

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского® 5.5
для Samba Servers

РУКОВОДСТВО

администратора

АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ SAMBA SERVERS

Руководство администратора

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

Дата редакции: ноябрь 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. Аппаратные и программные требования к системе	9
1.4. Комплект поставки.....	11
1.4.1. Лицензионное соглашение.....	11
1.4.2. Регистрационная карточка	12
1.5. Сервис для зарегистрированных пользователей	12
1.6. Принятые обозначения.....	13
ГЛАВА 2. ВНУТРЕННЯЯ АРХИТЕКТУРА АНТИВИРУСА КАСПЕРСКОГО	15
2.1. Компонентный состав	15
2.2. Алгоритм работы	16
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО.....	17
3.1. Установка приложения на сервер под управлением Linux.....	17
3.2. Установка приложения на сервер под управлением FreeBSD	18
3.3. Процесс установки	18
3.4. Конфигурация приложения	19
3.5. Схема расположения файлов по каталогам	20
3.6. Обновление версии Samba-сервера	22
3.7. Удаление Антивируса Касперского.....	23
ГЛАВА 4. ПОСТИНСТАЛЛЯЦИОННАЯ НАСТРОЙКА	25
4.1. Настройки приложения по умолчанию	25
4.2. Установка антивирусных баз	26
4.3. Настройка совместной работы с Webmin	26
4.4. Рекомендуемые режимы работы.....	27
4.4.1. Оптимальный режим работы	27
4.4.2. Режим максимального быстродействия.....	29
4.4.3. Режим максимальной надежности.....	29
4.4.4. Режим проверки часто обновляемых файлов	31

ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО ДЛЯ SAMBA SERVERS.....	33
5.1. Обновление антивирусных баз	33
5.1.1. Автоматическое обновление антивирусных баз	35
5.1.2. Обновление антивирусных баз по требованию	36
5.1.3. Создание сетевого каталога для хранения и копирования антивирусных баз.....	37
5.2. Антивирусная защита Samba-сервера в реальном времени.....	38
5.2.1. Настройка уведомления пользователя.....	39
5.2.1.1. Мониторинг с уведомлением посредством smbclient	39
5.2.1.2. Мониторинг с уведомлением посредством почтовых сообщений	40
5.3. Антивирусная защита файловых систем.....	41
5.3.1. Проверка файлов по запросу.....	42
5.3.2. Проверка каталога по расписанию (cron).....	42
5.3.3. Дополнительные возможности: использование скрипт-файлов.....	43
5.3.3.1. Отправка администратору уведомления	43
ГЛАВА 6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА	44
6.1. Настройка антивирусной защиты в реальном времени.....	44
6.1.1. Область мониторинга.....	44
6.1.2. Режим проверки и лечения файлов	45
6.1.3. Действия над файлами.....	46
6.1.4. Изоляция зараженных объектов	47
6.1.5. Режим резервного копирования объектов	48
6.2. Настройка антивирусной защиты файловых систем	48
6.2.1. Область проверки	49
6.2.2. Режим проверки и лечения файлов.....	50
6.2.3. Действия над файлами.....	50
6.2.4. Режим резервного копирования	51
6.3. Оптимизация работы Антивируса Касперского для Samba Servers	52
6.4. Перезагрузка Антивируса Касперского	54
6.5. Локализация отображаемого формата даты и времени	56
6.6. Параметры формирования отчета Антивируса Касперского.....	56
ГЛАВА 7. УПРАВЛЕНИЕ ЛИЦЕНЗИОННЫМИ КЛЮЧАМИ	59
7.1.1. Просмотр информации о лицензионном ключе	60
7.1.2. Продление лицензии.....	61

7.1.3. Удаление лицензионного ключа.....	62
ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА	63
ГЛАВА 9. ВОЗМОЖНЫЕ ВОПРОСЫ ПРИ РАБОТЕ С ПРИЛОЖЕНИЕМ.....	65
ПРИЛОЖЕНИЕ А. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ПРИЛОЖЕНИИ	70
А.1. Конфигурационный файл Антивируса Касперского.....	70
А.2. Ключи командной строки компонента kav samba.....	79
А.3. Коды возврата компонента kav samba.....	80
А.4. Ключи командной строки компонента kavscanner	80
А.5. Коды возврата компонента kavscanner.....	84
А.6. Ключи командной строки компонента licensemanager.....	85
А.7. Коды возврата компонента licensemanager	85
А.8. Ключи командной строки компонента keeprp2date	86
А.9. Коды возврата компонента keeprp2date	87
ПРИЛОЖЕНИЕ В. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"	89
В.1. Другие разработки Лаборатории Касперского	90
В.2. Наши координаты	97

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® 5.5 для Samba Servers** (далее также **Антивирус Касперского**) обеспечивает антивирусную проверку объектов на Samba-серверах, работающих под управлением операционной системы Linux или FreeBSD.

Приложение выполняет двухуровневую проверку файловой системы сервера: как в масштабе реального времени, так и по требованию. В случае нахождения вредоносных программ Антивирус Касперского позволяет эффективно лечить или блокировать зараженные объекты во избежание дальнейшего распространения эпидемии и оперативно уведомлять системного администратора о произошедшем инциденте.



Также приложение использует iChecker™ – интеллектуальную технологию, позволяющую существенно увеличить скорость проверки файлов.

Антивирус Касперского для Samba Servers представляет собой набор компонентов, выполняющих следующие функции:

- *Постоянная защита* файлового сервера Samba от вредоносного кода (**On-Access Scanner**).
- *Поиск и обезвреживание* вредоносного кода в файловой системе сервера *по требованию* (**On-Demand Scanner**).
- *Уведомление администратора* о нахождении зараженных или подозрительных объектов.
- *Поддержка актуального состояния антивирусных баз* (**keepup2date**).
- *Локальное и удаленное администрирование* с помощью модуля веб-администрирования (**Webmin**).

Кроме того, Антивирус Касперского предоставляет своим пользователям следующую дополнительную функциональность:

- Возможность исполнять заданные пользователем скрипты в случае возникновения событий типа "найден зараженный файл".
- Возможность переноса зараженных (или подозрительных) объектов в специальное хранилище (карантин).
- Сохранение оригинала инфицированного объекта перед лечением (Backup) с возможностью его восстановления в случае возникновения нештатной ситуации.
- Сохранение данных об уже проверенных файлах в оперативном кеше, что позволяет значительно уменьшить время проверки файла при последующих его запросах (данные в кеше сохраняются до перезагрузки приложения).
- Возможность ограничения максимального количества одновременно проверяемых в режиме реального времени файлов с постановкой остальных запрошенных на проверку файлов в очередь.
- Возможность автоматически приостановить антивирусную проверку файлов в фоновом режиме при превышении уровня нагрузки на сервер сверх указанного пользователем значения и возобновить работу при снижении нагрузки до допустимого уровня.
- Возможность для каждой папки общего доступа задать любую комбинацию режимов "проверки при открытии" и "проверки при сохранении".
- Возможность проведения индивидуальных настроек антивирусной защиты выборочно для каждой папки общего доступа.
- При обновлении антивирусных баз определяется наименее загруженный сервер обновлений Лаборатории Касперского. Кроме того, в случае разрыва соединения после его восстановления процесс обновления продолжает свою работу с момента прерывания.
- Возможность отката как обновлений антивирусных баз, так и обновлений приложения.

1.3. Аппаратные и программные требования к системе

Для работы **Антивируса Касперского для Samba Servers** необходимы:

- 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.
 - SUSE Linux Enterprise Server 9.0 SP3.
 - SUSE Linux Professional 10.1.
 - Debian GNU/Linux версия 3.1 R2.
 - Mandriva 2006.
 - FreeBSD версия 4.11.
 - FreeBSD версия 5.4.
 - FreeBSD версия 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 Linux Enterprise Server 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.
 - Установленный Samba-сервер версий 2.2.7 и выше либо версий от 3.0.0 до 3.0.23с.



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.

Кроме того, если на вашем сервере установлена защита с помощью списков контроля доступа файловой системы (File System Access Control Lists, ACLs), необходимо настроить сервер Samba для поддержки данной функциональности.

1.4. 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.

1.4.1. 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.

1.4.2. 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", высылается информация о выходе новых программных продуктов.

1.5. 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.

1.6. 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.
 Внимание!	Информация, на которую следует обратить особое внимание.
 <i>Чтобы выполнить действие,</i> 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

Оформление	Смысловое назначение
[ключ] – назначение ключа.	Ключи командной строки.
Текст информационных сообщений и командной строки	Текст конфигурационных фай, информационных сообщений программы и командной строки.

ГЛАВА 2. ВНУТРЕННЯЯ АРХИТЕКТУРА АНТИВИРУСА КАСПЕРСКОГО

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

2.1. Компонентный состав

Антивирус Касперского для Samba Servers состоит из следующих компонентов:

- *kavsamba* (On-Access Scanner);
- *kavscanner* (On-Demand Scanner);
- *keepup2date*.

Компонент *kavsamba* в свою очередь включает в себя модули *kavsamba.so* и *kavsamba*. Модуль *kavsamba.so* выполнен в виде динамической библиотеки, интегрируемой в сервер Samba, для перехвата обращений через него к файлам. Модуль *kavsamba* является процессом-демоном, который анализирует переданные *kavsamba.so* файлы и производит их обработку в соответствии с текущими настройками. Обмен данными между модулем и процессом-демоном выполняется через локальный сокет (Unix Domain sockets).

Компонент *kavscanner* предназначен для антивирусной защиты файловых систем. Проверка файловых систем сервера или файлов отдельных каталогов производится по требованию администратора или по расписанию (в зависимости от выбранных настроек).

Компонент *keepup2date* обновляет антивирусные базы, используемые при поиске и лечении вирусов, а также скачивает патчи для обновления программных модулей приложения.

2.2. Алгоритм работы

В данном разделе мы рассмотрим внутреннюю архитектуру приложения в контексте антивирусной защиты в реальном времени, поскольку процесс проверки по требованию достаточно прост и не нуждается в отдельном изучении.

Итак, предусмотрен следующий алгоритм работы:

1. При попытке доступа пользователя к какому-либо файлу через сервер Samba запрос перехватывается самим сервером и передается модулю *kavsamba.so*.
2. Модуль *kavsamba.so* отправляет данные о запросе (имя файла, полный путь к нему, идентификационный номер (ID) пользователя, запросившего файл, доменное имя компьютера) модулю *kavsamba* с помощью IPC по бинарному протоколу.
3. Модуль *kavsamba* выполняет проверку на присутствие вирусов и обработку запрошенного объекта в соответствии с настройками конфигурационного файла (в том числе и лечение с помощью антивирусных баз, если данная опция включена).
4. По окончании проверки и действий над файлом *kavsamba.so* получает от *kavsamba* код доступа (разрешен/запрещен), определяющий статус файла.
5. В соответствии со статусом объекта *kavsamba.so* передает серверу Samba разрешение на доступ к объекту, либо блокирует его.

Доступ к файлу блокируется, если он является зараженным либо подозревается на заражение вирусом (Infected, CureFailed, Warning, Suspicion). Во всех остальных случаях доступ к файлу разрешается.

ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

Прежде чем приступить к установке Антивируса Касперского мы рекомендуем вам:

- Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. п. 1.3 на стр. 9).
- Войти в систему под пользователем **root**.

3.1. Установка приложения на сервер 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 сервер под управлением FreeBSD

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



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

```
pkg_add <имя_пакета>
```

3.3. Процесс установки



По ряду причин процесс установки может завершиться с кодом ошибки. В этом случае убедитесь, что ваш компьютер соответствует аппаратным и программным требованиям (см. п. 1.3 на стр. 9), а также что вход в систему выполнен с правами root.

Инсталляция приложения на сервер включает в себя несколько этапов:

1. Копирование файлов дистрибутива на сервер.
2. Конфигурация компонента *keepup2date*.
3. Установка (обновление) антивирусных баз.



Не забудьте установить антивирусные базы перед началом использования приложения. Процедура поиска и лечения вирусов основывается на записях антивирусных баз, содержащих описание всех известных на настоящий момент вирусов и способов лечения зараженных ими объектов. Без антивирусных баз проверка и обработка файлов невозможна!

Обратите внимание, что в случае если антивирусные базы не будут установлены, автоматическая конфигурация приложения не выполняется.

4. Установка лицензионного ключа.

Если лицензионный ключ не установлен, процесс конфигурации не выполняется, и работа с приложением 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.

5. Установка модуля Webmin.

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

3.4. Конфигурация приложения

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

Процесс конфигурации приложения включает в себя:

- Поиск установленного сервера Samba и проверка его версии на соответствие программным требованиям.
- Поиск и изменение конфигурационного файла сервера Samba.
- Проверка конфигурационного файла сервера Samba на наличие VFS-объектов. Если в конфигурационном файле сервера Samba уже присутствуют строки с используемыми VFS-объектами, производится комментирование данных строк.



Если вы используете операционную систему FreeBSD и Samba-сервер версий от 3.0 до 3.0.9, из-за специфики операционной системы существует вероятность некорректной работы с VFS-модулями.

Для обеспечения правильного функционирования приложения с VFS-объектами мы рекомендуем обновить версию сервера Samba либо установить патч для Samba-сервера (подробнее о патче см. https://bugzilla.samba.org/show_bug.cgi?id=2100).

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

Если все описанные выше шаги конфигурации завершились успешно, приложение готово к работе, и дополнительное оповещение не производится.

Конфигурационный файл, входящий в поставку приложения, содержит все необходимые для начала работы настройки.



Не забудьте перед началом работы произвести перезагрузку сервера Samba.

3.5. Схема расположения файлов по каталогам

После установки Антивируса Касперского (при условии принятия всех предлагаемых по умолчанию во время инсталляции путей) файлы дистрибутива будут расположены следующим образом:

Если у вас установлена ОС Linux:

/etc/opt/kaspersky/ – каталог, содержащий конфигурационный файл Антивируса Касперского и другие файлы настроек:

kav4samba.conf – конфигурационный файл.

/var/opt/kaspersky/kav4samba/bases и */var/opt/kaspersky/kav4samba/licenses* – каталоги, содержащие антивирусные базы и лицензионные ключи.

/opt/kaspersky/kav4samba – основной каталог Антивируса, включающий:

/bin/ – каталог исполняемых файлов всех компонентов Антивируса Касперского для Samba Servers:

kav4samba-kavscanner – исполняемый файл компонента антивирусной защиты файловых серверов *kavscanner* (On-Demand Scanner);

kav4samba-licensemanager – исполняемый файл компонента работы с лицензионными ключами *licensemanager*;

kav4samba-keepup2date – исполняемый файл компонента *keepup2date*, обновляющего антивирусные базы.

/sbin/kav4samba-kavsamba – исполняемый файл компонента антивирусной защиты в реальном времени *kavsamba* (On-Access Scanner).

/lib/bin/setup/kavsamba_setup.pl – скрипт, выполняющий интеграцию с Samba-сервером.

/share/man – каталог *man*-файлов.



Для подключения справочной системы Антивируса Касперского (*manual pages*) добавьте в переменную окружения *MANPATH* значение */opt/kaspersky/kav4samba/share/man*.

/opt/kaspersky/kav4samba/lib/ – каталог, содержащий модули Samba для 32-битных операционных систем.

/opt/kaspersky/kav4samba/lib64/ – каталог, содержащий модули Samba для 64-битных операционных систем.

/opt/kaspersky/kav4samba/share/contrib/kavsamba.wbm – каталог хранения модуля Webmin.

/opt/kaspersky/kav4samba/share/contrib/vox.sh – скрипт лечения архивов.

/opt/kaspersky/kav4samba/share/doc/ – каталог хранения лицензий и документации Samba.

/opt/kaspersky/kav4samba/src/ – каталог, содержащий исходный код модуля для Samba-сервера.

/var/opt/kaspersky/kav4samba/bases/ – каталог хранения антивирусных баз.

/var/opt/kaspersky/kav4samba/bases.backup/ – каталоги, содержащие резервные копии антивирусных баз (на случай необходимости отката баз).

/var/log/kaspersky /- каталог хранения файлов отчета (log-файлов) по работе компонентов приложения.

Если у вас установлена ОС FreeBSD:

/usr/local/etc/kaspersky/ – каталог, содержащий конфигурационный файл Антивируса Касперского и другие файлы настроек:

kav4samba.conf – конфигурационный файл.

kav4samba.conf.default – конфигурационный файл с настройками, принятыми по умолчанию.

/var/db/kaspersky/kav4samba/bases/ и */var/db/kaspersky/kav4samba/licenses/-* каталоги, содержащие антивирусные базы и лицензионные ключи.

/usr/local/ – системная папка, предназначенная для установки программ администратором. В данную папку Антивирус Касперского добавляет исполняемые файлы всех компонентов:

kav4samba-kavscanner – исполняемый файл компонента антивирусной защиты файловых серверов kavscanner (On-Demand Scanner);

kav4samba-licensemanager – исполняемый файл компонента работы с лицензионными ключами licensemanager;

kav4samba-keepup2date – исполняемый файл компонента keepup2date, обновляющего антивирусные базы.

/usr/local/sbin/kav4samba-kavsamba – исполняемый файл компонента антивирусной защиты в реальном времени kavsamba (On-Access Scanner).

/usr/local/libexec/kaspersky/kav4samba/setup/kavsamba_setup.pl – скрипт, выполняющий интеграцию с Samba-сервером.

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

/usr/local/lib/kaspersky/kav4samba/ – каталог, содержащий модули Samba для 32-битных операционных систем.

`/usr/local/share/kav4samba/contrib/kavsamba.wbm` – каталог хранения модуля Webmin.

`/usr/local/share/kav4samba/contrib/vox.sh` – скрипт лечения архивов.

`/usr/local/share/doc/kav4samba/` – каталог хранения лицензий и документации Samba.

`/usr/local/src/kav4samba/` – каталог, содержащий исходный код модуля для Samba-сервера.

`/var/db/kaspersky/kav4samba/bases.backup/`– каталоги, содержащие резервные копии антивирусных баз (на случай необходимости отката баз).

`/var/log/kaspersky/`– каталог хранения файлов отчета (log-файлов) по работе компонентов приложения.



В дальнейшем при рассмотрении примеров решения задач будет предполагаться, что Антивирус Касперского установлен на сервер под управлением операционной системы Linux.

3.6. Обновление версии Samba-сервера



Дистрибутив Антивируса Касперского содержит бинарные vfs-модули для поддерживаемых версий Samba.

Если установлена новая версия Samba Servers, не поддерживаемая Антивирусом Касперского, возможно вручную выполнить переборку vfs-модуля приложения.

Для этого:

Если у вас установлена операционная система Linux, в командной строке введите:

```
cd /opt/kaspersky/kav4samba/src
./configure --with-sambasrc=<path_to_samba> && make
```

где `<path_to_samba>` – путь к исходным модулям сервера Samba.

Если у вас установлена операционная система FreeBSD, в командной строке введите:

```
cd /usr/local/src/kav4samba
./configure --with-sambasrc=<path_to_samba> && make
```

где `<path_to_samba>` – путь к исходным модулям сервера Samba.

Подкаталог `lib` будет содержать обновленную версию vfs-модуля. Задача конфигурации и установки данного модуля возлагается на администратора.

3.7. Удаление Антивируса Касперского

Выполнение процедуры деинсталляции для Samba-сервера требует:

- Наличия прав привилегированного пользователя (**root** или другой пользователь с UID=0). Если на момент деинсталляции вы не обладаете такими правами, то вам необходимо войти в систему под пользователем **root**.
- Остановки сервера Samba.



Процесс деинсталляции самостоятельно не останавливает работу сервера Samba!

Процесс удаления Антивируса Касперского будет выполнен в автоматическом режиме. Запуск процесса происходит различными способами в зависимости от используемого дистрибутива.



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

```
rpm -e <имя_пакета>
```



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

```
dpkg -r <имя_пакета>
```



В связи с особенностями операционной системы Debian GNU/Linux, автоматически удалить скрипты управления Антивируса Касперского невозможно. По завершению процедуры деинсталляции администратору необходимо вручную удалить из системы скрипт **/opt/kaspersky/kav4samba/lib/bin/kav4samba**.



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

```
pkg_delete <имя_пакета>
```

В случае успешного завершения процедуры удаления дополнительных оповещений не производится.



Если при инсталляции приложения была произведена установка модуля удаленного управления к пакету **Webmin**, его необходимо удалить вручную.

Для этого в главном окне программы Webmin необходимо перейти на закладку **Webmin Modules** и в списке **Delete Modules** выбрать строку **KAV for Samba Servers**, после чего нажать на кнопку **Delete Selected Modules**.

ГЛАВА 4.

ПОСТИНСТАЛЛЯЦИОННАЯ НАСТРОЙКА

В процессе инсталляции выполняется анализ системы, на которую устанавливается Антивирус Касперского, и некоторые параметры его конфигурации определяются автоматически. Ряд параметров конфигурационного файла приложения определен по умолчанию как наиболее удобный для работы с приложением (см. п. 4.1 на стр. 25).



Прежде чем приступить к работе с приложением, мы рекомендуем вам установить или обновить антивирусные базы, если это не было сделано во время инсталляции!

Кроме того, проведите настройку совместной работы Антивируса Касперского с пакетом Webmin.

В данной главе мы рассмотрим, какие установки Антивируса Касперского приняты по умолчанию, а также ознакомимся с необходимой для работы с приложением конфигурацией.

4.1. Настройки приложения по умолчанию

Все параметры функционирования Антивируса Касперского хранятся в конфигурационном файле приложения, используемом по умолчанию.



Вы можете создавать собственные конфигурационные файлы и использовать их как при выполнении текущей задачи, так и в качестве конфигурационного файла по умолчанию.

Рассмотрим подробнее, какие параметры заданы в данном файле по умолчанию. Исходя из информации данного раздела вы сможете определить, нуждается ли Антивирус Касперского в дополнительной конфигурации (см. Глава 6 на стр. 44) для наиболее полного его использования в условиях вашего предприятия.

По умолчанию конфигурация Антивируса Касперского выполнена таким образом, что компонент антивирусной защиты в реальном времени (*kavsamba*) начинает свою работу при старте операционной системы. При

запуске компонента проверки по требованию (*kavscanner*) без дополнительных ключей командной строки *антивирусная проверка* каталогов и файловых систем сервера проводится, начиная с текущего каталога.

При этом в случае обнаружения инфицированных, подозрительных или поврежденных файлов на консоль и в файл отчета выводятся соответствующие сообщения.



Обратите внимание на то, что **ПО УМОЛЧАНИЮ НЕ ВЫПОЛНЯЕТСЯ ЛЕЧЕНИЕ** обнаруженных инфицированных файлов!

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/ kav4samba-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 вкладке **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!**

4.4. Рекомендуемые режимы работы

В зависимости от величины нагрузки на сервер Лаборатория Касперского рекомендует несколько вариантов настройки для оптимальной работы Антивируса Касперского. Рассмотрим их подробнее.

4.4.1. Оптимальный режим работы

При использовании данного режима достигается оптимальный баланс между скоростью работы сервера и обеспечиваемым уровнем безопасности.



Для настройки оптимального режима работы внесите следующие изменения в конфигурационный файл:

- Установите значение размера файлового кеша примерно соответствующее количеству файлов, доступных через сервер Samba. Рекомендуется исходить из расчета, что запись о неинфицированном файле в кеше занимает порядка 50 байт (секция **[samba.options]** параметр **FileCacheSize**).

- В секции **[path]** установите следующее значение для параметра:

```
IcheckerDbFile=/var/opt/kaspersky/kav4samba/ichecker.db
```

- В секции **[samba.options]** установите следующие значения для параметров:

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
Ichecker=yes
CheckFilesLimit=20
BgCheckFilesLimit=5
BgSheduleTime=10
HashType=md5
```

- В секции **[samba.path]** установите следующие значения для параметров:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
SambaConfigFile=/etc/samba/smb.conf
```

- В секции **[samba.actions]** установите следующие значения для параметров:

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

- В секции **[samba.shares]** установите следующие значения для параметров:

```
CheckOnOpen=yes
CheckOnClose=yes
```



Кроме того, убедитесь, что в *kavscanner* включено использование технологии **iChecker** (секция **[scanner.options]** параметр **IChecker=yes**). Также компоненты *kavsamba* и *kavscanner* должны использовать одинаковые опции настройки параметров **Packed Archives SelfExtArchives MailBases MailPlain Heuristic** (секции **[scanner.options]** и **[samba.options]**).

4.4.2. Режим максимального быстродействия

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

Рекомендуется отключить проверку архивов и не производить проверку файлов при закрытии. Соответственно, приложение не проверяет архивы, которые могут быть инфицированы. Также на сервер могут быть записаны зараженные объекты, которые будут проверены только при их открытии (обращении к ним пользователей на чтение).



Для настройки данного режима необходимо внести следующие изменения в конфигурационный файл:

- В секции **[samba.options]** установите следующие значения для параметров:

```
Ichecker=no  
FileCacheSize=15000  
CheckFilesLimit=0  
HashType=crc32
```

- В секции **[samba.shares]** установите следующие значения для параметров:

```
CheckOnOpen=yes  
CheckOnClose=no
```

4.4.3. Режим максимальной надежности

При данном варианте настроек достигается максимальная надежность защиты сервера, так как файлы проверяются и при чтении и при записи. Однако работа приложения будет несколько замедлена.



Для настройки данного режима необходимо внести следующие изменения в конфигурационный файл:

- В секции **[samba.options]** установите следующие значения для параметров:

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
FileCacheSize=0
CheckFilesLimit=0
BgCheckFilesLimit=0
BgScheduleTime=0
HashType=md5
```

- В секции **[samba.path]** установите следующее значение для параметра:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
```

- В секции **[samba.actions]** установите следующие значения для параметров:

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```



Кроме того, убедитесь, что в *kavscanner* включено использование технологии **iChecker** (секция **[scanner.options]** параметр **IChecker=yes**). А также компоненты *kavsamba* и *kavscanner* должны использовать одинаковые опции настройки параметров **Packed Archives SelfExtArchives MailBases MailPlain Heuristic** (секции **[scanner.options]** и **[samba.options]**).

4.4.4. Режим проверки часто обновляемых файлов

Данный режим рекомендован для настройки антивирусной защиты папок общего доступа, в которых происходит частое обновление файлов.

Режим проверки часто обновляемых файлов отличается от **рекомендованного режима** (см. п. 4.4.1 на стр. 27) тем, что для увеличения быстродействия предлагается не проверять файлы в некоторых папках общего доступа после записи (в рассматриваемом ниже примере это папка public).

Для таких папок рекомендуется отключить проверку содержащихся в них файлов при закрытии. В таком случае содержимое папки будет проверено на присутствие вирусов либо при обращении к нему пользователя, либо при проверке в фоновом режиме.

Общие настройки для всех остальных папок аналогичны **рекомендуемому режиму**.



Для настройки данного режима необходимо внести следующие изменения в конфигурационный файл:

- В секции **[path]** установите следующее значение для параметра:

```
IcheckerDbFile=  
/var/opt/kaspersky/kav4samba/ichecker.db
```

- В секции **[samba.options]** установите следующие значения для параметров:

```
Packed=yes  
Archives=yes  
SelfExtArchives=yes  
MailBases=yes  
MailPlain=yes  
Heuristic=yes  
Cure=yes  
Ichecker=yes  
FileCacheSize=20000  
CheckFilesLimit=20  
BgCheckFilesLimit=5  
BgSheduleTime=10  
HashType=md5
```

- В секции **[samba.path]** установите следующие значения для параметров:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected  
SambaConfigFile=/etc/samba/smb.conf
```

- В секции **[samba.actions]** установите следующие значения для параметров:

```
OnInfected=remove  
OnSuspicion=remove  
OnWarning=remove
```

- В секции **[samba.shares]** установите следующие значения для параметров:

```
CheckOnOpen=yes  
CheckOnClose=yes
```

- В секции **[samba.shares:public]** установите следующие значения для параметров:

```
CheckOnOpen=yes  
CheckOnClose=no
```

ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО ДЛЯ SAMBA SERVERS

Обеспечение антивирусной безопасности осуществляется как в режиме постоянной защиты, так и по требованию. Рассмотрим эти возможности подробнее.

Режим *постоянной защиты* (защиты в реальном времени) реализуется путем перехвата компонентом *kavsamba* обращений к файлам на открытие, проходящих через Samba-сервер, а также проверки файлов в фоновом режиме при закрытии. Файлы анализируются на присутствие вирусов и обрабатываются в соответствии с настройками. Доступ к опасным файлам блокируется.

При *проверке по требованию*, осуществляемой компонентом *kavscanner*, можно запросить проверку любых файлов (в том числе почтовых баз, архивных файлов и т.п.). По ее результатам к зараженным файлам будет применено действие, установленное в настройках конфигурационного файла.

Кроме того, важным компонентом обеспечения антивирусной безопасности является *обновление антивирусных баз* посредством компонента *keepup2date*. Этот компонент осуществляет обновление антивирусных баз и программных модулей как локально, так и удаленно.



Обратите внимание на то, что во всех рассматриваемых далее для компонента *kavsamba* примерах после внесения изменений в конфигурационный файл необходимо произвести перезагрузку Антивируса Касперского. Подробнее о способах проведения перезагрузки см. п. 6.4 на стр. 54.

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 несколько раз в 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. 5.1.3 на стр. 37.

Обновление может быть организовано по расписанию с помощью программы **cron** (см. п. 5.1.1 на стр. 35) или же выполняться по требованию администратора, запускаясь вручную из командной строки (см. п. 5.1.2 на стр. 36).



Настоятельно рекомендуем настроить обновление антивирусных баз не реже раза в час!

Также в версии 5.5 Антивируса Касперского реализована возможность выбора набора используемых антивирусных баз, что позволяет обеспечивать оптимальную степень надежности антивирусной защиты.

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.

5.1.1. Автоматическое обновление антивирусных баз

Вы можете спланировать регулярное автоматическое обновление антивирусных баз при помощи программы cron.



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=4
```

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

```
0 0-23/3 * * */opt/kaspersky/kav4samba/bin/kav4samba-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 **UseUpdateServerUrl** и **UseUpdateServerUrlOnly** секции **[updater.options]** значение **Yes**. Кроме того, параметр **UpdateServerUrl** 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 **UseUpdateServerUrl** секции **[updater.options]** значение **Yes**, а параметру **UseUpdateServerUrlOnly** значение **No**. Кроме того, параметр **UpdateServerUrl** должен содержать адрес сервера обновлений.

5.1.2. 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:

```
# kav4samba-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:

```
# kav4samba-keepup2date -l /tmp/report.txt
```

5.1.3. 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:

```
# kav4samba-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 Samba-сервера в реальном времени

Антивирусная защита Samba-сервера в реальном времени производится посредством компонента *kavsamba*, который отслеживает обращения к файлам через Samba-сервер. *Kavsamba* запускается при старте сервисов операционной системы. После анализа запрошенного файла с помощью

антивирусного ядра, встроенного в компонент, *kavsamba* принимает решение о дальнейшей работе с ним (разрешать/запрещать доступ).

По умолчанию режим лечения инфицированных объектов отключен, при обнаружении зараженных, подозрительных или поврежденных объектов доступ к ним блокируется, и соответствующая информация заносится в отчет.



Все настройки компонента *kavsamba* сгруппированы в секциях **[samba.*]** конфигурационного файла приложения.

Вы можете дополнительно включить режимы лечения инфицированных объектов, переноса их в отдельный каталог и т.д. Для этого необходимо произвести соответствующие настройки конфигурационного файла. Подробнее об этом см. п. 6.1.3 на стр.46.

5.2.1. Настройка уведомления пользователя

Так как *kavsamba* работает в фоновом режиме, то на консоль выводится только стартовая и справочная информация. Дополнительная настройка получения уведомлений может быть реализована, например, посредством почтовых сообщений или через стандартную утилиту **smclient**. Рассмотрим эти возможности подробнее.

5.2.1.1. Мониторинг с уведомлением посредством smclient

Стандартная утилита **smclient** служит для передачи **winpopup**-сообщения локальному компьютеру. В операционной системе Windows такие сообщения (**winpopup**) выводятся на экран, если включена служба Messenger. В ряде случаев данная утилита устанавливается автоматически, однако перед началом работы следует убедиться, что **smclient** установлена.

Данную возможность полезно использовать для предупреждения пользователей при попытке обращения к инфицированному файлу через Samba-сервер.

Рассмотрим на примере такой способ уведомления:



Задача: выводить на экран пользователя уведомление при попытке обратиться к инфицированному файлу через Samba-сервер.



Решение: для реализации поставленной задачи выполните следующие действия:

1. Задайте действие (в данном случае вывод на экран уведомления) над инфицированным файлом. Для этого в конфигурационном файле в секции **[samba.notify]** в качестве действия укажите следующую строку:

```
OnInfected=exec echo "%USER%  
%FULLPATH%/%FILENAME% is infected by %VIRUSNAME%"  
| smbclient -M %USERHOST%
```

2. Перезагрузите Антивирус Касперского.

5.2.1.2. Мониторинг с уведомлением посредством почтовых сообщений

При организации мониторинга с передачей через электронную почту предупреждения о попытке обращения к зараженному или подозрительному файлу отправляются в теле электронного сообщения на указанный адрес.



Для того чтобы получать уведомления по электронной почте, почтовая система должна быть настроена!



Задача: уведомить администратора о попытке пользователя обратиться к инфицированному или подозрительному файлу через Samba-сервер.



Решение: для реализации поставленной задачи выполните следующие действия:

1. Задайте действие над инфицированным объектом. Для этого в конфигурационном файле в секции **[samba.notify]** в качестве действия укажите следующую строку:

```
OnInfected=exec echo "%USER%  
%FULLPATH%/%FILENAME% from %USERHOST% is infected  
by %VIRUSNAME%" | mail -s 'Virus notification'  
spam-virus@localhost.ru  
OnWarning=exec echo "%USER% %FULLPATH%/%FILENAME%  
from %USERHOST% is probably infected by  
%VIRUSNAME%" | mail -s 'Virus notification' spam-  
virus@localhost.ru  
OnSuspicion=exec echo "%USER%  
%FULLPATH%/%FILENAME% from %USERHOST% is probably  
infected by %VIRUSNAME%" | mail -s 'Virus notifi-  
cation' spam-virus@localhost.ru
```



Не забудьте произвести перезагрузку Антивируса Касперского (см. п. 6.4 на стр. 54).

5.3. Антивирусная защита файловых систем



Запуск проверки по требованию может выполнить только пользователь **root!**

Антивирусная защита файловых систем сервера осуществляется с помощью компонента *kavscanner*, который проверяет файлы сервера на присутствие вирусов и выполняет обработку зараженных и/или подозрительных объектов в соответствии с установленными настройками. Обработка объектов может носить как сугубо информационный характер (вывод информации в отчет и на консоль сервера, уведомление администратора), так и приводить к изменению объекта (лечение, перенос в отдельный каталог, удаление).



Все настройки компонента *kavscanner* сгруппированы в секциях **[scanner.*]** конфигурационного файла приложения.



По умолчанию *kavscanner* только уведомляет пользователя/администратора об обнаружении инфицированных объектов. О дополнительной настройке каких-либо действий над файлом см. п. 6.2.3 на стр. 50.

Проверка файловых систем вашего сервера может быть выполнена по запросу администратора из командной строки либо автоматически, по расписанию, с помощью стандартной утилиты **cron**. Вы можете задавать проверку как всех файловых систем сервера, так и отдельного каталога. Также могут проверяться сектора блочных устройств.

Далее мы подробно рассмотрим наиболее типичные задачи антивирусной защиты файловых систем сервера.



Процесс проверки всего компьютера на присутствие вирусов – достаточно ресурсоемкая процедура. Следует помнить, что при ее проведении скорость работы сервера будет замедлена, следовательно, рекомендуется для проверки выбрать время, когда нагрузка на сервер будет наименьшей.

5.3.1. Проверка файлов по запросу

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



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

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



Решение: чтобы реализовать поставленную задачу, в командной строке введите:

```
#./kav4samba-kavscanner -rlq  
-o kavscanner-`date +%F`.log -i3 -ePASBME -j3 -mCn  
/tmp
```

5.3.2. Проверка каталога по расписанию (cron)

С помощью утилиты запуска программ по расписанию **cron** вы можете задать автоматическое выполнение любой задачи Антивируса Касперского для Samba Servers, в том числе и проверку каталога по расписанию.



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

```
0 0 * * * /path/to/kav4samba-kavscanner -c  
/etc/kav/kavscaner.cron /home
```

5.3.3. Дополнительные возможности: использование скрипт-файлов

Антивирус Касперского предоставляет возможность дополнительной обработки объектов, прошедших антивирусный анализ, путем использования различных стандартных команд Unix/Linux, 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.

5.3.3.1. Отправка администратору уведомления

Посредством Антивируса Касперского с использованием стандартных средств Unix/Linux вы можете настроить уведомление администратора сервера об обнаружении в файловых системах инфицированных, подозрительных и поврежденных файлов.



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



Решение: для реализации поставленной задачи выполните следующие действия:

Задайте правила обработки простых объектов и объектов-контейнеров в конфигурационном файле приложения:

```
[scanner.object]
```

```
OnInfected=exec echo %FULLPATH%/%FILENAME% is  
infected by %VIRUSNAME% | mail -s kav4samba-  
kavscanner admin@localhost.ru
```

```
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is  
infected, viruses list is in the attached file %LIST%  
| mail -s kav4samba-kavscanner -a %LIST%  
admin@localhost.ru
```

ГЛАВА 6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА

В данном разделе мы подробно остановимся на дополнительных настройках функциональности Антивируса Касперского. В отличие от необходимых настроек, выполняемых в процессе инсталляции (см. п. 3.3 на стр. 18), без которых использование приложения невозможно, дополнительные настройки осуществляются по усмотрению администратора. Они направлены на расширение возможностей приложения и его настройку для использования в рамках конкретного предприятия.

6.1. Настройка антивирусной защиты в реальном времени

Как отмечалось выше, антивирусная защита Samba-сервера в реальном времени осуществляется посредством компонента *kavsamba*.

Конфигурация компонента предполагает возможность настройки следующих параметров:

- Области проверки: путь и объекты защиты (см. п. 6.1.1. на стр. 44).
- Режима проверки и лечения файлов (см. п. 6.1.2 на стр. 45).
- Действий над файлами (см. п. 6.1.3. на стр. 46).
- Режима резервного копирования (см. п. 6.1.5 на стр. 51).
- Формирования отчета и оповещений (см. п. 6.5 на стр. 56).

6.1.1. Область мониторинга

Область проверки компонента *kavsamba* включает в себя *путь* и *объекты защиты*.

Под *путем* подразумеваются все файловые системы, доступные пользователю через сервер Samba. Ограничить путь можно только исключением некоторых каталогов и файлов в конфигурационном файле приложения (секция **[samba.options]**, параметры **ExcludeMask** и **ExcludeDirs**).

Объекты защиты (типы файлов, которые проверяются на вирусы) определяются только параметрами конфигурационного файла приложения в секции **[samba.options]**.



При запуске компонента *kavsamba* вы не можете задавать или ограничивать область мониторинга из командной строки. Такая опция реализована только для антивирусной проверки файловых систем сервера (компонент *kavscanner*).

6.1.2. Режим проверки и лечения файлов

Kavsamba поддерживает следующие операции по доступу к файлам: открытие и закрытие. По умолчанию при открытии проверяются все непустые файлы, при закрытии файл проверяется, если в него были внесены изменения.

По умолчанию режим лечения перехваченных инфицированных файлов отключен, что предполагает только уведомление пользователя (и/или администратора) об обнаружении вирусов и подозрительных объектов. Оповещение осуществляется путем вывода сообщений в файл отчета (см. п. 6.6 на стр. 56). Доступ к таким объектам автоматически блокируется.

Включение режима лечения зараженных объектов осуществляется в конфигурационном файле (секция **[samba.options]**, параметр **Cure=yes**). Проверив файл, *kavsamba*, в случае, если он инфицирован (то есть имеет статус **Infected**), производит действия согласно настройкам конфигурационного файла (см. п. 6.1.3 на стр. 46).

В результате проверки (и лечения) файлу присваивается один из следующих статусов:

- **Clear** – файл не инфицирован.
- **Infected** – файл инфицирован.
- **Cured** – инфицированный файл был успешно вылечен.
- **CureFailed** – инфицированный файл вылечить не удалось.
- **Warning** – код файла похож на код известного вируса.
- **Suspicion** – файл подозревается на заражение неизвестным вирусом.
- **Protected** – файл проверить невозможно из-за того, что он зашифрован.

- **Corrupted** – файл поврежден.

В зависимости от статуса файла доступ к нему либо блокируется (**Infected**, **CureFailed**, **Warning**, **Suspicion**), либо разрешается (все остальные статусы).



К файлам со статусом **CureFailed** применяются действия, заданные для инфицированных объектов!

Обратите внимание на то, что для ускорения работы при проверке объектов-контейнеров (архивов) *kavsamba* прекращает свою работу и присваивает статус **Infected** всему архиву после первого же найденного вируса. Это означает, что даже если объект заражен многими вирусами, *kavsamba* выведет в лог только один.

6.1.3. Действия над файлами

Для файлов со статусами **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** и **Error** можно настроить выполнение ряда действий, таких как:

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

Обратите внимание на то, что компонент *kavsamba* не различает действие над файлами и объектами-контейнерами. Поэтому в отчете, например, могут быть указаны несколько имен вирусов, которыми заражен объект.

Настроить правила обработки объектов можно следующими способами:

- Задать их в конфигурационном файле приложения, если их предполагается использовать как действия по умолчанию (секция **[samba.actions]**).
- Указать правила обработки в альтернативном конфигурационном файле и использовать его при запуске компонента.

Обратите внимание, что сетевая папка **/homes** является виртуальной и указывает на домашние директории всех пользователей. Для подобной папки нельзя установить индивидуальные параметры антивирусной защиты.



Поэтому для определения параметров защиты домашних директорий пользователей используются настройки секции **[samba.shares]**. В случае если антивирусная проверка в секции **[samba.shares]** отключена, домашние каталоги пользователей не защищаются.

6.1.4. Изоляция зараженных объектов

Возможность переноса инфицированных файлов в отдельный каталог используется для изоляции зараженного объекта (секция **[samba.actions]** параметр **MovePath**). Перенос осуществляется в случае, если лечение файла произвести не удалось (например, из трех вирусов, которыми заражен файл, удалось удалить только два).



Администратор может настроить перемещение объектов в разные каталоги в зависимости от статуса файла.

Если такой каталог предполагается хранить, рекомендуем вам исключить его из области проверки с помощью параметра **ExcludeDirs** (секция **[samba.options]**) конфигурационного файла.



Задача: проверить на присутствие вирусов все файлы, запрашиваемые через Samba-сервер и, в случае, если объект заражен, произвести лечение. В случае неудачного лечения перенести инфицированные объекты с полными путями к ним в каталог **/tmp/infected**.



Решение: для реализации поставленной задачи выполните следующие действия:

1. В конфигурационном файле приложения включите режим лечения зараженных объектов (**Cure=yes** в секции **[samba.options]**).
2. Задайте правила изоляции инфицированных объектов. Для этого в секции **[samba.actions]** конфигурационного файла укажите следующие настройки:

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

3. Выполните перезагрузку Антивируса Касперского (см. п. 6.4 на стр. 54).

6.1.5. Режим резервного копирования объектов

В случае если файлы оказались заражены, а в качестве действия над инфицированными объектами определено удаление их из файловой системы, существует возможность потери ряда важных данных. Чтобы избежать этого, Антивирус Касперского предлагает возможность копирования файлов в backup-хранилище.

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

Обратите внимание: по умолчанию режим сохранения в Backup не включен и, соответственно, путь к каталогу, в котором предполагается хранить резервные копии, не определен. Для использования данной возможности вам необходимо задать этот путь самостоятельно.



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

6.2. Настройка антивирусной защиты файловых систем

Антивирусная защита файловых систем сервера осуществляется с помощью компонента *kavscanner*. Параметры функционирования компонента *kavscanner*, используемые по умолчанию, содержатся в конфигурационном файле приложения (секция **[scanner]**) и настроены на максимальную проверку файловых систем, доступных с рабочей станции, на которой установлено приложение. На присутствие вирусов проверяются все доступные файлы, в том числе:

- упакованные файлы;
- архивы;
- самораспаковывающиеся архивы;
- почтовые базы;

- почтовые сообщения.

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

- Область проверки (см. п. 6.2.1 на стр. 49) (этот параметр аналогичен области мониторинга при осуществлении защиты в реальном времени).
- Режим проверки и лечения файлов (см. п. 6.2.2 на стр. 50).
- Действия над файлами (см. п. 6.2.3 на стр. 50).

Рассмотрим подробнее настройку каждой из этих групп.

6.2.1. Область проверки

Область проверки можно условно разделить на две части:

- *путь проверки* – список каталогов и файлов, в которых производится поиск вирусов;
- *объекты проверки* – типы файлов, которые будут проверяться на предмет вирусов (архивы, почтовые сообщения и т.д.).

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



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

Вы можете переопределить путь проверки следующими способами:

- Перечислив через пробел каталоги и файлы с абсолютными или относительными (относительно текущего каталога) путями непосредственно в командной строке при запуске компонента.
- Задав пути проверки в текстовом файле и указав 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 сначала проверяются объекты, указанные в командной строке, а затем обозначенные в файле.

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

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

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

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

- ключами командной строки при запуске компонента;
- путем использования альтернативного конфигурационного файла.

6.2.2. Режим проверки и лечения файлов

Режим проверки и лечения файлов для компонента *kavscanner* полностью аналогичен для компонента *kavsamba*, за исключением того, что *kavscanner* производит различные действия и над файлами со статусом **Corrupted** (подробнее о действиях см. п. 6.1.3 на стр. 46).

Напомним, что по умолчанию опция лечения отключена, производится только проверка файлов на присутствие вирусов и информирование об обнаружении инфицированных, подозрительных или поврежденных объектов путем вывода сообщений на консоль и в отчет.

В результате проверки на присутствие вирусов каждому файлу присваивается какой-либо статус (**Clear**, **Infected**, **Warning** и т.п.), на основании которого над объектом производятся действия, указанные в конфигурационном файле.

Напомним, что в случае включенного режима лечения (секция **[scanner.options]**, параметр **Cure=yes**) будет проведена попытка лечения файлов со статусом **Infected**.

6.2.3. Действия над файлами

В зависимости от статуса файла к нему могут применяться те или иные действия. По умолчанию выполняется только уведомление об обнаружении файлов с определенным статусом путем выдачи сообщений на консоль и в отчет.

Однако для файлов со статусами **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** и **Error** (аналогично компоненту *kav samba*) и можно настроить выполнение ряда действий, таких как:

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

При осуществлении проверки файловых систем сервера компонент *kav scanner* Антивируса Касперского различает объект *простой* (файл) и *объект-контейнер* (состоящий из нескольких объектов – архив). Действия, выполняемые над такими объектами, также различаются; в конфигурационном файле они разнесены по отдельным секциям. Для простого объекта – секция **[scanner.object]**, для объекта-контейнера – **[scanner.container]**.

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

Указать действия над тем или иным файлом можно:

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

6.2.4. Режим резервного копирования

Возможности настройки резервного копирования при осуществлении антивирусной защиты файловых систем аналогичны приведенным в п. 6.1.5 на стр. 48 для антивирусной защиты в реальном времени. Поэтому в данном разделе мы не будем останавливаться на настройке этого режима подробно.



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



Решение: для реализации поставленной задачи выполните следующие действия:

1. Создайте альтернативный конфигурационный файл `scan_sample.conf`
2. Убедитесь, что включен режим лечения зараженных объектов (**Cure=yes** в секции **[scanner.options]**).
3. Задайте правила обработки инфицированных объектов. Для этого в секциях **[scanner.object]** и **[scanner.container]** конфигурационного файла `scan_sample.conf` укажите следующие настройки:

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

4. В командной строке введите:

```
# kav4samba-kavscanner - -@/tmp/downloads.lst -c
sample_scan.conf
```

6.3. Оптимизация работы Антивируса Касперского для Samba Servers

Для снижения нагрузок на сервер Антивирус Касперского предлагает несколько эффективных способов оптимизации своей работы. Рассмотрим их подробнее.



Использование базы данных iChecker и кеша 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:

При первичной проверке 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 как по объектам, проверенным компонентом *kavsamba*, так и компонентом *kavscanner*.
- Кеш проверенных файлов – база, содержащая информацию о проверенных компонентом *kavsamba* файлах. Данная база существует в оперативной памяти и после окончания работы компонента *kavsamba* не сохраняется.

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 базе iChecker, а затем (если в первой базе объект не обнаружен) – в кеше. 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.



Проведение фоновой проверки.

Так как поиск информации о запрашиваемых объектах в указанных выше базах проходит очень быстро, это позволяет существенно снизить нагрузку на сервер, и появляется возможность дальнейшего повышения эффектив-

ности использования возможностей сервера, а именно: *проведение фоновой проверки файлов*.

Во время работы Антивирус определяет свою загруженность и, если она не превышает заданную, проверяет в фоновом режиме файлы из папок общего доступа, а также те файлы, которые были изменены в процессе работы.

Нагрузка задается максимальным количеством файлов, которые могут быть проверены одновременно (секция **[samba.options]** параметр **CheckFilesLimit**). Также задается количество файлов, одновременно проверяемых в фоновом режиме (секция **[samba.options]** параметр **BgCheckFilesLimit**), и временной интервал, по истечению которого на антивирусную проверку запрашивается новый файл (секция **[samba.options]** параметр **BgSheduleTime**).

В случае, когда количество запрашиваемых на проверку файлов превышает максимально допустимое, вновь поступившие файлы ставятся в очередь и не проверяются до снижения нагрузки ниже допустимого уровня.

В таком случае пользователи, запросившие проверку, будут ожидать ответ несколько дольше, чем предполагалось. По окончании проверки файл удаляется из очереди. Дополнительного уведомления при этом не производится.



Если частота запроса не определена (**BgSheduleTime=0**), проверка в фоновом режиме не производится.

Тем самым удается устанавливать максимально допустимую нагрузку сервера.

6.4. Перезагрузка Антивируса Касперского



В процессе выполнения любой перезагрузки Антивируса Касперского доступ к **[samba.shares]**, защищаемым Антивирусом Касперского, будет заблокирован.

Возможны несколько вариантов перезагрузки Антивируса:

- "Горячая" перезагрузка, которую рекомендуется выполнять после обновления антивирусных баз.

При этом происходит перезагрузка антивирусных баз с сохранением всех соединений. В данном режиме не происходит перезапуск компонента *kavsamba*, поэтому сохраняется файловый кеш и т.д.

"Горячая" перезагрузка осуществляется путем ввода в командной строке следующей команды:

Для дистрибутивов Linux:

```
/etc/init.d/kav4samba reload_avbase
```

Для дистрибутивов FreeBSD:

```
/usr/local/etc/rc.d/kav4samba.sh reload_avbase
```

В этом случае процесс *kavsamba* получает сигнал **SIGUSR1**.

- "Холодная" перезагрузка, которую рекомендуется выполнять при внесении изменений в конфигурационный файл, в настройки или при установке нового лицензионного ключа.

При этом происходит перечитывание конфигурационного файла, баз, а также разрываются все соединения с пользователем, так как фактически приложение сначала прекращает свою работу, а потом запускается снова.

Осуществляется путем ввода в командной строке следующей команды:

Для дистрибутивов Linux:

```
/etc/init.d/kav4samba reload
```

Для дистрибутивов FreeBSD:

```
/usr/local/etc/rc.d/kav4samba.sh reload
```

В этом случае процесс *kavsamba* получает сигнал **SIGHUP**.

- Принудительное завершение работы Антивируса Касперского, осуществляется путем ввода в командной строке следующей команды:

Для дистрибутивов Linux:

```
/etc/init.d/kav4samba stop
```

Для дистрибутивов FreeBSD:

```
/usr/local/etc/rc.d/kav4samba.sh stop
```

Команда отправит процессу *kavsamba* сигнал **SIGTERM**, по которому завершается работа *kavsamba* с закрытием всех порожденных им копий, и Антивирус корректно прекращает свою работу.



Настоятельно рекомендуем вам не использовать для завершения работы с процессом *kavsamba* команду **kill -9**. В результате выполнения данной команды работа процесса будет завершена, однако в системе сохранится ряд временных и рабочих файлов, которые удаляются только вручную. Некоторые приложения по наличию в системе таких файлов определяют процесс как запущенный.

6.5. 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 формату `strftime`:

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

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

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

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

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

6.6. Параметры формирования отчета Антивируса Касперского

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



Результаты антивирусной обработки файловых систем сервера также выводятся на консоль. По умолчанию информация, выводимая в отчет и на экран, дублирует друг друга. Если вы хотите, чтобы на консоль выводилась отличная от файла-отчета информация, вам необходимо выполнить ряд дополнительных настроек.

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
0	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.
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.

Уровни	Название уровня	Значение
4	Activity	Сообщения о проверке объектов в соответствии с уровнем детализации отчета о проверке.
10	Debug	Все сообщения отладочного характера; например, содержание конфигурационного файла.

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

ГЛАВА 7. УПРАВЛЕНИЕ ЛИЦЕНЗИОННЫМИ КЛЮЧАМИ

В Антивирусе Касперского для Samba Servers предусмотрено ограничение работы с приложением по сроку его использования (как правило, это срок в один год со дня приобретения). По истечении срока действия лицензии на использование Антивируса Касперского приложение будет продолжать работу, но обновление антивирусных баз станет невозможным. Антивирус по-прежнему будет выполнять лечение инфицированных объектов, но с использованием старых антивирусных баз.

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

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

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

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

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

7.1.1. Просмотр информации о лицензионном ключе

Вы можете просматривать информацию об установленных лицензионных ключах в отчетах о работе компонентов *kavscanner* и *kavsamba*, 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 дополнительные данные.

Вся информация может быть выведена на консоль сервера или просмотрена удаленно с любого компьютера вашей сети с помощью Webmin.



Чтобы просмотреть информацию обо всех установленных лицензионных ключах,

в командной строке введите:

```
#!/kav4samba-licensemanager -s
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006.  
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
```



Чтобы просмотреть информацию о лицензионном ключе,

в командной строке введите, например, такую строку:

```
#!/kav4samba-licensemanager -k 00053E3D.key
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006.  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

7.1.2. 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. Глава 7 на стр. 59.

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 с помощью утилиты *licensmanager* (параметр **LicensePath** конфигурационного файла приложения).



Чтобы установить новый ключ вам необходимо:

в командной строке ввести, например, такую строку:

```
#./kav4samba-licensmanager -a 00053E3D.key
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998–2006.
```

Key file 00053E3D.key is successfully registered

После этого рекомендуем вам обновить антивирусные базы.

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

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

7.1.3. Удаление лицензионного ключа



Чтобы удалить все установленные лицензионные ключи,

в командной строке введите такую строку:

```
#./kav4samba-licensemanager -da
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Active key was successfully removed
```



Чтобы удалить резервный ключ,

в командной строке введите такую строку:


```
#./kav4samba-licensemanager -dr
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Additional key was successfully removed
```

ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА

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

Тестовый "вирус" был специально разработан организацией  (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 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 сайта компании **EICAR** или создали в текстовом редакторе описанным выше способом, содержит тело стандартного тестового "вируса". Антивирус обнаруживает его, присваивает тип **Инфицированный**, не подвергающийся лечению, и выполняет действие, установленное администратором для объекта с таким типом.

Для того чтобы проверить реакцию Антивируса при обнаружении объектов других типов, вы можете модифицировать содержание стандартного тестового "вируса", добавив к нему один из префиксов (см. таблицу 1).



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

Таблица 1. Модификации тестового "вируса"

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый "вирус"	Infected. Объект не подвергается лечению.
CORR–	Corrupted. Объект поврежден
SUSP–	Suspicious (код неизвестного вируса).
WARN–	Warning (модифицированный код известного вируса).
ERRO–	Error. В результате проверки объекта произошла ошибка.
CURE–	Cured. Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURED.
DELE–	Объект автоматически удаляется.

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

ГЛАВА 9. ВОЗМОЖНЫЕ ВОПРОСЫ ПРИ РАБОТЕ С ПРИЛОЖЕНИЕМ

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



***Вопрос:** 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 сервера и ощутимо нагружает процессор?*

Детектирование вирусов является в чистом виде 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. Это вынужденная плата за надежность и безопасность ваших данных.

В отличие от других антивирусов, урезающих время проверки путем исключения из антивирусных баз более сложных в детектировании или более редких (в том месте, где географически расположена компания-производитель) вирусов, а также более сложных в анализе форматов файлов (например, pdf), Лаборатория Касперского считает, что задача антивируса – обеспечивать реальную, а не мнимую, антивирусную безопасность пользователей, поскольку нельзя быть защищенным наполовину. При этом быть "частично защищенным" хуже, чем не быть защищенным вообще (поскольку в этом случае пользователь принимает меры предосторожности самостоятельно).

Антивирус Касперского позволяет пользователю чувствовать себя максимально защищенным. Безусловно, Антивирус Касперского позволяет опытному пользователю ускорить антивирусную проверку в ущерб общей безопасности путем отключения антивирусной проверки различных типов файлов, но мы не рекомендуем этого делать, если пользователь хочет чувствовать себя максимально защищенным.

Для максимальной защиты пользователей Антивирус Касперского распознает более 40 архивов и инсталляторов, и способен детектировать вирусы в более чем 350 различных форматах файлов. Это очень важно для антивирусной безопасности, поскольку каждый из распознаваемых форматов может содержать исполняемый вредоносный код. Тем не менее, нельзя не отметить, что несмотря на ежедневное увеличение общего количества обнаруживаемых Антивирусом Касперского вирусов (около 30 новых вирусов в день), а также постоянное увеличение количества распознаваемых форматов, каждая версия продукта работает быстрее, чем предыдущая. Это следствие использования новых уникальных технологий, разработанных в Лаборатории Касперского, таких как i-Checker. При этом файл проверяется на вирусы только один раз, при первой проверке. При всех последующих проверках файл не анализируется на присутствие вирусов при условии, что он не был изменен. Вследствие этого производительность антивируса резко возрастает после первой проверки файла.



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

Без лицензионного ключа Антивирус Касперского не работает.

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



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

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

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

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



Вопрос: 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, не описан ли метод решения вашей проблемы в данной документации, в частности в этом разделе, или на нашем сайте (**Постоянная защита → База знаний → Антивирус Касперского 5.5 для Samba Servers**).

Также мы рекомендуем обратиться к фирме, продавшей вам Антивирус Касперского или написать запрос в службу технической поддержки (<http://www.kaspersky.ru/helpdesk.html>).



Вопрос: может ли злоумышленник подменить антивирусные базы?

Злоумышленник может загрузить антивирусные базы с сайта Лаборатории Касперского и скопировать их в каталог хранения антивирусных баз, однако Антивирус Касперского не будет их использовать в процессе работы!

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



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

Данные виды процессоров в текущей версии приложения не поддерживаются.



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

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

На дистрибутивах, не входящих в список поддерживаемых Лабораторией Касперского, возможна некорректная работа приложения. Это, прежде всего, связано со спецификой операционной системы. Например, дистрибутив вашей системы использует другую версию

библиотеки или имеет место нестандартное расположение скриптов инициализации системы. В таком случае Служба Технической Поддержки Лаборатории Касперского не сможет вам помочь.



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

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

```
tar zxvf <имя_архива>
```



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

Использование Network Control Centre для Windows при работе с Антивирусом Касперского для Unix 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?

Одним из вариантов решения данной задачи является следующий: введите в командной строке:

```
$ 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:

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

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

ПРИЛОЖЕНИЕ А. 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 *kav4sambaservers.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 **[samba.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.

ExcludeMask=маска1:маска2:...:маскаN – маски файлов, которые исключаются из проверки; по умолчанию проверяются все файлы.

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 – количество записей о неинфицированных объектах, содержащихся в файловом кеше.

BgCheckFilesLimit – максимальное количество одновременно проверяемых в фоновом режиме объектов. Если параметру присвоено значение **0**, проверка в фоновом режиме не производится.

BgSheduleTime – время, по истечению которого в фоновом режиме запускается антивирусная проверка нового файла из папок общего доступа (в сек.).

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

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

Секция **[samba.path]** содержит параметры, определяющие пути к важнейшим файлам, без которых компонент kavsamba не будет функционировать:

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

SambaConfigFile=путь – полный путь к конфигурационному файлу сервера Samba.

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

Секция **[samba.shares]** содержит параметры, определяющие опции проверки файлов в папках общего доступа:

CheckOnOpen –антивирусная проверка файла при запросе на открытие.

CheckOnClose –антивирусная проверка файла при сохранении.

Секции вида **[samba.shares:SHARENAME]** могут быть созданы в конфигурационном файле и должны содержать параметры, определяющие опции антивирусной защиты для отдельной папки общего доступа (например, папке **SHARENAME**):

CheckOnOpen –антивирусная проверка файла при запросе на открытие.

CheckOnClose –антивирусная проверка файла при сохранении.



Если вы определили индивидуальные параметры защиты для папки общего доступа, то в случае, если Антивирус Касперского не запущен, доступ к данной папке будет заблокирован.

Секция **[samba.actions]** содержит параметры, определяющие действия над объектами того или иного типа:

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.

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 используются:

- %VIRUSNAME% – имя обнаруженного вируса.
- %FULLPATH% – полный путь до каталога.
- %FILENAME% – имя файла без пути.

Секция **[samba.notify]** содержит параметры, определяющие отправку оповещений при обнаружении объектов того или иного типа:

OnInfected=действие – оповещение в случае обнаружения зараженного файла.

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

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

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

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

OnCorrupted=действие – оповещение в случае обнаружения поврежденного файла.

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

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 используются:

- %USER% – имя пользователя, запросившего файл.
- %USERIP% – IP пользователя, запросившего файл.
- %USERHOST% – хост пользователя, с которого был запрошен файл.
- %VIRUSNAME% – имя обнаруженного вируса.
- %FULLPATH% – полный путь до каталога.
- %FILENAME% – имя файла без пути.

Секция **[samba.report]** содержит параметры формирования отчета о результатах работы компонента kavsamba:

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

ReportMaxSize – размер файла отчета (в байтах).

ReportLevel – уровень детализации отчета.

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:

ExcludeDirs=маска1:маска2:...:маскаN – маски каталогов, которые исключаются из проверки; по умолчанию проверяются все каталоги.

ExcludeMask=маска1:маска2:...:маскаN – маски файлов, которые исключаются из проверки; по умолчанию проверяются все файлы.

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**.

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

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

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

UseAVbasesSet=standard|extended – набор антивирусных баз, используемых приложением. Набор **extended** помимо записей, содержащихся в наборе **standard**, 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**, раскрываются все символьные ссылки. Если параметру присвоено значение **no**, символьные ссылки на директории раскрываться не будут.

MaxLoadAvg – числовой параметр, отражающий степень загруженности сервера. В случае если загрузка превышает указанное значение, антивирусная проверка временно приостанавливается. Проверка будет возобновлена после того, как нагрузка на сервер снизится до установленного параметром значения.

Секция **[scanner.path]** содержит параметр, определяющий пути к важнейшим файлам, без которых компонент kavscanner не будет функционировать:

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

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

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.

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

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

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

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

ReportLevel=4 – уровень детализации отчета.

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**.

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 **[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.options]** содержит параметры работы компонента keeprupdate:

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.

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 (две первые буквы названия региона); 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.

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.

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**.

Секция **[updater.report]** содержит параметры формирования отчета о работе компонента keerp2date:

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.

А.2. Ключи командной строки компонента kavsamba

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 kavsamba;
-v	Показать версию программы.
Опции конфигурации:	

-c (-y) <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу> .
---	---

A.3. Коды возврата компонента **kavsamba**

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

0	Компонент запущен;
64	Лицензионная информация отсутствует либо не найдено ни одного лицензионного ключа по пути, указанному в конфигурационном файле;
65	Невозможно загрузить конфигурационный файл;
70	Компонент kavsamba поврежден.

A.4. 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)	Использовать альтернативный конфигурационный

<путь_к_файлу>	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 (для отключения режима проверки самораспаковывающихся архивов необходимо, чтобы проверка архивов также была отключена);
V/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;
-l	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.
10	Выводить/не выводить сообщения отладочного характера.
-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.5. 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.6. Ключи командной строки компонента `licensmanager`

Опции помощи:	
-h	Вывести на консоль справочную информацию о компоненте <code>licensmanager</code> .
-v	Показать версию программы.
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 <a r>	Удалить все лицензионные ключи/ удалить резервный лицензионный ключ.

А.7. 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.8. 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 полный список серверов обновлений с кодом региона;
Опции работы:	
-r	Откат последнего обновления на предыдущую версию;
-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 антивирусных 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> ;
-s <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> .

А.9. 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. 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.

В.1. Другие разработки Лаборатории Касперского

Новостной Агент Лаборатории Касперского

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

Новостной Агент также позволяет:

- визуализировать в системной панели состояние "вирусной погоды";
- подписываться и отказываться от подписки на новостные каналы Лаборатории Касперского;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении неп прочитанных 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 антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в веб-браузере. Таким образом, пользователи могут максимально оперативно получить ответ на опасения, связан-

ные 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 и 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.
- *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.

¹ В зависимости от типа поставки

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 (спам) 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 уникаль-

ный 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, позволяющих 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.

В.2. Наши координаты

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

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700
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