

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского® 5.5 для Linux и
FreeBSD Workstation и File Server

РУКОВОДСТВО
АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ
LINUX И FREEBSD WORKSTATION И FILE SERVER

Руководство администратора

© ЗАО "Лаборатория Касперского"
Тел./факс: +7 (495) 797-87-00
<http://www.kaspersky.ru>

Дата редакции: сентябрь 2006 года

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	6
1.1. Компьютерные вирусы и вредоносные программы	7
1.2. Назначение и основные функции Антивируса Касперского	8
1.3. Что нового в версии 5.5	9
1.4. Схема лицензирования	10
1.5. Аппаратные и программные требования к системе	10
1.6. Комплект поставки.....	11
1.6.1. Лицензионное соглашение.....	12
1.6.2. Регистрационная карточка	12
1.7. Сервис для зарегистрированных пользователей.....	13
1.8. Принятые обозначения.....	13
ГЛАВА 2. АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ.....	15
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО.....	17
3.1. Установка приложения на компьютер под управлением Linux	17
3.2. Установка приложения на компьютер под управлением FreeBSD	18
3.3. Процесс установки	18
3.4. Процесс обновления приложения до версии 5.5.....	19
3.5. Установка лицензионного ключа	19
3.6. Расположение файлов приложения по каталогам	20
3.7. Завершение установки	23
ГЛАВА 4. НАСТРОЙКА ПРИЛОЖЕНИЯ ПОСЛЕ УСТАНОВКИ.....	24
4.1. Настройка приложения по умолчанию	24
4.2. Установка антивирусных баз	25
4.3. Настройка совместной работы с Webmin	25
ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО.....	27
5.1. Обновление антивирусных баз	27
5.1.1. Новые возможности компонента обновлений	28
5.1.2. Автоматическое обновление антивирусных баз	30
5.1.3. Обновление антивирусных баз по требованию	31

5.1.4. Создание сетевого каталога для хранения и копирования антивирусных баз.....	32
5.2. Антивирусная защита файловых систем.....	33
5.2.1. Область проверки.....	34
5.2.2. Режим проверки и лечения объектов.....	35
5.2.3. Действия над объектами.....	36
5.2.4. Проверка по требованию отдельного каталога.....	37
5.2.5. Проверка по расписанию.....	38
5.2.6. Дополнительные возможности: использование скрипт-файлов.....	38
5.2.6.1. Лечение зараженных объектов в архиве.....	38
5.2.6.2. Отправка администратору уведомления.....	39
5.3. Антивирусная защита в режиме реального времени.....	40
5.4. Управление лицензионными ключами.....	41
5.4.1. Просмотр информации о лицензионном ключе.....	42
5.4.2. Продление лицензии.....	43
ГЛАВА 6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА.....	45
6.1. Оптимизация работы Антивируса Касперского.....	45
6.2. Перенос объектов в карантинный каталог.....	47
6.3. Режим резервного копирования объектов (backup).....	48
6.4. Локализация отображаемого формата даты и времени.....	49
6.5. Параметры формирования отчета Антивируса Касперского.....	50
ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО.....	52
ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА.....	53
ПРИЛОЖЕНИЕ А. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ПРИЛОЖЕНИИ.....	55
A.1. Конфигурационный файл Антивируса Касперского.....	55
A.2. Ключи командной строки компонента kavscanner.....	63
A.3. Коды возврата компонента kavscanner.....	66
A.4. Ключи командной строки компонента kavmonitor.....	67
A.5. Ключи командной строки компонента licensemanager.....	68
A.6. Коды возврата компонента licensemanager.....	68
A.7. Ключи командной строки компонента keepup2date.....	69
A.8. Коды возврата компонента keepup2date.....	70
ПРИЛОЖЕНИЕ В. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ.....	72

ПРИЛОЖЕНИЕ С. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"	79
С.1. Другие разработки Лаборатории Касперского	80
С.2. Наши координаты	87

ГЛАВА 1. ВВЕДЕНИЕ

С увеличением количества людей, пользующихся компьютером, и возможностей обмена между ними данными по электронной почте и через интернет возросла угроза заражения компьютера вирусами, а также порчи или хищения информации прочими вредоносными программами.

Среди источников проникновения вредоносных программ наиболее опасными являются:

Интернет

Глобальная информационная сеть является основным источником распространения любого рода вредоносных программ. Как правило, вирусы и другие вредоносные программы размещаются на популярных веб-сайтах интернета, "маскируются" под полезное и бесплатное программное обеспечение. Множество скриптов, запускаемых автоматически при открытии веб-сайтов, могут также содержать в себе вредоносные программы.

Электронная почтовая корреспонденция

Почтовые сообщения, поступающие в почтовый ящик пользователя и хранящиеся в почтовых базах, могут содержать в себе вирусы. Вредоносные программы могут находиться как во вложении письма, так и в его теле. Как правило, электронные письма содержат вирусы и почтовые черви. При открытии письма, при сохранении на диск вложенного в письмо файла вы можете заразить данные на вашем компьютере.

Уязвимости в программном обеспечении

Так называемые "дыры" в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к вашему компьютеру, а, следовательно, к вашим данным, к доступным вам ресурсам локальной сети, к другим источникам информации.

В среде Unix-систем вирусы распространены значительно меньше, чем, например, в среде Windows ввиду особенности данных платформ. Однако это не означает, что угроза информационной безопасности для пользователей операционных систем Unix отсутствует. Рассмотрим подробнее виды вредоносных программ.

1.1. Компьютерные вирусы и вредоносные программы

Чтобы знать, какого рода опасности могут угрожать вашим данным, полезно узнать, какие бывают вредоносные программы и как они работают. В целом вредоносные программы можно разделить на следующие три класса:

- **Черви (Worms)** – данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

- **Вирусы (Viruses)** – программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – *заражение*. Скорость распространения вирусов несколько ниже, чем у червей.
- **Троянские программы (Trojans)** – программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ в среде Unix-систем, стали *черви* и *троянские программы*.



Далее по тексту Руководства в качестве обозначения вирусов, троянских программ и червей мы будем использовать термин "вирус". Акцент на конкретный вид вредоносной программы будет делаться только в случае, когда это необходимо.

1.2. Назначение и основные функции Антивируса Касперского

Программное приложение **Антивирус Касперского®** для Linux и FreeBSD Workstation и File Server (далее также *Антивирус Касперского, Приложение*) предназначен для антивирусной защиты файловых серверов и рабочих станций, работающих под управлением операционных систем Linux или FreeBSD.

Антивирус Касперского для Linux и FreeBSD позволяет:

- *Осуществлять постоянную защиту файловой системы от вредоносного кода:* перехватывать обращения к файлам; анализировать их; лечить или удалять зараженные объекты.
- *Проверять объекты по требованию:* искать зараженные и подозрительные файлы (в том числе и в заданных областях проверки); анализировать их; лечить или удалять зараженные объекты.
- *Помещать подозрительные и поврежденные объекты на карантин:* сохранять подозрительные файлы в карантинном каталоге.
- *Создавать копию зараженного объекта в резервном хранилище перед лечением и удалением* в целях возможного восстановления объекта, если он представляет информационную ценность.
- *Обновлять антивирусные базы;* ресурсом для обновления баз являются сервера обновлений Лаборатории Касперского. Также есть возможность настроить приложение на обновление баз из локального каталога.
- *Управлять и конфигурировать Антивирус Касперского* через конфигурационный файл приложения и веб-интерфейс программы Webmin.

1.3. Что нового в версии 5.5

В версии **Антивируса Касперского 5.5 для Linux и FreeBSD Workstation и File Server** по сравнению с версией 5.0 произведены следующие изменения:

- В состав приложения добавлен новый компонент *kavmonitor*, обеспечивающий антивирусную защиту файлов в режиме реального времени.
- Внедрены новые технологии получения обновлений антивирусных баз и программных модулей приложения, в том числе проверка целостности и возможности использования скачиваемых баз. Это позволяет существенно экономить сетевой трафик.
- Добавлена возможность выбора варианта скачиваемых антивирусных баз (стандартный или расширенный набор). При этом для каждого компонента приложения можно отдельно задать используемый набор баз.
- Упрощена процедура установки и удаления приложения.
- При установке приложения стал возможен импорт настроек предыдущих версий Антивируса (версии 5.0). Это позволяет существенно ускорить процесс получения работоспособной конфигурации.
- Появилась возможность создания резервного хранилища (backup-хранилища) для хранения копий подозрительных или зараженных объектов перед их лечением или удалением. Это позволяет избежать потери исходных данных в случае возникновения нештатных ситуаций в процессе лечения объекта.
- Для снижения нагрузок на процессор при осуществлении антивирусной проверки внедрены технологии использования базы данных iChecker™ и двухуровневого кеширования проверенных объектов.
- Добавлена возможность ограничения количества одновременно проверяемых в фоновом режиме объектов, что позволяет оптимизировать загрузку компьютера.
- Добавлена возможность генерации списка обнаруживаемых вирусов.
- Расширен набор возможных действий при обнаружении объектов различных статусов.
- Реализована поддержка приложением 64-битной платформы.
- Расширены опции антивирусной проверки по требованию.

1.4. Схема лицензирования

Политика лицензирования Антивируса Касперского предполагает ограничения на использование приложения по **времени использования** (как правило, на срок в один год со дня приобретения приложения).

1.5. Аппаратные и программные требования к системе

Для работы Антивируса Касперского необходимо соответствие системы следующим аппаратным и программным требованиям:

- Аппаратные требования:
 - Процессор Intel Pentium® 133 МГц или выше.
 - 64 МБ оперативной памяти.
 - 100 МБ на жестком диске для установки приложения и хранения временных файлов.
- Программные требования:
 - Для 32-битной платформы одна из следующих операционных систем:
 - RedHat Linux 9.0.
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Enterprise Server 9.0 SP3.
 - Novell Linux Desktop 9.
 - SUSE Linux Professional 10.1.
 - Debian GNU/Linux версия 3.1 R2.
 - Mandriva 2006.
 - FreeBSD version 4.11.
 - FreeBSD version 5.4.
 - FreeBSD version 6.1.

- Для 64-битной платформы одна из следующих операционных систем:
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Professional 10.1.
 - SUSE LES 9 SP3.
- Программа Webmin (www.webmin.com) – для удаленного администрирования Антивируса Касперского.
- Интерпретатор языка Perl версии 5.0 или выше (www.perl.org).
- Установленная утилита which.
- Установленные пакеты для компиляции программ (gcc, binutils, glibc-devel, make, ld), а также установленный исходный код ядра операционной системы – для использования компонента *kavmonitor*.



Обратите внимание, что Антивирус Касперского не поддерживает совместную работу с SELinux. Использование SELinux может привести к появлению различных видов предупреждений в системном файле отчета приложения.

1.6. Комплект поставки

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

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

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта.
- Руководство пользователя.
- Лицензионный ключ, записанный на специальную дискету.
- Регистрационная карточка (с указанием серийного номера продукта).
- Лицензионное соглашение.



Перед тем как распечатать конверт с компакт-диском (или с дискетами), внимательно ознакомьтесь с Лицензионным соглашением.

При покупке Антивируса Касперского в интернет-магазине вы копируете продукт с веб-сайта Лаборатории Касперского, в дистрибутив которого помимо самого продукта включено также данное Руководство. Лицензионный ключ будет вам отправлен по электронной почте по факту оплаты.

1.6.1. Лицензионное соглашение

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

Внимательно прочитайте Лицензионное соглашение!

Если вы не согласны с условиями Лицензионного соглашения, вы можете вернуть коробку с продуктом дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за продукт. При этом конверт с установочным компакт-диском (или с дискетами) должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском (или с дискетами), вы тем самым принимаете все условия Лицензионного соглашения.

1.6.2. Регистрационная карточка

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

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

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

1.7. Сервис для зарегистрированных пользователей

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

Приобретая лицензию, вы становитесь зарегистрированным пользователем программы и в течение срока действия лицензии 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").



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

1.8. Принятые обозначения

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

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

Оформление	Смысловое назначение
 Внимание!	Информация, на которую следует обратить особое внимание.
 <i>Чтобы выполнить действие,</i> <ol style="list-style-type: none"> 1. Шаг 1. 2. ... 	Описание последовательности выполняемых пользователем шагов и возможных действий.
 Задача, пример	Постановка задачи, примера для реализации возможностей программного продукта
 Решение	Реализация поставленной задачи
[ключ] – назначение ключа.	Ключи командной строки.
Текст информационных сообщений и командной строки	Текст конфигурационных фай, информационных сообщений программы и командной строки.

ГЛАВА 2. АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ

Прежде чем приступить к изучению функциональных возможностей Антивируса Касперского, рассмотрим подробнее его внутреннюю архитектуру. Это поможет получить наиболее полное представление об алгоритме работы Антивируса.

Антивирус Касперского включает в себя:

- Компонент антивирусной проверки по требованию *kavscanner*;
- Компонент антивирусной проверки в режиме реального времени *kavmonitor*;
- Модуль обновления антивирусных баз *keepup2date*;
- Утилиту работы с лицензионными ключами *licensemanager*;
- *Модуль удаленного управления* к программе Webmin.

Рассмотрим подробнее алгоритм работы приложения на примере антивирусной защиты в реальном времени (то есть с помощью компонента *kavmonitor*).

Итак, предусмотрен следующий порядок работы:

1. При обращении какой-либо программы к некоторому объекту файловой системы (запрос на открытие, запуск или закрытие файла) обращение перехватывается модулем ядра компонента *kavmonitor* и файл перенаправляется на антивирусную проверку.
2. Обработка перехваченного файла производится с помощью программы-демона, входящей в состав компонента *kavmonitor*. Демон выполняет проверку запрошенного объекта на присутствие вирусов и его обработку в соответствии с параметрами конфигурационного файла (в том числе и лечение с помощью антивирусных баз, если данная опция включена).
3. После обработки файла модуль ядра отправляет *kavmonitor* код доступа (разрешен/запрещен), определяющий статус файла.
4. В соответствии со статусом объекта компонент *kavmonitor* разрешает доступ к файлу, либо блокирует его (в этом случае запрашившая файл программа получает код ошибки (Access denied)).

Статус файла, присваиваемый ему в процессе проверки (и обработки), может быть следующим:

- **Clean** – объект не заражен.
- **Infected** – объект заражен.
- **Cured** – зараженный объект был успешно вылечен.
- **CureFailed** – зараженный объект вылечить не удалось.
- **Warning** – код объекта похож на код известного вируса.
- **Suspicion** – объект подозревается на заражение неизвестным вирусом.
- **Protected** – объект проверить невозможно из-за того, что он зашифрован.
- **Corrupted** – объект поврежден.
- **Error** – при проверке объекта возникла системная ошибка.

Действия, производимые над объектом конкретного статуса, определяются параметрами конфигурационного файла (подробнее см. Приложение А на стр. 55).

ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

Прежде чем приступить к установке Антивируса Касперского, мы рекомендуем вам выполнить следующую подготовку вашей системы:

- Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. п. 1.5 на стр. 10). Если не установлены какие-либо из приложений, например, Perl, рекомендуется установить их, иначе часть функциональности Антивируса будет недоступна.
- Настроить интернет-соединение.
- Войти систему под пользователем **root**.

3.1. Установка приложения на компьютер под управлением Linux

Антивирус Касперского для компьютеров под управлением операционной системы Linux распространяется в двух форматах:

- **.rpm** – для систем, поддерживающих RPM Package Manager;
- **.deb** – для дистрибутивов Debian.



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

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



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

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

3.2. Установка приложения на компьютер под управлением FreeBSD

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



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

```
pkg_add <имя_пакета>
```

3.3. Процесс установки

Установка приложения *выполняется в автоматическом режиме* и включает в себя следующие шаги:

1. Копирование файлов дистрибутива на компьютер.
2. Установка лицензионного ключа.

Если лицензионный ключ не установлен, работа Антивируса Касперского будет невозможна.

Если ключ временно отсутствует (например, приложение приобретено через интернет, и лицензионный ключ еще не получен по электронной почте), можно установить его не в процессе инсталляции, а позже, непосредственно перед началом использования приложения (подробнее об установке ключа см. п. 0 на стр. 41).

3. Конфигурация компонента обновления антивирусных баз *keepup2date*.
4. Установка (обновление) антивирусных баз.



Не забудьте установить антивирусные базы перед началом использования приложения. Без антивирусных баз проверка и обработка файлов невозможна!

5. Установка модуля Webmin.

Модуль удаленного управления будет установлен, только если *при установке пакета Webmin были использованы инсталляционные пути по умолчанию*. После установки модуля будут даны соответ-

ствующие рекомендации по настройке его совместной работы с приложением.



При работе с операционной системой Linux необходимо помнить, что при обновлении модуля ядра операционной системы также необходимо обновить модуль ядра компонента `kavmonitor`.

3.4. Процесс обновления приложения до версии 5.5

После установки приложения производится инспекция системы на предмет установленного Антивируса Касперского версии ниже 5.5.

Если обнаружено приложение предыдущей версии, будет произведен импорт *некоторых прежних настроек* Антивируса Касперского в конфигурационный файл для версии 5.5.



В процессе установки не выполняется удаление дистрибутива предыдущей версии Антивируса Касперского. Эта задача возлагается на администратора.

Часть стандартных параметров конфигурационного файла (например, путь к каталогу хранения антивирусных баз) *не экспортируется*, а определяется в процессе установки.

Кроме того, в приложении версии 5.5 по сравнению с версией 5.0 внесены некоторые изменения в логику работы отдельных компонентов, а также добавлен ряд опций. Поэтому рекомендуем вам проверить правильность заполнения конфигурационного файла перед началом использования приложения.

3.5. Установка лицензионного ключа

На данном этапе установки в текущем каталоге выполняется поиск лицензионного ключа – файла (с расширением `key`), необходимого для работы Антивируса Касперского. Этот файл позволяет получить доступ к полной функциональности приложения. До тех пор пока вы не установите лицензионный ключ, работа с Антивирусом Касперского будет невозможна.

Если лицензионный ключ найден, то на консоль выводится соответствующая информация и процесс установки переходит к следующему этапу – установке антивирусных баз.

Если лицензионный ключ не обнаружен, администратору предлагается указать полный путь к нему. В случае отсутствия ключа, необходимо отказаться от указания пути к лицензионному ключу и продолжить процесс установки приложения.

Как только лицензионный ключ будет получен, его необходимо будет установить (подробнее об этом см. 0 на стр. 41).

3.6. Расположение файлов приложения по каталогам



После установки Антивируса Касперского на рабочую станцию под управлением операционной системы Linux по умолчанию файлы дистрибутива будут расположены следующим образом:

`/etc/opt/kaspersky/` – каталог, содержащий конфигурационный файл Антивируса Касперского:

`kav4ws.conf` – конфигурационный файл.

`/opt/kaspersky/kav4ws/` – основной каталог Антивируса Касперского, включающий:

`/bin/` – каталог исполняемых файлов всех компонентов Антивируса Касперского:

`kav4ws-kavscanner` – исполняемый файл компонента антивирусной защиты;

`kav4ws-keepup2date` – исполняемый файл компонента обновления антивирусных баз;

`kav4ws-licensemanager` – исполняемый файл компонента работы с лицензионными ключами.

`/lib/` – каталог хранения служебных файлов Антивируса Касперского.

`/man/` – каталог хранения man-файлов.

`/sbin/` – каталог хранения служебных сервисов Антивируса Касперского:

`kav4ws-kavmonitor` – исполняемый файл компонента антивирусной защиты.

`/src/` – каталог хранения модуля антивирусного ядра приложения.

`/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm` – плагин к программе Webmin.

`/opt/kaspersky/kav4ws/share/contrib/vox.sh` – скрипт `vox.sh`, используемый для лечения архивов.

`/opt/kaspersky/kav4ws/share/doc/LICENSE` – лицензионное соглашение.

`/var/opt/kaspersky/kav4ws/bases` – каталог хранения антивирусных баз.

`/var/opt/kaspersky/kav4ws/bases.backup` – каталог хранения антивирусных баз актуальных до последнего обновления.



Для подключения справочной системы Антивируса Касперского (manual pages) присвойте переменной окружения **MANPATH** значение `/opt/kaspersky/kav4ws/man`.



После установки Антивируса Касперского на рабочую станцию под управлением операционной системы FreeBSD по умолчанию файлы дистрибутива будут расположены следующим образом:

`/usr/local/etc/kaspersky/` – каталог, содержащий конфигурационный файл Антивируса Касперского:

`kav4ws.conf` – конфигурационный файл.

`/usr/local/bin/` – каталог исполняемых файлов всех компонентов Антивируса Касперского:

`kav4ws-kavscanner` – исполняемый файл компонента антивирусной защиты;

`kav4ws-keepup2date` – исполняемый файл компонента обновления антивирусных баз;

`kav4ws-licensemanager` – исполняемый файл компонента работы с лицензионными ключами.

`/usr/local/sbin/` – каталог хранения служебных сервисов Антивируса Касперского:

`kav4ws-kavmonitor` – исполняемый файл компонента антивирусной защиты.

`/usr/local/man/` – каталог хранения man-файлов.

`/usr/local/src/kav4ws/` – каталог хранения модуля антивирусного ядра приложения.

`/usr/local/share/kav4ws/contrib/kav4ws.wbm` – плагин к программе Webmin.

`/usr/local/share/kav4ws/contrib/vox.sh` – скрипт `vox.sh`, используемый для лечения архивов.

`/usr/local/share/doc/kav4ws/LICENSE` – лицензионное соглашение.

`/var/db/kaspersky/kav4ws/bases` – каталог хранения антивирусных баз;

`/var/db/kaspersky/kav4ws/bases.backup` – каталог хранения антивирусных баз актуальных до последнего обновления.



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

`/etc/opt/kaspersky/` – каталог, содержащий конфигурационный файл Антивируса Касперского:

kav4fs.conf – конфигурационный файл.

/opt/kaspersky/kav4fs/ – основной каталог Антивируса Касперского, включающий:

/bin/ – каталог исполняемых файлов всех компонентов Антивируса Касперского:

kav4fs-kavscanner – исполняемый файл компонента антивирусной защиты;

kav4fs-keepup2date – исполняемый файл компонента обновления антивирусных баз;

kav4fs-licensemanager – исполняемый файл компонента работы с лицензионными ключами.

/lib/ – каталог хранения служебных файлов Антивируса Касперского.

/man/ – каталог хранения man-файлов.

/sbin/ – каталог хранения служебных сервисов Антивируса Касперского:

kav4fs-kavmonitor – исполняемый файл компонента антивирусной защиты.

/src/ – каталог хранения модуля антивирусного ядра приложения.

/opt/kaspersky/kav4fs/share/contrib/kav4fs.wbm – плагин к программе Webmin.

/opt/kaspersky/kav4fs/share/contrib/vox.sh – скрипт *vox.sh*, используемый для лечения архивов.

/opt/kaspersky/kav4fs/share/doc/LICENSE – лицензионное соглашение.

/var/opt/kaspersky/kav4fs/bases – каталог хранения антивирусных баз.

/var/opt/kaspersky/kav4fs/bases.backup – каталог хранения антивирусных баз актуальных до последнего обновления.



Для подключения справочной системы Антивируса Касперского (manual pages) присвойте переменной окружения **MANPATH** значение ***/opt/kaspersky/kav4fs/man***.



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

/usr/local/etc/kaspersky/ – каталог, содержащий конфигурационный файл Антивируса Касперского:

kav4fs.conf – конфигурационный файл.

/usr/local/bin/ – каталог исполняемых файлов всех компонентов Антивируса Касперского:

kav4fs-kavscanner – исполняемый файл компонента антивирусной защиты;

kav4fs-keepup2date – исполняемый файл компонента обновления антивирусных баз;

kav4fs-licensemanager – исполняемый файл компонента работы с лицензионными ключами.

/usr/local/sbin/ – каталог хранения служебных сервисов Антивируса Касперского:

kav4fs-kavmonitor – исполняемый файл компонента антивирусной защиты.

/usr/local/man/ – каталог хранения ман-файлов.

/usr/local/src/kav4fs/ – каталог хранения модуля антивирусного ядра приложения.

/usr/local/share/kav4fs/contrib/kav4fs.wbm – плагин к программе Webmin.

/usr/local/share/kav4fs/contrib/vox.sh – скрипт *vox.sh*, используемый для лечения архивов.

/usr/local/share/doc/kav4fs/LICENSE – лицензионное соглашение.

/var/db/kaspersky/kav4fs/bases – каталог хранения антивирусных баз;

/var/db/kaspersky/kav4fs/bases.backup – каталог хранения антивирусных баз актуальных до последнего обновления.



В дальнейшем в качестве примеров мы будем рассматривать названия компонентов, принятых при установке на сервер под управлением операционной системы Linux!

3.7. Завершение установки

Если процесс установки завершен корректно, на консоль будет *выведено соответствующее сообщение*. Конфигурационный файл, входящий в поставку приложения, содержит все необходимые настройки для начала работы.

Однако существует ряд параметров, которые не определяются в процессе установки. Тем не менее, эти настройки помогают использовать функциональность Антивируса Касперского в полном объеме. Поэтому после завершения процедуры установки мы рекомендуем вам выполнить постинсталляционную настройку (см. Глава 4 на стр. 24).

ГЛАВА 4. НАСТРОЙКА ПРИЛОЖЕНИЯ ПОСЛЕ УСТАНОВКИ

В процессе установки выполняется анализ системы, на которую устанавливается Антивирус Касперского, и некоторые параметры его конфигурации определяются автоматически. Кроме того, ряд параметров конфигурационного файла приложения определен по умолчанию как наиболее удобный для работы с Антивирусом (см. п. 4.1 на стр. 24).

Рассмотрим подробнее, какие настройки Антивируса Касперского приняты по умолчанию, а также какие параметры администратору *рекомендуется определить до начала использования приложения*.

4.1. Настройка приложения по умолчанию

Все параметры функционирования Антивируса Касперского хранятся в конфигурационном файле **kav4fs.conf**, используемом по умолчанию.

Конфигурация Антивируса Касперского выполнена следующим образом:

- При запуске операционной системы Антивирус Касперского автоматически начинает свою работу. Приложение перехватывает все обращения к файловой системе и анализирует их. При обнаружении зараженных, подозрительных или поврежденных объектов Антивирус Касперского выводит соответствующие сообщения в файл отчета **kavmonitor.log**.
- При запуске проверки по требованию без дополнительных ключей командной строки антивирусная проверка каталогов и файловых систем компьютера проводится, начиная с текущего каталога. Сообщения по результатам проверки Антивирус Касперского выводит сообщения на консоль и в файл отчета **kavscanner.log**.



Обратите внимание на то, что по умолчанию зараженные объекты не лечатся и не изолируются!

4.2. Установка антивирусных баз

Поиск вирусов и лечение зараженных объектов Антивирусом Касперского производится на основании записей в антивирусных базах. Антивирусные базы содержат описание всех известных на настоящий момент вредоносных программ и способов лечения пораженных ими объектов. Поэтому крайне важно поддерживать антивирусные базы в актуальном состоянии.



Каждый день появляются новые вирусы. Рекомендуется обязательно провести обновление антивирусных баз **сразу** после установки приложения, поскольку базы, входящие в состав дистрибутива, к моменту установки теряют актуальность.

Обновление баз производится Антивирусом Касперского с помощью компонента *keepup2date*. Для запуска обновления в командной строке введите:

```
/путь/к/ kav4fs-keepup2date
```

Антивирусные базы будут скопированы с серверов обновлений Лаборатории Касперского и размещены в специальном каталоге, указанном в конфигурационном файле.

4.3. Настройка совместной работы с Webmin

Если предполагается удаленное управление Антивирусом Касперского, то рекомендуем вам настроить его совместную работу с пакетом Webmin.

Средствами Webmin можно, например, ограничить доступ к работе с программой, организовав систему паролей для пользователей.

По умолчанию все настройки Антивируса, выполненные удаленно посредством программы Webmin, сохраняются в конфигурационном файле приложения, используемом по умолчанию.



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

1. Скопировать данные из существующего конфигурационного файла в новый, который необходимо сохранить под другим именем. После этого провести корректировку нового (альтернативного) конфигурационного файла в соответствии с вашими задачами.

2. Указать имя альтернативного конфигурационного файла на закладке **Config edit** в поле ввода параметра **Full path to KAV config**.



Подробную информацию о различных настройках программы Webmin смотрите в документации по данному продукту. Также при наличии вопросов по модулю удаленного администрирования приложения вы можете воспользоваться справочной системой к программе Webmin.

В дальнейшем при рассмотрении настройки и запуска каких-либо задач работа удаленно через программу Webmin **приводиться не будет!**

ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

Посредством Антивируса Касперского вы можете организовать систему антивирусной защиты вашего компьютера: от отдельного файла, до всей файловой системы в целом.

Функциональность приложения складывается из задач, которые может выполнить с его помощью администратор. Все задачи, реализуемые посредством Антивируса Касперского, можно разделить на следующие группы:

- Обновление антивирусных баз, используемых для поиска вирусов и лечения зараженных объектов (подробнее см. п. 5.1 на стр. 27).
- Антивирусная защита файловых систем компьютера (проверка по расписанию и \ или по требованию) (подробнее см. п. 5.2 на стр. 33).
- Постоянная антивирусная защита (защита в масштабе реального времени) (подробнее см. п. на стр.40).

Данная глава содержит описание типовых задач, возникающих при работе с Антивирусом Касперского. В рамках конкретного предприятия администратор может комбинировать и усложнять их.

5.1. Обновление антивирусных баз

Неотъемлемым фактором полноценной антивирусной защиты является обновление антивирусных баз, проводимое компонентом *keepup2date* приложения. Источником обновлений антивирусных баз, используемых Антивирусом Касперского в процессе поиска и лечения зараженных объектов, являются сервера 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 *updcfg.xml*, включенном в дистрибутив приложения.

В процессе обновления компонент *keepup2date* обращается к данному списку, выбирает адрес и пытается скопировать с сервера антивирусные базы. Если выполнить обновление с выбранного адреса невозможно, компонент обращается по следующему адресу и вновь пытается обновить базы.



Обновления для антивирусных баз публикуются на серверах обновлений Лаборатории Касперского каждый час.

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



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

Если структура вашей локальной сети достаточно сложная, мы рекомендуем каждый час скачивать обновления антивирусных баз 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. в п. 5.1.4 на стр. 32.

Обновление может быть организовано по расписанию с помощью программы **cron** (см. п. 5.1.2 на стр. 30) или же выполняться по требованию администратора, запускаясь вручную из командной строки (см. п. 5.1.3 на стр. 31).



Настоятельно рекомендуем настроить ежечасное обновление антивирусных баз!

5.1.1. Новые возможности компонента обновлений

В версии 5.5. Антивируса Касперского в отличие от предыдущих версии заменен компонент обновления антивирусных баз. В новом компоненте усовершенствован ряд существующих функций, а также добавлены новые возможности:

- возможность автоматического выбора географически ближайшего сервера обновлений, исходя из указанного в конфигурационном файле региона;

- возможность скачивания и установки инкрементальных обновлений при выходе кумулятивного обновления, что позволяет экономить сетевой трафик;
- в случае обрыва соединения в момент копирования антивирусных баз или смены сервера обновления после восстановления соединения компонент автоматически скачает оставшуюся часть антивирусных баз, а не начнет копирование сначала;
- проверка целостности скаченных баз;
- анализ полноты установленных антивирусных баз и загрузка только измененных или добавленных элементов базы. Эта возможность также направлена на экономию сетевого трафика;
- возможность запускать указанную пользователем команду перезагрузки антивирусных баз сразу после успешного обновления;
- поддержка возможности возврата к предыдущей версии антивирусных баз (rollbacks);
- для работы нового компонента не требуется наличия программы wget;
- возможность выбора варианта копируемых баз (стандартный или расширенный набор баз).

Стандартные базы – антивирусные базы, содержащие подробное описание всех существующих на данный момент вирусов, методов их обнаружения и лечения. Данные антивирусные базы используются по умолчанию.

Расширенные базы – антивирусные базы, которые помимо вирусов содержат также информацию о программах группы риска (RiskWare) и программ-распространителей рекламы (AdWare).

Программы группы риска содержат уязвимости, которые могут использоваться для хакерских атак, внедрения неавторизованных программ и т.п.

Программы-распространители рекламы устанавливаются совместно с каким-либо программным обеспечением и в дальнейшем выводят рекламную информацию, либо отображая ее в дополнительных окнах, либо вынуждая пользователя посещать веб-сайт рекламодателя. Помимо того, что происходит навязывание рекламной информации, подобные программы также существенно загружают линии связи и увеличивают суммарный трафик.

Для обычного режима работы достаточно выбрать стандартные антивирусные базы. Расширенные антивирусные базы используются для обеспечения более высокого уровня защиты информации. Использование более полных антивирусных баз приводит к увеличению затрат ресурсов на проверку данных.

5.1.2. Автоматическое обновление антивирусных баз

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



Задача: задать автоматическое обновление антивирусных баз каждые 3 часа. В системном журнале фиксировать только ошибки при работе программы. Вести общий журнал по всем запускам задачи, на консоль никакой информации не выводить.



Решение: 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 0-23/3 * * * /opt/kaspersky/bin/kav4fs-keepup2date
```



Задача: настроить скачивание обновлений антивирусных баз с сайтов-источников обновлений Лаборатории Касперского. Адрес сайта обновлений автоматически определить из списка, включенного в состав компонента *keepup2date*.



Решение: для реализации поставленной задачи выполните следующие действия:

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



Задача: настроить скачивание обновлений антивирусных баз с адреса, указанного администратором. Если проведение обновлений с данного адреса невозможно, прервать процесс обновления.



Решение: для реализации поставленной задачи выполните следующие действия:

Присвойте параметрам **UseUpdateServerUri** и **UseUpdateServerUriOnly** секции **[updater.options]** значение **Yes**. Кроме того, параметр **UpdateServerUri** должен содержать адрес сервера обновлений.



Задача: настроить скачивание обновлений антивирусных баз с адреса, указанного администратором. Если проведение обновлений с данного адреса невозможно, обновить базы с адреса, указанного в списке встроенного в Антивирус Касперского списка обновлений.



Решение: для реализации поставленной задачи выполните следующие действия:

Присвойте параметру **UseUpdateServerUri** секции **[updater.options]** значение **Yes**, а параметру **UseUpdateServerUriOnly** значение **No**. Кроме того, параметр **UpdateServerUri** должен содержать адрес сервера обновлений.

5.1.3. Обновление антивирусных баз по требованию

В любой момент времени вы можете запустить обновление антивирусных баз из командной строки.



Задача: запустить обновление антивирусных баз, сохранив результаты работы в файле `/tmp/updatesreport.log`.



Решение: для реализации поставленной задачи в командной строке введите:

```
# kav4fs-keepup2date -l /tmp/updatesreport.log
```

Если вам необходимо обновить антивирусные базы 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.



Задача: организовать обновление антивирусных баз из сетевого каталога **/home/bases**, а если этот каталог недоступен или пуст, проводить обновление баз с серверов Лаборатории Касперского. Результаты работы вывести в файл отчета **report.txt**.



Решение: для реализации поставленной задачи выполните следующие действия:

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

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

2. В командной строке введите:

```
# kav4fs-keepup2date -l /tmp/report.txt
```

5.1.4. Создание сетевого каталога для хранения и копирования антивирусных баз

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



Задача: создать сетевой каталог, откуда антивирусные базы будут копироваться на локальные компьютеры сети.



Решение: для реализации поставленной задачи выполните следующие действия:

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

```
# kav4fs-keepup2date -u <dir>
```

где *<dir>* – полный путь к созданному каталогу.
3. Предоставьте для локальных компьютеров сетевой доступ на чтение к данному каталогу.



Задача: настроить обновление антивирусных баз через прокси-сервер.



Решение: 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 авторизация 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**.

5.2. Антивирусная защита файловых систем

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



Все параметры компонента *kavscanner* сгруппированы в опциях **[scanner.*]** конфигурационного файла приложения.



По умолчанию запуск проверки по требованию может выполнить только пользователь **root**.

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. 5.2.1 на стр. 34).
- Режим проверки и лечения объектов (см. п. 5.2.2 на стр. 35).
- Действия над объектами (см. п. 5.2.3 на стр. 36).
- Параметры формирования отчета о результатах работы (см. п. 6.5 на стр. 50).

Процесс проверки файловых систем вашего компьютера может быть запущен:

- Разово из командной строки (см. п. 5.2.4 на стр. 37).
- По расписанию при помощи программы **cron** (см. п. 5.2.5 на стр.38).



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

5.2.1. 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 вирусов (архивы и т.д.).

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



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 каталоги 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.



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.

- Ограничить пути, принятые по умолчанию (все, начиная с текущего каталога) или перечисленные в командной строке, путем ввода в

конфигурационном файле **kav4fs.conf** масок файлов и каталогов, которые будут исключены из области проверки (секция **[scanner.options]**, параметры **ExcludeMask** и **ExcludeDirs**).

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

Объекты проверки по умолчанию также задаются в конфигурационном файле **kav4fs.conf** (секция **[scanner.options]**) и могут быть переопределены:

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

5.2.2. Режим проверки и лечения объектов

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

По умолчанию опция отключена, что предполагает только проверку объектов и информирование об обнаружении вирусов и других подозрительных или поврежденных файлов путем вывода сообщений на консоль и в отчет (см. п. 6.5 на стр. 50).

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.
- **Corrupted** – объект поврежден.
- **Protected** – объект проверить невозможно из-за того, что он зашифрован (защищен паролем).

При включенном режиме лечения (секция **[scanner.options]**, параметр **Cure=yes**) на антивирусную обработку 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.
- **Error** – при проверке объекта произошла ошибка.

5.2.3. Действия над объектами

В зависимости от статуса объекта (см. Глава 2 на стр. 15) 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]**.



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 **kav4fs.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.



Если в командной строке при запуске компонента не указывается какой-либо конфигурационный файл, то параметры функционирования берутся из файла **kav4fs.conf**. Использование данного файла при запуске специально не указывается!

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

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

5.2.4. Проверка по требованию отдельного каталога

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



Задача: запустить проверку каталога **/tmp** с автоматическим лечением всех обнаруженных зараженных объектов. Все объекты, вылечить которые не удалось, – удалить.

В этом же каталоге 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.

Результаты работы компонента (дату запуска, информацию обо всех файлах, кроме незараженных) выводить только в файл-отчет *kav4fs-kavscanner-текущая_дата-pid.log*, который сохранить в том же каталоге.



Решение: для реализации поставленной задачи в командной строке введите:

```
# kav4fs-kavscanner -rlq -pi/tmp/infected.lst
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst
-pw/tmp/warning.lst -o /tmp/kav4fs-kavscanner-`date
"+%Y-%m-%d-$$"`.log -i3 -ePASBMe -j3 -mCn /tmp
```

5.2.5. Проверка по расписанию

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



Задача: каждый день в 0 часов 00 минут запускать проверку на присутствие вирусов каталога **/home**; использовать параметры проверки, заданные в конфигурационном файле **/etc/kav/scanhome.conf**.



Решение: 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 * * * /path/to/kav4fs-kavscanner -c  
/etc/kav/scanhome.conf /home
```

5.2.6. Дополнительные возможности: использование скрипт-файлов

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

5.2.6.1. Лечение зараженных объектов в архиве

Антивирус Касперского не лечит зараженные файлы, запакованные в архивы, он лишь обнаруживает в них подозрительные и зараженные объекты. Однако такая возможность может быть реализована посредством дополнительного скрипт-файла. В настоящем документе приводится пример лечения архивов типа **tar**, **rar** и **zip** при помощи скрипт-файла **vox.sh**. Данный скрипт включен в поставку Антивируса Касперского.

При работе скрипт распакует проверяемый архив, выполнит антивирусную проверку и обработку отдельных объектов, а затем проведет архивацию проверенных файлов. Поэтому необходимо, чтобы в системе были установлены архиваторы.



Задача: С помощью скрипта `vox.sh` проверить архив типа `tar` или `zip`.



Решение: для реализации поставленной задачи выполните следующее:

В командной строке введите:

```
# /opt/kaspersky/kav4fs/share/contrib/vox.sh <путь-к-архивному файлу>
```

5.2.6.2. Отправка администратору уведомления

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



Задача: настроить уведомление администратора при обнаружении в файловых системах зараженных файлов и архивов при каждой проверке компьютера, выполняемой в соответствии с параметрами конфигурационного файла `kav4fs.conf`. При проверке включить режим раскрытия символьных ссылок.



Решение: для реализации поставленной задачи выполните следующие действия:

Задайте следующие правила обработки простых объектов и контейнеров в конфигурационном файле `kav4fs.conf`:

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% |
mail -s kav4fs-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
```

```
| mail -s kav4fs-kavscanner -a %LIST%  
admin@localhost.ru
```



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

5.3. Антивирусная защита в режиме реального времени

Антивирусная защита файловой системы компьютера в режиме реального времени осуществляется посредством компонента *kavmonitor*.



Все параметры функционирования компонента *kavmonitor* содержатся в секции **[monitor.*]** конфигурационного файла приложения.

Конфигурация компонента *kavmonitor* выполнена таким образом, что при проведении каких-либо операций по доступу к файлам (открытие, закрытие или запуск) компонент *kavmonitor* производит антивирусную проверку (при закрытии файл проверяется, только если он был изменен). По умолчанию на присутствие вирусов и вредоносных программ проверяются все запрошенные пользователем объекты, в том числе:

- запакованные файлы;
- архивы;
- самораспаковывающиеся архивы;
- почтовые базы;
- почтовые сообщения.

По результатам проверки производится антивирусная обработка объекта в соответствии с параметрами конфигурационного файла приложения.



По умолчанию режим лечения обнаруженных зараженных объектов отключен! Для настройки этой опции присвойте параметру **Cure** секции **[monitor.options]** конфигурационного файла приложения значение **Yes**.

Для объектов со статусами **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** и **CureFailed** возможно настроить выполнение ряда действий, таких как:

- *перемещение в некоторый каталог* – перенос объектов определенного статуса в некоторый каталог; возможен *простой* и *рекурсивный* (с восстановлением полного пути) *перенос*;

- удаление объекта из файловой системы.

Настроить правила обработки объектов можно, определив их в конфигурационном файле приложения (секция **[monitor. actions]**).

Вы также можете произвести дополнительную настройку:

- С помощью параметров **ExcludeDirs** и **ExcludeMask** определить каталоги, которые необходимо исключать из проверки.
- Использовать технологии эвристического анализатора кода и iChecker.
- Снижать нагрузку на сервер с помощью определения максимального количества одновременно проверяемых объектов.

5.4. Управление лицензионными ключами

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

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

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

По окончании срока действия лицензии вы автоматически лишаетесь приведенных выше возможностей. Антивирус Касперского по-прежнему будет осуществлять антивирусную обработку файлов, но только с использованием антивирусных баз, актуальных на дату окончания срока действия лицензии. Функция обновления антивирусных баз будет не доступна.

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

5.4.1. Просмотр информации о лицензионном ключе

Вы можете просматривать информацию об установленных лицензионных ключах в отчетах о работе компонентов *kavscanner*, *kavmonitor* и *keerup2date*, поскольку при старте каждый из этих компонентов загружает информацию о ключах.

Помимо этого в Антивирусе Касперского предусмотрен специальный компонент *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 лицензионных ключах,

в командной строке введите:

```
kav4fs-licensemanager -s
```

На экран будет выведена информация подобного рода:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2007.
Portions Copyright (C) Lan Crypto
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix", expires
04-07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Linux File Srv
(licence per e-mail address)", expires 25-01-2004 in
234 days
```



Чтобы просмотреть информацию о конкретном ключе,

в командной строке введите такую строку:

```
kav4fs-licensemanager -k 0003D3EA.key
```

На консоли отразится информация подобного рода:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2007.
```

Portions Copyright (C) Lan Crypto
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Linux", expires 04-07-2003 in 28 days

5.4.2. Продление лицензии

Продление лицензии на использование Антивируса Касперского дает вам право на восстановление полной функциональности приложения – обновления антивирусных баз. Кроме того, возобновляются дополнительные услуги, приведенные в п. 5.4 на стр. 41.

Срок действия лицензии зависит от типа лицензирования, который вы выбрали, приобретая приложение.



Чтобы продлить лицензию на использование Антивируса Касперского, вам необходимо:

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

или:

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



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

Приобретенный лицензионный ключ необходимо установить.



Чтобы установить новый лицензионный ключ,

в командной строке введите:

```
kav4fs-licensemanager -a <имя файла ключа>
```

После этого рекомендуем вам обновить антивирусные базы (см. п. 5.1 на стр. 27).



Чтобы удалить лицензионный ключ,

в командной строке введите:

```
kav4fs-licensemanager -d <имя файла ключа>
```

ГЛАВА 6.

ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА

В данном разделе мы остановимся на дополнительной настройке функциональности Антивируса Касперского. Она направлена на расширение функциональности приложения и его адаптацию под условия использования в рамках конкретного предприятия.

6.1. Оптимизация работы Антивируса Касперского

Для снижения нагрузок на процессор и увеличения скорости антивирусной обработки объектов Антивирус Касперского предлагает эффективные способы оптимизации своей работы. Рассмотрим его подробнее.



Использование базы данных iChecker и технологии двухуровневого кеширования проверенных файлов.

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

После первичной проверки любого файла информация о нем (имя, контрольная сумма) фиксируется в одной из следующих баз данных:

- База iChecker – общая база, включающая информацию о проверенных **незараженных** файлах определенных форматов. Такая база содержит информацию по объектам, проверенным компонентами *kavmonitor* и *kavscanner*.
- Кеш проверенных файлов – база, содержащая информацию о проверенных компонентом *kavmonitor* файлах. Кеш состоит из двух уровней: на первом уровне хранится информация о **незараженных файлах**, обращение к которым производится наиболее часто. Кеш первого уровня расположен в модуле ядра, что позволяет существенно снизить время, затрачиваемое на обращение к нему. Если

приложение обнаруживает данные о запрашиваемом файле в кеше первого уровня, то оно автоматически присваивает объекту статус **Clean**, и дальнейшая антивирусная проверка не производится. Если первый уровень кеша не содержит требуемую информацию, то производится поиск на втором уровне, содержащем данные **обо всех проверенных файлах**. Обе базы кеша существуют в оперативной памяти, и после окончания работы приложения не сохраняются.

Таким образом, если при проверке информация о файле не попадает в базу iChecker (файл не является чистым или его формат не поддерживается данной технологией), она фиксируется в кеше.

При каждом последующем обращении пользователя к файлу производится его поиск сначала в кеше первого уровня, а затем (если в первой базе объект не обнаружен) – в базе iChecker, и в кеше второго уровня. Критерием поиска является имя файла. Если такой файл будет обнаружен в любой из баз, информация о файле сравнивается с указанной в базе. При условии полной идентичности текущего состояния объекта и его описания в базе файл считается неизменным и не проверяется на присутствие вирусов.

Если информации о запрашиваемом файле не обнаружено ни в базе iChecker, ни в кеше, производится полная антивирусная проверка файла.



Если при работе с приложением вы изменили используемый набор антивирусных баз, необходимо вручную удалить информацию из базы iChecker (полный путь к базе определяется параметром **IcheckerDbFile** секции **[path]** конфигурационного файла приложения).

Это связано с тем, что база может содержать зараженные объекты, не обнаруженные с помощью стандартных антивирусных баз, но детектированные с помощью расширенного набора. Файлы, информация о которых содержится в базе iChecker, не проверяются повторно, что может привести к заражению компьютера.



Ограничение нагрузки на процессор.

Проверка файловых систем компьютера при большом объеме данных может занять значительное время. В этом случае нагрузка на процессор значительно возрастает. В то же время процессор должен выполнять текущие задачи, а потому было бы желательно иметь механизм, который бы приостанавливал антивирусную проверку компьютера при превышении некоего порога нагрузки.

В Антивирусе Касперского такой механизм существует. В версии 5.5 приложения в конфигурационный файл добавлен параметр **MaxLoadAvg** в сек-

цию **[scanner.options]**. В случае если параметр задан, *kavscanner* при проверке каждого нового файла считывает текущую степень загруженности процессора **load average**, и, в случае ее превышения указанного в конфигурационном файле значения, *kavscanner* приостанавливает работу до момента, когда значение параметра **load average** снизится до указанного уровня.

Кроме того, дополнительно можно ограничить количество одновременно проверяемых в режиме реального времени объектов с помощью параметра **CheckFileLimit** секции **[monitor.options]** конфигурационного файла приложения. Это также позволит снизить нагрузку на процессор и увеличить скорость проверки отдельных объектов.

6.2. Перенос объектов в карантинный каталог

Вы можете организовать работу Антивируса Касперского таким образом, что все зараженные объекты будут переноситься в отдельный каталог.

Такая возможность может быть использована, например, *если лечение объекта произвести не удалось* (например, из трех вирусов, которыми заражен файл, удалось удалить только два), однако сам файл представляет высокую информационную ценность.

Если каталог с изолированными объектами предполагается хранить в структуре файловой системы компьютера, рекомендуем исключить его из области последующих проверок, указав полный путь к нему в качестве значения параметра **ExcludeDirs** в секции **[scanner.options]** конфигурационного файла.

Рассмотрим задачи изоляции зараженных объектов, обнаруженных в процессе антивирусной проверки по требованию файловой системы компьютера, и при проверке в режиме реального времени.



Задача: проверить на присутствие вирусов все объекты, перечисленные в файле */tmp/download.lst*, и перенести обнаруженные зараженные объекты с полными путями к ним в каталог */tmp/infected*. Информацию о зараженных, а также подозрительных и поврежденных объектах вывести в файл отчета.



Решение: для реализации поставленной задачи выполните следующие действия:

1. В качестве действий над зараженными объектами в секциях **[scanner.object]** и **[scanner.container]** конфигурационного файла укажите следующую строку:

```
OnInfected=MovePath /tmp/infected
```

- Отключите режим лечения (**Cure=no**), если он был включен.
- В командной строке введите:

```
# kav4fs-kavscanner -@/tmp/download.lst -ePASBME
-rq
-i0 -o /tmp/report.log -j3 -mCn
```

Теперь усложним задачу, задав требование ограничения доступа к файлам каталога */tmp/infected* только возможностью их чтения и записи. Это достигается с помощью стандартных инструментов Unix (команда **chmod**). Следовательно, в схему реализации задачи необходимо внести следующие изменения:

В секциях **[scanner.object]** и **[scanner.container]** конфигурационного файла приложения в качестве правила обработки зараженных объектов укажите следующую строку:

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



Задача: проверять на присутствие вирусов все запрашиваемые файлы, в случае, если объект заражен, произвести лечение. В случае неудачного лечения перенести зараженные объекты с полными путями к ним в каталог **/tmp/infected**.



Решение: для реализации поставленной задачи выполните следующие действия:

- В конфигурационном файле приложения включите режим лечения зараженных объектов (**Cure=yes** в секции **[monitor.options]**).
- Задайте правила изоляции зараженных объектов. Для этого в секции **[monitor.actions]** конфигурационного файла выполните следующую настройку:

```
OnInfected=MovePath /tmp/infected
```

6.3. Режим резервного копирования объектов (backup)

В случае если проверяемые файлы оказались заражены, а в качестве действия над зараженными объектами определено удаление их из файловой

системы, возможен риск потери с ряда важных данных. Чтобы избежать этого, в Антивирусе Касперского предусмотрена возможность копирования файлов в резервное хранилище (backup-хранилище).

Перед лечением или удалением объекта его копия автоматически создается в backup-хранилище (секция **[monitor.path]**, параметр **BackupPath**). Это позволяет сохранить резервную копию (и, при необходимости, восстановить первоначальный файл) в случае, если сам объект будет поврежден в процессе лечения. Объект сохраняется в резервном хранилище с полным путем. При повторной записи в backup-хранилище ранняя копия объекта автоматически заменяется более поздней.

Обратите внимание: по умолчанию режим сохранения в резервное хранилище не включен и, соответственно, путь к каталогу, в котором предполагается хранить резервные копии, не определен.

Для включения режима самостоятельно определите путь к каталогу хранения резервных копии объектов.



В случае удаления объекта из файловой системы его копия будет храниться в backup до тех пор, пока ее не удалит администратор.



Действия, указанные в настройках конфигурационного файла для инфицированных объектов, не выполняются над файлами в резервном хранилище!

6.4. Локализация отображаемого формата даты и времени

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

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

%H:%M:%S – отображаемый формат времени.

%d/%m/%y – отображаемый формат даты.

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

%I:%M:%S %P – для отображения времени в двенадцатичасовом формате (параметр **TimeFormat**) с указанием am/pm.

%y/%m/%d и **%m/%d/%y** – для отображения даты (параметр **DateFormat**) в формате год/месяц/день и месяц/день/год соответственно.

6.5. Параметры формирования отчета Антивируса Касперского

Результаты работы всех компонентов Антивируса Касперского фиксируются в отчете, который выводится в файл.



Результаты антивирусной обработки файловых систем компьютера также выводятся на консоль. По умолчанию информация, выводимая в отчет и на экран, дублирует друг друга.

Если вы хотите, чтобы информация о работе приложения фиксировалась в системном лог-файле, присвойте параметру **ReportFileName** секций **[monitor.report]**, **[scanner.report]**, **[updater.report]** значение **syslog**.

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

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

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

Уровни	Название уровня	Значение
	Критические ошибки	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 лицензионных ключей.

Уровни	Название уровня	Значение
1	Errors	Информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов; например, информация об ошибке проверки объекта.
2	Warning	Информация об ошибках, которые могут привести к завершению работы продукта (например, информация об отсутствии свободного места на диске).
3	Info, Notice	Важные сообщения информационного характера; например: информация о том, запущен ли компонент, путь к конфигурационному файлу, область проверки, информация об антивирусных базах, о лицензионных ключах, результирующая статистика.
4	Activity	Сообщения о проверке объектов в соответствии с уровнем детализации отчета о проверке.

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

ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Выполнение процедуры удаления Антивируса Касперского требует:

- Наличия прав привилегированного пользователя (**root**). Если на момент удаления приложения вы не обладаете такими правами, то вам необходимо войти в систему под пользователем **root**.
- Наличия файла отчета о процессе установки.
- Полного соответствия имен и размеров установленных файлов Антивируса Касперского приведенным в файле отчета об установке.

Также перед началом процедуры удаления приложения необходимо остановить работу компонента **kavmonitor**.



Если при установке вы использовали rpm-пакет Антивируса Касперского, для запуска процедуры деинсталляции в командной строке введите:

```
rpm -e <имя_пакета>
```



Если при установке вы использовали deb-пакет Антивируса Касперского, для запуска процедуры деинсталляции в командной строке введите:

```
dpkg -r <имя_пакета>
```




Если при установке вы использовали rpm-пакет Антивируса Касперского, для запуска процедуры деинсталляции в командной строке введите:

```
pkg_delete <имя_пакета>
```

Процедура удаления будет выполнена автоматически. По завершении на консоль будет выведено соответствующее сообщение.

ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить 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.



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

Загрузить тестовый "вирус" можно с официального веб-сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm. При отсутствии доступа к интернету вы можете самостоятельно создать тестовый "вирус". Для этого в любом текстовом редакторе наберите следующую строку, а затем сохраните в файле с именем **eicar.com**:

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

Файл, который вы загрузили с веб-сайта компании **EICAR** или создали в текстовом редакторе описанным выше способом, содержит тело стандартного тестового "вируса". Антивирус обнаруживает его, присваивает тип **Зараженный**, не подвергающийся лечению, и выполняет действие, установленное администратором для объекта с таким типом.

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

Таблица. Модификации тестового "вируса"

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый "вирус"	Зараженный. Объект не подвергается лечению.
CORR–	Поврежденный.
SUSP–	Подозрительный (код неизвестного вируса).
WARN–	Подозрительный (модифицированный код известного вируса).
ERRO–	Не проверенный из-за сбоя.
CURE–	Вылеченный. Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURE.
DELE–	Объект автоматически удаляется.

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

ПРИЛОЖЕНИЕ А. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ПРИЛОЖЕНИИ

Данное приложение содержит описание дерева каталогов дистрибутива Антивируса Касперского после установки, конфигурационного файла, а также ключей командной строки компонентов и их кодов возврата, в качестве примеров приведен скрипт-файл для лечения архивов.

А.1. Конфигурационный файл Антивируса Касперского

В поставку Антивируса Касперского включен конфигурационный файл **kav4fs.conf**, содержащий параметры функционирования приложения. В данном разделе мы подробно рассмотрим каждую секцию параметров файла. При описании параметров файла будут указаны значения по умолчанию, если таковые предусмотрены.

Секция **[path]** включает параметры, определяющие пути к важнейшим файлам, без которых программное приложение не будет функционировать:

BasesPath – полный путь к антивирусным базам.

LicensePath – полный путь к каталогу расположения лицензионных ключей.

IcheckerDbFile – полный путь к каталогу хранения баз, проверенных с помощью технологии iChecker.

Секция **[locale]** содержит параметры, определяющие форматы даты и времени:

TimeFormat=%H:%M:%S – формат представления времени согласно strftime.



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

DateFormat=%d/%m/%y – формат представления даты согласно strftime.



Вы можете изменить формат представления даты, например, на: %y/%m/%d или %m/%d/%y.

Секция **[monitor.options]** содержит параметры проверки при антивирусной защите в режиме реального времени:

ExcludeDirs=маска1:маска2:...:маскаN – маски каталогов, которые исключаются из проверки; по умолчанию проверяются все каталоги. Маски задаются в виде стандартных shell-масок.

ExcludeMask=маска1:маска2:...:маскаN – маски файлов, которые исключаются из проверки; по умолчанию проверяются все файлы. Маски задаются в виде стандартных shell-масок.

IncludeDirs=маска1:маска2:...:маскаN – маски каталогов, которые проверяются. Маски задаются в виде стандартных shell-масок.

Packed=yes – режим проверки запакованных файлов. Для отключения режима присвойте параметру значение **no**.

Archives=yes – режим проверки архивов. Для отключения режима присвойте параметру значение **no**.

SelfExtArchives=yes – режим проверки самораспаковывающихся архивов. Для отключения режима присвойте параметру значение **no**. Если включен режим проверки архивов (**Archives=yes**), самораспаковывающиеся архивы будут проверены, даже если настройке **SelfExtArchives** присвоено значение **no**.

MailBases=yes – режим проверки почтовых баз. Для отключения режима присвойте параметру значение **no**.

MailPlain=yes – режим проверки почтовых сообщений в виде plain text. Для отключения режима присвойте параметру значение **no**.

Heuristic=yes – режим использования во время проверки эвристического анализатора кода. Для отключения режима присвойте параметру значение **no**.

Cure=no – режим лечения инфицированных объектов. Для включения режима присвойте параметру значение **yes**.

Ichecker=yes – режим использования при антивирусной проверке технологии iChecker. Для отключения режима присвойте параметру значение **no**.

FileCacheSize– размер файлового кеша (в Мб).

KereneelCacheSize – размер кеша, хранящегося антивирусным ядром (в Мб).

CheckFileLimit=20 – максимальное количество одновременно проверяемых объектов.

HashType=md5|crc32 – тип используемого хеша. По умолчанию установлен тип **md5**.

UseAVbasesSet=standart|extended – набор антивирусных баз, используемых приложением. Набор **extended** помимо записей, содержащихся в наборе **standart**, содержит также сигнатуры потенциально опасных программ, таких как: рекламные программы, программы удаленного администрирования и проч.

Секция **[monitor.path]** содержит параметры, определяющие пути к важнейшим файлам, без которых модуль kavmonitor не будет функционировать:

BackupPath=путь – полный путь к каталогу хранения резервных копий проверяемых объектов.

PidFile=путь – полный путь к pid-файлу компонента kavmonitor.

Секция **[monitor.actions]** содержит параметры, определяющие действия над объектами того или иного типа при антивирусной защите в режиме реального времени:

OnInfected=действие – действия в случае обнаружения зараженного файла. Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, вылечить которые не удалось.

OnSuspicion=действие – действия в случае обнаружения подозрительного файла, код которого напоминает код вируса, пока неизвестного Лаборатории Касперского.

OnWarning=действие – действия в случае обнаружения файла, код которого сходен с кодом известного вируса.

OnCured=действие – действия в случае обнаружения и успешного лечения зараженного объекта.

OnProtected=действие – действия в случае обнаружения объекта, зашифрованного паролем. Такие объекты проверить невозможно.

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

OnError=действие – действия в случае возникновения при проверке объекта системной ошибки.

Секция **[monitor.report]** содержит параметры формирования отчета о результатах работы компонента kavmonitor:

ReportLevel=4 – уровень детализации отчета.

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента.

Append=yes – режим добавления новых сообщений в файл отчета. Для отключения режима присвойте параметру значение **no**.

ShowOK=yes – режим вывода в отчет сообщений о незараженных файлах. Для отключения режима присвойте параметру значение **no**.

Секция **[scanner.options]** содержит параметры проверки файловых систем сервера:

Archives=yes – режим проверки архивов. Для отключения режима присвойте параметру значение **no**.

Cure=no – режим лечения инфицированных объектов. Для включения режима присвойте параметру значение **yes**.

ExcludeDirs=маска1:маска2:...:маскаN – маски каталогов, которые исключаются из проверки; по умолчанию проверяются все каталоги. Маски задаются в виде стандартных shell-масок.

ExcludeMask=маска1:маска2:...:маскаN – маски файлов, которые исключаются из проверки; по умолчанию проверяются все файлы. Маски задаются в виде стандартных shell-масок.

Heuristic=yes – режим использования во время проверки эвристического анализатора кода. Для отключения режима присвойте параметру значение **no**.

LocalFS=no – режим проверки только локальной файловой системы. Для включения режима присвойте параметру значение **yes**.

MailBases=yes – режим проверки почтовых баз. Для отключения режима присвойте параметру значение **no**.

MailPlain=yes – режим проверки почтовых сообщений в виде plain text. Для отключения режима присвойте параметру значение **no**.

Packed=yes – режим проверки запакованных файлов. Для отключения режима присвойте параметру значение **no**.

Recursion=yes – режим рекурсивного прохода каталогов при проверке на присутствие вирусов. Для отключения режима присвойте параметру значение **no**.

SelfExtArchives=yes – режим проверки самораспаковывающихся архивов. Для отключения режима присвойте параметру значение **no**. Если включен режим проверки архивов (**Archives=yes**), самораспаковывающиеся архивы будут проверены, даже если настройке **SelfExtArchives** присвоено значение **no**.

Ichecker=yes – режим использования при антивирусной проверке технологии iChecker. Для отключения режима присвойте параметру значение **no**.

UseAVbasesSet=standart|extended – набор антивирусных баз, используемых приложением. Набор **extended** помимо записей, содержащихся в наборе **standart**, содержит также сигнатуры потенциально опасных программ, таких как: рекламные программы, программы удаленного администрирования и проч.

FollowSymlinks – режим работы с символьными ссылками. Если параметру присвоено значение **yes**, при проверке будут раскрываться ссылки, указывающие на директорию.

MaxLoadAvg – максимальная загрузка процессора.

Секция **[scanner.report]** содержит параметры формирования отчета о результатах работы компонента kavscanner:

Append=yes – режим добавления новых сообщений в файл отчета. Для отключения режима присвойте параметру значение **no**.

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента.

ReportLevel=4 – уровень детализации отчета.

ShowOK=yes – режим вывода в отчет сообщений о незараженных файлах. Для отключения режима присвойте параметру значение **no**.

ShowContainerResultOnly=no – режим отображения в отчете результатов проверки архива в кратком формате. Для отображения краткого отчета присвойте параметру значение **yes**.

ShowObjectResultOnly=no – режим отображения в отчете результатов проверки простого объекта в кратком формате. Для отображения в кратком формате присвойте параметру значение **yes**.

Секция **[scanner.container]** включает параметры, определяющие действия над архивами при антивирусной защите файловых систем сервера:

OnCorrupted=действие – действия в случае обнаружения поврежденного контейнера.

OnInfected=действие – действия в случае обнаружения зараженного объекта в контейнере. Если включен режим лечения зараженных файлов, то данное действие применяется к контейнерам, вылечить которые не удалось, и выполняется после всех действий с объектами контейнера.

OnSuspicion=действие – действия в случае обнаружения внутри контейнера подозрительного объекта.

OnWarning=действие – действия в случае обнаружения внутри контейнера объекта, код которого сходен с кодом известного вируса.

OnCured=действие – действия в случае обнаружения внутри контейнера зараженного объекта, который был успешно вылечен.

OnProtected=действие – действия в случае обнаружения внутри контейнера объекта, зашифрованного паролем. Такие объекты проверить невозможно.

OnError=действие – действия в случае возникновения при проверке контейнера ошибки.

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> – выполнить над объектом действие, определенное значением <параметр>.

В качестве макросов дополнительного параметра действия **exec** для контейнеров используются:

- %LIST% – имя файла или список инфицированных, подозрительных и поврежденных файлов, обнаруженных в контейнере. Формат файла имеет следующий вид: <имя вируса>\t<имя файла>.
- %FULLPATH% – полный путь до контейнера.
- %FILENAME% – имя файла без пути.
- %CONTAINERTYPE% – тип контейнера в виде строки.

Секция [**scanner.object**] содержит параметры, определяющие действия над простыми объектами того или иного типа при антивирусной защите файловых серверов:

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

OnInfected=действие – действия в случае обнаружения зараженного файла. Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, вылечить которые не удалось.

OnSuspicion=действие – действия в случае обнаружения подозрительного файла, код которого напоминает код вируса, пока неизвестного Лаборатории Касперского.

OnWarning=действие – действия в случае обнаружения файла, код которого сходен с кодом известного вируса.

OnCured=действие – действия в случае обнаружения и успешного лечения зараженного объекта.

OnProtected=действие – действия в случае обнаружения объекта, зашифрованного паролем. Такие объекты проверить невозможно.

OnError=действие – действия в случае возникновения при проверке объекта ошибки.

Синтаксис действий над всеми перечисленными видами объектов аналогичен описанному выше для контейнеров в секции **[scanner.container]**.

Секция **[scanner.display]** содержит параметры вывода отчета на консоль:

ShowContainerResultOnly=no – режим отображения на консоли результатов проверки архива в кратком формате. Для отображения краткого формата присвойте параметру значение **no**.

ShowObjectResultOnly=no – режим отображения на консоли результатов проверки простого объекта в кратком формате. Для отображения краткого отчета присвойте параметру значение **no**.

ShowOK=yes – режим вывода на консоль сообщений о незараженных файлах. Для отключения режима присвойте параметру значение **no**.

ShowProgress=yes – режим отражения на консоли текущей работы компонента (процесс загрузки антивирусных баз, информация о проверке текущего файла). Для отключения режима присвойте параметру значение **no**.

Секция **[scanner.path]** содержит параметры, определяющие путь к файлам, без которых модуль **kavscanner** не будет функционировать:

BackupPath=путь – полный путь к каталогу хранения резервных копий проверяемых компонентом объектов.

Секция **[updater.path]** включает параметры, определяющие пути к необходимым для работы компонента обновления антивирусных баз файлам:

AVBasesTestPath – полный путь к каталогу хранения антивирусных баз.

BackUpPath – полный путь к каталогу хранения резервной копии антивирусных баз.

Секция **[updater.report]** содержит параметры формирования отчета о работе компонента `keepup2date`:

Append=yes – режим добавления новых сообщений в файл отчета. Для отключения режима присвойте параметру значение **no**.

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента.

ReportLevel=4 – уровень детализации отчета.

Секция **[updater.options]** содержит параметры работы компонента `keepup2date`:

KeepSilent=no – режим вывода на консоль информации о работе компонента `keepup2date`. Для отключения режима присвойте параметру значение **yes**.

ProxyAddress – адрес используемого для соединения прокси-сервера. Параметр задается в виде **http://username:password@url:port**. В адресе прокси-сервера **username** и/или **password** могут отсутствовать. Если адрес не указан, то его значение берется из переменной окружения **http_proxy**.

UseProxy – режим использования прокси-сервера при соединении с сервером обновлений Лаборатории Касперского. Если значение параметра **no**, прокси-сервер не используется. Если значение параметра **yes**, используется адрес прокси-сервера, определенный параметром **ProxyAddress**. Если значение параметра **ProxyAddress** не определено, будет использовано значение переменной окружения **http_proxy**. Если значение переменной окружения не определено, прокси-сервер не используется.

UseUpdateServerUrl=no режим использования обновления с адреса, определенного параметром **UpdateServerUrl**.

UseUpdateServerUrlOnly=no режим использования для обновления антивирусных баз только адреса, указанного в настройке **UpdateServerUrl**. Если опции присвоено значение **no**, то в случае неудачной попытки обновления баз с адреса **UpdateServerUrl** будет использован другой адрес из списка серверов обновлений.

UpdateServerUrl=no http://url/ | ftp://url/ | /local_path/ – адрес для обновления антивирусных баз.

PostUpdateCmd – команда, выполняемая сразу после успешного завершения обновления антивирусных баз. Значение, указанное в конфигурационном файле, включенном в поставку приложения, запустит автоматическое перечитывание приложением обновленных антивирусных баз. Изменение значения этого параметра не рекомендуется.

RegionSettings=Ru код региона пользователя; применяется для выбора наиболее удобного для скачивания обновлений антивирусных баз сервера обновления Лаборатории Касперского.

ConnectTimeout=30 сетевой тайм-аут для обновления баз (в секундах). Если во время загрузки баз в течение указанного промежутка времени данные от сервера не приходят, производится выбор другого сервера из списка серверов обновлений Лаборатории Касперского.

PassiveFtp=no режим использования для соединения passive FTP.

А.2. Ключи командной строки компонента kavscanner

Параметры конфигурационного файла можно переопределить из командной строки при запуске программы с помощью ключей командной строки. Рассмотрим их подробнее.

Опции помощи:

- h** Вывести на консоль справочную информацию о компоненте kavscanner;
- v** Показать версию программы.

Опции конфигурации:

- c (-C) <путь_к_файлу>** Использовать альтернативный конфигурационный файл **<путь_к_файлу>**;
- g<путь_к_файлу>** Записать в файл **<путь_к_файлу>** список всех известных вирусов, записи о которых содержатся в антивирусных базах.
- f** Игнорировать испорченную подпись компонента kavscanner и пытаться вылечить компонент.

Опции проверки:

- e <опция>** Изменить опцию проверки, используемую по умолчанию. В качестве **<опции>** могут быть использованы следующие режимы:

P/p	Включить/выключить проверку упакованных файлов;
A/a	Включить/выключить проверку архивов;
S/s	Включить/выключить проверку самораспаковывающихся архивов;
B/b	Включить/выключить проверку почтовых баз;
M/m	Включить/выключить проверку сообщений в виде plain text;
E/e	Включить/выключить эвристический анализатор кода.
-R/r	Включить/выключить рекурсивную проверку;
-S/s	Включить/выключить режим раскрытия символьных ссылок;
-I	Проверять только локальные файловые системы.

Опции формирования отчета:

-q	Не выводить на консоль сообщения;
-o <имя>	Задать имя файла, в который будет выводиться отчет о работе компонента; если имя файла не задано, то отчет формироваться не будет;
-j<число>	Задать уровень детализации отчета по объему содержащейся в нем информации. В качестве <опции> можно использовать следующие уровни детализации:
1	Выводить/не выводить сообщения о прочих ошибках;
2	Выводить/не выводить информационные сообщения;
3	Выводить/не выводить сообщения о проверке.
-x<опция>	Задать уровень детализации отчета о проверке, выводимого на консоль. В качестве <опции> можно использовать следующие уровни детализации:

O/o	Краткий/расширенный формат сообщений о проверке простого объекта;
C/c	Краткий/расширенный формат сообщений о проверке архива;
N/n	Включить/выключить вывод на экран сообщений о незараженных файлах;
P/p	Включить/выключить вывод на консоль информации о текущей работе компонента.
-m<опция>	Задать уровень детализации отчета о проверке, выводимого в файл отчета. В качестве <опции> могут быть использованы:
O/o	Краткий/расширенный формат сообщений о проверке простого объекта;
C/c	Краткий/расширенный формат сообщений о проверке архива;
N/n	Включить/выключить вывод в файл отчета сообщений о незараженных файлах.

Опции файлов:

-p<опция> <имя_файла>	Сохранить список объектов в заданный файл; сохранять каждый объект с полным путем с новой строки. В качестве <опции> могут быть:
i	Сохранить в файл <имя_файла> список инфицированных объектов;
s	Сохранить в файл <имя_файла> список подозрительных объектов;
c	Сохранить в файл <имя_файла> список поврежденных объектов;
w	Сохранить в файл <имя_файла> список объектов, код которых похож на код известных вирусов.
-@ <filelist.lst>	Проверить объекты, путь к которым приведен в файле

<filelist.lst>.

Опции обработки файлов (определение данных ключей в командной строке отменяет выполнение действий, заданных в конфигурационном файле):

- i0** Только проверять на присутствие вирусов;
- i1** Лечить инфицированные объекты; в случае если лечение невозможно – пропустить;
- i2** Лечить инфицированные объекты; в случае если лечение невозможно, и объект является простым – удалить; инфицированный объект из контейнера не удалять;
- i3** Лечить инфицированные объекты; в случае если лечение невозможно и объект является простым – удалить; если инфицированный объект находится в контейнере – удалить контейнер целиком;
- i4** Удалить инфицированные объекты и контейнеры.

A.3. Коды возврата компонента kavscanner

В процессе работы компонент kavscanner может возвращать следующие коды:

- 0** Вирусы не найдены;
- 5** Все инфицированные объекты были вылечены;
- 10** Обнаружены архивы, защищенные паролем;
- 15** Обнаружены поврежденные файлы;
- 20** Обнаружены подозрительные файлы;
- 21** Обнаружены файлы, код которых похож на код известных вирусов;
- 25** Обнаружены зараженные файлы;

- 30 При проверке файлов возникла системная ошибка;
- 50 Невозможно загрузить антивирусные базы (путь, указанный в конфигурационном файле, не найден);
- 55 Антивирусные базы повреждены;
- 60 Дата антивирусных баз выходит за пределы срока действия лицензионного ключа;
- 64 Лицензионная информация отсутствует либо не найдено ни одного лицензионного ключа по пути, указанному в конфигурационном файле;
- 65 Невозможно загрузить конфигурационный файл;
- 66 Неверная опция конфигурационного файла;
- 70 Компонент kavscanner поврежден;
- 75 Компонент kavscanner поврежден и не может быть вылечен.

А.4. Ключи командной строки компонента kavmonitor

Опции помощи:

- h** Вывести на консоль справочную информацию о компоненте;
- v** Показать версию приложения.

Опции конфигурации:

- с<путь_к_файлу>** Использовать альтернативный конфигурационный файл **<путь_к_файлу>**.

A.5. Ключи командной строки компонента `licensmanager`

Опции помощи:

-h Вывести на консоль справочную информацию о компоненте `licensmanager`.

-v Показать версию компонента.

Опции работы с лицензионными ключами:

-s Вывести на консоль информацию обо всех установленных лицензионных ключах;

-c (-C) `<путь_к_файлу>` Использовать альтернативный конфигурационный файл `<путь_к_файлу_ключа>`;

-k `<путь_к_файлу>` Отобразить на консоли информацию о ключе `<путь_к_файлу_ключа>`;

-a `<путь_к_файлу>` Установить лицензионный ключ `<путь_к_файлу_ключа>`;

-d `<путь_к_файлу >` Удалить лицензионный ключ.

A.6. Коды возврата компонента `licensmanager`

В процессе работы компонент `licensmanager` может возвращать следующие коды:

0 Компонент успешно загрузил информацию лицензионном ключе и завершил свою работу;

30 При работе компонента возникла системная ошибка;

- 64 Лицензионная информация отсутствует либо не найдено ни одного лицензионного ключа по пути, указанному в конфигурационном файле;
- 65 Невозможно загрузить конфигурационный файл;
- 66 Неверная опция конфигурационного файла.

А.7. Ключи командной строки компонента **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;
-s	Вывести на консоль список серверов обновлений;
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 антивирусных баз;
-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 анти-вирусных баз в каталоге <путь> .
-x <путь_к_файлу>	Копировать все обновления антивирусных баз в локальный каталог <путь_к_файлу> .
-t <путь>	Использовать каталог <путь> для хранения временных файлов.
-u <путь_к_файлу>	Копировать последнее обновление антивирусных баз в локальный каталог <путь_к_файлу> ;
-с <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу> . Ключ работает, если на сервере установлено только одно приложение Лаборатории Касперского или если обновляемое приложение определено ключом -p (в противном случае будет выведено системное сообщение о нескольких установленных приложениях);
-g <URL>	Адрес для обновления антивирусных баз. 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> .

A.8. Коды возврата компонента **keepup2date**

В процессе работы компонент *keepup2date* может возвращать следующие коды:

0	Обновления антивирусных баз не требуется;
1	Обновление антивирусных баз выполнено успешно;
10	Возникла критическая ошибка, процесс обновления прерывается;
12	Возникла ошибка при откате последней версии обновления антивирусных баз;
30	Не удалось запустить команду PostUpdateCmd после обновления баз;
60	Лицензионная информация отсутствует либо не найдено ни одного лицензионного ключа по пути, указанному в конфигурационном файле;
75	Невозможно загрузить конфигурационный файл либо ошибка в его параметрах.

ПРИЛОЖЕНИЕ В. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

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



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

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



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

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

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



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

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

В отличие от других антивирусов, сокращающих время проверки путем исключения из антивирусных баз более сложных в обнаружении или более редких (например, в географическом отношении)

вирусов, а также более сложных в анализе форматов файлов (например, pdf), Лаборатория Касперского считает, что задача Антивируса – обеспечивать реальную антивирусную безопасность пользователей.

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

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



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

Без лицензионного ключа Антивирус Касперского не работает.

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



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

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

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

зии в компанию, где был приобретен Антивирус Касперского или непосредственно в ЗАО "Лаборатория Касперского".



Вопрос: лицензионный ключ к Антивирусу Касперского записан на дискету. Что делать, если в моем компьютере нет привода для чтения дискет?

Существует несколько вариантов решения этой проблемы.

Вы можете написать письмо с описанием проблемы на адрес Отдела продаж Лаборатории Касперского (sales@kaspersky.com). В письме обязательно укажите дату и место покупки Антивируса Касперского, а также его полный регистрационный номер. Менеджеры отдела продаж отправят на указанный вами электронный адрес ваш ключевой файл.

Вы также можете считать содержимое дискеты на другом компьютере, который имеет соответствующий привод и записать его на носитель, содержимое которого вы можете считать на своем компьютере. При установке Антивируса Касперского укажите данный носитель в качестве источника лицензионного ключа.

Либо считайте содержимое дискеты на другом компьютере, который имеет соответствующий привод, и отправьте ключевой файл по электронной почте на ваш почтовый адрес. Примите письмо на своем компьютере, сохраните его в любой папке на жестком диске, и при установке Антивируса Касперского укажите данную папку в качестве источника лицензионного ключа.



Вопрос: мой Антивирус не работает.

Что мне делать?

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

Также мы рекомендуем обратиться к фирме, где вы приобрели Антивирус Касперского или обратиться к разделу База Знаний на сайте Лаборатории Касперского (<http://www.kaspersky.ru/faq>).



Вопрос: Зачем нужны ежедневные обновления?

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

Лаборатория Касперского с каждым годом увеличивает частоту обновления антивирусных баз. Сейчас они обновляются каждые три часа.

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



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

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

Преимущества нового сервиса обновления:

- *Дозагрузка файлов при разрыве соединения. Теперь не нужно повторно скачивать уже полученные обновления после восстановления соединения.*
- *Двукратное уменьшение размера кумулятивного обновления. Кумулятивное обновление содержит в себе всю антивирусную базу, поэтому размер кумулятива значительно превышает размер обычного обновления. В новом сервисе применена специальная технология, позволяющая использовать уже имеющиеся антивирусные базы для кумулятивного обновления.*

- Ускорение загрузки из интернета. Антивирус Касперского выбирает сервер обновления Лаборатории Касперского, расположенный в вашем регионе. Кроме того, нагрузка на сервера распределяется в соответствии с их производительностью, то есть вы не попадете на перегруженный сервер, в то время как другой сервер будет простаивать.
- Применение "черных списков" ключей. Это позволяют исключить обновление для пользователей, не имеющих лицензии на использование Антивируса Касперского. В результате лицензированные пользователи не страдают от перегруженности серверов обновлений.
- Для корпоративных продуктов реализована возможность создания локального сервера обновлений. Такая функция востребована для организаций, где в одной локальной сети объединены компьютеры, защищенные приложениями Лаборатории Касперского. В этом случае любой компьютер может быть превращен в сервер обновлений, который будет получать обновления из интернета, помещать их в локальный каталог и предоставлять к ним доступ другим компьютерам сети.



Вопрос: *может ли злоумышленник подменить антивирусные базы?*

Все антивирусные базы имеют уникальную подпись, и при обращении к базам Антивирус Касперского проверяет ее. Если подпись не соответствует присвоенной в Лаборатории Касперского, и дата баз – более поздняя, чем день окончания лицензии на использование продукта, Антивирус Касперского не будет использовать такие базы.



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

Тестирование Антивируса Касперского версии 5.5 производилось на дистрибутивах RedHat, Debian, SUSE и Mandriva, и именно для них собирались дистрибутивы Антивируса Касперского.

О версиях поддерживаемых операционных систем см. п. 1.5 на стр. 10.

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



Вопрос: почему компонент *kavmonitor* запускает одновременно несколько процессов?

Количество запущенных процессов *kavmonitor* задается параметром **CheckFileLimit** конфигурационного файла приложения и определяет количество одновременно обрабатываемых файлов. Поэтому количество процессов монитора всегда более одного (по умолчанию запущено 20 процессов). Если файлов для проверки нет, процессы не тратят ресурсы системы.



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

Использование *Network Control Centre* для *Windows* при работе с Антивирусом Касперского для *Linux* и *FreeBSD Workstation* и *File Server* невозможно. В данной версии приложения мы предусмотрели возможность удаленной конфигурации при помощи специального модуля к пакету *Webmin*.



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

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

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

где:

`some_app` – приложение, строки стандартного вывода и вывода сообщений об ошибках в работе которого вы хотите сохранить в файле;

`text_file` – полный путь к файлу, в котором будет храниться информация.

Например:

```
$kav4fs-keepup2date > ./updater.log 2>&1
```

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

ПРИЛОЖЕНИЕ С. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

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

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

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

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

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

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

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

С.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 отдельный продукт, так и входить в состав различных интегрированных решений Лаборатории Касперского.

Kaspersky® OnLine Scanner

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

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

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные антивирусные 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 веб-браузере. В рамках проверки пользователь может:

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

Антивирус Касперского® 6.0

Антивирус Касперского 6.0 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, каталогов и дисков. Кроме этого, 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 6.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения нормальных процессов.
- **Мониторинг изменений в реестре операционной системы** благодаря контролю состояния системного реестра.
- **Блокирование опасных макросов** Visual Basic for Applications в документах Microsoft Office.
- **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 6.0

Kaspersky® Internet Security 6.0 – 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, каталоги и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;
- **проактивную защиту:** программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные изменения

файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных сценариев на веб-страницах, всплывающих окон и рекламных баннеров). Функция **блокирования платных телефонных звонков** помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и заблокировать их работу.

Kaspersky® Internet Security 6.0 **фиксирует попытки сканирования портов вашего компьютера**, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы хакерских атак. На **основе заданных правил** программа осуществляет контроль всех сетевых взаимодействий, отслеживая все **входящие и исходящие пакеты данных**. **Режим невидимости** (технология SmartStealth™) **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.

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на карманных персональных компьютерах (КПК) различных типов, а также смартфонах. В состав программы входит оптимальный набор средств антивирусной защиты:

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

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

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus 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 в карантинный каталог или удаляется;
- **постоянную проверку**: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;
- **проверку по расписанию** информации, хранимой в памяти мобильного устройства;
- **защиту от sms и mms спама.**

Антивирус Касперского® Business Optimal

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

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту¹:

- *рабочих станций* под управлением Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation, Linux.
- *файловых серверов* под управлением Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD и Linux; *файловых хранилищ* под управлением Samba.
- *почтовых систем* Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail и qmail.

¹ В зависимости от типа поставки

- *интернет-шлюзов*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition.

Антивирус Касперского® Business Optimal также включает систему централизованной установки и управления – Kaspersky® Administration Kit.

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstations и Linux.
- *файловых серверов* под управлением Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; *файловых хранилищ* под управлением Samba.
- *почтовых систем* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, sendmail, postfix, exim и qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition; Microsoft ISA Server 2004 Enterprise Edition.
- *карманных компьютеров*, работающих под управлением Symbian OS, Microsoft Windows CE и Palm OS, а также смартфонов, работающих под управлением Microsoft Windows Mobile 2003 for Smartphone и Microsoft Smartphone 2002.

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

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

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая 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.

Kaspersky Security® для Microsoft Exchange 2003

Kaspersky Security® для Microsoft Exchange обеспечивает антивирусную проверку входящих, исходящих и хранящихся на сервере почтовых сообщений, в том числе сообщений в общих папках, а также осуществляет фильтрацию нежелательной корреспонденции, используя интеллектуальные технологии распознавания спама в сочетании с технологиями компании Microsoft. Приложение проверяет все сообщения, поступающие на Exchange-сервер по SMTP-протоколу, на наличие вирусов и признаков спама. При этом программа использует уникальные антивирусные технологии, осуществляет фильтрацию по формальным признакам (почтовому адресу, IP-адресу, размеру письма, заголовку), а также анализирует содержимое письма и его вложений с помощью интеллектуальных технологий (включая уникальные графические сигнатуры для распознавания спама в виде изображений). Проверке подвергается как тело сообщения, так и прикрепленные файлы.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway – универсальное решение для комплексной защиты пользователей почтовой системы. Установленное между корпоративной сетью и сетью интернет, приложение осуществляет проверку всех элементов электронного письма на присутствие вирусов и других вредоносных программ (Spyware, Adware, и т.д.), а также производит централизованную фильтрацию спама в потоке почтовых сообщений. Приложение содержит ряд дополнительных инструментов фильтрации почтового трафика – по именам и MIME-типам вложенных файлов, а также ряд средств, позволяю-

щих снизить нагрузку на почтовую систему и предотвратить хакерские атаки.

Антивирус Касперского® для Proxy Server

Антивирус Касперского® для Proxy Server – антивирусное решение для защиты веб-трафика, проходящего по HTTP-протоколу через прокси-сервер. В режиме реального времени приложение осуществляет антивирусную проверку интернет-трафика, защищает от проникновения вредоносного программного обеспечения в результате веб-сёрфинга, сканирует файлы, скачиваемые из сети интернет.

Антивирус Касперского® для MIMESweeper for SMTP

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

Программа выполнена в виде plug-in для приложения MIMESweeper for SMTP компании Clearswift и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

С.2. Наши координаты

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

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700
Экстренная круглосуточная помощь:	+7 (495) 797-8707
Поддержка пользователей персональных продуктов и Business Optimal:	+7 (495) 797-8707 (с 10 до 19 часов) http://www.kaspersky.ru/helpdesk.html

Поддержка пользователей Corporate Suite:	Телефоны и электронный адрес предоставляются при покупке Corporate Suite в зависимости от пакета технической поддержки.
База знаний Лаборатории Касперского:	http://www.kaspersky.ru/faq
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-8700 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru