kav4lms:server.log]` и `[kav4lms:filter.log]` конфигурационного файла `kav4lms.conf`

Антивирус Каперского позволяет создавать отчеты о работе центральной службы и фильтра. Результаты их работы могут сохраняться в системном журнале или файле отчета. Место хранения отчета назначается параметром **Destination**, который может принимать следующие значения:

- `syslog:<имя>@<категория>` – отчет записывается в системный журнал. Название приложения задается аргументом `<имя>`, категория системного журнала задается аргументом `<категория>`;
- `file:<log_file_path>` – отчет записывается в указанный файл.

Внимание!

Не следует использовать один и тот же файл для записи отчетов центральной службы приложения и фильтра, так как только один процесс может иметь доступ к файлу.

Категория и уровень детализации записываемой информации задается параметром **Options**. Значение данного параметра состоит из двух частей, разделенных точкой:

1. Категория функциональности приложения, отчет о которой собирается. Возможен выбор следующих значений:
 - **all** – все аспекты функциональности приложения;
 - **config** – сообщения, относящиеся к конфигурации приложения;
 - **app** – сообщения, относящиеся к внутренней логике работы приложения;

- **scan** – сообщения о статусе проверки и действиях в ее результате;
 - **cfilter** – сообщения о статусе фильтрации и действиях в ее результате;
 - **backup** – сообщения, касающиеся резервного копирования;
 - **notif** – сообщения, относящиеся к отправке уведомлений;
 - **admin** – сообщения, относящиеся к управлению приложением (например, выполнению команд SNMP);
 - **smtp** – сообщения об обмене информацией между приложением и почтовой системой.
2. Уровень детализации, который представляет собой важность записываемой информации. Описание возможных способов задания уровня детализации приведено в таблице ниже.

Обозначение уровня	Название уровня	Описание
0, F	fatal	Информация только о критических ошибках (ошибках, которые приводят к завершению работы приложения из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при проверке, загрузке баз и ключей. В файле отчета сообщения о критических ошибках отмечаются символом F.
1, E	error	Информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов; например, информация об ошибке проверки объекта. В файле отчета сообщения о некритических ошибках отмечаются символом E.

Обозначение уровня	Название уровня	Описание
2, W	warning	Информация об ошибках, которые могут привести к завершению работы продукта (например, информация об отсутствии свободного места на диске или истечении срока действия ключа). В файле отчета сообщения о таких ошибках отмечаются символом W.
3, I	info	Важные сообщения информационного характера, например: информация о том, запущен ли компонент, путь к конфигурационному файлу, информация о базах антивируса, о ключах, результирующая статистика. В файле отчета информационные сообщения отмечаются символом I.
4, A	activity	Сообщения о текущей активности приложения (например, имя проверяемого файла). В файле отчета сообщения об активности приложения отмечаются символом A.
9, D	debug	Сообщения с отладочной информацией. В файле отчета отладочная информация отмечаются символом D.

Пример:

```
[kav4lms:server.log]
```

```
Options = backup.all, config.error, scan.all, -scan.debug
```

```
Options = backup.all, config.E, scan.all, -scan.9
```

Данные значения параметра **Options** включают запись сообщений о резервном копировании и антивирусной проверке на всех уровнях детализации, сообщений об ошибках в конфигурации приложения и отключают запись отладочной информации об антивирусной проверке. Второй пример демонстрирует другой вариант записи настроек отчета приложения.

Внимание!

Уровни детализации не включают предыдущие (более низкие) уровни. Для выбора нескольких уровней детализации все они должны быть перечислены.

Для предотвращения чрезмерного роста файлов отчета можно включить режим ротации файла отчета. Для этого необходимо установить параметры **RotateSize** и **RotateRounds** в ненулевые значения.

Если ротация файла отчета включена, то он растет в размере, пока не достигнет значения параметра **RotateSize**. Затем к имени файла отчета добавляется суффикс «.1». Если файл с таким суффиксом уже существует, создаются файлы с суффиксами «.2», «.3» и так далее. Количество файлов увеличивается до тех пор, пока значение суффикса не достигнет значения параметра **RotateRounds**. По достижении этого значения снова используется файл с суффиксом «.1».

9.2. Статистика работы приложения

Примечание

Параметры сбора статистики о работе приложения находятся в секции **[kav4lms:server.statistics]** главного конфигурационного файла приложения.

Во время работы приложения идет сбор статистики двух типов:

- **общая**, которая собирается время от времени и отражает общую активность приложения;
- **детализированная статистика**, которая собирается по каждому обработанному сообщению.

Тип статистики задается параметром **Options**, возможные значения которого приведены в таблице ниже.

Категория статистики	Значение параметра Options	Собираемая информация
Сообщения	messages	Число входящих сообщений; число проверенных сообщений; число сообщений со статусом protected ; число сообщений со статусом infected ; число сообщений со статусом error ; средний размер сообщения (в байтах); среднее время проверки одного сообщения (в миллисекундах)
Системные ресурсы	resources	Время, прошедшее с последнего запроса статистики (в секундах); общий объем трафика (в килобайтах); общая загрузка процессора пользовательскими приложениями; общая загрузка процессора системными службами
Обнаруженные угрозы	viruses	10 последних обнаруженных угроз; 10 IP-адресов, с которых поступило наибольшее число угроз
Фильтрация	filters	Число сообщений, отфильтрованных по MIME-типу; число сообщений, отфильтрованных по имени вложений; число сообщений, отфильтрованных по размеру вложений; число сообщений, отфильтрованных по имени обнаруженной угрозы
Все категории	all	Все вышеприведенные категории
Детальная статистика	raw	Подробная статистика по каждому сообщению
Сбор статистики отключен	none	

Если параметр **Options** установлен в значение **none**, статистика не формируется.

Примеры.

Для формирования общей статистики по всем категориям (сообщения, системные ресурсы, угрозы, фильтрация) установите параметр **Options** в следующее значение:

```
Options = all
```

Для формирования общей статистики по всем категориям, а также детализированной статистики по каждому сообщению, установите параметр **Options** в следующее значение:

```
Options = all, raw
```

Для формирования только детализированной статистики установите параметр **Options** в следующее значение.

```
Options = none, raw
```

Внимание!

Установка параметра **Options** в значение **all** не включает сбор детализированной статистики! Данный режим должен быть задан явно.

Пример записи в файле raw-статистики:

```
1210247100      1208      from@example.com  
rcpt@example.com  infected      EICAR-Test-File 127.0.0.1  
1Ju4YW-000Du9-0U Default
```

Где:

- 1210247100 – время обработки сообщения в формате UNIX;
- 1208 – размер сообщения;
- from@example.com – адрес отправителя сообщения;
- rcpt@example.com – адрес получателя сообщения;
- infected – статус, присвоенный сообщению по результатам проверки;
- EICAR-Test-File – имя обнаруженной в сообщении угрозы;
- 127.0.0.1 – IP-адрес, с которого было отправлено сообщение;
- 1Ju4YW-000Du9-0U – идентификатор сообщения в очереди почтовой системы;
- Default – имя группы, с параметрами которой сообщение было обработано.

Для записи собранной статистической информации в файл выполните следующую команду:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \  
write
```

Запуск данной команды также обновляет информацию в существующем файле статистики.

Для сброса значений внутренних счетчиков статистики выполните следующую команду:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \  
reset
```

Примечание

После сброса счетчиков файл статистики должен быть перезаписан.

Общая статистика сохраняется в файл, заданный параметром **Destination**. Детализированная статистика собирается в файл, заданный параметром **RawDestination**. Эти файлы могут быть двух форматов:

- **txt**-файл;
- **xml**-файл.

Формат файлов статистики задается параметром **Format**.

Внимание!

Если различным частям сообщения в результате проверки были присвоены разные статусы, то данное сообщение будет учтено всеми соответствующими счетчиками. Таким образом, сумма всех счетчиков может не показать общее число проверенных сообщений.

Например, если сообщение содержит три вложения: зараженное, защищенное паролем и типа `application/msword`, то такое сообщение будет учтено счетчиками:

- **total_messages;**
- **scanned_messages;**
- **protected_messages;**
- **infected_messages;**
- **filtered_mime.**

ГЛАВА 10. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

10.1. Контроль состояния защиты с помощью протокола SNMP

Приложение предоставляет доступ только на чтение к следующей информации по протоколу SNMP:

- *конфигурация приложения* – информация по всем параметрам всех секций конфигурационных файлов (включая файлы, описывающие группы);
- *статистика работы* – статистическая информация по работе приложения (если приложение настроено на сбор статистики, подробнее см. п. 9.2 на стр. 94).

Примечание

Приложение работает с мастер-агентами, поддерживающими протокол SNMP v1, v2 и v3. Обратите внимание, что приложение отправляет ловушки версии 2, и приемник ловушек должен быть настроен соответственно.

Для определения информации, доступной по протоколу SNMP, служит параметр **SNMPServices**, расположенный в секции **[kav4lms:server.snmp]** конфигурационного файла *kav4lms.conf*. Возможны следующие значения данного параметра:

- **config** – информация о конфигурации приложения;
- **statistics** – статистика работы приложения; (см. п. 9.2 на стр. 94);
- **admin** – административная информация, к которой относятся:
 - **Status.StartedOn** – дата запуска приложения в формате ISO 8601;
 - **Status.UpTime** – время в секундах, прошедшее с момента запуска приложения.
- **update** – информация об обновлении приложения, к которой относятся:

- **Last.Checked** – дата последней проверки наличия обновлений в формате ISO 8601;
- **Last.Result** – статус последнего обновления:
 - **updated** – обновление прошло успешно;
 - **not-needed** – обновление завершилось корректно, но новые файлы не были загружены;
 - **error** – обновление завершилось с ошибкой;
 - **rolled-back** – обновление прошло успешно, но в связи с тем, что новые базы оказались поврежденными, был совершен откат к использованию предыдущей версии баз антивируса;
 - **unknown** – статус не может быть определен;
 - **Current.Loaded** – дата последнего успешного обновления в формате ISO 8601;
 - **Current.Records** – общее количество записей в используемых базах антивируса;
 - **Current.Released** – дата выпуска обновления, используемого приложением.
- **all** – вся перечисленная выше информация;
- **none** – не предоставлять информацию по протоколу SNMP.

Для реализации взаимодействия по протоколу SNMP в Антивирусе Касперского применяется SNMP-субагент, использующий в свою очередь протокол *AgentX* для связи с мастер-агентом SNMP. Параметры протокола *AgentX*:

- **Socket** – определяет сокет взаимодействия; допускается использование локального и сетевого сокета. Например:

```
Socket=local:/var/agentx/master
```

или

```
Socket=inet:705@127.0.0.1
```

Внимание!

При использовании локального сокета удостоверьтесь, что мастер-агент имеет доступ к этому сокету. Для этого необходимо внести изменения в значения параметров **RunAsUser** и **RunAsGroup**, в права доступа к сокету и файлам данных, используемых мастер-агентом. Если мастер-агент запускается на одном компьютере с центральной службой приложения, то необходимо внести аналогичные изменения в права доступа центральной службы.

- **Timeout** – тайм-аут (в секундах) на отправку запроса мастер-агенту. Значение по умолчанию **5**.
- **Retries** – количество попыток отправки запроса мастер-агенту. Значение по умолчанию **10**. Если параметр не задан, используется значение **5**.

Внимание!

Число попыток отправки запроса может отличаться от заданного значения **Retries**. Это происходит из-за активности утилиты *watchdog* и не является ошибкой.

- **PingInterval** – интервал (в секундах), с которым субагент будет пытаться подключиться к мастер-агенту в случае разрыва соединения.

В качестве мастер-агента допускается использование любого агента, поддерживающего протокол AgentX. В данном разделе рассматривается пример использования агента *NET-SNMP*. Взаимодействие осуществляется через локальный сокет.

Внимание!

Для корректного взаимодействия с приложением по протоколу AgentX рекомендуется использовать агент *NET-SNMP* версии 5.1.2 и выше, а также любой другой тип мастер-агента, соответствующий требованиям стандарта.

Для настройки агента необходимо выполнить следующие шаги:

1. Изменить конфигурационный файл *snmpd.conf*, добавив следующие строчки:

```
master agentx
AgentXSocket /var/agentx/master
AgentXPerms 770 770 root kluser
rocommunity public localhost
trapsink localhost
```

или, в случае использования сетевого сокета, замените вторую строку на:

```
AgentXSocket tcp:127.0.0.1:705
```

2. Изменить конфигурационный файл *snmp.conf*, добавив следующие строки:

```
mibdirs +/opt/kaspersky/kav4lms/share/snmp-mibs  
mibs all
```

где путь */opt/kaspersky/kav4lms/share/snmp-mibs* указывает на директорию, в которой по умолчанию находятся MIB-файлы Антивируса Касперского.

3. Перезапустите NET-SNMP и Антивирус Касперского.

Примечание

Более детальную информацию по настройке агента *NET-SNMP* вы найдете на официальном сайте <http://www.net-snmp.org/>. Для получения информации о файлах *snmpd.conf* и *snmp.conf* воспользуйтесь файлами справки (manual pages).

При доступе к информации по протоколу SNMP используется следующий OID (идентификатор объекта):

.1.3.6.1.4.1.23668.1043

или в символьной форме записи:

iso.org.dod.internet.private.enterprises.kaspersky.kav4lms

Данный узел содержит следующие подгруппы:

- **config** – конфигурационные параметры приложения, расположенные согласно секциям конфигурационного файла, а также параметры групп;
- **statistics** – статистическая информация по обработанным сообщениям, использованным ресурсам и обнаруженным вирусам;
- **update** – информация об обновлении приложения;
- **admin** – административная информация (время запуска приложения, ошибки в работе и т.д.).

Внимание!

Для получения значений объектов подгруппы **config.Groups** вместо метода *Get* необходимо применять метод *Walk*

У администратора также есть возможность настроить приложение на отправку SNMP-ловушек (traps) при наступлении определенных событий. События, при которых приложение производит отправку SNMP-ловушек, определяются параметром **SNMPTraps** секции **[kav4lms:server.snmp]** конфигурационного файла *kav4lms.conf*. Возможны следующие значения данного параметра:

- **config** – отправка SNMP-ловушки выполняется, если произошла перезагрузка баз антивируса (*BasesReloaded trap*) или конфигурации приложения (*ConfigReloaded trap*);
- **admin** – отправка SNMP-ловушки выполняется, если приложение было запущено / остановлено (*ProductStart trap*, *ProductStop trap*) или при работе возникла критическая ошибка (*ProductError trap*); также, если значение параметра **AlertThreshold** отлично от нуля, то выполняется отправка SNMP-ловушки, свидетельствующей, что количество обнаруженных в течение последнего часа зараженных сообщений превысило заданное значение (*OutbreakAlert trap*). Отправка ловушки *OutbreakAlert* производится каждый час с момента превышения допустимого значения и прекращается после того, как процентное содержание зараженных сообщений снизится до допустимого предела.

Примечание

Перезагрузке приложения соответствует SNMP-ловушка **ConfigReloaded**. Однако при перезагрузке приложения также отправляются ловушки: **ProductStart**, **ProductStop** и **BasesReloaded**. Это происходит вследствие того, что утилита *watchdog* перезапускает приложение.

- **update** – отправка SNMP-ловушки выполняется, если запущено обновление приложения (*UpdateStatus trap*), а также, если с момента последнего обновления прошло более пяти дней (*ObsoleteBases trap*);
- **all** – отправка SNMP-ловушки выполняется при возникновении всех вышеперечисленных событий;
- **none** – отключить отправку SNMP-ловушек.

Внимание!

При использовании мастер-агента NET-SNMP для приема ловушек необходимо запустить сервис *snmptrapd*.

10.2. Использование скрипта настройки приложения

В комплект поставки Антивируса Касперского входит скрипт, позволяющий настраивать приложение после установки (до запуска).

Скрипт настройки приложения запускается следующим образом:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh <опции>
```

Используются следующие опции:

- `--install-services` – зарегистрировать службы приложения (центральную службу и фильтр) для запуска вместе с операционной системой;
- `--remove-services` – отменить запуск служб приложения вместе с операционной системой;
- `--check-services` – проверить регистрацию служб приложения;
- `--install-filter=<МТА>` - интегрировать фильтр в указанную почтовую систему. Данная команда также регистрирует службу в системе;
- `--remove-filter=<МТА>` - удалить заданный фильтр приложения из почтовой системы;
- `--remove-filters` – удалить все установленные фильтры приложения;
- `--check-filter=<МТА>` - проверить корректность интеграции фильтра в указанной почтовой системы;
- `--filter-options=<параметр>` – настройка фильтра. Эта команда используется только в качестве дополнения команды `--install-filter`. Фильтр для Sendmail поддерживает следующие параметры: **tempfail**, **reject**, **pass**;
- `--install-cron=<имя_компонента>` – настроить запуск указанного компонента по расписанию;
- `--remove-cron=<имя_компонента>` – отменить запуск компонента по расписанию;
- `--check-cron=<имя_компонента>` – проверить наличие расписания для компонента;

- `--user=<имя_пользователя>` – задать имя пользователя, с правами которого будет запускаться центральная служба и фильтр приложения. При использовании совместно с параметрами `...install-cron` и `--remove-cron` определяет пользователя для которого создается расписание.

Например:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-cron=updater --user=root
```

или

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-cron=updater --user=qmailq
```

- `--add-components-info` – записывает информацию о приложении в файл *applications.setup*;
- `--del-components-info` – удаляет информацию о приложении из файла *applications.setup*;
- `--check-components-info` – проверить наличие информации о приложении в файле *applications.setup*;
- `--install-webmin-module` – установить модуль удаленного управления приложением в программу Webmin;
- `--remove-webmin-module` – удалить управляющий модуль приложения из программы Webmin;
- `--check-webmin-module` – проверить установку управляющего модуля в программе Webmin;
- `--register-key=key-id` – зарегистрировать ключ, заданный с помощью полного пути или идентификатора;
- `--group=<имя_группы>` - задать группу, под которой будут работать компоненты Антивируса Касперского; в результате будет изменено значение параметра **Group** в секции **[options]** конфигурационного файла приложения.
- `--switch-credentials=<имя_пользователя>[,<имя_группы>]` – задать пользователя и, если указано, группу, с правами которых будут запускаться центральная служба и фильтр приложения; в результате будут изменены параметры **RunAsUser** и, если указано, **RunAsGroup** конфигурационного файла приложения в секциях **[kav4lms:server.settings]** и **[kav4lms:filter.settings]**. После использование этой опции будут перезапущены центральная служба приложения и фильтр.

Параметр <МТА> может принимать следующие значения:

- **exim** – при post-queue интеграции с Exim;
- **exim-dlfunc** – при pre-queue интеграции с Exim с использованием динамически подгружаемой библиотеки;
- **postfix** – при post-queue интеграции с Postfix;
- **qmail** – при интеграции с qmail;
- **sendmail-milter** – при интеграции с Sendmail.

Параметр <имя_компонента> в данной версии приложения поддерживает только значение **updater**.

Примечание

Все команды типа **--check** срабатывают без вывода на консоль и возвращают 0 при наличии проверяемого параметра или ненулевое значение при его отсутствии.

10.3. Управление приложением из командной строки

В поставку Антивируса Касперского входит инструмент для управления приложением из командной строки. Исполняемый файл инструмента *kav4lms-cmd* находится в директории */opt/kaspersky/kav4lms/bin*.

Внимание!

Инструмент *kav4lms-cmd* работает только при запущенной центральной службе приложения.

Существует две категории аргументов командной строки *kav4lms-cmd*:

1. Общие свойства приложения:
 - **-v** или **--version** – отобразить версию приложения;
 - **-h** или **--help** – отобразить справочную информацию о командах *kav4lms-cmd*;
 - **-m** или **--module** <название_компонента> – переключает *kav4lms-cmd* на управление одним из следующих компонентов приложения: *config*, *filter*, *kavmd*, *statistics*, *update*;

- `-c` или `--config <имя_файла>` – использовать альтернативный конфигурационный файл;
- `-l` или `--list` – вывести список модулей приложения.

2. Свойства функциональных модулей приложения.

- а) Модуль **Config**. Данный модуль вносит изменения в конфигурационный файл и запрашивает значения параметров работы приложения:

`-q <параметр>` – запросить значение параметра, например:
`-q Path.TempPath.`

- б) Модуль **Filter**. Данный модуль управляет службой фильтра:

○ `-x <команда>` – выполнить указанную команду. Список доступных команд: `start, stop, restart, status, test-service.`

- в) Модуль **Central service (kavmd)**. Данный модуль управляет центральной службой приложения:

○ `-x <команда>` – выполнить указанную команду. Список доступных команд: `start, stop, restart, reload, status, test-service, test-config.`

- г) Модуль **Statistics**. Данный модуль управляет сбором статистики:

○ `-x <команда>` – выполнить указанную команду; список доступных команд: `write, reset.`

- д) Модуль **Update**. Данный модуль управляет компонентом `kav4lms-keepup2date`:

○ `-e <событие> [-w <информация_о_событии>]` – сгенерировать одно из следующих событий: `OnUpdated, OnNotNeeded, OnError, OnRolledback, OnUnknown.`

10.4. Дополнительные информационные поля в сообщениях

Приложение также позволяет добавлять в почтовое сообщение некоторую дополнительную информацию. Рассмотрим подробнее два способа включения в письмо новых информационных полей:

- Добавлять информацию в заголовок почтового сообщения.

Это может быть информация о версии приложения, дате последнего обновления баз антивируса, времени и результате антивирусной проверки данного письма (задается параметром **AddXHeaders** секции **[kav4lms:groups.<имя_группы>.settings]** конфигурационного файла группы).

Формат дополнительного заголовка:

```
X-Anti-Virus: <имя продукта и его версия>, bases:
<дата обновления баз в формате YYYYMMDDTННММSS> #<ко-
личество записей в AV-базах>, check: <дата проверки в
формате YYYYMMDD> <статус проверки или not_checked>
```

где:

YYYY – обозначение года в четырехсимвольном формате;

MM – обозначение месяца;

DD – обозначение числа;

НН – обозначение часа;

ММ – обозначение минуты;

SS – обозначение секунды.

Например:

```
X-Anti-Virus: Kaspersky Anti-Virus for Linux Mail
Server 5.6.17/RELEASE build 4, bases: 20080415
#705877, check: 20080415 clean
```

- Добавлять информацию в тело почтового сообщения.

Сообщение добавляется в виде plain text и может содержать любой текст, заданный в соответствии с политикой безопасности (или другими правилами) конкретной организации, и задается параметром **AddDisclaimer** в секции

[kav4lms:groups.<имя_группы>.settings]. Текст сообщения по умолчанию уведомляет, что письмо было проверено Антивирусом Касперского. По требованию администратора вид информации можно изменить (например, сформировать сообщение в виде HTML-текста).

- Заменять удаленные части сообщения уведомлением.

В результате действий над сообщением его части могут быть удалены и заменены уведомлением. Для добавления уведомлений установите **yes** в качестве значения параметра **UsePlaceholderNotice** в секции **[kav4lms:groups.<имя_группы>.settings]** в конфигурационном файле группы. Если добавление уведомлений отключено, то части сообщения будут удалены из сообщения полностью.

Текст уведомления берется из шаблона в файле *part_<action_taken>*, который поддерживает макро-язык уведомлений (см. п. 5.7 на стр. 60).

10.5. Локализация формата отображаемых дат и времени

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

По умолчанию Антивирус Касперского использует форматы даты и времени в соответствии с соглашениями, принятыми для строки формата strftime:

%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 *kav4lms.conf*. Например, вы можете задать следующие форматы:

%I:%M:%S %P – для отображения времени в двенадцатичасовом формате (параметр **TimeFormat**).

%y/%m/%d and %m/%d/%y – для отображения даты (параметр **DateFormat**) (гг.мм.дд. и мм.дд.гг., соответственно).

ГЛАВА 11. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ ПРИЛОЖЕНИЯ

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

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

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

Внимание!

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

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

Примечание

Перед загрузкой необходимо отключить антивирусную защиту, поскольку файл *anti_virus_test_file.htm* будет идентифицирован и обработан установленным на компьютере антивирусом как зараженный объект, перемещаемый по HTTP-протоколу.

Не забудьте включить антивирусную защиту сразу после загрузки тестового «вируса».

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

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

рование текста может выполняться с помощью любого текстового редактора.

Примечание

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

Таблица 1. Модификации тестового «вируса»

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый «вирус»	Зараженный. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR-	Поврежденный.
SUSP-	Подозрительный (код неизвестного вируса).
WARN-	Подозрительный (модифицированный код известного вируса).
ERRO-	Вызывающий ошибку проверки, соответствующую обнаружению поврежденного объекта.
CURE-	Зараженный (излечимый). Объект подвергается лечению, при этом текст тела «вируса» изменяется на CURED.

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

После добавления префикса к тестовому «вирусу» сохраните его в файл с другим именем, например, *ecar_corr.com* (аналогично дайте названия всем модифицированным «вирусам»).

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

ПРИЛОЖЕНИЕ А. СПРАВОЧНАЯ ИНФОРМАЦИЯ

А.1. Конфигурационный файл приложения *kav4lms.conf*

В поставку Антивируса Касперского включен конфигурационный файл *kav4lms.conf*, содержащий параметры приложения. В данном разделе представлено детальное описание параметров конфигурационного файла, включая значения по умолчанию при стандартной установке приложения.

Конфигурационный файл разбит на секции, описывающие параметры работы отдельной группы функциональности приложения. Каждая секция описывается следующим образом: первая строка – заголовок секции вида **[имя_секции]** далее следует описание параметров секции.

Примечание

В конфигурационном файле для булевских параметров, которые могут принимать значения **true|false**, можно также указывать эквивалентные значения: либо **yes|no**, либо **y|n**, либо **1|0**.

Параметры, принимающие численные значения, имеют верхний предел – **UINT_MAX=4294967295**.

Внимание!

Параметры, отмеченные в описании как «обязательный параметр», являются необходимыми для корректной работы приложения. Данные параметры обязательно должны быть определены! Без них Антивирус неработоспособен!

А.1.1. Секция *[kav4lms:server.settings]*

Секция **[kav4lms:server.settings]** содержит параметры работы центральной службы приложения:

RunAsUser – имя пользователя, с правами которого запускается центральная служба приложения.

Обязательный параметр.

Значение параметра по умолчанию: **kluser**.

Примечание

Если фильтр и центральная служба установлены на одном компьютере, убедитесь, что параметр **RunAsUser** для этих компонентов имеет оно и тоже значение, что обеспечит корректный доступ к совместно используемым файлам.

RunAsGroup – имя группы, с правами которой запускается центральная служба приложения.

Обязательный параметр.

Значение параметра по умолчанию – **klusers**.

ServiceSocket=inet:<port>@<ip-address>|local:<path_to_socket> – сокет (локальный или сетевой), по которому осуществляется передача данных между центральной службой и фильтром Антивируса Касперского (конечная точка соединения «центральная служба - фильтр»).

Внимание!

Перед изменением данного параметра следует остановить центральную службу приложения; после изменения для применения нового значения параметра следует запустить службу.

Формат записи:

`ServiceSocket=inet:<port>@<ip-address>` – для сетевого сокета;

`ServiceSocket=local:<path_to_socket>` – для локального сокета.

Где:

- **<port>**: порт взаимодействия;
- **<ip-address>**: IP-адрес;
- **<path_to_socket>**: путь к локальному сокету.

Обязательный параметр.

Значение параметра по умолчанию – **local:/var/run/kav4lms/kavmd.sock**.

Примечание

В случае использования локального сокета убедитесь, что каталог расположения файла сокета и сам файл сокета доступны для чтения и записи как службе фильтра, так и центральной службе приложения.

ServiceSocketPerms – права доступа к **ServiceSocket**, в случае использования локального сокета. Владелец сокета задается парой **RunAsUser:RunAsGroup**.

Значение по умолчанию **0600** (данное значение используется, если параметр не задан).

AdminSocket – локальный сокет, используемый для управления центральной службой приложения (например, по протоколу SNMP).

Внимание!

Перед изменением данного параметра следует остановить центральную службу приложения; после изменения для применения нового значения параметра следует запустить службу.

Обязательный параметр.

Значение параметра по умолчанию –
local:/var/run/kav4lms/kavmdctl.sock.

Внимание!

При установке параметра убедитесь, что каталог расположения файла сокета и сам файл сокета доступны для записи только пользователю, с правами которого выполняется приложение.

AdminSocketPerms – права доступа к **AdminSocket**. Владелец сокета: **RunAsUser:RunAsGroup**.

Значение параметра по умолчанию – **0600**.

MaxWatchdogRetries=0...UINT_MAX – максимальное количество попыток перезагрузки Антивируса Касперского утилитой *watchdog*. Значение **-1** (минус один) соответствует отсутствию ограничения. Значение **0** соответствует отключению утилиты *watchdog*.

Значение параметра по умолчанию – **10**.

MaxClientRequests=0...UINT_MAX – максимальное число запросов фильтра, обрабатываемое центральной службой. Значение **0** соответствует отсутствию ограничения.

Значение параметра по умолчанию – **20**.

MaxScanRequests=0..UINT_MAX – максимальное число запросов на проверку сообщений. Значение **0** соответствует отсутствию ограничения.

Значение параметра по умолчанию – **0**.

LicensedUsersDomains – список доменов, почтовый трафик которых, согласно схеме лицензирования, использует антивирусную защиту. Данный параметр определяется только в случае использования схемы лицензирования по почтовым адресам. Вы можете указать несколько значений, разделенных запятой.

Значение параметра по умолчанию –
localhost, localhost.localdomain.

A.1.2. Секция *[kav4lms:server.log]*

Секция **[kav4lms:server.log]** содержит параметры формирования отчетов о работе центральной службы приложения:

Options=<категория_функциональности>.<уровень_детализации>
– категория сообщений, фиксируемых в отчете, где:

- **<категория_функциональности>** может принимать одно из следующих значений: **all, config, app, scan, cfilter, backup, no-tif, admin, smtp** (см. п. 9.1 на стр. 91);
- **<уровень_детализации>** может принимать одно из следующих значений: **debug, activity, info, warning, error, fatal** (см. п. 9.1 на стр. 91).

Вы можете указать несколько уровней, разделенных запятой.

Например:

```
Options = backup.all, config.error, \
scan.all, -scan.debug
Options = backup.all, config.E, \
scan.all, -scan.9
```

Обязательный параметр.

Значение параметра по умолчанию: **all,-all.debug**.

Destination=syslog:<имя>@<категория>|file:<путь_к_файлу> – путь к файлу, в который будет записываться отчет о работе центральной службы приложения:

- **syslog:<имя>@<категория>**: записывать отчет в системный журнал; в качестве имени приложения использовать <имя>, в качестве категории (**syslog facility**) – <категория>.
- **file:<путь_к_файлу>**: записывать отчет в файл, расположенный по указанному адресу.

Обязательный параметр.

Значение параметра по умолчанию – **syslog:kavmd@mail**.

Append=yes|no – режим записи отчета о работе центральной службы в файл:

- **yes** – добавлять новую информацию в существующий файл;
- **no** – создавать новый файл отчета при каждом запуске приложения.

Значение параметра по умолчанию – **yes**.

RotateRounds=0...UINT_MAX – максимальное количество формируемых в результате ротации отчетов. При превышении этого числа выполняется перезапись самого старого файла отчета. Ротация файла отчета происходит, если значение данного параметра больше 0.

Значение параметра по умолчанию – **10**.

RotateSize – максимальный размер файла отчета в байтах, при достижении которого формируется новый файл отчета.

Значение параметра по умолчанию – **1M**.

Внимание!

Параметры **Append**, **RotateRounds** and **RotateSize** вступают в действие, только если в качестве расположения отчета задан файл.

А.1.3. Секция *[kav4lms:server.statistics]*

Секция **[kav4lms:server.statistics]** содержит параметры формирования статистики работы приложения:

Options=none|all|messages|resources|viruses|filters|raw – категория информации для ведения статистики (см. п. 9.2 на стр. 94). Вы можете указать несколько категорий, разделенных запятой.

Например:

```
Options=none, raw
```

Обязательный параметр.

Значение параметра по умолчанию – **none**.

Format=xml|txt – формат, в котором выводится статистика.

Значение параметра по умолчанию – **xml**.

Destination=file:<путь_к_файлу> – расположение статистики центральной службы приложения. В текущей версии Антивируса Касперского поддерживается только файл.

Значение параметра по умолчанию –

file:/var/opt/kaspersky/kav4lms/stats/statistics.xml (для Linux)

file:/var/db/kaspersky/kav4lms/stats/statistics.xml (для FreeBSD).

RawDestination=file:<путь_к_файлу> – расположение детализированной статистики по каждому сообщению. В текущей версии Антивируса Касперского поддерживается только запись статистики в файл.

Обязательный параметр.

Значение параметра по умолчанию –

file:/var/opt/kaspersky/kav4lms/stats/statistics.raw (для Linux)

file:/var/db/kaspersky/kav4lms/stats/statistics.raw (для FreeBSD).

A.1.4. Секция *[kav4lms:server.snmp]*

Секция **[kav4lms:server.snmp]** содержит параметры, определяющие взаимодействие с приложением по протоколу SNMP:

SNMPServices=config|statistics|admin|update|all|none – информация, предоставляемая на чтение по SNMP- протоколу:

- **config**: информация по всем параметрам всех секций конфигурационного файла приложения;
- **statistics**: сводная статистическая информация по работе приложения;
- **admin**: информация по управлению работой приложения (время запуска, время бесперебойной работы и т.п.);
- **update**: информация об обновлении баз антивируса (дата последнего обновления, количество записей в базах и т.п.);
- **all**: вся статистическая информация и информация о конфигурации приложения;

- **none**: доступ к информации по SNMP- протоколу не предоставляется.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке.

Например:

```
SNMPServices=config
```

```
SNMPServices=admin
```

Обязательный параметр.

Значение параметра по умолчанию – **none**.

SNMPTraps=config|admin|update|all|none – события, при возникновении которых приложение отправляет SNMP-ловушки (traps):

- **config**: при изменении конфигурации приложения или успешном обновлении баз антивируса;
- **admin**: при запуске и остановке приложения либо возникновении критических ошибок в его работе, а также при обнаружении зараженных объектов в случае выполнения условия, заданного параметром **AlertThreshold**;
- **update**: при обновлении баз антивируса независимо от его результата;
- **all**: при возникновении всех перечисленных выше событий;
- **none**: отправка SNMP-ловушек отключена.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке.

Например:

```
SNMPTraps=config
```

```
SNMPTraps=admin
```

Обязательный параметр.

Значение параметра по умолчанию – **none**.

AlertThreshold=0...100 – количество зараженных сообщений (в процентах) по отношению к общему объему почтового трафика, обработанного приложением в течение часа, при достижении которого приложение отправляет SNMP-ловушку (при этом необходимо задать следующее значение параметра: **SNMPTraps=admin**).

Значение параметра по умолчанию – **10**.

Socket – сокет взаимодействия с мастер-агентом; допускается использование локального или сетевого сокета.

Формат записи:

`inet:<port>@<ip-address>` – для сетевого сокета;

`local:<path_to_socket>` – для локального сокета.

Где:

- **<port>**: порт взаимодействия;
- **<ip-address>**: IP-адрес;
- **<path_to_socket>**: путь к локальному сокету.

Примечание

Для локального сокета должен быть указан файл с именем «*master*», это обусловлено функциональностью SNMP. Поэтому в качестве **<path_to_socket>** следует задать абсолютный путь, включая имя файла «*master*».

Значение параметра по умолчанию – **inet:705@127.0.0.1**.

Timeout=0...UINT_MAX – тайм-аут (в секундах) на отправку запроса мастер-агенту.

Значение параметра по умолчанию – **5**.

Retries=0...UINT_MAX – количество попыток отправки запроса мастер-агенту.

Значение параметра по умолчанию – **10**.

Внимание!

Число попыток отправки запроса может отличаться от заданного значения **Retries**. Это происходит из-за активности утилиты *watchdog* и не является ошибкой.

PingInterval=0...UINT_MAX – интервал (в секундах), с которым суб-агент будет пытаться подключиться к мастер-агенту в случае разрыва соединения.

Значение параметра по умолчанию – **30**.

А.1.5. Секция

[kav4lms:server.notifications]

Секция **[kav4lms:server.notifications]** содержит параметры уведомлений:

ProductAdmins – почтовый адрес администратора Антивируса Касперского. Можно задавать несколько адресов через запятую.

Значение параметра по умолчанию – **postmaster**.

ProductNotify=fault|update|license|all|none – оповещать администратора Антивируса Касперского о наступлении событий:

- **fault** – критических ошибках;
- **update** – результатах обновления баз антивируса;
- **license** – окончании срока действия ключа и превышении заложенного в ключе лицензионного ограничения;
- **all** – обо всех событиях;
- **none** – отключить уведомление.

Можно указать несколько значений через запятую.

Обязательный параметр.

Значение параметра по умолчанию – **all**.

Subject – стандартный текст, отображаемый в поле **Тема (Subject)** уведомления.

Значение параметра по умолчанию – **Anti-virus notification message**.

Charset – название кодировки (набор знаков) отправляемых сообщений.

Значение параметра по умолчанию: **us-ascii**.

TransferEncoding – название алгоритма кодировки отправляемых уведомлений. Значение параметра по умолчанию: **7bit**.

NotifierRelay – адрес почтовой службы, отправляющей уведомление.

Формат записи:

```
NotifierRelay=<protocol>:<host>:<port>
```

Значение параметра по умолчанию – **smtp:127.0.0.1:25**.

NotifierQueue – директория хранения файлов очереди почтовой службы уведомлений.

Значение параметра по умолчанию –
/var/opt/kaspersky/kav4lms/nqueue/ (для Linux)
/var/db/kaspersky/kav4lms/nqueue/ (для FreeBSD).

NotifierTimeout=0...UINT_MAX – тайм-аут отправки уведомлений (в секундах).

Значение параметра по умолчанию: **5**.

NotifierPersistence=yes|no – необходимость поддержания активности соединения с почтовой службой уведомлений.

Значение параметра по умолчанию: **no**.

Templates – директория, содержащая шаблоны уведомлений администратора.

Значение параметра по умолчанию –
/etc/opt/kaspersky/kav4lms/templates-admin/en (для Linux),
/usr/local/etc/kaspersky/kav4lms/templates-admin/en (для FreeBSD).

A.1.6. Секция **[kav4lms:filter.settings]**

Секция **[kav4lms:filter.settings]** содержит параметры фильтра Антивируса Касперского:

RunAsUser – имя пользователя, с правами которого запускается служба фильтра.

Обязательный параметр.

Значение параметра по умолчанию – **kluser**.

Примечание

Если фильтр и главная служба установлены на одном компьютере, убедитесь, что параметр **RunAsUser** для этих компонентов имеет оно и тоже значение, что обеспечит корректный доступ к совместно используемым файлам.

RunAsGroup – имя группы, с правами которой запускается служба фильтра.

Обязательный параметр.

Значение параметра по умолчанию – **klusers**.

FilterSocket=inet:<port>@<ip-address>|local:<path_to_socket> – сокет (локальный или сетевой), по которому осуществляется передача данных между почтовой службой и фильтром Антивируса Касперского (конечная точка соединения «фильтр-почтовая система»).

Внимание!

Перед изменением данного параметра следует остановить службу фильтра; после изменения для применения нового значения параметра следует запустить службу.

Формат записи:

`FilterSocket=inet:<port>@<ip-address>` – для сетевого сокета;

`FilterSocket=local:<path_to_socket>` – для локального сокета.

Где:

- **<port>**: порт взаимодействия;
- **<ip-address>**: IP-адрес;
- **<path_to_socket>**: путь к локальному сокету.

Обязательный параметр.

Значение параметра по умолчанию – **inet:10025@127.0.0.1**.

Примечание

В случае использования локального сокета убедитесь, что каталог расположения файла сокета и сам файл сокета доступны для чтения и записи как службе фильтра, так и центральной службе приложения.

FilterSocketPerms – права доступа к **FilterSocket**, в случае использования локального сокета. Владелец сокета задается парой **RunAsUser:RunAsGroup**.

Значение параметра по умолчанию – **0600**.

ServiceSocket=inet:<port>@<ip-address>|local:<path_to_socket> – сокет (локальный или сетевой), по которому осуществляется передача данных между центральной службой и фильтром Антивируса Касперского (конечная точка соединения «фильтр-центральная служба»).

Внимание!

Перед изменением данного параметра следует остановить службу фильтра; после изменения для применения нового значения параметра следует запустить службу.

Формат записи аналогичен параметру **FilterSocket**.

Обязательный параметр.

Значение параметра по умолчанию –
local:/var/run/kav4lms/kavmd.sock.

AdminSocket=local:<path_to_socket> – локальный сокет, используемый для управления фильтром Антивируса (например, по протоколу SNMP).

Внимание!

Перед изменением данного параметра следует остановить службу фильтра; после изменения для применения нового значения параметра следует запустить службу.

Обязательный параметр.

Значение параметра по умолчанию –
local:/var/run/kav4lms/kavmdctl.sock.

Внимание!

При установке параметра убедитесь, что каталог расположения файла сокета и сам файл сокета доступны для записи только пользователю, с правами которого выполняется приложение.

AdminSocketPerms=0600 – права доступа к **AdminSocket**. Владелец сокета: **RunAsUser:RunAsGroup**.

Значение параметра по умолчанию – **0600**.

ForwardSocket=inet:<port>@<ip-address>|local:<path_to_socket> – сокет, по которому осуществляется передача данных между фильтром Антивируса Касперского и почтовой системой (конечная точка соединения «приложение-почтовая система»).

Внимание!

Перед изменением данного параметра следует остановить службу фильтра; после изменения для применения нового значения параметра следует запустить службу.

Формат записи аналогичен параметру **FilterSocket**.

Обязательный параметр.

Значение параметра по умолчанию – **inet:10026@127.0.0.1**.

Примечание

Параметр `ForwardSocket` используется при интеграции с Postfix или Exim.

FilterTimeout=0...UINT_MAX – тайм-аут (в секундах) обмена информацией между почтовой системой и фильтром. Если никаких команд или данных не пересылается в течение указанного периода, то соединение с почтовой службой будет закрыто.

Значение параметра по умолчанию – **600**.

FilterThreads=0...UINT_MAX – число потоков, используемых фильтром для приема запросов почтовой системы.

Значение параметра по умолчанию – **10**.

MaxMilterThreads=0...UINT_MAX – максимальное число потоков, одновременно запускаемых библиотекой Milter. Значение **0** соответствует отсутствию ограничения.

Значение параметра по умолчанию – **0**.

Внимание!

Данный параметр применяется только в случае работы приложения с Sendmail!

А.1.7. Секция `[kav4lms:filter.log]`

Секция `[kav4lms:filter.log]` включает параметры формирования отчетов о работе фильтра Антивируса Касперского:

- Options=<категория_функциональности>.<уровень_детализации>**
– категория сообщений о работе фильтра, фиксируемых в отчете, где:
- **<категория_функциональности>** может принимать одно из следующих значений: **all**, **config**, **app**, **scan**, **cfilter**, **backup**, **no-tif**, **admin**, **smtp** (см. п. 9.1 на стр. 91);
 - **<уровень_детализации>** может принимать одно из следующих значений: **debug**, **activity**, **info**, **warning**, **error**, **fatal** (см. п. 9.1 на стр. 91).

Вы можете указать несколько уровней, разделенных запятой.

Обязательный параметр.

Значение параметра по умолчанию – **all,-all.debug**.

Destination=syslog:<имя>@<категория>|file:<путь_к_файлу> – путь к файлу, в который будет записываться отчет о работе фильтра:

- **syslog:<имя>@<категория>**: записывать отчет в системный журнал; в качестве имени приложения использовать **<имя>**, в качестве категории (**syslog facility**) – **<категория>**.
- **file:<путь_к_файлу>**: записывать отчет в файл, расположенный по указанному адресу.

Обязательный параметр.

Значение параметра по умолчанию – **syslog:kav4lms-filters@mail**.

Append=yes|no – режим записи отчета о работе фильтра в файл:

- **yes** – добавлять новую информацию в существующий файл;
- **no** – создавать новый файл отчета при каждом запуске приложения.

Значение параметра по умолчанию – **yes**.

RotateRounds=0...UINT_MAX – максимальное количество формируемых в результате ротации отчетов. При превышении этого числа выполняется перезапись самого старого файла отчета. Ротация файла отчета происходит, если значение данного параметра больше 0.

Значение параметра по умолчанию – **10**.

RotateSize – максимальный размер файла отчета в байтах, при достижении которого формируется новый файл отчета.

Значение параметра по умолчанию – **1M**.

Внимание!

Параметры **Append**, **RotateRounds** and **RotateSize** вступают в действие, только если в качестве расположения отчета задан файл

А.1.8. Секция **[kav4lms:groups]**

Секция **[kav4lms:groups]** содержит ссылки на конфигурационные файлы групп:

_includes=<путь_к_директории> – путь к директории, хранящей конфигурационные файлы групп. В качестве пути следует использовать относительный путь к директории по сравнению с расположением главного конфигурационного файла приложения.

Обязательный параметр.

Значение параметра по умолчанию – **groups.d/**.

А.1.9. Секция **[path]**

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

BasesPath – полный путь к каталогу хранения баз антивируса.

Обязательный параметр.

Значение параметра по умолчанию –
/var/opt/kaspersky/kav4lms/bases (для Linux) и
/var/db/kaspersky/kav4lms/bases (для FreeBSD).

LicensePath – полный путь к директории хранения ключей приложения.

Обязательный параметр.

Значение параметра по умолчанию –
/var/opt/kaspersky/kav4lms/licenses (для Linux) и
/var/db/kaspersky/kav4lms/licenses (для FreeBSD).

PidPath – путь к файлу содержащему ID процесса центральной службы приложения.

Обязательный параметр.

Значение параметра по умолчанию – **/var/run/kav4lms/**.

TempPath – путь к директории хранения временных файлов. По заданному пути создаются поддиректории **.kav4lms-*<id>***.

Обязательный параметр.

Значение параметра по умолчанию – **/var/tmp/**.

iCheckerDBFile – путь к базе данных iChecker™.

Обязательный параметр.

Значение параметра по умолчанию –
/var/opt/kaspersky/kav4lms/iChecker.db (для Linux) и
/var/db/kaspersky/kav4lms/iChecker.db (для FreeBSD).

A.1.10. Секция *[locale]*

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

DateFormat – формат отображения даты в отчете о работе приложения.

Обязательный параметр.

Значение параметра по умолчанию – **%d-%m-%Y**.

TimeFormat – формат отображения времени в отчете.

Обязательный параметр.

Значение параметра по умолчанию – **%H:%M:%S**.

Примечание

Вы можете изменить формат представления времени на двенадцатичасовой (am, pm): **%I:%M:%S %P**.

Strings – путь к файлу, содержащему строковые константы, используемые при работе приложения. В качестве пути следует использовать относительный путь к файлу по сравнению с расположением главного конфигурационного файла приложения.

Обязательный параметр.

Значение параметра по умолчанию – **locale.d/strings.en**.

A.1.11. Секция *[options]*

Секция **[options]** содержит различные параметры приложения, не вошедшие в другие группы:

- **User** – системный пользователь, под которым работают компоненты приложения.

Обязательный параметр.

Значение параметра по умолчанию – **kluser**.

- **Group** – системная группа, под которой работают компоненты приложения.

Обязательный параметр.

Значение параметра по умолчанию – **klusers**.

A.1.12. Секция *[updater.path]*

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

BackUpPath=/var/opt/kaspersky/kav4lms/bases.backup/ – полный путь к директории хранения резервной копии баз антивируса.

A.1.13. Секция *[updater.options]*

Секция **[updater.options]** включает параметры, определяющие процесс обновления:

UpdateComponentsList – список компонентов, которые будут обновляться.

Значение параметра по умолчанию – **AVS, AVS_OLD, CORE, Updater, BLST**.

RetranslateComponentsList – список компонентов, для которых обновления будут сохраняться в сетевой директории.

Если значение параметра не задано (по умолчанию), используется значение параметра **UpdateComponentsList**.

KeepSilent=yes|no – режим вывода отчета об обновлении на консоль. Задайте параметру значение **yes**, если вы не хотите, чтобы отчет выводился на консоль.

Значение параметра по умолчанию – **no**.

UseUpdateServerUrl=yes|no – использовать в качестве ресурса обновлений сервер «Лаборатории Касперского», определяемый параметром **UpdateServerUrl**.

Значение параметра по умолчанию – **no**.

UpdateServerUrl=http://url/ftp://url//local_path/ – адрес сервера, используемого в качестве ресурса для обновлений.

По умолчанию значение параметра не задано.

UseUpdateServerUrlOnly=yes|no – параметр, определяющий будет ли приложение использовать для обновления только адрес, заданный параметром **UpdateServerUrl**. Если параметру присвоено значение **no**, то в случае неудачной попытки обновления баз с адреса **UpdateServerUrl** будет использован другой адрес из списка серверов обновлений.

Значение параметра по умолчанию – **no**.

RegionSettings – название региона пользователя; применяется для выбора наиболее удобного для скачивания обновлений баз антивируса с сервера обновлений «Лаборатории Касперского».

Значение параметра по умолчанию – **ru**.

ConnectTimeout – время в секундах, в течение которого выполняется соединение с источником обновления.

Значение параметра по умолчанию – **30**.

ProxyAddress – IP-адрес прокси-сервера, если таковой используется для выхода в интернет.

По умолчанию значение не задано.

UseProxy=yes|no – режим использования прокси-сервера при соединении с сервером обновлений. Если значению параметра присвоено **no**, прокси-сервер не используется. Если значению параметра присвоено **yes**, используется адрес прокси-сервера, определенный параметром **ProxyAddress**.

PassiveFtp=yes|no – режим использования пассивного режима работы FTP-сервера при загрузке обновлений по FTP.

По умолчанию значение параметра – **yes**.

Index=u0607g.xml – файл главного индекса системы обновления, в соответствии с которым выбирается набор обновлений на серверах «Лаборатории Касперского». Изменять значения этого параметра не рекомендуется.

IndexRelativeServerPath=index/6 – путь к файлу главного индекса системы обновления. В качестве пути следует использовать относительный путь к файлу по сравнению с расположением главного конфигурационного файла приложения. Изменять значения этого параметра не рекомендуется.

А.1.14. Секция *[updater.report]*

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

Append=yes|no – режим записи отчета о работе компонента *kav4lms-keepup2date* в файл:

- **yes** – добавлять новую информацию в существующий файл;
- **no** – создавать новый файл отчета при каждом запуске компонента; в этом случае файл отчета будет содержать только информацию о результатах последнего обновления.

Значение параметра по умолчанию – **yes**.

ReportFileName – полный путь к файлу, в котором будет храниться отчет о работе компонента *kav4lms-keepup2date*.

По умолчанию значение не задано.

ReportLevel=0|1|2|3|4|9 – уровень детализации отчета об обновлении (0 – Fatal, 1 – Error, 2 – Warning, 3 – Info, 4 – Activity, 9 – Debug).

Значение параметра по умолчанию – **3**.

А.1.15. Секция *[updater.actions]*

Секция **[updater.actions]** содержит действия, совершаемые по наступлению особых событий в ходе обновления:

OnAny – команда, выполняемая при наступлении любого события. По умолчанию выполняется уведомление других компонентов приложения о событии.

Значение параметра по умолчанию –

```
/opt/kaspersky/kav4lms/bin/kav4lms-cmd -m update -e  
%EVENT_NAME% (для Linux),  
/usr/local/bin/kav4lms-cmd -m update -e %EVENT_NAME% (для  
FreeBSD).
```

OnStarted – команда, выполняемая при запуске компонента *kav4lms-keepup2date*.

По умолчанию значение параметра не задано.

OnUpdated – команда, выполняемая при успешном завершении обновления.

По умолчанию будет перезапущено приложение –
`/opt/kaspersky/kav4lms/bin/kav4lms-cmd -x bases` (для Linux),
`/var/db/kaspersky/kav4lms/bin/kav4lms-cmd -x bases` (для
FreeBSD).

OnRetranslated – команда, выполняемая после успешной загрузки обновления баз из сетевой директории в директорию расположения баз, используемых Антивирусом.

По умолчанию значение параметра не задано.

OnNotUpdated – команда, выполняемая в случае, если обновление не было выполнено.

По умолчанию значение параметра не задано.

OnFailed – команда, выполняемая в случае аварийного завершения процесса обновления.

По умолчанию значение параметра не задано.

OnRolledBack – команда, выполняемая в случае, возврата к предыдущей версии баз антивируса.

По умолчанию значение параметра не задано.

OnBasesCheck – команда проверки корректности баз антивируса после обновления. По умолчанию запускается утилита проверки корректности баз антивируса `avbasesetest`, входящая в состав дистрибутива. Она проверяет скопированные с источника и размещенные во временной директории обновления. Если обновления не повреждены, они копируются в директорию расположения баз, используемых Антивирусом.

Примечание

Запуск утилиты `avbasesetest` выполняется автоматически и не требует вмешательства пользователя.

Значение параметра по умолчанию –
`/opt/kaspersky/kav4lms/lib/bin/avbasesetest`
`%TEMP_BASES_PATH% %BASES_PATH%` (для Linux),
`/usr/local/libexec/kaspersky/kav4lms/avbasesetest`
`%TEMP_BASES_PATH% %BASES_PATH%` (для FreeBSD).

Примечание

Вышеперечисленные параметры поддерживают следующие макросы:

- `%EVENT_NAME%` – имя события, запустившего команду;
- `%BASES_PATH%` – путь к текущей версии баз антивируса;
- `%TEMP_BASES_PATH%` – путь к временной директории, хранящей обновление баз антивируса;
- `%AVS_UPDATE_DATE%` – время наступления события в формате **ММ:ДД:ГГГГ ЧЧ:ММ:СС**.

А.1.16. Секция *[scanner.display]*

Секция **[scanner.display]** содержит параметры вывода отчета компонента *kav4lms-kavscanner* на консоль:

ShowContainerResultOnly=true|false – режим отображения на консоли результатов проверки архива. Для отображения результатов в кратком формате, присвойте параметру значение **true**. По умолчанию используется расширенный формат сообщений.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

ShowObjectResultOnly=true|false – режим отображения на консоли результатов проверки простого объекта. Для отображения результатов в кратком формате, присвойте параметру значение **true**. По умолчанию используется расширенный формат сообщений.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

ShowOK=true|false – режим вывода на консоль сообщений о незараженных файлах. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

ShowProgress=true|false – режим отражения на консоли текущей работы компонента (процесс загрузки баз антивируса, информация о проверке текущего файла). Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

A.1.17. Секция *[scanner.options]*

Секция **[scanner.options]** содержит параметры компонента *kav4lms-kavscanner*:

ExcludeDirs=маска1:маска2:...:маскаN – маски каталогов, которые исключаются из проверки. Маски задаются в виде стандартных shell-масок.

Значение параметра по умолчанию – **/dev:/udev:/proc**.

ExcludeMask=маска1:маска2:...:маскаN – маски файлов, которые исключаются из проверки; по умолчанию проверяются все файлы. Маски задаются в виде стандартных shell-масок.

Значение параметра по умолчанию – **не задано**.

Packed=true|false – режим проверки упакованных объектов. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

Archives=true|false – режим проверки архивов. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

Cure=true|false – режим лечения инфицированных объектов. Для включения режима присвойте параметру значение **true**.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

Heuristic=true|false – режим использования при проверке эвристического анализатора кода. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

LocalFS=true|false – режим проверки только локальной файловой системы. Для включения режима присвойте параметру значение **true**.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

MailBases=true|false – режим проверки почтовых баз. Для отключения режима присвойте параметру значение – **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

MailPlain=true|false – режим проверки почтовых сообщений в виде plain text. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

Packed=true|false – режим проверки упакованных файлов. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

Recursion=true|false – режим рекурсивного прохода директорий при проверке на присутствие вирусов. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

SelfExtArchives=true|false – режим проверки самораспаковывающихся архивов. Для отключения режима присвойте параметру значение **false**. Если включен режим проверки архивов (**Archives=true**), самораспаковывающиеся архивы будут проверены, даже если параметру **SelfExtArchives** присвоено значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

Ichecker=true|false – режим использования при антивирусной проверке технологии iChecker. Для отключения режима присвойте параметру значение **false**.

Значение параметра по умолчанию – **true**.

MaxLoadAvg – максимальная загрузка процессора. В случае превышения данного значения компонент *kav4lms-kavscanner* приостанавливает работу.

Значение параметра по умолчанию не задано.

UseAVbasesSet=standard|extended – набор баз антивируса, используемых при проверке. Набор **extended** помимо записей, содержащихся в наборе **standard**, содержит также описание потенциально опасных программ, таких как: рекламные программы, программы удаленного администрирования и т.п.

Значение параметра по умолчанию – **standard**.

FollowSymlinks=true|false – режим работы с символьными ссылками. Если параметру присвоено значение **true**, при проверке будут открываться ссылки и проверяться расположенные по указанному адресу объекты. Для отключения режима присвойте параметру значение **false**.

Значение параметра по умолчанию – **true**.

A.1.18. Секция *[scanner.report]*

Секция **[scanner.report]** содержит параметры формирования отчета о результатах работы компонента *kav4lms-kavscanner*.

Append=true|false – режим добавления новых сообщений в файл отчета о результатах антивирусной проверки файловой системы:

- **true** – добавлять новую информацию в существующий файл;
- **false** – создавать новый файл отчета при каждом запуске приложения.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента.

По умолчанию значение параметра не установлено.

ReportLevel=0|1|2|3|4|9 – уровень детализации отчета (**0** – Fatal, **1** – Error, **2** – Warning, **3** – Info, **4** – Activity, **9** – Debug).

Обязательный параметр.

Значение параметра по умолчанию – **4**.

ShowOK=true|false – режим вывода в отчет сообщений о незараженных файлах. Для отключения режима присвойте параметру значение **false**.

Обязательный параметр.

Значение параметра по умолчанию – **true**.

ShowContainerResultOnly=true|false – режим отображения в отчете результатов проверки архива в кратком формате. Для отображения краткого отчета присвойте параметру значение **true**.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

ShowObjectResultOnly=true|false – режим отображения в отчете результатов проверки простого объекта в кратком формате. Для отображения в кратком формате присвойте параметру значение **true**.

Обязательный параметр.

Значение параметра по умолчанию – **false**.

A.1.19. Секция *[scanner.container]*

Section **[scanner.container]** содержит параметры, определяющие действия над архивами при антивирусной защите файловых систем компьютера:

OnInfected=действие – действия в случае обнаружения зараженного файла. Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, вылечить которые не удалось.

Значение параметра по умолчанию не задано.

OnSuspicion=действие – действия в случае обнаружения подозрительного файла, код которого напоминает код угрозы, пока неизвестной «Лаборатории Касперского».

Значение параметра по умолчанию не задано.

OnWarning=действие – действия в случае обнаружения файла, код которого сходен с кодом известной угрозы.

Значение параметра по умолчанию не задано.

OnCured=действие – действия в случае обнаружения и успешного лечения зараженного объекта.

Значение параметра по умолчанию не задано.

OnProtected=действие – действия в случае обнаружения объекта, зашифрованного паролем. Такие объекты проверить невозможно.

Значение параметра по умолчанию не задано.

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

Значение параметра по умолчанию не задано.

OnError=действие – действия в случае возникновения при проверке объекта системной ошибки.

Значение параметра по умолчанию не задано.

Синтаксис параметра **действие** состоит из двух частей: непосредственно действия и его дополнительного параметра, разделяемых пробелом. Значение дополнительного параметра заключаются в кавычки.

Например:

```
OnInfected=move "/tmp/infected"
```

Действие может принимать одно из следующих значений:

- *move* <каталог> – переместить файл в <каталог>;
- *movePath* <каталог> – переместить файл в <каталог> рекурсивно (с абсолютным путем);
- *remove* – удалить файл;
- *exec* <параметр> – запустить внешнюю команду, заданную переменной <параметр>.

В качестве макросов дополнительного параметра действия **exec** для контейнеров используются:

- %VIRUSNAME% – имя обнаруженной угрозы или наименование ошибки.
- %LIST% – имя файла или список инфицированных, подозрительных и поврежденных файлов, обнаруженных в контейнере. Формат записи имеет следующий вид: <имя вируса>\t<имя файла>.
- %FULLPATH% – полный путь до контейнера.
- %FILENAME% – имя файла без пути.
- %CONTAINERTYPE% – тип контейнера в виде строки.

А.1.20. Секция [*scanner.object*]

Секция [*scanner.object*] содержит параметры, определяющие действия над простыми объектами того или иного типа при антивирусной защите файловой системы компьютера:

OnInfected=действие – действия в случае обнаружения зараженного файла. Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, вылечить которые не удалось.

Значение параметра по умолчанию не задано.

OnSuspicion=действие – действия в случае обнаружения подозрительного файла, код которого напоминает код угрозы, пока неизвестной «Лаборатории Касперского».

Значение параметра по умолчанию не задано.

OnWarning=действие – действия в случае обнаружения файла, код которого сходен с кодом известной угрозы.

Значение параметра по умолчанию не задано.

OnCured=действие – действия в случае обнаружения и успешного лечения зараженного объекта.

Значение параметра по умолчанию не задано.

OnProtected=действие – действия в случае обнаружения объекта, зашированного паролем. Такие объекты проверить невозможно.

Значение параметра по умолчанию не задано.

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

Значение параметра по умолчанию не задано.

OnError=действие – действия в случае возникновения при проверке объекта системной ошибки.

Значение параметра по умолчанию не задано.

Синтаксис параметра **действие** совпадает с синтаксисом параметра для секции [*scanner.container*] (см. п. А.1.19 на стр. 135).

В качестве макросов дополнительного параметра действия **exes** для простых объектов используются:

- **%VIRUSNAME%** – имя обнаруженной угрозы или наименование ошибки.

- %LIST% – имя инфицированного, подозрительного и поврежденного файла. Формат записи имеет следующий вид: <имя вируса>\t<имя файла>.
- %FULLPATH% – полный путь к файлу.
- %FILENAME% – имя файла без пути.

A.1.21. Секция *[scanner.path]*

Секция **[scanner.path]** содержит параметры, определяющие путь к файлам, без которых модуль *kav4lms-kavscanner* не будет функционировать:

BackupPath=путь – полный путь к каталогу хранения резервных копий проверяемых компонентом объектов.

Значение параметра по умолчанию не задано.

A.2. Конфигурационный файл группы

В данном разделе описан конфигурационный файл группы и приведены значения параметров, заданные в конфигурационном файле *default.conf* группы **Default**, включенном в состав дистрибутива приложения.

Параметры, заданные для группы **Default**, используются, если:

- не сформировано ни одной группы;
- ни отправитель, ни получатель сообщения не обнаружены ни в одной из сформированных групп;
- значение параметра в группе не определено.

Внимание!

Если конфигурационный файл группы создается на основе конфигурационного файла *default.conf* группы **Default**, не забудьте изменить название группы, входящее в названия секций конфигурационного файла.

А.2.1. Секция

[kav4lms:groups.<имя_группы>.definition]

Секция **[kav4lms:groups.<имя_группы>.definition]** содержит параметры идентификации группы:

Priority – приоритет группы; если почтовое сообщение соответствует нескольким группам, то оно будет обрабатываться по правилам той группы, приоритет которой выше. В качестве значения параметра может быть указано любое натуральное число. Не допускается создание групп с одинаковым приоритетом и приоритетом **0**.

Обязательный параметр.

Значение параметра для группы **Default – 0**.

Senders – список электронных адресов отправителей почтового сообщения. Каждый адрес должен быть указан на отдельной строке. Допускается использование масок и регулярных выражений (regular expressions).

Например:

```
Senders=user1@mycompany.com
Senders=reporter*@mycompany.com
Senders=re:office@.*\example\.com
```

Значение параметра для группы **Default** не задано.

Recipients – список электронных адресов получателей почтовых сообщений. Каждый адрес должен быть указан на отдельной строке. Допускается использование масок и регулярных выражений (regular expressions).

Например:

```
Recipients=user2@mycompany.com
Recipients=reporter*@mycompany.com
Recipients=re:office\d+@central\.mydomain\.com
```

Значение параметра для группы **Default** не задано.

Внимание!

Если значения параметров **Senders** и **Recipients** не заданы, то правила, заданные для группы, не применяются ни к одному сообщению. Если эти параметры отсутствуют в конфигурационном файле группы, их значения считывается из файла *default.conf*.

А.2.2. Секция

[kav4lms:groups.<имя_группы>.settings]

Секция **[kav4lms:groups.<имя_группы>.settings]** содержит параметры, определяющие политику проверки почтовых сообщений и правила добавления специальных заголовков:

Check=anti-virus|content-filter|all|none – режим проверки сообщений для группы.

Обязательный параметр.

Значение параметра для группы **Default – all**.

ScanPolicy=message|combined – политика проверки почтовых сообщений.

Обязательный параметр.

Значение параметра для группы **Default – message**.

ScanArchives=yes|no – режим проверки архивов. Для отключения режима присвойте параметру значение **no**.

Значение параметра для группы **Default – yes**.

ScanPacked=yes|no – режим проверки запакованных файлов. Для отключения режима присвойте параметру значение **no**.

Значение параметра для группы **Default – yes**.

UseAVBasesSet=standard|extended – набор баз антивируса, используемый приложением. Набор **extended** помимо записей, содержащихся в наборе **standard**, содержит также описание потенциально опасных программ, таких как: рекламные программы, программы удаленного администрирования, сетевые сканеры, вирусные симуляторы.

Значение параметра для группы **Default – standard**.

UseCodeAnalyzer=yes|no – режим использования во время проверки эвристического анализатора кода. Для отключения режима присвойте параметру значение **no**.

Значение параметра для группы **Default** – **yes**.

MaxScanTime – максимальное время (в секундах), допустимое для проверки сообщения или объекта. Если время проверки превышает заданное ограничение, проверка завершается с ошибкой.

Значение параметра для группы **Default** – **30**.

Примечание

Возможны случаи, когда общее время проверки сообщения превышает ограничение **MaxScanTime**, но ошибка не возникает. Это происходит, если выбрана политика проверки сообщений типа **combined**: общее время проверки сообщения складывается из времени проверки сообщения целиком и времен проверки отдельных частей сообщения.

MaxScanDepth=0...UINT_MAX – максимально допустимый для одного сообщения уровень вложенности MIME-объектов. В случае превышения заданного ограничения проверка завершается с ошибкой. Значение **0** означает, что ограничение отсутствует.

Значение параметра для группы **Default** – **10**.

MIMEEncodingHeuristics=yes|no – режим разборки MIME-объектов, не соответствующих RFC-стандартам.

По умолчанию фильтр передает на антивирусную проверку только сообщения, соответствующие RFC-стандартам. Если значение параметра **MIMEEncodingHeuristics** – **yes**, сообщение, не соответствующее RFC-стандартам, разбирается с использованием эвристических алгоритмов, и в случае успешной перекодировки передается на проверку. Если перекодировать сообщение не удалось или значение параметра **MIMEEncodingHeuristics** – **no**, сообщение на проверку не передается.

Значение параметра для группы **Default** – **no**.

Примечание

Использование данного параметра может несколько замедлить скорость проверки.

AddXHeaders=none|message|parts|all – режим использования информационных заголовков о результатах проверки почтового сообщения (подробнее см. п. 10.4 на стр. 107).

Обязательный параметр.

Значение параметра для группы **Default – message**.

AddDisclaimer=yes|no – режим использования дополнительного текста в проверенном почтовом сообщении или созданном в процессе обработки письма. Текст содержится в шаблоне *disclaimer* и добавляется в конец письма, никак не изменяя его исходное содержание. Вы можете редактировать текст уведомления.

Значение параметра для группы **Default – no**.

UsePlaceholderNotice=yes|no – режим использования сообщения, замещающего удаленный объект.

Значение параметра для группы **Default – yes**.

RejectReply – заголовок уведомления об отклоненном сообщении. При интеграции с qmail этот параметр не используется.

Значение параметра для группы **Default – Message rejected because it contains malware**.

A.2.3. Секция

[kav4lms:groups.<имя_группы>.actions]

Секция **[kav4lms:groups.<имя_группы>.actions]** содержит параметры, определяющие порядок обработки объектов почтовых сообщений по результатам антивирусной проверки:

InfectedAction=warn|drop|reject|cure|delete|skip – действие над зараженным объектом.

Обязательный параметр.

Значение параметра для группы **Default – skip**.

SuspiciousAction=warn|drop|reject|delete|skip – действие над объектом, который подозревается на заражение неизвестной угрозой.

Обязательный параметр.

Значение параметра для группы **Default – skip**.

ProtectedAction=warn|drop|reject|skip|delete – действие над защищенным (например, паролем) объектом, который не удалось проверить на присутствие угроз.

Обязательный параметр.

Значение параметра для группы **Default – skip**.

ErrorAction=warn|skip|delete – действие над поврежденным объектом или объектом, при проверке которого произошла ошибка.

Обязательный параметр.

Значение параметра для группы **Default – skip**.

VirusNameAction=warn|drop|reject – действие над почтовым сообщением или его частью, в случае обнаружения угроз, заданных параметром **VirusNameList**.

Обязательный параметр.

Значение параметра для группы **Default – drop**.

FilteredMimeAction=skip|delete|drop|reject|warn – действие над вложенным объектом, при проверке которого сработал фильтр по MIME-типу, заданный параметром **IncludeMime**.

Значение параметра для группы **Default – skip**.

FilteredNameAction=skip|delete|drop|reject|rename|warn – действие над вложенным объектом, имя которого соответствует маске, заданной параметром **IncludeName**.

Значение параметра для группы **Default – skip**.

FilteredSizeAction=skip|delete|drop|reject|warn – действие над вложенным объектом, размер которого соответствует значению, заданному параметром **IncludeSize**.

Значение параметра для группы **Default – skip**.

А.2.4. Секция

[kav4lms:groups.<имя_группы>.contentfiltering]

Секция **[kav4lms:groups.<имя_группы>.contentfiltering]** содержит параметры фильтрации вложений:

IncludeMime – маска-включение фильтрации по MIME-типу. Будут отфильтрованы те объекты, MIME-тип которых удовлетворяет заданным маскам и не попадает под действие масок в списке исключения (параметр **ExcludeMime**).

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Допускается использование специальных символов «*», «?» и регулярных выражений (regular expressions).

Например:

```
IncludeMime=application/octet-stream
IncludeMime=application/vnd.*
IncludeMime=re:image/. *
IncludeMime=re:multipart/(encrypted|signed)
```

Если значение параметра не указано или установлено пустое значение, фильтрация по MIME-типу не производится.

Для группы **Default** значение параметра не указано.

ExcludeMime – маска-исключение фильтрации по MIME-типу. Будут пропущены объекты, MIME-тип которых удовлетворяет заданным маскам.

Если список **ExcludeMime** задан, а список **IncludeMime** - нет, то будут отфильтрованы все объекты, маски которых не входят в список **ExcludeMime**.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Допускается использование специальных символов «*», «?» и регулярных выражений (regular expressions).

Например:

```
ExcludeMime=application/octet-stream
ExcludeMime=application/vnd.*
ExcludeMime=re:image/. *
ExcludeMime=re:multipart/(encrypted|signed)
```

Для группы **Default** значение параметра не указано.

IncludeName – маска-включение фильтрации по имени вложения. Будут отфильтрованы те объекты, чье имя удовлетворяет заданным маскам и не попадает под действие масок в списке исключения (параметр **ExcludeName**).

Если значение параметра не указано или установлено пустое значение, фильтрация по имени вложения не производится.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Допускается ис-

пользование специальных символов «*», «?» и регулярных выражений (regular expressions).

Например:

```
IncludeName=*accounting*
IncludeName=re:.*\.(doc|xls|ppt)
IncludeName=re:.*\.(pif|com|exe)
```

Для группы **Default** значение параметра не указано.

ExcludeName – маска-исключение фильтрации по имени вложения. Будут пропущены объекты, чье имя удовлетворяет заданным маскам.

Если список **ExcludeName** задан, а список **IncludeName** - нет, то будут отфильтрованы все объекты, маски которых не входят в список **ExcludeName**.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Допускается использование специальных символов «*», «?» и регулярных выражений (regular expressions).

Например:

```
ExcludeName=re:.*\.(txt|rtf)
ExcludeName=re:.*\.(doc|xls|ppt)
ExcludeName=re:.*\.(pif|com|exe)
```

Для группы **Default** значение параметра не указано.

IncludeSize – размер вложения почтового сообщения, подвергающегося фильтрации. Вы можете указать значение в байтах, например, **3456261**, либо использовать сокращенный формат записи, указав размерность величины: **10KB**, **100MB**. Чтобы отфильтровывать пустые вложения, присвойте параметру значение **0**.

Формат записи:

IncludeSize=размер_вложения – будут отфильтрованы вложения, размер которых совпадает с указанной величиной;

IncludeSize=<размер_вложения – будут отфильтрованы вложения, размер которых строго меньше указанной величины;

IncludeSize=<=размер_вложения – будут отфильтрованы вложения, размер которых меньше или равен указанной величине;

IncludeSize=>размер_вложения – будут отфильтрованы вложения, размер которых строго больше указанной величины;

IncludeSize=>=размер_вложения – будут отфильтрованы вложения, размер которых больше или равен указанной величине;

IncludeSize=0 – будут отфильтрованы все пустые вложения.

Если значение параметра не указано, фильтрация по размеру вложения не производится.

Для группы **Default** значение параметра не указано.

ExcludeSize – размер вложения почтового сообщения, не подвергающегося фильтрации. Формат записи аналогичен параметру **IncludeSize**. Чтобы пропускались пустые вложения, присвойте параметру значение **0**.

Для группы **Default** значение параметра не указано.

VirusNameList – список угроз, при обнаружении которых над почтовым сообщением или его объектом будет выполняться действие, заданное параметром **VirusNameAction**. Следует указать имя угрозы, как оно представлено в Вирусной энциклопедии на сайте www.viruslist.ru. Допускается использование масок и регулярных выражений. Чтобы указать несколько значений, перечислите их через запятую.

Например:

```
VirusNameList=re:trojan.*, backdoor*
```

Если значение параметра не задано, объекты будут обрабатываться в соответствии со статусом, присвоенным им при проверке.

Для группы **Default** значение параметра не задано.

RenameTo=<имя_файла>|.<расширение> – режим переименования объекта при выполнении действия **rename**:

- **RenameTo=<имя_файла>** – имя файла будет полностью заменяться указанным значением;
- **RenameTo=|.<расширение>** – к имени файла будет добавлено указанное расширение.

Например:

```
RenameTo=.vir
```

Файл *file.doc* будет переименован в *file.doc.vir*.

RenameTo=VIRUS-DO-NOT-OPEN

Файл *file.doc* будет переименован в *VIRUS-DO-NOT-OPEN*.

Если значение параметра не задано, объекты переименовываться не будут.

Значение параметра для группы **Default** – **.vir**.

А.2.5. Секция

[kav4lms:groups.<имя_группы>.notifications]

Секция **[kav4lms:groups.<имя_группы>.notifications]** содержит параметры уведомлений:

NotifySender=all|filtered|infected|protected|suspicious|error|none – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, при котором будет отправлено уведомление отправителю оригинального почтового сообщения.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Если задано пустое значение, то отправителю оригинального сообщения уведомление отправляться не будет.

Обязательный параметр.

Значение параметра для группы **Default** – **none**.

Примечание

Для того чтобы настроить приложение на отправку уведомлений при обнаружении объектов с различными статусами, создайте в конфигурационном файле несколько одноименных параметров **NotifySender**. Например:

```
NotifySender=filtered  
NotifySender=infected
```

Аналогично задаются значения параметров **NotifyRecipients** и **NotifyAdmin**.

NotifyRecipients=all|filtered|infected|protected|suspicious|error|none – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, при котором будет отправлено уведомление получателю оригинального почтового сообщения.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Если задано пустое значение, то получателю оригинального почтового сообщения уведомление отправляться не будет.

Обязательный параметр.

Значение параметра для группы **Default – all**.

NotifyAdmin=all|filtered|infected|protected|suspicious|error|none – статус почтового сообщения или его части, присвоенный в результате антивирусной проверки, при котором будет отправлено уведомление администратору на адрес, заданный параметром **AdminAddresses**.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке. Если задано пустое значение, то администратору уведомление отправляться не будет.

Обязательный параметр.

Значение параметра для группы **Default – none**.

AdminAddresses – электронный адрес администратора информационной безопасности. Вы можете указать несколько адресов через запятую.

Значение параметра для группы **Default – postmaster**.

Примечание

Параметр **AdminAddresses** задает адрес администратора информационной безопасности, в то время как параметр **ProductAdmins** в секции **[kav4lms:server.notifications]** файла *kav4lms.conf* задает адрес администратора Антивируса Касперского.

PostmasterAddresses – почтовый адрес, используемый приложением в качестве адреса отправителя уведомлений в поле **От (From)**.

Значение параметра для группы **Default – POSTMASTER@localhost**.

Templates – каталог хранения шаблонов уведомлений.

Значение параметра для группы **Default – /etc/opt/kaspersky/kav4lms/templates/en** (для Linux)
/usr/local/etc/kaspersky/kav4lms/templates/en (для FreeBSD).

Subject – заголовок стандартного уведомления, который добавляется в поле **Тема (SUBJECT)**.

Значение параметра для группы **Default – Anti-virus notification message**.

Charset – название кодировки (набор знаков), в которой формируется уведомление.

Значение параметра для группы **Default – us-ascii**.

TransferEncoding – название алгоритма кодировки отправляемых уведомлений.

Значение параметра для группы **Default – 7bit**.

UseCustomTemplates=yes|no – режим использования пользовательских шаблонов для формирования уведомлений. Для включения режима задайте **yes** в качестве значения параметра.

Значение параметра для группы **Default – no**.

SenderSubject – заголовок уведомления для отправителя.

Значение параметра для группы **Default – Anti-virus notification message**.

AdminSubject – заголовок уведомления для администратора информационной безопасности.

Значение параметра для группы **Default – Anti-virus notification message**.

A.2.6. Секция

[kav4lms:groups.<имя_группы>.backup]

Секция **[kav4lms:groups.<имя_группы>.backup]** содержит параметры, определяющие формирование резервных копий объектов почтовых сообщений перед любой их модификацией:

Policy=message|info|none – политика формирования резервных копий почтовых сообщений.

Значение параметра для группы **Default – info**.

Options=cured|deleted|dropped|rejected|warning|renamed|all – тип почтовых сообщений, для которых создаются резервные копии.

Вы можете задать несколько значений в виде списка, каждый параметр должен быть указан на отдельной строке.

Обязательный параметр.

Значение параметра для группы **Default – all**.

Destination – каталог хранения резервных копий почтовых сообщений, создаваемых приложением перед любой модификацией писем.

Значение параметра для группы **Default –**
/var/opt/kaspersky/kav4lms/backup/ (для Linux)
/var/db/kaspersky/kav4lms/backup/ (для FreeBSD).

A.3. Параметры командной строки компонента *kav4lms-licensemanager*

Опции помощи:	
-h	Вывести на консоль справочную информацию о компоненте <i>kav4lms-licensemanager</i> .
-v	Показать версию приложения
Опции работы с ключами:	
-s	Вывести на консоль информацию обо всех установленных ключах.
-c (-C) <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу> .
-k <путь_к_файлу>	Отобразить на консоли информацию о ключе <путь_к_файлу> .
-a <путь_к_файлу>	Установить ключ <путь_к_файлу> .
-d(a r)	Удалить активный ключ (опция -da) или удалить резервный ключ (опция -dr).
-i	Вывести на консоль детальную информацию об ограничениях ключа.

А.4. Коды возврата компонента *kav4lms-licensemanager*

В процессе работы компонент *kav4lms-licensemanager* может возвращать следующие коды:

0	Компонент успешно загрузил информацию о ключе и завершил свою работу.
30	При работе компонента возникла системная ошибка.
64	Информация отсутствует либо не найдено ни одного ключа по пути, указанному в конфигурационном файле.
65	Невозможно загрузить конфигурационный файл.
66	Неверная опция конфигурационного файла.
70	Компонент <i>kav4lms-licensemanager</i> поврежден.

A.5. Параметры командной строки компонента *kav4lms-keepup2date*

Опции помощи:	
-v	Вывести на консоль версию приложения и завершить работу компонента;
-h	Вывести на консоль справочную информацию о ключах командной строки, поддерживаемых компонентом и завершить работу компонента;
Опции работы:	
-r	Откат последнего обновления на предыдущую версию;
-s	Вывести на консоль список серверов обновлений;
-k	Не выполнять команду PostUpdateCmd после успешного завершения обновления баз антивируса.
-q	Режим работы компонента, при котором на консоль не выводится никаких системных сообщений.
-e	Режим работы компонента, при котором на консоль выводятся только сообщения о критических системных ошибках.
-b <путь>	При обновлении создавать копию имеющихся баз антивируса в каталоге <путь> .
-x <путь_к_файлу>	Копировать все обновления баз антивируса в локальный каталог <путь_к_файлу> .
-t <путь>	Использовать каталог <путь> для хранения временных файлов.

-u <путь_к_файлу>	Копировать последнее обновление баз антивируса в локальный каталог <путь_к_файлу>;
-c <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу>;
-g <URL>	Адрес для обновления баз антивируса. При определении этого ключа обновление будет производиться с указанного адреса.
-d <путь_к_файлу>	Использование rid-файла компонента, расположенного в локальном каталоге <путь_к_файлу>.
Опции формирования отчета:	
-l <путь_к_файлу>	Фиксировать результаты работы компонента в файле <путь_к_файлу>.

А.6. Коды возврата компонента

kav4lms-keepup2date

В процессе работы компонент *kav4lms-keepup2date* может возвращать следующие коды:

0	Обновления баз антивируса не требуется.
1	Обновление баз антивируса выполнено успешно.
10	Возникла критическая ошибка, процесс обновления прерывается.
12	Возникла ошибка при откате последней версии обновления баз антивируса.
30	Не удалось запустить команду PostUpdateCmd после обновления баз.
60	Информация отсутствует либо не найдено ни одного ключа по пути, указанному в конфигурационном файле.
75	Невозможно загрузить конфигурационный файл либо ошибка в его параметрах.

ПРИЛОЖЕНИЕ В. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

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

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

В.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

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

Новостной Агент также позволяет:

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

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

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в браузере. Таким образом, пользователи

могут максимально оперативно получать ответ на вопросы, связанные с заражением вредоносными программами. В рамках проверки пользователь может:

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

Kaspersky® OnLine Scanner Pro

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

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

Антивирус Касперского® 7.0

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

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

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

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе.* Программа позволяет создавать список приложений, компонентный состав которых будет

контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.

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

Kaspersky® Internet Security 7.0

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

Функции антивирусной защиты включают в себя:

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

темы и объектов, загружаемых при старте операционной системы Microsoft Windows;

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

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

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

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

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

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Symbian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

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

Антивирус Касперского для файловых серверов

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

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

Преимущества и функциональные возможности:

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

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуются их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;
- *ведение детальных отчетов*;
- *автоматическое обновление баз* программного продукта.

Kaspersky Open Space Security

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

Программный продукт включает в себя четыре продукта:

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

Рассмотрим подробнее каждый продукт.

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

Преимущества и функциональные возможности:

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

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

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

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз*;
- *использование технологии iSwift для исключения повторных проверок* в рамках сети;
- *распределение нагрузки между процессорами сервера*;

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

Kaspersky Enterprise Space Security

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

Преимущества и функциональные возможности:

- *защита рабочих станций и серверов от вирусов, троянских программ и червей*;
- *защита почтовых серверов Sendmail, Qmail, Postfix и Exim*;
- *проверка всех сообщений на сервере Microsoft Exchange*, включая общие папки;
- *обработка сообщений, баз данных и других объектов серверов Lotus Domino*;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *предотвращение массовых рассылок и вирусных эпидемий*;

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

Kaspersky Total Space Security

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

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама* на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *защита почтовых серверов и серверов совместной работы*;
- *проверка интернет-трафика* (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;

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

Kaspersky Security для почтовых серверов

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

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Антивирус Касперского для Lotus Domino.
- Антивирус Касперского для Microsoft Exchange.

Среди его возможностей:

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

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- [Kaspersky Administration Kit](#).
- [Антивирус Касперского для Proxy Server](#).
- [Антивирус Касперского для Microsoft ISA Server](#).
- [Антивирус Касперского для Check Point FireWall-1](#).

Среди его возможностей:

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

Kaspersky® Anti-Spam

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

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

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

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

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

В.2. Наши координаты

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

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр. 1
Факс:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей персональных и бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com

Общая информация:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru

ПРИЛОЖЕНИЕ С. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СТОРОННИХ ПРОИЗВОДИТЕЛЕЙ

Данный раздел содержит перечень программного обеспечения сторонних производителей, использованного при разработке Антивируса Касперского 5.6 для Linux Mail Server, и описание условий его использования.

С.1. Библиотека *Pcre*

Библиотека Pcre используется на следующих условиях:

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.2. Библиотека *Expat*

Библиотека Expat используется на следующих условиях:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

C.3. Библиотека **AgentX++v1.4.16**

Библиотека **AgentX++v1.4.16** используется на следующих условиях:

AGENTX++ LICENSE AGREEMENT

=====

THIS LICENSE AGREEMENT (this "Agreement") is made effective as of the date the product is installed by and between (i) Frank Fock, the author of AgentX++ ("LICENSOR") and the party executing this Agreement as Licensee ("LICENSEE").

1. DEFINITIONS.

1.1 The term "Software Product" means Frank Fock's AgentX++ computer software (including Source Code, derived Object Code, and derived Executable Code as defined in Section 1.3, 1.4, and 1.5) and documentation thereof, as specified in Exhibit A, that is provided by LICENSOR to LICENSEE hereunder, including bug fixes and updates thereto provided by LICENSOR to LICENSEE in connection with this Agreement. The term "derived" in the above context refers to the process of creating machine executable code from the original Source Code only. It does not refer to amendment or alteration of the original Source Code by LICENSOR or any third party.

1.2 The term "Intellectual Property Rights" means patent rights, copyright rights, trade secret rights, and any other intellectual property rights.

1.3 The term "Executable Code" is a fully compiled and linked program that contains any code derived from the Software Product. It can no longer be altered or combined with any other code. Executable code is ready to be executed by a computer and is essentially a complete software image for use in a specific product.

1.4 The term "Object Code" is any compiled version of the Software Product that can be linked and therefore combined with other code to create Executable Code. Examples of Object Code are libraries and software development kits, in particular SNMP agent development kits.

1.5 The term "Source Code" is the human readable form of the Software Product, as specified in Exhibit A.

1.6 Documentation means the documentation regarding the Licensed Software provided by LICENSOR to LICENSEE hereunder.

1.7 The term "Site" is a specific address belonging to a single business unit operating at that address.

2. GRANT OF LICENSE.

2.1 Source Code Site License. Subject to the terms and conditions of this Agreement, and upon payment by LICENSEE to LICENSOR of the one-time license fee set forth in Addendum A, LICENSOR grants LICENSEE a perpetual (subject to termination rights in Section 6), non-exclusive, non-transferable license to reproduce, use, modify, or have modified by a third party contractor (modifications in accordance to Section 2.6) subject to a confidentiality agreement no less restrictive than this Agreement, the Source Code for internal use only, for the sole purpose of developing AgentX-enabled SNMP agents at the Site (hereafter "Licensed Site") specified by LICENSEE during license purchase. Additionally, Customer's contractors and employees reporting directly and only to a manager at the Licensed Site, such as telecommuters, may use the Software Product at remote locations. Off-site employees reporting in any way to a manager at their location are not covered under this Site License.

2.2 Except as specified in 2.1, neither the Software Product Source Code nor Object Code derived from the Software Product may be redistributed or resold. Executable Code programs derived from the Software Product may be redistributed and resold without limitation and without royalty, provided that LICENSEE added significant functionality to those derived Executable Code programs. Functionality in this context refers to the program's behavior, not appearance.

2.3 No Sublicense Right. LICENSEE has no right to transfer, or sublicense the Licensed Software to any third party, except as specified in 2.2 and except if the third party takes over the business of LICENSEE.

2.4 Other Restrictions in License Grants. LICENSEE may not: (i) copy the Licensed Software, except as necessary to use the Licensed Software in accordance with the license granted under Section 2.1 and 2.2, and except for a reasonable number of backup copies.

2.5 No Trademark License. LICENSEE has no right or license to use any trademark of LICENSOR during or after the term of this Agreement.

2.6 Proprietary Notices. The Licensed Software is copyrighted. All proprietary notices incorporated in, marked on, or affixed to the Licensed Software by LICENSOR shall be duplicated by LICENSEE on all copies, in whole or in part, in any form of the Licensed Software and not be altered, removed, or obliterated on such copies.

2.7 Reservation. LICENSOR reserve all rights and licenses to the Licensed Software not expressly granted to LICENSEE under this Agreement.

2.8 Delivery. Upon execution of this Agreement, and payment of the amounts due and owing under this Agreement, LICENSOR will provide LICENSEE with one (1) copy of the Software Product by downloading from LICENSOR's Web site.

3. PRODUCT WARRANTY.

3.1. LICENSOR warrants to LICENSEE that, at the date of delivery of the Software Product to LICENSEE and for a period ending 90 days following the date of

delivery of the Software Product to LICENSEE the Software Product shall perform substantially in accordance with the published specifications and Documentation. If notified in writing by LICENSEE, LICENSOR may, at its option, correct significant program errors in the Software Product within a reasonable time period. THE FOREGOING PRODUCT WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHETHER IMPOSED BY CONTRACT, STATUTE, COURSE OF DEALING, CUSTOM OR USAGE OR OTHERWISE.

3.2. In no event shall LICENSOR be liable to LICENSEE, in excess of the price paid to LICENSOR by LICENSEE for the Software Product hereunder, for any breach of warranty or any claim, loss or damage arising from or relating to the installation, use or performance of the Software Product (including, without limitation, any indirect, special, incidental or consequential damages).

3.3. LICENSOR reserves the right at any time to make changes to the Software Product.

3.4. IN NO EVENT SHALL LICENSOR BE LIABLE (WHETHER IN TORT, NEGLIGENCE, CONTRACT, WARRANTY, PRODUCT LIABILITY OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS OF PROFITS OR SAVINGS ARISING OUT OF ITS PERFORMANCE OR NONPERFORMANCE OF TERMS OF THIS AGREEMENT OR THE USE, INABILITY TO USE OR RESULTS OF USE OF THE SOFTWARE PRODUCT EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 In no event will LICENSOR be liable for any third-party products used with, or installed in, the Software Product. LICENSOR does not warrant the compatibility of the Software Product with any third-party products, whether hardware or software.

3.6 The above sections do not apply for liability for damages caused by gross negligence or wilful default.

3.7 General Provision. This warranty shall not apply in any case of amendment or alterations of the Software Product made by LICENSEE.

4. INTELLECTUAL AND PROPERTY INDEMNIFICATION.

4.1. LICENSOR agrees to indemnify and hold LICENSEE harmless from any final award of costs and damages against LICENSEE for any action based on infringement of any German intellectual property rights as a result of the use of the Licensed Software: (i) under the terms and conditions specified herein; (ii) under normal use; and (iii) not in combination with other items; provided that LICENSOR is promptly notified in writing of any such suit or claim against

LICENSEE and further provided that LICENSEE permits LICENSOR to defend, compromise or settle the same and gives LICENSOR all available information, reasonable assistance and authority to enable LICENSOR to do so. LICENSOR'S LIABILITY TO LICENSEE PURSUANT TO THIS ARTICLE IS LIMITED TO THE TOTAL FEES PAID BY LICENSEE TO LICENSOR IN THE CALENDAR YEAR IN WHICH ANY FINAL AWARD OF COSTS AND DAMAGES IS DUE AND OWING.

5. TRADE SECRETS AND PROPRIETARY INFORMATION.

5.1. LICENSEE acknowledges that LICENSOR is the owner of the Software Product, that the Software Product is confidential in nature and not in the public domain, that LICENSOR claims all intellectual and industrial property rights granted by law therein and that, except as set forth herein, LICENSOR does not hereby grant any rights or ownership of the Software Product to LICENSEE or any third party. Except as set forth herein, LICENSEE agrees not to copy or otherwise reproduce the Software Product, in whole or in part, without LICENSOR's prior written consent. LICENSEE further agrees to take all reasonable steps to ensure that no unauthorized persons shall have access to the Software Product and that all authorized persons having access to the Software Product shall refrain from any such disclosure, duplication or reproduction except to the extent reasonably required in the performance of LICENSEE'S rights under this Agreement.

5.2. LICENSEE agrees to accord the Software Product and the Documentation and all other confidential information relating to this Agreement the same degree and methods of protection as LICENSEE undertakes with respect to its confidential information, trade secrets and other proprietary data.

5.3. LICENSEE agrees not to challenge, directly or indirectly, the right, title and interest of LICENSOR in and to the Software Product, nor the validity or enforceability of LICENSOR's rights under applicable law. LICENSEE agrees not to directly or indirectly, register, apply for registration or attempt to acquire any legal protection for the Software Product or any proprietary rights therein or to take any other action which may adversely affect LICENSOR's right, title or interest in or to the Software Product in any jurisdiction.

5.4. LICENSEE acknowledges that, in the event of a material breach by LICENSEE of its obligations under this Article 5, LICENSOR may immediately terminate this Agreement, without liability to LICENSEE and may bring an appropriate legal action to enjoin any such breach hereof, and shall be entitled to recover from LICENSEE reasonable legal fees and costs in addition to other appropriate relief.

5.5. LICENSEE agrees to notify LICENSOR immediately and in writing of all circumstances surrounding the unauthorized possession or use of the Software Product and Documentation by any person or entity. LICENSEE agrees to cooperate fully with LICENSOR in any litigation relating to or arising from such unauthorized possession or use.

6. TERMINATION.

6.1. LICENSOR may terminate this Agreement at any time after the occurrence of any of the following events if LICENSOR provides 30 days notice of its intention to terminate as a result of the occurrence and LICENSEE fails to cure such occurrence within such 30 days:

(a) LICENSEE is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors of LICENSEE;

(b) LICENSEE assigns or transfers this Agreement or any of its rights to obligations hereunder, without LICENSOR's prior written consent; or (c) LICENSEE violates any material provision of this Agreement, including without limitation, the payment obligations set forth in Addendum A.

6.2. LICENSEE may terminate this Agreement at any time after the occurrence of any of the following events if LICENSEE provides 30 days notice of its intention to terminate as a result of the occurrence and LICENSOR fails to cure such occurrence within such 30 days:

(a) LICENSOR is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors or LICENSOR; or

(b) LICENSOR violates any material provision of this Agreement.

6.3. Upon the termination of this Agreement for any reason, LICENSEE will discontinue all use of the Software Product and, within ten (10) days after termination, will destroy or delete all copies of the Software Product then in its possession, including but not limited to, any back-up or archival copies of the Software Product and Documentation. At LICENSOR's request, LICENSEE will verify in writing to LICENSOR that such actions have been taken.

6.4. No termination of this Agreement for any reason whatsoever shall in any way affect the continuing obligations of the parties under Articles 5 hereof.

7. APPLICABLE LAW

This LICENSE shall be deemed to have been made in, and shall be construed pursuant to, the laws of Germany, without reference to conflicts of laws principles. All controversies and disputes arising out of or relating to this Agreement shall be submitted to the exclusive jurisdiction of Esslingen am Neckar, Germany, as long as LICENSEE is deemed to be a merchant (as defined by Handelsgesetzbuch, §1-7). The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

8. GENERAL PROVISIONS.

8.1. This Agreement does not create any relationship of association, partnership, joint venture or agency between the parties.

8.2. This Agreement (including the Exhibit and Addendum attached to the Agreement) sets forth the entire agreement and understandings between the parties hereto with respect to the subject matter hereof. This Agreement merges all previous discussions and negotiations between the parties and supersedes and replaces any and every other agreement, which may have existed between LICENSOR and LICENSEE with respect to the contents hereof.

8.3. Except to the extent and in the manner specified in this Agreement, any modification or amendment of any provision of this Agreement must be in writing and bear the signature of the duly authorized representative of each party.

8.4. The failure of either party to exercise any right granted herein, or to require the performance by the other party hereto of any provision of this Agreement, or the waiver by either party of any breach of this Agreement, shall not prevent a subsequent exercise or enforcement of such provisions or be deemed a waiver of any subsequent breach of the same or any other provision of this Agreement.

8.5. Except in the case of merger, acquisition or the sale of substantial assets or equity of Licensee or assignment to any direct or indirect subsidiary or affiliate of LICENSEE, LICENSEE shall not sell, assign or transfer any of its rights, duties or obligations hereunder without the prior written consent of LICENSOR. LICENSOR reserves the right to assign or transfer this Agreement or any of its rights, duties and obligations hereunder, to any direct or indirect subsidiary or affiliate of LICENSOR.

8.6. All notices required by this Agreement must be sent by certified mail in order to be deemed effective when sent to the following:

FOR LICENSOR:

Frank Fock

Schlossstrasse 8

73765 Neuhausen, Germany

EXHIBIT A

Licensed Software

AgentX++

a. Source Code - (ANSI C++ for Linux, Solaris, Win32) Includes AgentX++ and Agent++Win32 Source Code.

b. Executable Code - AgentX++Win32 Master Agent (Win XP/2000/NT4)

ADDENDUM A

For evaluation purposes and non commercial use only, a free license is granted, provided that the LICENSEE accepts this license agreement.

In order to obtain a license to use AgentX++ in a commercial environment,

LICENSEE has to purchase a commercial license from LICENSOR. The actual pricing list and other related information can be found at <http://www.agentpp.com>

C.4. Библиотека *Agent++v3.5.28a*

Библиотека Agent++v3.5.28a используется на следующих условиях:

AGENT++ API Version 3.x

Copyright (C) 2001 Frank Fock, Jochen Katz

LICENSE AGREEMENT

WHEREAS, Frank Fock and Jochen Katz are the owners of valuable intellectual property rights relating to the AGENT++ API and wish to license AGENT++ subject to the terms and conditions set forth below; and WHEREAS, you ("Licensee") acknowledge that Frank Fock and Jochen Katz have the right to grant licenses to the intellectual property rights relating to AGENT++, and that you desire to obtain a license to use AGENT++ subject to the terms and conditions set forth below; Frank Fock and Jochen Katz grants Licensee a non-exclusive, non-transferable, royalty-free license to use AGENT++ and related materials without charge provided the Licensee adheres to all of the terms and conditions of this Agreement.

By downloading, using, or copying AGENT++ or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of Germany, and to all of the terms and conditions of this Agreement, and agrees to take all necessary steps to ensure that the terms and conditions of this Agreement are not violated by any person or entity under the Licensee's control or in the Licensee's service.

Licensee shall maintain the copyright and trademark notices on the materials within or otherwise related to AGENT++, and not alter, erase, deface or overprint any such notice.

Except as specifically provided in this Agreement, Licensee is expressly prohibited from copying, merging, selling, leasing, assigning, or transferring in any manner, AGENT++ or any portion thereof.

Licensee may copy materials within or otherwise related to AGENT++ that bear the author's copyright only as required for backup purposes or for use solely by the Licensee.

Licensee may not distribute in any form of electronic or printed communication the materials within or otherwise related to AGENT++ that bear the author's copyright, including but not limited to the source code, documentation, help files, examples, and benchmarks, without prior written consent from the authors. Send any requests for limited distribution rights to sales@agentpp.com.

Licensee hereby grants a royalty-free license to any and all derivatives based upon this software code base, that may be used as a SNMP agent development environment or a SNMP agent development tool.

Licensee may modify the sources of AGENT++ for the Licensee's own purposes. Thus, Licensee may not distribute modified sources of AGENT++ without prior written consent from the authors.

The Licensee may distribute binaries derived from or contained within AGENT++ provided that:

- 1) The Binaries are not integrated, bundled, combined, or otherwise associated with a SNMP agent development environment or SNMP agent development tool; and
- 2) The Binaries are not a documented part of any distribution material.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.5. Библиотека *Boost v 1.0*

Библиотека Boost v 1.0 используется на следующих условиях:

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT

SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE

FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER

DEALINGS IN THE SOFTWARE.

C.6. Библиотека *Milter*

Библиотека *Milter* используется на следующих условиях:

The following license terms and conditions apply, unless a different license is obtained from Sendmail, Inc., 6425 Christie Ave, Fourth Floor, Emeryville, CA 94608, USA, or by electronic mail at license@sendmail.com.

License Terms:

Use, Modification and Redistribution (including distribution of any modified or derived work) in source and binary forms is permitted only if each of the following conditions is met:

1. Redistributions qualify as "freeware" or "Open Source Software" under one of the following terms:

a) Redistributions are made at no charge beyond the reasonable cost of materials and delivery.

b) Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means the complete compilable and linkable source code of sendmail including all modifications.

2. Redistributions of source code must retain the copyright notices as they appear in each source code file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 1998-2004 Sendmail, Inc. All rights reserved."

4. Neither the name of Sendmail, Inc. nor the University of California nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. The name "sendmail" is a trademark of Sendmail, Inc.

5. All redistributions must comply with the conditions imposed by the University of California on certain embedded code, whose copyright notice and conditions for redistribution are as follows:

a) Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

b) Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

i. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

ii. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

iii. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

6. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY SENDMAIL, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C.7. Библиотека *libkavexim.so*

Библиотека *libkavexim.so* распространяются под лицензией GPLv2 и используется на следующих условиях:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into an-

other language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General

Public License instead of this License.