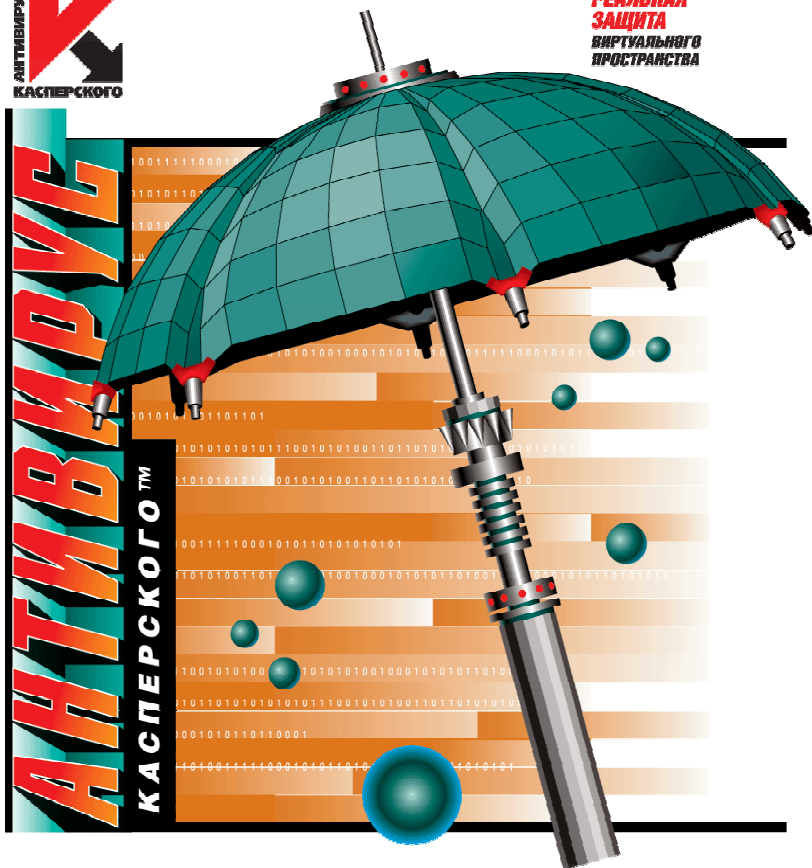


# ЛАБОРАТОРИЯ КАСПЕРСКОГО

---



**РЕАЛЬНАЯ  
ЗАЩИТА  
ВИРТУАЛЬНОГО  
ПРОСТРАНСТВА**



---

## **Антивирус Касперского® 5.0 для Samba Servers**

**РУКОВОДСТВО АДМИНИСТРАТОРА**

АНТИВИРУС КАСПЕРСКОГО® 5.0 ДЛЯ SAMBA SERVERS

---

# Руководство администратора

© ЗАО "Лаборатория Касперского"  
Тел. +7 (095) 797-87-00 • Факс +7 (095) 948-43-31  
<http://www.kaspersky.ru>

Дата редакции: декабрь 2003 года

# Содержание

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ SAMBA SERVERS .....	6
1.1. Аппаратные и программные требования к системе .....	7
1.2. Комплект поставки.....	8
1.2.1. Лицензионное соглашение.....	8
1.2.2. Регистрационная карточка .....	9
1.3. Сервис для зарегистрированных пользователей.....	9
1.4. Принятые обозначения.....	10
ГЛАВА 2. ВНУТРЕННЯЯ АРХИТЕКТУРА АНТИВИРУСА КАСПЕРСКОГО® .....	12
2.1. Компонентный состав .....	12
2.2. Алгоритм работы .....	13
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО® .....	14
3.1. Установка приложения на сервер под управлением Linux.....	14
3.2. Установка приложения на сервер под управлением FreeBSD или OpenBSD .....	15
3.3. Процесс инсталляции .....	15
3.4. Конфигурация приложения .....	16
3.5. Схема расположения файлов по каталогам .....	17
3.6. Деинсталляция Антивируса Касперского® .....	18
ГЛАВА 4. ПОСТИНСТАЛЛЯЦИОННАЯ НАСТРОЙКА .....	20
4.1. Настройки приложения по умолчанию .....	20
4.2. Установка/обновление антивирусных баз .....	21
4.3. Настройка совместной работы с Webmin .....	22
4.4. Рекомендуемые режимы работы .....	22
4.4.1. Оптимальный режим работы .....	23
4.4.2. Режим максимального быстродействия.....	24
4.4.3. Режим максимальной надежности.....	25
4.4.4. Режим проверки часто обновляемых файлов.....	26
ГЛАВА 5. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО® ДЛЯ SAMBA SERVERS.....	28

5.1. Обновление антивирусных баз .....	28
5.1.1. Планирование обновлений антивирусных баз посредством cron .....	29
5.1.2. Разовое обновление антивирусных баз .....	30
5.1.3. Создание сетевого каталога для хранения и копирования антивирусных баз .....	31
5.2. Антивирусная защита Samba-сервера в реальном времени .....	32
5.2.1. Настройка уведомления пользователя .....	32
5.2.1.1. Мониторинг с уведомлением посредством smbclient .....	33
5.2.1.2. Мониторинг с уведомлением посредством почтовых сообщений .....	33
5.3. Антивирусная защита файловых систем .....	34
5.3.1. Проверка файлов по запросу .....	35
5.3.2. Ежедневная проверка каталога по расписанию (cron) .....	35
5.3.3. Дополнительные возможности: использование скрипт-файлов .....	36
5.3.3.1. Лечение зараженных объектов в архиве .....	36
5.3.3.2. Отправка администратору уведомления .....	37
ГЛАВА 6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА .....	39
6.1. Настройка антивирусной защиты в реальном времени .....	39
6.1.1. Область мониторинга .....	39
6.1.2. Режим проверки и лечения файлов .....	40
6.1.3. Действия над файлами .....	41
6.1.4. Изоляция зараженных объектов .....	42
6.1.5. Режим резервного копирования объектов .....	42
6.2. Настройка антивирусной защиты файловых систем .....	43
6.2.1. Область проверки .....	44
6.2.2. Режим проверки и лечения файлов .....	45
6.2.3. Действия над файлами .....	45
6.2.4. Режим резервного копирования .....	46
6.3. Оптимизация работы Антивируса Касперского® для Samba Servers .....	47
6.4. Перезагрузка Антивируса Касперского® .....	49
6.5. Локализация отображаемого формата даты и времени .....	50
6.6. Параметры формирования отчета Антивируса Касперского® .....	51
6.6.1. Формат сообщений о проверке .....	53
6.6.2. Формат сообщений, выводящихся на консоль .....	55
ГЛАВА 7. РАБОТА С ЛИЦЕНЗИЯМИ .....	56

---

7.1. Управление лицензионными ключами.....	56
7.1.1. Просмотр информации о лицензионном ключе.....	57
7.1.2. Продление лицензии.....	58
7.1.3. Удаление лицензионного ключа.....	59
ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА .....	61
ГЛАВА 9. ВОЗМОЖНЫЕ ВОПРОСЫ ПРИ РАБОТЕ С ПРИЛОЖЕНИЕМ.....	63
ПРИЛОЖЕНИЕ А. ВРЕДОНОСНЫЕ ПРОГРАММЫ В UNIX-СРЕДЕ.....	68
А.1. Вирусы .....	68
А.2. Троянские программы .....	70
А.3. Сетевые черви .....	71
ПРИЛОЖЕНИЕ В. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО" .....	73
В.1. Другие разработки "Лаборатории Касперского" .....	74
В.2. Наши координаты .....	78

---

# ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ SAMBA SERVERS

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

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.

## 1.1. Аппаратные и программные требования к системе

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

- Аппаратные требования:
  - Процессор класса Pentium и выше.
  - Объем свободной оперативной памяти не менее 32 Mb.
  - Свободного места на диске не менее 100 Mb.

- Программные требования:
  - Одна из следующих операционных систем:
    - Linux RedHat (версии 7.3, 8.0 и 9.0), Linux SuSE (версии 8.1 и 8.2) или Linux Debian (версия 3.0).
    - FreeBSD версии 4.7 и выше.
    - OpenBSD версии 3.3.
  - Установленный Samba-сервер версии 2.2.6 и выше.
  - Установленный Perl версии 5.0 и выше.

## 1.2. Комплект поставки

Программный продукт вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, [www.kaspersky.ru](http://www.kaspersky.ru), раздел **Купить онлайн**).

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 администратора;
- лицензионный ключ, записанный на установочный компакт-диск;
- регистрационная карточка (с указанием серийного номера продукта);
- лицензионное соглашение.



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

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

### 1.2.1. Лицензионное соглашение

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



**Внимательно прочитайте лицензионное соглашение!**

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

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

## **1.2.2. Регистрационная карточка**

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

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

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

## **1.3. Сервис для зарегистрированных пользователей**

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

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



- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов Лаборатории Касперского и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского").




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

## 1.4. 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
<b>Жирный шрифт</b>	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.
 <b>Примечание.</b>	Дополнительная информация, примечания.
 <b>Внимание!</b>	Информация, на которую следует обратить особое внимание.
 <b>Чтобы выполнить действие,</b>  1. Шаг 1. 2. ...	Описание последовательности выполняемых пользователем шагов и возможных действий.

Оформление	Смысловое назначение
 <p>Задача, пример</p>	<p>Постановка задачи, примера для реализации возможностей программного продукта.</p>
 <p>Решение</p>	<p>Реализация поставленной задачи.</p>
<p><b>[ключ]</b> – назначение ключа.</p>	<p>Ключи командной строки.</p>
<p>Текст информационных сообщений и командной строки</p>	<p>Текст конфигурационных файлов, информационных сообщений программы и командной строки.</p>

---

# 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 инфицированным (Infected, CureFailed). 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. 1.1 на стр. 7).
- Войти в систему под пользователем **root**.

## 3.1. Установка приложения на сервер под управлением Linux

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



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

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



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

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

Также вы можете воспользоваться стандартным дистрибутивом, единым для всех ОС Linux. Этот вариант может быть задействован в случае, если соответствующий дистрибутив Linux не поддерживается rpm или deb-форматами (например, Slackware) или если администратор не использует встроенный менеджер пакета.

Универсальный дистрибутив Антивируса Касперского® поставляется в виде архива. Архив содержит дерево каталогов файлов дистрибутива и инсталляционный скрипт *install.sh*, осуществляющий установку.



Для запуска установки Антивируса Касперского® на сервер выполните следующие действия:

1. Скопируйте архив дистрибутива в каталог файловой системы сервера и распакуйте его.
2. Запустите инсталляционный скрипт: `install.sh`.

## 3.2. Установка приложения на сервер под управлением FreeBSD или OpenBSD

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



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

```
pkg_add <имя_пакета>
```

## 3.3. Процесс инсталляции



По ряду причин процесс инсталляции может завершиться с кодом ошибки. В этом случае убедитесь, что ваш компьютер соответствует аппаратным и программным требованиям (см. п. 1.1 на стр. 7), 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. Подробнее об этом см. п. 7.1 на стр. 56.

#### 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, на экран выдается сообщение об этом и запрос на их комментирование. В случае отказа от комментирования этих строк процесс конфигурации завершает свою работу.

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:

*/etc/kav/5.0/kavsamba* – каталог, содержащий конфигурационный файл Антивируса Касперского® и другие файлы настроек:

*kav4sambaservers.co* – конфигурационный файл.

*/var/db/kav/5.0/kavsamba/bases* и */var/db/kav/5.0/kavsamba/license* – каталоги, содержащие антивирусные базы и список серверов обновления этих баз.

*/var/db/kav/5.0/kavsamba/patches* – каталог, содержащий скаченные патчи приложения.

### Если у вас установлена ОС Linux:

*/opt/kav/5.0/kavsamba* – основной каталог Антивируса, включающий:

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

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

*kavsamba* – исполняемый файл компонента антивирусной защиты в реальном времени *kavsamba* (On-Access Scanner);

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

*/man/* – каталог man-файлов.

*/setup/* - каталог хранения служебных скриптов и модуля Webmin.

### Если у вас установлена ОС FreeBSD или OpenBSD:

`/usr/local/share/kav/5.0/kavsamba` – основной каталог Антивируса, включающий:

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

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

`kavsamba` – исполняемый файл компонента антивирусной защиты в реальном времени `kavsamba` (On-Access Scanner);

`keerup2date` – исполняемый файл компонента `keerup2date`, обновляющего антивирусные базы.

`/man/` – каталог `man`-файлов.

`/setup/` – каталог хранения служебных скриптов и модуля Webmin.

## 3.6. Деинсталляция 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!

Также администратору необходимо самостоятельно остановить работу приложения Антивирус Касперского®. Для этого можно воспользоваться, например, командой:

```
/etc/init.d/kavsamba stop
```

После выполнения вышеуказанных действий можно приступить непосредственно к процедуре деинсталляции, которая будет выполнена автоматически. Запуск деинсталляции происходит различными способами в зависимости от используемого менеджера пакета. Рассмотрим эти варианты подробнее.



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>
```



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

```
install.pl uninstall
```



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

```
pkg-delete <имя_пакета>
```

В случае успешного завершения процедуры деинсталляции дополнительных оповещений не производится.

---

## 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. 20).



**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. 39) 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/обновление антивирусных баз

Сразу после установки Антивируса Касперского® на сервер мы рекомендуем вам установить/обновить антивирусные базы.

Для этого вам нужно запустить компонент *keepup2date*. В командной строке введите:

```
/путь/к/keepup2date
```

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



Рекомендуем вам **ЕЖЕДНЕВНО** обновлять антивирусные базы, поскольку каждый день в мире появляются новые вирусы, и необходимо поддерживать приложение в актуальном состоянии. Подробнее о вариантах организации обновлений см. в пп. 5.2.1-5.3.3.2 на стр. 32-37.

Также обратите особое внимание на то, что в процессе обновления антивирусных баз Антивирус Касперского® для Samba Servers использует новую версию компонента *keepup2date*. Для этого компонента разработаны антивирусные базы специального (расширенного) формата. Поэтому в случае, если администратор проводит обновление самостоятельно, необходимо использовать именно расширенный набор баз!

## 4.3. Настройка совместной работы с Webmin

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

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

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 необходимо провести корректировку нового (альтернативного) конфигурационного файла в соответствии с вашими задачами.
2. Указать имя альтернативного конфигурационного файла на закладке **Config edit** в поле ввода параметра **Full path to KAV config**.
3. Задать необходимые параметры антивирусной защиты файловых систем на соответствующих закладках.

## 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.



*Подробное описание значения каждого параметра см. в соответствующем [map](#).*

## 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/db/kav/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/db/kav/5.0/kavsamba/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
```



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
```

```
BgCheckFilesLimit=3
```

```
BgSheduleTime=5
```

```
NashType=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 **[path]** установите следующее значение для параметра:

```
IcheckerDbFile=/var/db/kav/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=0
CheckFilesLimit=0
BgCheckFilesLimit=0
BgSheduleTime=0
HashType=md5
```
- В секции **[samba.path]** установите следующее значение для параметра:

```
BackupPath=/var/db/kav/5.0/kavsamba/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. 23) 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/db/kav/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/db/kav/5.0/kavsamba/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 "холодную" перезагрузку Антивируса Касперского®. Подробнее о способах проведения перезагрузки см. п. 6.4 на стр. 49.

## 5.1. Обновление антивирусных баз

Компонент *keepup2date* предназначен для проведения различных видов обновлений, источником которых являются сервера обновлений Лаборатории Касперского. Например, такие как:

<http://downloads1.kaspersky-labs.com/updates/>  
<http://downloads2.kaspersky-labs.com/updates/>  
<http://downloads1.kaspersky-labs.com/updates/> и другие.

Список адресов, с которых можно копировать обновления, приведен в файле *updcfg.xml*, включенном в поставку приложения.

В процессе обновления компонент *keepup2date* обращается к данному списку, выбирает адрес и пытается скопировать с сервера антивирусные базы либо иные обновления (например, программные патчи). Если выполнить обновление с выбранного адреса невозможно, то программа обращается по следующему адресу и вновь пытается обновить базы. После успешного обновления по умолчанию происходит автоматическая перезагрузка приложения (параметр **PostUpdateCmd** секции **[updater.options]**).



Все настройки компонента *keepup2date* сгруппированы в опциях **[updater.\*]** конфигурационного файла *kav4sambaservers.conf*.

Если структура вашей локальной сети достаточно сложная, мы рекомендуем один раз в день скачивать обновления с серверов обновлений, размещать их в некоторой сетевой папке, а для локальных компьютеров сети настроить копирование баз из этой папки. Подробнее о создании задачи подобного рода см. п. 5.1.3 на стр. 31



Настоятельно рекомендуем обновлять антивирусные базы ежедневно!

Обновление может быть организовано при помощи **cron** (см. п. 5.1.1 на стр. 29) или же из командной строки (см. п. 5.1.2 на стр. 30).



Компонент *keepup2date* выполняет обновления всех приложений Лаборатории Касперского, в состав которых он входит.

## 5.1.1. Планирование обновлений антивирусных баз посредством **cron**

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



**Задача:** задать автоматическое обновление антивирусных баз ежедневно в 07.00. Установить выбор сервера обновлений из файла *updcfg.xml*. В системном журнале фиксировать только ошибки при работе программы. Вести общий журнал по всем запускам задачи, на консоль никакой информации не выводить.



**Решение:** для реализации поставленной задачи выполните следующие действия:

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

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

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

```
0 7 * * * /opt/kav/bin/keepup2date
```

## 5.1.2. Разовое обновление антивирусных баз

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:

```
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 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, то обновлять с серверов Лаборатории Касперского. Результаты работы вывести в файл отчета.



**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:

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



**Задача:** посмотреть список всех доступных для обновления приложений Лаборатории Касперского.



**Решение:** для реализации поставленной задачи в командной строке введите:

```
keepup2date -i
```

В этом случае на экране будет выведен список, включающий имена всех приложений, в состав которых входит компонент *keepup2date*, а также их идентификационные номера (id).

### 5.1.3. Создание сетевого каталога для хранения и копирования антивирусных баз

Так как сайты-источники обновления антивирусных баз Лаборатории Касперского имеют сложную структуру, то при настройке обновления локальных компьютеров вашей сети из некоторой сетевой папки, необходимо в этой папке создать аналогичную файловую структуру.



**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:  

```
keepup2date -u rdir
```

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

## 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.41.

### 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 **smbclient**. Рассмотрим эти возможности подробнее.

### 5.2.1.1. Мониторинг с уведомлением посредством smbclient

При инсталляции Samba-сервера автоматически устанавливается утилита **smbclient**, с помощью которой **winpopup**-сообщения передаются клиентской машине. В операционной системе Windows такие сообщения (**winpopup**) выводятся на экран пользователя, если включена служба Messenger.

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%
```



Не забудьте произвести "холодную" перезагрузку Антивируса Касперского® (см. п. 6.4 на стр. 49).

### 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.



**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 spam-virus@localhost.ru
OnWarning=exec echo "%USER% %FULLPATH%/FILENAME%
from %USERHOST% is probably infected by
%VIRUSNAME%" | mail spam-virus@localhost.ru
OnSuspicion=exec echo "%USER%
%FULLPATH%/FILENAME% from %USERHOST% is probably
infected by %VIRUSNAME%" | mail spam-
virus@localhost.ru
```



Не забудьте произвести "холодную" перезагрузку Антивируса Касперского® (см. п. 6.4 на стр. 49).

## 5.3. Антивирусная защита файловых систем

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. 45.

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:

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

### 5.3.2. Ежедневная 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/kavscanner.cron`



**Решение:** для реализации поставленной задачи выполните следующие действия:

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

```
0 0 * * * /path/to/kavscanner -c
/etc/kav/kavscanner.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. Лечение зараженных объектов в архиве

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



**Задача:** проверить все доступные на сервере архивы типа *tar* и *zip* и с помощью скрипта *vox.sh* попытаться вылечить все обнаруженные внутри архива инфицированные объекты. В качестве конфигурационного файла использовать */etc/kav/kavscanner.conf.in*, где предварительно указать использование скрипт-файла для лечения архивов.

Список всех инфицированных объектов с полными путями к ним привести в файле */tmp/infected\_archive.lst*. Отчет о работе компонента вывести только в файл */tmp/logfile.log*.



**Решение:** для реализации поставленной задачи выполните следующие действия:

1. Создайте альтернативный файл *kavscanner.conf.in*.
2. Задайте правила обработки инфицированных объектов. Для этого в секции **[scanner.container]** данного файла введите строку:

```
OnInfected=exec /tmp/kavscanner/test/vox.sh
%FULLPATH%/%FILENAME%
```

3. В командной строке введите:

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

### 5.3.3.2. 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 kavscanner
admin@localhost.ru
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s 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. 15), 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 мониторинга: путь и объекты мониторинга (см. п. 6.1.1. на стр. 39).
- Режима проверки и лечения файлов (см. п. 6.1.2 на стр. 40).
- Действий над файлами (см. п. 6.1.3. на стр. 41).
- Режима резервного копирования (см. п. 6.1.5 на стр. 46).
- Формирования отчета и оповещений (см. п. 6.5 на стр. 51).

### 6.1.1. Область мониторинга

Область мониторинга компонента *kavsamba* включает в себя *путь* и *объекты мониторинга*.

Под *путем мониторинга* 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 мониторинга* (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. 51). 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. 41).

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**), 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** 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 Unix/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.

## 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 **ExcludeDir** (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 "холодную" перезагрузку Антивируса Касперского® (см. п. 6.4 на стр. 49).

## 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:

- запакованные 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. 44) (этот параметр аналогичен области мониторинга при осуществлении защиты в реальном времени).
- Режим проверки и лечения файлов (см. п. 6.2.2 на стр. 45).
- Действия над файлами (см. п. 6.2.3 на стр. 45).

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. 41).

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** (аналогично компоненту *kavsamba*) и **Corrupted** 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 *kavscanner* 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 самораспаковываемыми 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 *kavscanner*.

## 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. 42 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:

```
# kavscanner -@/tmp/downloads.lst -c sam-
  ple_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 неизмененным 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.



#### *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 эффективности 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]** параметры **CheckFilesLimit**). Также задается количество файлов, одновременно проверяемых в фоновом режиме (секция **[samba.options]** параметр **BgCheckFilesLimit**). 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.

Тем самым удается устанавливать максимально допустимую нагрузку сервера.

## 6.4. Перезагрузка Антивируса Касперского®

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/kavsamba reload avebases
```

Для дистрибутивов OpenBSD:

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
reload avebases
```

Для дистрибутивов FreeBSD:

```
/usr/local/etc/rc.d/kavsamba.sh/ reload avebases
```

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/kavsamba reload
```

Для дистрибутивов Open BSD:

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
reload
```

Для дистрибутивов Free BSD:

```
/usr/local/etc/rc.d/kavsamba.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/kavsamba stop
```

Для дистрибутивов Open BSD:

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
stop
```

Для дистрибутивов Free BSD:

```
/usr/local/etc/rc.d/kavsamba.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 (см. п. 6.6.2 на стр.55).

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

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

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

Уровни	Название уровня	Значение
	Фатальные ошибки	Информация только о критических ошибках (ошибках, которые приводят к завершению работы программы из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при 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 при проверке файла.
2	Info	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.
3	Activity	Сообщения о проверке файлов в соответствии с уровнем детализации отчета о проверке.
10	Debug	Все сообщения отладочного характера; например, содержание конфигурационного файла.

Информация о фатальных ошибках в работе компонента выводится всегда вне зависимости от установленного уровня детализации. Оптимальным уровнем для работы компонента является уровень **3**, который задан по умолчанию.

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

[дата время уровень\_детализации] STRING

где:

[дата время уровень\_детализации]- параметр, формирующийся системно и содержащий дату и время (в формате, указанном администратором) и уровень детализации отчета (первая буква, соответствующая названию уровня детализации).

`String` – строка отчета; имеет различный формат в зависимости от вида сообщения. Предусмотрены следующие виды сообщений:

- Сообщения о проверке.
- Прочие сообщения (о старте компонента, о загрузке антивирусных баз, коды возврата и т.д.).
- Сообщения, выводимые на консоль.

Рассмотрим подробнее виды сообщений и соответствующий им формат.

## 6.6.1. Формат сообщений о проверке



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

Формат отчета о проверке каждого файла, формируемого компонентом *kavscanner*, зависит от того, к какому типу объектов (простому или объекту-контейнеру) он относится.

Для **простого объекта** сообщения о проверке имеют следующий формат:

- Расширенный формат сообщений (секция **[scanner.report]** параметр **ShowObjectResultOnly=no**):

```
"имя_файла" результат [имя_вируса]
```

- Краткий формат сообщений (секция **[scanner.report]** параметр **ShowObjectResultOnly=yes**):

```
"имя_файла" результат
```

где:

`имя_вируса` – имя вируса для событий CURED, INFECTED, CUREFAILED, WARNING, SUSPICION. Для остальных событий это поле пустое.

`результат` – статус, который присваивается файлу в результате проверки и лечения. Полный перечень возможных результатов приведен в таблице ниже.

Для **объектов-контейнеров** (архивов) формат сообщений о проверке также может быть расширенным или кратким:

- Расширенный формат сообщений (секция **[scanner.report]** параметр **ShowContainerResultOnly=no**):

"имя\_архива"

"имя\_файла" результат [имя\_вируса]

"имя\_файла" результат [имя\_вируса]

- Краткий формат сообщений (секция **[scanner.report]** параметр **ShowContainerResultOnly=yes**):

"имя\_файла" результат

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

Для компонента *kavsamba* сообщения о проверке имеет формат, аналогичный расширенному формату сообщений для компонента *kavscanner* (секция **[samba.report]**):

"имя\_файла" результат [имя\_вируса]

где:

`имя_вируса` – имя вируса (или нескольких вирусов, которыми заражен объект; перечислены через запятую) для событий CURED, INFECTED, CUREFAILED, WARNING, SUSPICION. Для остальных событий это поле пустое.

`результат` – статус, который присваивается файлу в результате проверки и лечения. Полный перечень возможных результатов приведен в таблице выше.

## 6.6.2. Формат сообщений, выводящихся на консоль



Вывод сообщений на консоль присущ только компоненту *kavscanner*.

Вывод информации компонента *kavscanner* на консоль регулируется наличием или отсутствием в командной строке запуска компонента ключа `-q`. Если ключ указан, то информация на консоль не выводится.

По умолчанию формат и объем информации, выводимой на экран, полностью соответствует включаемой в файл-отчет.

Для компонента *kavscanner* вы можете изменить состав выводимой на консоль информации. Для этого вам необходимо в конфигурационном файле приложения внести соответствующие изменения в секцию `[scanner.display]`.

В этой секции вы можете отрегулировать необходимость вывода на экран информации о проверке объектов внутри архива (**ShowArchiveContent**, **ShowContainerResultOnly**), незараженных файлах (**ShowOK**) и результатов текущей работы компонента (**ShowProgress**).

Детализация отчета о проверке при наличии секции `[display]` регулируется из командной строки ключем `-x<опция>`.

---

# ГЛАВА 7. РАБОТА С ЛИЦЕНЗИЯМИ

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.

## 7.1. Управление лицензионными ключами

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

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

- круглосуточную техническую поддержку;
- ежедневное обновление антивирусных баз *2 раза в день*;
- 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 *licensmanager*, 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:

```
#./licensmanager -s
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2003.
```

```
Active key info:
```

```
Product name: Kaspersky Anti-Virus 5 Business Optimal 1  
month (Samba Servers)
```

```
Key file 00053BC3.key
```

```
Type: Commercial
```

```
Expiration date: 17-11-2003, expires in 60 days
```

```
Serial: 02B1-000454-00053BC
```

```
Additional key info:
```

```
Product name: Kaspersky Anti-Virus 5 Business Optimal 1  
month (Samba Servers)
```

```
Key file 00053E3D.key
```

```
Type: Commercial
```

Expiration date: expired  
Serial: 02B1-000454-00053E3



*Чтобы просмотреть информацию о лицензионном ключе,*

в командной строке введите, например, такую строку:

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

На консоль сервера будет выведена информация подобного рода:

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

## 7.1.2. Продление лицензии

Продление лицензии на использование Антивируса Касперского® дает вам право на восстановление полной функциональности приложения. Кроме того, возобновляются дополнительные услуги, приведенные в п. 7.1 на стр. 56.

Срок действия лицензии зависит от типа лицензирования, который вы выбрали, приобретая приложение (на Антивирус Касперского® для Samba Servers срок составляет, как правило, один год).



*Чтобы продлить лицензию на использование Антивируса Касперского® для Samba Servers, 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](mailto:sales@kaspersky.com)) или заполнив соответствующую форму на нашем сайте ([www.kaspersky.ru](http://www.kaspersky.ru)) в разде-

ле **Купить онлайн → Для пользователей систем Linux**. По факту оплаты вам будет отправлен лицензионный ключ по электронной почте, адрес которой был указан вами в форме заказа.



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

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:

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

На консоль сервера будет выведена следующая информация:

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

После этого рекомендуем вам обновить антивирусные базы.

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

Установка резервного ключа 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 активный ключ,*

в командной строке введите такую строку:

```
#./licensmanager -da
```

На консоль сервера будет выведена следующая информация:

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



*Чтобы удалить резервный ключ,*

в командной строке введите такую строку:

```
#./licensmanager -dr
```


На консоль сервера будет выведена следующая информация:

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

---

# ГЛАВА 8. 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](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"	<b>Infected.</b> Объект не подвергается лечению.
CORP-	<b>Corrupted.</b> Объект поврежден
SUSP-	<b>Suspicious</b> (код неизвестного вируса).
WARN-	<b>Warning</b> (модифицированный код известного вируса).
ERRO-	<b>Error.</b> В результате проверки объекта произошла ошибка.
CURE-	<b>Cured.</b> 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, CORP-X50!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:** 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-Shecker. 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:** 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 (**Сервисы → Для клиентов компании → Техническая поддержка → Поддержка онлайн**).

Также мы рекомендуем обратиться к фирме, продавшей вам Антивирус Касперского® или написать письмо в Службу Технической Поддержки ([support@kaspersky.com](mailto:support@kaspersky.com)).

Чтобы ваш запрос был обработан как можно скорее:

1. В заголовке сообщения укажите операционную систему вашего сервера, имя компонента, который вы не можете настроить, и проблему. Например:  
**Linux, Webmin, нет доступа к настройкам списка лицензированных пользователей.**
2. Пишите сообщения в виде plain text. Сообщения HTML-формата труднее читать.
3. В начале сообщения укажите точную версию операционной системы, дистрибутива Антивируса Касперского® и имени вашего лицензионного ключа.
4. Кратко, но наиболее понятно опишите проблему. Помните, что Служба Поддержки на момент чтения вашего письма ещё ничего не знает о вашей проблеме и сможет помочь вам, только полностью поняв и воспроизведя её.
5. Отправьте в Службу Технической Поддержки следующие данные, предварительно запаковав их в один архив:
  - файл отчета компонентов Антивируса;
  - лицензионный ключ.
6. Обязательно укажите в письме о наличии:
  - SCSI-контроллера;
  - очень старого или нового процессора, нескольких процессоров;
  - памяти меньше, чем 64 МБ или больше 2 ГБ.
7. Укажите примерный размер дневного трафика и бывают ли пики нагрузки.



**Вопрос:** может ли злоумышленник подменить антивирусные базы?

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 Антивирус Касперского® проверяет ее. Если подпись не соответствует присвоенной в Лаборатории Касперского, и дата баз – более поздняя, чем день окончания лицензии на использование продукта, Антивирус Касперского® не будет использовать такие базы.



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

Данные виды процессоров в текущей версии приложения не поддерживаются.



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

Тестирование Антивируса Касперского® для Samba Servers производилось на дистрибутивах RedHat, Debian и SuSE и именно для них собирались дистрибутивы Антивируса Касперского®



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

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



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

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

```
tar zxvf <имя_архива>
```



**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.

## ВРЕДОНОСНЫЕ ПРОГРАММЫ В UNIX- СРЕДЕ

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

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

### А.1. Вирусы

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

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

По особенностям алгоритма работы можно выделить:

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

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

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

Приведем примеры некоторых вирусов под Unix-системы:

**ELF\_SNOOPY** – вирус, инфицирующий исполняемые Unix-файлы.

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

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

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

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

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

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

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

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

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

## A.2. Троянские программы

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

Распространение троянских программ осуществляется по сети.

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

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

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

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

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

## А.3. Сетевые черви

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

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

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

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

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

*Алгоритм работы:* используя проблемы буферного переполнения червь отправляет на удаленные компьютеры короткий кусок своего кода. При старте основного компонента червя (файл *start.sh*) поочередно вызываются прочие компоненты, которые определяют адреса атакуемых систем, посредством атаки "переполнение буфера" засылают туда "загрузчик" червя, который затем докачивает и запускает основной код червя. Главная страница веб-сервера подменяется HTML-файлом с текстом: "RameN Crew – Hackers loooooooooooooove noodles". Наконец, червь отправляет сообщение e-mail по двум адресам, перезагружает систему и начинает сканировать интернет заново.

Червь также добавляет команду запуска своего основного файла к файлу инициализации системы */etc/rc.d/rc.sysinit*. В результате, червь запускается каждый раз при последующих запусках зараженной системы.

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

*Алгоритм работы:* червь сканирует интернет в поиске систем, имеющих уязвимость в безопасности root-доступа. Найдя подобную систему, червь инфицирует ее, собирает информацию о ней (ip-адрес, логины, пароли) в файл с именем *mail.log* и затем отправляет его на электронный адрес *1i0nsniffer@china.com*.

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

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

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

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

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

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

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

---

# ПРИЛОЖЕНИЕ 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, Бенилюксе, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

"Лаборатория Касперского" сегодня – это более двухсотпятидесяти высококвалифицированных специалистов, девять из которых имеют дипломы MBA, пятнадцать – степени кандидатов наук и двое являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

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

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. "Лаборатория Касперского" первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых шлюзов, межсетевых экранов и 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 дважды в день. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

## **В.1. Другие разработки "Лаборатории Касперского"**

### **Антивирус Касперского® Lite**

Программа является самым простым в использовании антивирусным продуктом "Лаборатории Касперского", предназначенным для защиты компьютера домашнего пользователя, работающего под управлением операционных систем Windows 98/Me, Windows 2000/NT Workstation, Windows XP.

В состав Антивируса Касперского® Lite входят:

- **антивирусный сканер** для проведения полной проверки локальных и сетевых дисков по требованию пользователя;
- **антивирусный монитор**, автоматически проверяющий все используемые файлы в масштабе реального времени;
- **модуль проверки почтовых баз MS Outlook Express** на присутствие вирусов по требованию пользователя.

### **Антивирус Касперского® Personal**

Антивирус Касперского® Personal обеспечивает защиту домашних компьютеров, работающих под управлением операционных систем Windows 98/ME, Windows 2000/NT, Windows XP от всех известных видов вирусов, включая Троянских коней, интернет-червей, скрипт-вирусы, опасные ActiveX и Java-апплеты и др. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д. Антивирус Касперского Personal включает программу загрузки ежедневных обновлений через интернет. Уникальная система эвристического анализа данных второго поколения эффективно нейтрализует неизвестные вирусы. Удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского Personal обеспечивает:

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

Антивирус Касперского Personal поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP.

### **Антивирус Касперского® Personal Pro**

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

Помимо функций автоматической проверки всех файлов в режиме реального времени и по запросу пользователя, а также почтового фильтра Антивирус Касперского® Personal Pro включает в себя **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов.

### **Kaspersky® Anti-Hacker**

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

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

Благодаря технологии SmartStealth™ значительно затрудняется обнаружение компьютера извне: режим невидимости вашего компьютера обеспечивает защиту от хакерских атак, не оказывая никакого негативного

влияния на вашу работу в интернете. Программа обеспечивает стандартную прозрачность и доступность информации.

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

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

### **Kaspersky® Security для PDA**

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

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

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

### **Антивирус Касперского® Business Optimal**

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

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту<sup>1</sup>:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.

---

<sup>1</sup> В зависимости от типа поставки

- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *почтовых систем* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail и Qmail.

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

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

### **Kaspersky® Corporate Suite**

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

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *потоков данных, проходящих через межсетевые экраны.*
- *карманных компьютеров.*

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

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

## Kaspersky® Anti-Spam

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

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

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

## V.2. Наши координаты

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

Адрес:	Россия, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700, 948-4331, 948-8350	
Экстренная круглосуточная помощь	+7 (095) 797-8707, 495-0300	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	<a href="mailto:smb-support@kaspersky.com">smb-support@kaspersky.com</a>
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	

Антивирусная лаборатория	<a href="mailto:newvirus@kaspersky.com">newvirus@kaspersky.com</a> (только для отправки новых вирусов в архивированном виде)	
Департамент продаж	+7 (095) 797-8700 +7 (095) 948-4331 +7 (095) 948-8350	<a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>
Департамент маркетинговых коммуникаций	+7 (095) 948-5650	<a href="mailto:info@kaspersky.com">info@kaspersky.com</a>
WWW:	<a href="http://www.kaspersky.ru">http://www.kaspersky.ru</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a>	