

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского® 5.7 для Linux

Workstation

РУКОВОДСТВО

АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО® 5.7 ДЛЯ
LINUX WORKSTATION

Руководство администратора

© ЗАО "Лаборатория Касперского"
Тел./факс: +7 (495) 797-87-00, +7 (495) 645-79-39
<http://www.kaspersky.ru>

Дата редакции: сентябрь 2008 года

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	6
1.1. Компьютерные вирусы и вредоносные программы	7
1.2. Назначение и основные функции Антивируса Касперского	8
1.3. Что нового в версии 5.7	9
1.4. Схема лицензирования	9
1.5. Аппаратные и программные требования к системе	9
1.6. Комплект поставки.....	10
1.6.1. Лицензионное соглашение.....	11
1.6.2. Регистрационная карточка	11
1.7. Сервис для зарегистрированных пользователей.....	12
1.8. Принятые обозначения.....	12
ГЛАВА 2. АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ.....	14
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО.....	16
3.1. Установка приложения на компьютер под управлением Linux	16
3.2. Процесс установки	17
3.3. Постинсталляционная настройка.....	17
3.4. Установка Агента Администрирования	18
3.5. Настройка Агента Администрирования.....	18
3.6. Процесс обновления приложения до версии 5.7	19
3.7. Расположение файлов приложения по каталогам	20
3.8. Завершение установки	21
ГЛАВА 4. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО	22
4.1. Обновление антивирусных баз	22
4.1.1. Автоматическое обновление антивирусных баз	24
4.1.2. Обновление антивирусных баз по требованию	25
4.1.3. Создание сетевого каталога для хранения и копирования антивирусных баз.....	26
4.2. Антивирусная защита файловых систем.....	27
4.2.1. Область проверки.....	28
4.2.2. Режим проверки и лечения объектов	30

4.2.3. Действия над объектами	30
4.2.4. Проверка по требованию отдельного каталога	32
4.2.5. Проверка по расписанию	32
4.2.6. Дополнительные возможности: использование скрипт-файлов	33
4.2.6.1. Лечение зараженных объектов в архиве	33
4.2.6.2. Отправка администратору уведомления	34
4.3. Антивирусная защита в режиме реального времени	34
4.4. Управление лицензионными ключами	36
4.4.1. Просмотр информации о лицензионном ключе	37
4.4.2. Продление лицензии	38
ГЛАВА 5. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА	40
5.1. Настройка совместной работы с Webmin	40
5.2. Оптимизация работы Антивируса Касперского	41
5.3. Перенос объектов в карантинный каталог	43
5.4. Режим резервного копирования объектов (backup)	45
5.5. Локализация отображаемого формата даты и времени	46
5.6. Параметры формирования отчета Антивируса Касперского	46
ГЛАВА 6. УПРАВЛЕНИЕ ПРИЛОЖЕНИЕМ С ПОМОЩЬЮ KASPERSKY ADMINISTRATION KIT	49
6.1. Управление приложением	51
6.1.1. Настройка параметров приложения	52
6.1.1.1. Закладка Параметры, раздел Постоянная Защита: Общие параметры	53
6.1.1.2. Закладка Параметры, раздел Постоянная Защита: Область и объекты защиты	54
6.2. Управление задачами	54
6.2.1. Создание задачи	55
6.2.1.1. Создание локальной задачи	56
6.2.1.2. Создание групповой задачи	58
6.2.1.3. Создание глобальной задачи	59
6.2.2. Настройка специфических параметров задач	60
6.2.2.1. Задача проверки по требованию	61
6.2.2.2. Задача обновления	62
6.2.3. Запуск и остановка задач	62
6.3. Управление политиками	63
6.3.1. Создание политики	63

6.3.2. Просмотр и редактирование параметров политики	65
6.3.2.1. Настройка области защиты	66
6.3.2.2. Определение типа проверяемых файлов	67
6.3.2.3. Настройка действий над объектами	67
6.3.2.4. Настройка дополнительных параметров	67
ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО	68
ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА	69
ПРИЛОЖЕНИЕ А. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ПРИЛОЖЕНИИ	71
А.1. Конфигурационный файл Антивируса Касперского	71
А.2. Ключи командной строки компонента kavscanner	80
А.3. Коды возврата компонента kavscanner	83
А.4. Ключи командной строки компонента kavmonitor	84
А.5. Ключи командной строки компонента licensemanager	85
А.6. Коды возврата компонента licensemanager	85
А.7. Ключи командной строки компонента keepup2date	86
А.8. Коды возврата компонента keepup2date	87
А.9. Ключи командной строки компонента kavmiddleware	88
ПРИЛОЖЕНИЕ В. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	89
ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	96
С.1. Другие разработки «Лаборатории Касперского»	97
С.2. Наши координаты	109

ГЛАВА 1. ВВЕДЕНИЕ

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

Среди источников проникновения вредоносных программ наиболее опасными являются:

Интернет

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

Электронная почтовая корреспонденция

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

Уязвимости в программном обеспечении

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

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

1.1. Компьютерные вирусы и вредоносные программы

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

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

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

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

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



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

1.2. Назначение и основные функции Антивируса Касперского

Программное приложение **Антивирус Касперского® 5.7 для Linux Workstation** (далее также *Антивирус Касперского, Приложение*) предназначен для антивирусной защиты рабочих станций, работающих под управлением операционных систем Linux.

Приложение позволяет:

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

1.3. Что нового в версии 5.7

В версии Антивируса Касперского 5.7 для Linux Workstation по сравнению с версией 5.5 произведено следующее изменение:

- Добавлена возможность настройки и управления работой Антивируса Касперского с помощью Kaspersky Administration Kit.

1.4. Схема лицензирования

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

1.5. Аппаратные и программные требования к системе

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

- Аппаратные требования:
 - Процессор Intel Pentium® 133 МГц или выше.
 - 64 МБ оперативной памяти.
 - 100 МБ на жестком диске для установки приложения и хранения временных файлов.
- Программные требования:
 - для 32-битной платформы одна из следующих операционных систем:
 - Red Hat Enterprise Linux 5.2 Desktop;
 - Fedora 9;
 - SUSE Linux Enterprise Desktop 10 SP2;
 - openSUSE Linux 11;
 - Debian GNU/Linux 4 R4;
 - Mandriva Corporate Desktop 4;

- Ubuntu 8.04.1 Desktop Edition;
- Linux XP 2008 Enterprise;
- для 64-битной платформы одна из следующих операционных систем:
 - Red Hat Enterprise Linux 5.2 Desktop;
 - Fedora 9;
 - SUSE Linux Enterprise Desktop 10 SP2;
 - openSUSE Linux 11.
- Программа Webmin (www.webmin.com) – для удаленного администрирования Антивируса Касперского.
- Интерпретатор языка Perl версии 5.0 или выше (www.perl.org).
- Установленная утилита which.
- Установленные пакеты для компиляции программ (gcc, binutils, glibc-devel, make, ld), а также установленный исходный код ядра операционной системы – для компиляции компонента *kavmonitor*.



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

1.6. Комплект поставки

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

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

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

- Лицензионное соглашение.



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

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

1.6.1. Лицензионное соглашение

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

Внимательно прочитайте Лицензионное соглашение!

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

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

1.6.2. Регистрационная карточка

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

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

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока действия лицензии. Кроме того, зарегистрированным пользователям, подписавшим-

ся на рассылку новостей ЗАО «Лаборатория Касперского», высылаются информация о выходе новых программных продуктов.

1.7. Сервис для зарегистрированных пользователей

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

Приобретая лицензию, вы становитесь зарегистрированным пользователем программы и в течение срока действия лицензии можете получать следующие услуги:

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



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

1.8. Принятые обозначения

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

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

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

ГЛАВА 2. АЛГОРИТМ РАБОТЫ ПРИЛОЖЕНИЯ

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

Антивирус Касперского включает в себя:

- компонент антивирусной проверки по требованию *kavscanner*;
- компонент антивирусной проверки в режиме реального времени *kavmonitor*;
- компонент обновления антивирусных баз *keepup2date*;
- утилиту работы с лицензионными ключами *licensmanager*;
- компонент удаленного управления для Kaspersky Administration Kit *kavmiddleware*;
- модуль удаленного управления к программе Webmin.

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

Итак, предусмотрен следующий порядок работы:

1. При обращении какой-либо программы к некоторому объекту файловой системы (запрос на открытие, запуск или закрытие файла) обращение перехватывается модулем ядра компонента *kavmonitor* и файл перенаправляется на антивирусную проверку.



Возможность перехвата операций закрытия файла не поддерживается в следующих версиях ядра:

- для 32-битных операционных систем: с версии ядра 2.6.21 и выше;
 - для 64-битных операционных систем: с версии ядра 2.6.18 и выше.
2. Обработка перехваченного файла производится с помощью программы-демона, входящей в состав компонента *kavmonitor*. Демон

выполняет проверку запрошенного объекта на присутствие вирусов и его обработку в соответствии с параметрами конфигурационного файла (в том числе и лечение с помощью антивирусных баз, если данная опция включена).

3. После обработки файла *kavmonitor* отправляет модулю ядра код доступа (разрешен/запрещен), определяющий статус файла.
4. В соответствии со статусом объекта компонент *kavmonitor* разрешает доступ к файлу, либо блокирует его (в этом случае запросившая файл программа получает код ошибки (Access denied)).

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

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

Действия, производимые над объектом конкретного статуса, определяются параметрами конфигурационного файла (подробнее см. приложение А на стр. 71).

ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

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

- Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. п. 1.5 на стр. 9).
- Настроить интернет-соединение.
- Войти систему под пользователем **root**.

3.1. Установка приложения на компьютер под управлением Linux

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

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



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

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



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

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

3.2. Процесс установки

Установка приложения проходит в два этапа. Первый этап включает в себя следующие шаги:

1. Создание пользователя `kluser` и группы `klusers`.
2. Распаковка файлов дистрибутива на компьютер.
3. Регистрация сервисов, в зависимости от устанавливаемой системы.
4. Настройка конфигурационных файлов компонентов на параметры по умолчанию.

3.3. Постинсталляционная настройка

Вторым этапом установки Антивируса Касперского является постинсталляционная настройка. Для запуска настройки используйте скрипт `postinstall.pl`, расположенный в каталоге `/opt/kaspersky/kav4ws/lib/bin/setup`.



При установке приложения на компьютер под управлением Debian скрипт постинсталляционной настройки запускается автоматически.

После запуска скрипта вам будет предложено выполнить следующие действия:

1. Указать путь к файлу лицензионного ключа.
2. Настроить параметры прокси-сервера, используемого для подключения к интернету в формате

```
http://<IP-адрес прокси сервера>:<порт>
```

или

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

в зависимости от того, требует ли данный прокси-сервер авторизации. Данное значение используется компонентом обновления (`keepup2date`) приложения для подключения к серверам Лаборатории Касперского и скачивания обновлений антивирусных баз.

Если вы не используете прокси-сервер для подключения к интернету, то задайте значение **no** для данного параметра.

3. Скопировать антивирусные базы с серверов Лаборатории Касперского. Укажите значение **yes** или **no**, в зависимости от того, хотите ли вы выполнить обновление сейчас.
4. Настроить работу с Webmin.
5. Запустить компиляцию модуля *kavmonitor*. На данном этапе компилируются библиотеки, необходимые для работы компонента *kavmonitor*. Если исходные коды ядра системы находятся не в директории по умолчанию, то для компиляции модуля *kavmonitor* в командной строке введите:

```
# /opt/kaspersky/kav4ws/src/kavmon.pl -b [PATH]
```

где [PATH] – путь к исходным кодам ядра.

3.4. Установка Агента Администрирования

Если планируется удаленное управление приложением в помощью Kaspersky Administration Kit, то необходимо произвести установку Агента Администрирования.



Для запуска установки Агента Администрирования из rpm-пакета в командной строке введите:

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



Для запуска установки Агента Администрирования из deb-пакета в командной строке введите:

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

3.5. Настройка Агента Администрирования

После установки Агент Администрирования необходимо настроить для обеспечения работы с Kaspersky Administration Kit. Для запуска настройки используйте скрипт *postinstall.pl*, расположенный в каталоге */opt/kaspersky/klnagent/lib/bin/setup*.



При установке Агента Администрирования на компьютер под управлением Debian скрипт постинсталляционной настройки запускается автоматически.

После запуска скрипта вам будет предложено выполнить следующие действия:

1. Указать DNS-имя или IP-адрес Сервера Администрирования.
2. Указать номера порта Сервера Администрирования.
3. Указать номер SSL-порта Сервера Администрирования.
4. Указать, использовать ли SSL-соединение для передачи данных.
5. Задать имя группы администрирования по умолчанию.

3.6. Процесс обновления приложения до версии 5.7



Корректно процедура обновления происходит для версии 5.5-27.

Перед запуском обновления необходимо остановить сервис *kavmonitor*. Для этого в командной строке наберите:

```
# /etc/init.d/kav4ws stop
```



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

```
# rpm -U <имя_файла_дистрибутива>
```



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

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

По завершению процедуры обновления конфигурационный файл версии 5.5 заменяется на файл версии 5.7. Внесите необходимые изменения в конфигурационный файл вручную.

3.7. Расположение файлов приложения по каталогам



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

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

kav4ws.conf – конфигурационный файл.

/etc/init.d/kav4ws/ – скрипт управления сервисом *kavmonitor*.

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

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

kav4ws-kavscanner – исполняемый файл компонента антивирусной защиты;

kav4ws-keepup2date – исполняемый файл компонента обновления антивирусных баз;

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

/lib/ – каталог хранения служебных файлов Антивируса Касперского;

/setup/ – каталог, содержащий скрипты для настройки приложения:

postinstall.pl – скрипт постинсталляционной настройки приложения.

uninstall.pl – скрипт удаления приложения.

setup.pl – скрипт настройки приложения.

/sbin/ – каталог хранения служебных сервисов Антивируса Касперского:

kav4ws-kavmonitor – исполняемый файл компонента антивирусной защиты.

kav4ws-kavmiddleware – исполняемый файл компонента удаленного управления *kavmiddleware*.

/src/ – каталог хранения модуля антивирусного ядра приложения.

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

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

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

/opt/kaspersky/kav4ws/share//man/ – каталог хранения man-файлов.

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

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

/var/opt/kaspersky/kav4ws/licenses – каталог хранения лицензионной информации.



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



После установки Агента Администрирования на рабочую станцию под управлением операционной системы Linux по умолчанию файлы Агента Администрирования будут расположены следующим образом:

/opt/kaspersky/klnagent/ – основной каталог Агента Администрирования, содержащий:

/bin/ – каталог, содержащий исполняемые файлы утилит Агента Администрирования, в том числе:

klmover – данная утилита предназначена для настройки соединения с Сервером Администрирования (для получения более полной информации см. «Справочное руководство Касперский Administration Kit»);

klmagchk – данная утилита предназначена для проверки соединения с Сервером Администрирования (для получения более полной информации см. «Справочное руководство Касперский Administration Kit»);

/lib/ – каталог, содержащий дополнительные файлы Агента Администрирования.

/bin/setup – каталог, содержащий скрипты для настройки Агента Администрирования;

/share/man/ – каталог, содержащий man-страницы.

/sbin/ – каталог, содержащий исполняемый файл службы Агента Администрирования.

3.8. Завершение установки

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

ГЛАВА 4. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

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

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

- Обновление антивирусных баз, используемых для поиска вирусов и лечения зараженных объектов (подробнее см. п. 4.1 на стр. 22).
- Антивирусная защита файловых систем компьютера (проверка по расписанию и \ или по требованию) (подробнее см. п. 4.2 на стр. 27).
- Постоянная антивирусная защита (защита в масштабе реального времени) (подробнее см. п. 4.3 на стр.34).

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

4.1. Обновление антивирусных баз

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

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

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

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

Список адресов, с которых можно копировать обновления, приведен в файле `/var/opt/kaspersky/kav4ws/bases/updcfg.xml`, включенном в дистрибутив

приложения. Для просмотра списка серверов обновлений введите в командной строке:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -s
```

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



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



В качестве источника обновлений можно использовать сервер обновлений, не принадлежащий «Лаборатории Касперского». Базы Антивируса Касперского, размещенные на этом сервере, могут быть более старой версии, чем те, что установлены на компьютере пользователя. В случае обновления с такого сервера базы старой версии заменят более актуальные.

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



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

Если структура вашей локальной сети достаточно сложная, мы рекомендуем каждый час скачивать обновления антивирусных баз с серверов обновлений, размещать их в некотором сетевом каталоге, а для локальных компьютеров сети настроить копирование баз из этого каталога. Подробнее о создании сетевого каталога см. в п. 4.1.3 на стр. 26.

Обновление может быть организовано по расписанию с помощью программы **cron** (см. п. 4.1.1 на стр. 24) или же выполняться по требованию администратора, запускаясь вручную из командной строки (см. п. 4.1.2 на стр. 25).



Настоятельно рекомендуем настроить ежечасное обновление антивирусных баз!

4.1.1. Автоматическое обновление антивирусных баз

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

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

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

```
0 0-23/1 * * * /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date
```



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



Решение: для реализации поставленной задачи выполните следующие действия:

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

4.1.2. Обновление антивирусных баз по требованию

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

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date
```



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



Решение: для реализации поставленной задачи в командной строке введите:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -l  
/tmp/updatesreport.log
```

Если вам необходимо обновить антивирусные базы на нескольких компьютерах, удобнее вместо многократного получения баз через интернет полу-

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

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

2. В командной строке введите:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -l
/tmp/report.txt
```

4.1.3. Создание сетевого каталога для хранения и копирования антивирусных баз

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

1. Создайте локальный каталог.

2. Запустите компонент *keepup2date* следующим образом:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -u  
<dir>
```

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

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



Задача: настроить обновление антивирусных баз через прокси-сервер.



Решение: для реализации поставленной задачи выполните следующие действия:

В секции **[updater.options]** конфигурационного файла присвойте параметру **UseProxy** значение **Yes**.

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

или:

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

4.2. Антивирусная защита файловых систем

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



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



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

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

- Область проверки (см. п. 4.2.1 на стр. 28).
- Режим проверки и лечения объектов (см. п. 4.2.2 на стр. 30).
- Действия над объектами (см. п. 4.2.3 на стр. 30).
- Параметры формирования отчета о результатах работы (см. п. 5.6 на стр. 46).

Процесс проверки файловых систем вашего компьютера может быть запущен:

- Разово из командной строки (см. п. 4.2.4 на стр. 32).
- По расписанию при помощи программы **cron** (см. п. 4.2.5 на стр.32).



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

4.2.1. Область проверки

Область проверки можно условно разделить на две части:

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

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



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

Вы можете переопределить путь проверки следующими способами:

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



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

- Ограничить пути, принятые по умолчанию (все, начиная с текущего каталога) или перечисленные в командной строке, путем ввода в конфигурационном файле **kav4ws.conf** масок файлов и каталогов, которые будут исключены из области проверки (секция **[scanner.options]**, параметры **ExcludeMask** и **ExcludeDirs**).
- Отключить *рекурсивную проверку каталогов* (секция **[scanner.options]**, параметр **Recursion** или ключ **-r**).
- Создать альтернативный конфигурационный файл и указать его использование посредством ключа **-с (-C) <имя_файла>** при запуске компонента.

Объекты проверки по умолчанию также задаются в конфигурационном файле **kav4ws.conf** (секция **[scanner.options]**) и могут быть переопределены:

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

4.2.2. Режим проверки и лечения объектов

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

По умолчанию опция отключена, что предполагает только проверку объектов и информирование об обнаружении вирусов и других подозрительных или поврежденных файлов путем вывода сообщений на консоль и в отчет (см. п. 5.6 на стр. 46).

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

- **Clean** – вирусов не обнаружено (объект не заражен).
- **Infected** – объект заражен.
- **Warning** – код объекта похож на код известного вируса.
- **Suspicious** – объект подозревается на заражение неизвестным вирусом.
- **Corrupted** – объект поврежден.
- **Protected** – объект проверить невозможно из-за того, что он зашифрован (защищен паролем).
- **Error** – при проверке объекта произошла ошибка.

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

- **Cured** – объект был успешно вылечен.
- **CureFailed** – объект вылечить не удалось. Файл с таким статусом будет обрабатываться по правилам, заданным для зараженных объектов.
- **Error** – при проверке объекта произошла ошибка.

4.2.3. Действия над объектами

В зависимости от статуса объекта (см. Глава 2 на стр. 14) к нему могут применяться те или иные действия. По умолчанию выполняется только уве-

домление об обнаружении объектов с определенным статусом. Однако для объектов со статусами **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** и **Corrupted** можно настроить выполнение ряда действий, таких как:

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

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



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

Выбрать действие над тем или иным объектом можно следующими способами:

- Задать их в конфигурационном файле **kav4ws.conf**, если их предполагается использовать как действия по умолчанию (секции **[scanner.object]** и **[scanner.container]**).
- Указать действия в альтернативном конфигурационном файле и использовать его при запуске компонента.



Если в командной строке при запуске компонента не указывается какой-либо конфигурационный файл, то параметры функционирования берутся из файла **kav4ws.conf**. Использование данного файла при запуске специально не указывается!

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

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

4.2.4. Проверка по требованию отдельного каталога

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



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

В этом же каталоге создать файлы `infected.lst`, `suspicion.lst`, `corrupted.lst` и `warning.lst`, в которых сохранить имена всех обнаруженных в результате проверки зараженных, подозрительных или поврежденных объектов соответственно.

Результаты работы компонента (дату запуска, информацию обо всех файлах, кроме незараженных) выводить в файл-отчет `kav4ws-kavscanner-текущая_дата-pid.log`, который сохранить в том же каталоге.



Решение: для реализации поставленной задачи в командной строке введите:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-kavscanner -rlq -
pi/tmp/infected.lst -ps/tmp/suspicion.lst -
pc/tmp/corrupted.lst -pw/tmp/warning.lst -o
/tmp/kav4ws-kavscanner-`date "+%Y-%m-%d-$$"` .log -i3
-ePASBMe -j3 -mCn /tmp
```

4.2.5. Проверка по расписанию

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

```
0 0 * * * /opt/kaspersky/kav4ws/bin/kav4ws-  
kavscanner -c /etc/kav/scanhome.conf /home
```

4.2.6. Дополнительные возможности: использование скрипт-файлов

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

4.2.6.1. Лечение зараженных объектов в архиве

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

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



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



Решение: для реализации поставленной задачи выполните следующее:

В командной строке введите:

```
# /opt/kaspersky/kav4ws/share/contrib/vox.sh <путь-к-  
архивному файлу>
```

4.2.6.2. Отправка администратору уведомления

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



Задача: настроить уведомление администратора при обнаружении в файловых системах зараженных файлов и архивов при каждой проверке компьютера, выполняемой в соответствии с параметрами конфигурационного файла **kav4ws.conf**. При проверке включить режим раскрытия символьных ссылок.



Решение: для реализации поставленной задачи выполните следующие действия:

Задайте следующие правила обработки простых объектов и контейнеров в конфигурационном файле **kav4ws.conf**:

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% |
mail -s kav4ws-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4ws-kavscanner -a %LIST%
admin@localhost.ru
```



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

4.3. Антивирусная защита в режиме реального времени

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



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

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

- архивов;
- самораспаковывающихся архивов;
- почтовых баз;
- почтовых сообщений.



В случае поступления на проверку символической ссылки проверен будет объект, на который указывает ссылка. Это происходит даже в том случае, если ссылка указывает на объект, исключенный из проверки. При проверке директорий из списка **IncludeDirs** символические ссылки не раскрываются.

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



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

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

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

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

Вы также можете произвести дополнительную настройку:

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



Если планируется удаленное управление приложением с помощью Kaspersky Administration Kit, не следует вносить изменения в секции **[monitor.*]** конфигурационного файла приложения на локальном компьютере. Параметры этих секций будут перезаписаны настройками, сделанными с помощью Kaspersky Administration Kit.

4.4. Управление лицензионными ключами

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

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

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

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

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

4.4.1. Просмотр информации о лицензионном ключе

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

Помимо этого в Антивирусе Касперского предусмотрен специальный компонент *licensemanager*, позволяющий вам просматривать не только более полную информацию о ключах, но и получать некоторые аналитические данные.

Вся информация может быть выведена на экран терминала.



Чтобы просмотреть информацию обо всех лицензионных ключах,

в командной строке введите:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -s
```

На экран будет выведена информация подобного рода:

```
Kaspersky license manager Version 5.7
Copyright (C) Kaspersky Lab. 1997-2007.
Portions Copyright (C) Lan Crypto
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix", expires 04-
07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Linux File Srv
(licence per e-mail address)", expires 25-01-2004 in
234 days
```



Чтобы просмотреть информацию о конкретном ключе,

в командной строке введите такую строку:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -k
<имя файла ключа>
```

где <имя имя файла ключа> - путь и имя файла ключа.

На консоли отразится информация подобного рода:

```
Kaspersky license manager Version 5.7  
Copyright (C) Kaspersky Lab. 1997-2007.  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus for  
Linux", expires 04-07-2003 in 28 days
```

4.4.2. Продление лицензии

Продление лицензии на использование Антивируса Касперского дает вам право на восстановление полной функциональности приложения – обновления антивирусных баз. Кроме того, возобновляются дополнительные услуги, приведенные в п. 4.4 на стр. 36.

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



Чтобы продлить лицензию на использование Антивируса Касперского, вам необходимо:

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

или:

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



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

Приобретенный лицензионный ключ необходимо установить.



Чтобы установить новый лицензионный ключ, в командной строке введите:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -a  
<имя файла ключа>
```

После этого рекомендуем вам обновить антивирусные базы (см. п. 4.1 на стр. 22).



Чтобы удалить лицензионный ключ, в командной строке введите:

для удаления активного лицензионного ключа:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -da
```

для удаления дополнительного лицензионного ключа:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -dr.
```

ГЛАВА 5. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА

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

5.1. Настройка совместной работы с Webmin

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

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

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



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

1. Скопировать данные из существующего конфигурационного файла в новый, который необходимо сохранить под другим именем. После этого провести корректировку нового (альтернативного) конфигурационного файла в соответствии с вашими задачами.
2. Указать имя альтернативного конфигурационного файла на закладке **Config edit** в поле ввода параметра **Full path to KAV config**.



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

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

5.2. Оптимизация работы Антивируса Касперского

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



Использование базы данных iChecker™ и технологии двухуровневого кэширования проверенных файлов.

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

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

- База iChecker™ – общая база, включающая информацию о проверенных **незараженных** файлах определенных форматов. Такая база содержит информацию по объектам, проверенным компонентами *kavmonitor* и *kavscanner*.
- Кеш проверенных файлов – база, содержащая информацию о проверенных компонентом *kavmonitor* файлах. Кеш состоит из двух уровней: на первом уровне хранится информация о **незараженных файлах**, обращение к которым производится наиболее часто. Кеш первого уровня расположен в модуле ядра, что позволяет существенно снизить время, затрачиваемое на обращение к нему. Если приложение обнаруживает данные о запрашиваемом файле в кеше первого уровня, то оно автоматически присваивает объекту статус **Clean**, и дальнейшая антивирусная проверка не производится. Если первый уровень кеша не содержит требуемому

информацию, то производится поиск на втором уровне, содержащем данные **обо всех проверенных файлах**. Обе базы кеша существуют в оперативной памяти, и после окончания работы приложения не сохраняются.

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

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

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



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

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



Ограничение нагрузки на процессор.

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

В Антивирусе Касперского такой механизм существует. В версии 5.7 приложения в конфигурационный файл добавлен параметр **MaxLoadAvg** в секции **[scanner.options]**. В случае если параметр задан, *kavscanner* при проверке каждого нового файла считывает текущую степень загруженности

процессора **load average**, и, в случае ее превышения указанного в конфигурационном файле значения, *kavscanner* приостанавливает работу до момента, когда значение параметра **load average** снизится до указанного уровня.

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

Дополнительной мерой, служащей снижению нагрузки на ресурсы системы, служит отключение *kavmiddleware*. Данный сервис предназначен для взаимодействия Антивируса Касперского и Kaspersky Administration Kit. В случае, если вы не используете возможности приложения по работе с Kaspersky Administration Kit, вы можете отключить сервис *kavmiddleware*. Для этого введите в командной строке:

```
# /etc/init.d/kavmiddleware stop
```

5.3. Перенос объектов в карантинный каталог

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

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

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

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

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

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

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

```
# /opt/kaspersky/kav4ws/bin/kav4ws-kavscanner -
@/tmp/download.lst -ePASBME -rq -i0 -o /tmp/report.log
-j3 -mCn
```

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

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

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



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



Решение: для реализации поставленной задачи выполните следующие действия:

1. В конфигурационном файле приложения включите режим лечения зараженных объектов (**Cure=yes** в секции **[monitor.options]**).

2. Задайте правила изоляции зараженных объектов. Для этого в секции **[monitor.actions]** конфигурационного файла выполните следующую настройку:

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

5.4. Режим резервного копирования объектов (backup)

В случае если проверяемые файлы оказались заражены, а в качестве действия над зараженными объектами определено удаление их из файловой системы, возможен риск потери с ряда важных данных. Чтобы избежать этого, в Антивирусе Касперского предусмотрена возможность копирования файлов в резервное хранилище (backup-хранилище).

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

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

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



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



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

5.5. 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 стандарту strftime:

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

%d/%m/%y – отображаемый формат даты.

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

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

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

5.6. Параметры формирования отчета Антивируса Касперского

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



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

Если вы хотите, чтобы информация о работе приложения фиксировалась в системном лог-файле, присвойте параметру **ReportFileName** секций **[monitor.report]**, **[scanner.report]**, **[updater.report]** значение **syslog**. Информация о работе приложения будет записана под категорией **daemon** системного лог-файла.

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

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

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

Уровни	Название уровня	Значение
0	Критические ошибки	Информация только о критических ошибках (ошибках, которые приводят к завершению работы приложения из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при проверке, загрузке баз и лицензионных ключей. В файле отчета сообщения о критических ошибках помечаются символом F.
1	Errors	Информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов; например, информация об ошибке проверки объекта. В файле отчета сообщения о некритических ошибках помечаются символом E.
2	Warning	Информация об ошибках, которые могут привести к завершению работы продукта (например, информация об отсутствии свободного места на диске или истечении срока действия лицензионного ключа). В файле отчета сообщения о таких ошибках помечаются символом W.

Уровни	Название уровня	Значение
3	Info, Notice	Важные сообщения информационного характера; например: информация о том, запущен ли компонент, путь к конфигурационному файлу, область проверки, информация об антивирусных базах, о лицензионных ключах, результирующая статистика. В файле отчета информационные сообщения помечаются символом I.
4	Activity	Сообщения о текущей активности приложения (например, имя проверяемого файла). В файле отчета сообщения об активности приложения помечаются символом A.
9	Debug	Сообщения с отладочной информацией. Данный уровень детализации предназначен для В файле отчета отладочная информация помечаются символом D.

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



В случае запуска задач проверки по требованию и обновления антивирусных баз с помощью Kaspersky Administration Kit файлы отчета по умолчанию не создаются.

Чтобы включить запись файлов отчета, необходимо указать директорию хранения файлов и уровень детализации отчетов с помощью параметров **ReportLevel** и **ReportsDir** в секции **[middleware.options]** конфигурационного файла приложения.

ГЛАВА 6. УПРАВЛЕНИЕ ПРИЛОЖЕНИЕМ С ПОМОЩЬЮ KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit – это система централизованного решения основных административных задач по управлению системой безопасности компьютерной сети предприятия, построенной на основе приложений, входящих в состав продуктов Антивирус Касперского Business Optimal.

Антивирус Касперского 5.7 один из продуктов «Лаборатории Касперского», управление которым возможно из командной строки (этот способ описан выше в данной документации), либо посредством приложения Kaspersky Administration Kit (если компьютер включен в состав системы удаленного централизованного управления).

Установка приложения проходит в два этапа:

- Разверните в сети *Сервер администрирования*; установите *Консоль администрирования* на рабочее место администратора (подробнее смотрите Руководство по внедрению «Kaspersky Administration Kit»);
- На компьютерах сети установите Антивирус Касперского 5.7 и *Агент администрирования*.

Доступ к управлению приложением через Kaspersky Administration Kit обеспечивает *Консоль администрирования* (см. рис. 1). Она представляет собой стандартный **интерфейс, интегрированный в ММС** (Microsoft Management Console), и позволяет администратору выполнять следующие функции:

- удаленно настраивать Антивирус Касперского на компьютерах сети;
- обновлять антивирусные базы Антивируса Касперского;
- просматривать информацию о работе приложения на клиентских компьютерах.

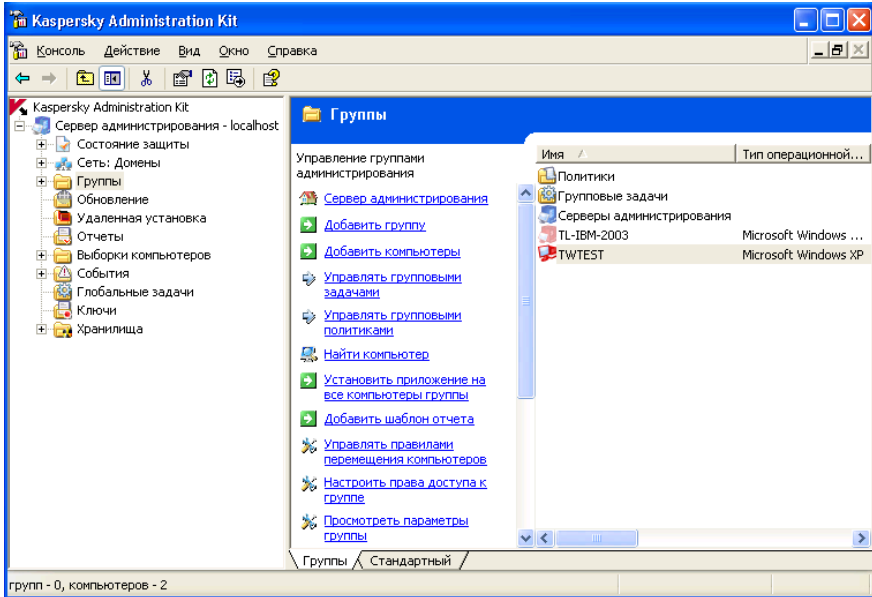


Рисунок 1. Консоль администрирования Kaspersky Administration Kit

При централизованном управлении через Kaspersky Administration Kit администратор определяет параметры политики, параметры задач и параметры приложения. Защита строится на основе настроек этих параметров.

Параметры приложения – набор общих параметров работы приложения, включающий общие параметры защиты, параметры области защиты и др.

Задача – именованное действие, выполняемое приложением. В соответствии с функциями задачи для приложения Антивирус Касперского разделяют по типам:

- задача проверки по требованию;
- задача обновления антивирусных баз.

Каждой конкретной задаче соответствует набор параметров работы Антивируса Касперского при ее выполнении – *настройки задачи*.

Особенностью централизованного управления является организация удаленных компьютеров в группы и управление их настройками через создание и определение групповых политик.

Политика – это набор параметров работы приложения, распространяемый на группу компьютеров в логической сети.

Политика позволяет управлять всей функциональностью приложения, поскольку содержит и настройки приложения и настройки всех типов задач за исключением параметров, которые следует определять непосредственно при запуске задачи (например, расписание выполнения задачи).

В состав политики также может входить набор ограничений на изменение заданных параметров при настройке приложения или задачи.

6.1. Управление приложением

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Антивируса Касперского на отдельном клиентском компьютере, а также настройки общих параметров работы приложения, таких как включение / отключение защиты компьютера, а также настройка параметров формирования отчетов.



Для управления параметрами приложения:

1. В папке **Группы** (см. рис. 1) выберите папку с названием группы, в состав которой входит клиентский компьютер.
2. В панели результатов выберите компьютер, для которого вам необходимо изменить параметры приложения. В контекстном меню или в меню **Действия** выберите команду **Свойства**.
3. В окне свойств клиентского компьютера на закладке **Приложения** (см. рис. 2) представлен полный список приложений «Лаборатории Касперского», установленных на клиентском компьютере. Выберите приложение **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**.

Под списком расположены следующие кнопки:

- **События** – просмотреть список событий в работе приложения, произошедших на рабочей станции и зарегистрированных на сервере администрирования.
- **Статистика** – просмотреть статистическую информацию о работе приложения.
- **Свойства** – произвести настройку приложения в открывшемся окне **Параметры приложения «Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server»**.

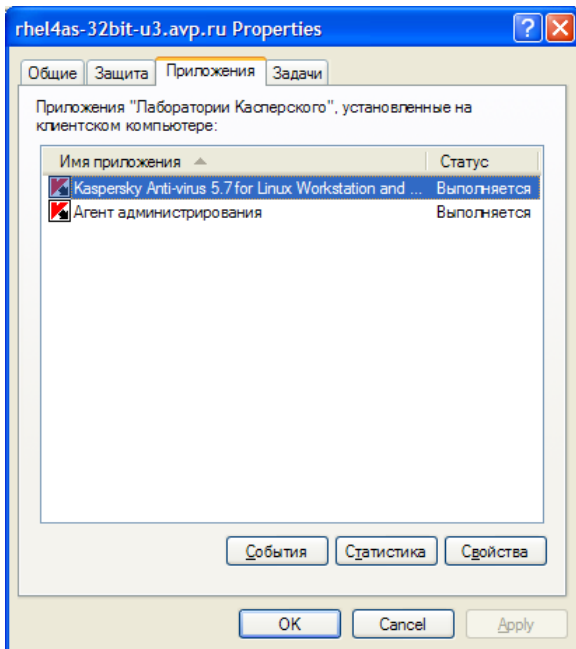


Рисунок 2. Список приложений «Лаборатории Касперского»

6.1.1. Настройка параметров приложения



Для того чтобы просмотреть или изменить параметры работы приложения:

1. Откройте окно свойств клиентского компьютера на закладке **Приложения** (см. рис. 1).
2. Выберите приложение **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**. Нажмите на кнопку **Свойства**, чтобы перейти в окно настройки параметров приложения.

Все закладки (кроме закладки **Параметры**) являются стандартными для приложения Kaspersky Administration Kit. Подробное описание стандартных закладок смотрите в одноименном Руководстве администратора.

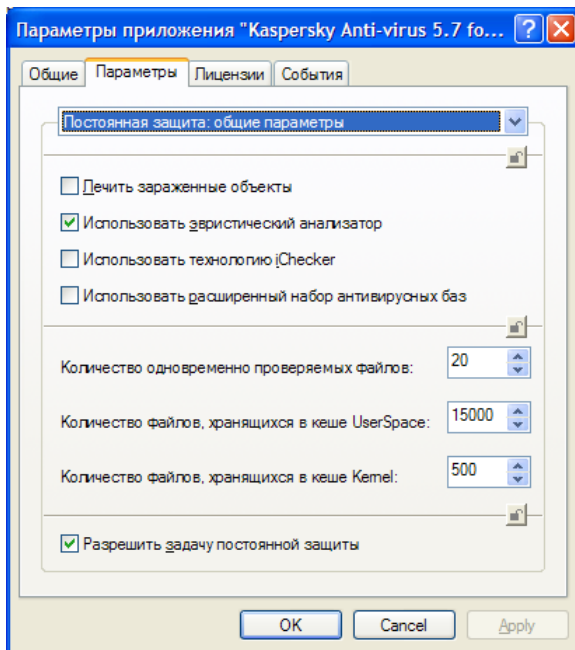


Рисунок 3. Настройка параметров Антивируса Касперского.
Закладка **Параметры**



Если для приложения создана политика (см. п. 6.3.1 на стр. 63), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров приложения будет недоступно.

На закладке **Параметры** можно настраивать общие параметры защиты и параметры области проверки.

6.1.1.1. Закладка Параметры, раздел Постоянная Защита: Общие параметры

В разделе **Общие параметры** вы можете:

- включать / отключать постоянную защиту компьютера;
- включать / отключать лечение зараженных объектов;

- включать / отключать эвристический анализатор и технологию iChecker;
- настраивать параметры производительности приложения (количество одновременно проверяемых файлов, количество файлов, хранящихся в Кеше Kernel и UserSpace).

6.1.1.2. Закладка Параметры, раздел Постоянная Защита: Область и объекты защиты

На закладке **Параметры** в разделе **Область и объекты защиты** вы можете:

- настраивать доверенную зону (список каталогов, исключенных из проверки);
- настраивать исключение файлов из проверки по маске (маски задаются в виде стандартных shell-масок);
- настраивать область защиты (список каталогов, включенных в проверку);
- выбирать типы проверяемых объектов.

6.2. Управление задачами

В данном разделе приведена информация о создании и настройке задач для Антивируса Касперского.

В рамках централизованного управления через Kaspersky Administration Kit вы можете создавать и использовать следующие задачи:

- задача проверки по требованию;
- задача обновления антивирусных баз.

6.2.1. Создание задачи



Для того чтобы просмотреть список задач, сформированных для клиентского компьютера:

1. В папке **Группы** (см. рис. 1) выберите папку с названием группы, в состав которой входит клиентский компьютер.
2. В панели результатов выберите компьютер, для которого вам необходимо просмотреть список локальных задач. Воспользуйтесь командой **Задачи** контекстного меню или аналогичным пунктом в меню **Действия**. В результате в главном окне приложения откроется окно просмотра свойств клиентского компьютера.

На закладке **Задачи** (см. рис. 4) представлен полный список задач, сформированных для данного клиентского компьютера.

При работе с приложением через Kaspersky Administration Kit вы можете создавать:

- локальные задачи – определяются для отдельного компьютера;
- групповые задачи – определяются для компьютеров, объединенных в одну логическую группу;
- глобальные задачи – определяются для произвольного набора компьютеров из произвольных групп логической сети.

Вы можете вносить изменения в настройки задач, наблюдать за их выполнением, копировать и переносить задачи из одной группы в другую, а также удалять при помощи стандартных команд контекстного меню **Копировать/Вставить**, **Вырезать/Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**.

Параметры работы приложения при выполнении задач на каждом компьютере устанавливаются в соответствии с политикой группы, настройками задач и настройками данного приложения на компьютере.

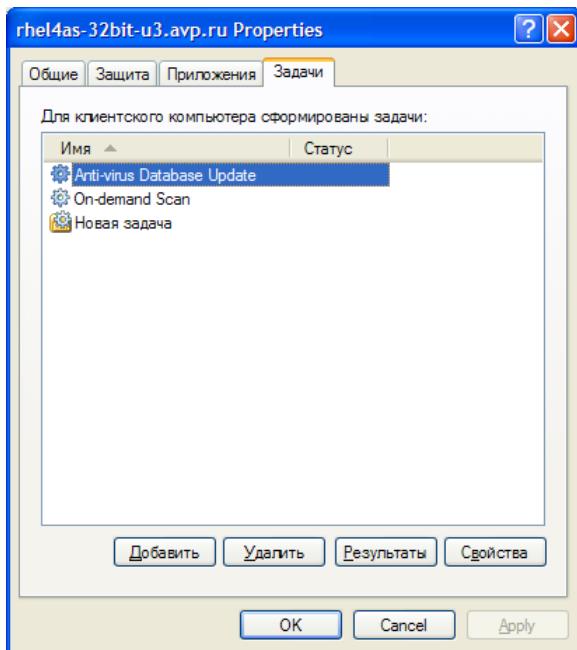


Рисунок 4. Список задач приложения

6.2.1.1. Создание локальной задачи



Для создания локальной задачи выполните следующие действия:

1. В папке **Группы** выберите папку с названием группы, в состав которой входит клиентский компьютер (см. рис. 4).
2. В панели результатов выберите компьютер, для которого вам необходимо создать локальную задачу, и воспользуйтесь командой **Свойства** контекстного меню или пунктом **Задачи** в меню **Действие**. В результате в главном окне приложения открывается окно просмотра свойств клиентского компьютера **Свойства: имя компьютера**.
3. На закладке **Задачи** (см. рис. 4) представлен перечень задач, сформированных для данного компьютера. Создание новой задачи осуществляется при помощи кнопки **Добавить**, настройка задачи при помощи кнопки **Свойства**. С помощью кнопки **Удалить** вы можете удалить выбранную задачу из списка.

При нажатии на кнопку **Добавить** запускается мастер создания задачи Microsoft Windows (Windows Wizard), состоящий из последовательности окон (шагов), перемещение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы – при помощи кнопки **Готово**. Для прекращения работы мастера на любом шаге служит кнопка **Отмена**.

Шаг 1. Ввод общих данных о задаче

Первое окно мастера является вводным: здесь необходимо указать имя задачи (поле **Имя**).

Шаг 2. Выбор приложения и типа задачи

Из списка **Имя приложения** выберите приложение **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Servers**. Тип задачи выбирается из списка **Тип задачи**. Для Антивируса Касперского вы можете создавать следующие задачи:

- Проверка по требованию.
- Обновление антивирусных баз.

Шаг 3. Настройка параметров выбранного типа задачи

В зависимости от типа задачи, выбранного на предыдущем шаге, содержание следующих окон варьируется.

НАСТРОЙКА ПАРАМЕТРОВ ЗАДАЧИ ПРОВЕРКИ ПО ТРЕБОВАНИЮ

Для задачи проверки по требованию необходимо задать:

- типы проверяемых объектов;
- область проверки в соответствующем поле в виде списка, разделенного двоеточиями;
- указать действия, которые будут производиться с зараженными в случае их обнаружения;
- задать дополнительные параметры работы: использование эвристического анализатора, технологии iChecker, расширенного набора антивирусных баз, возможность запуска задачи, как задачи полной проверки компьютера.

НАСТРОЙКА ПАРАМЕТРОВ ЗАДАЧИ ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

Для задачи обновления антивирусных баз необходимо задать:

- источник обновлений. В качестве источника обновлений может выступать либо сервер обновлений «Лаборатории Касперского», либо источник, указанный пользователем;
- использование пассивного режима FTP;
- тайм-аут соединения, в сек.

Включить / отключить использование прокси-сервера и настроить его параметры можно в окне, открывающемся по нажатию на гиперссылку **Настройка параметров прокси-сервера**.

Шаг 4. Настройка расписания

В окне **Расписание запуска задачи** вы можете настроить расписание, согласно которому данная задача будет функционировать.

В раскрывающемся списке **Запуск по расписанию** выберите нужный режим запуска задачи. В зависимости от выбранного варианта, центральная часть окна с полями для ввода данных будет изменять свой вид.

Подробнее о настройке расписания автоматического запуска задач смотрите Руководство администратора «Kaspersky Administration Kit».

Шаг 5. Завершение создания задачи

В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи.

6.2.1.2. Создание групповой задачи



Для создания групповой задачи выполните следующие действия:

1. В дереве консоли выберите группу, для которой вы будете создавать задачу.
2. Выберите входящую в ее состав папку **Задачи**, вызовите контекстное меню и выберите команду **Создать** → **Задачу**, или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, аналогичный мастеру создания локальной задачи (подробнее см. п. 6.2.1.1 на стр. 56). Следуйте его указаниям.

По окончании работы мастера задача будет добавлена в папку **Задачи** соответствующей группы, всех входящих в ее состав вложенных групп и представлена в панели результатов.

6.2.1.3. Создание глобальной задачи



Для создания глобальной задачи выполните следующие действия:

1. Выберите в дереве консоли узел **Глобальные задачи**, вызовите контекстное меню и выберите команду **Создать** → **Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В результате запускается мастер создания задачи, аналогичный мастеру создания локальной задачи (подробнее см. п. 6.2.1.1 на стр. 56). Исключением является наличие этапа определения списка клиентских компьютеров из состава логической сети, для которых формируется глобальная задача.
3. Выберите компьютеры из состава логической сети, на которых будет запускаться задача. Можно выбрать компьютеры из разных папок, можно выбрать сразу всю папку (подробнее см. Руководство администратора «Kaspersky Administration Kit»).



Глобальные задачи выполняются только для заданного набора компьютеров. Если в состав группы, для компьютеров которой сформирована задача удаленной установки, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести соответствующие изменения в настройки существующей.

По окончании работы мастера сформированная глобальная задача будет добавлена в состав узла **Глобальные задачи** дерева консоли и представлена в панели результатов.

6.2.2. Настройка специфических параметров задач



Для просмотра и изменения параметров задач клиентского компьютера:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи** (см. рис. 4).
2. Выберите задачу в списке и нажмите на кнопку **Свойства**. В результате будет открыто окно настройки параметров задачи (см. рис. 6).

Следующие закладки для всех задач являются аналогичными:

- **Общие** – просмотр общей информации о задаче, запуск ее на выполнение или остановка.
- **Расписание** – формирование расписания для выполнения задачи.
- **Уведомление** – настройка уведомления о результатах выполнения задачи (подробнее см. Руководство администратора «Kaspersky Administration Kit»).

Закладка **Параметры** содержит специфические параметры Антивируса Касперского; содержимое данной закладки варьируется в зависимости от выбранного типа задач.

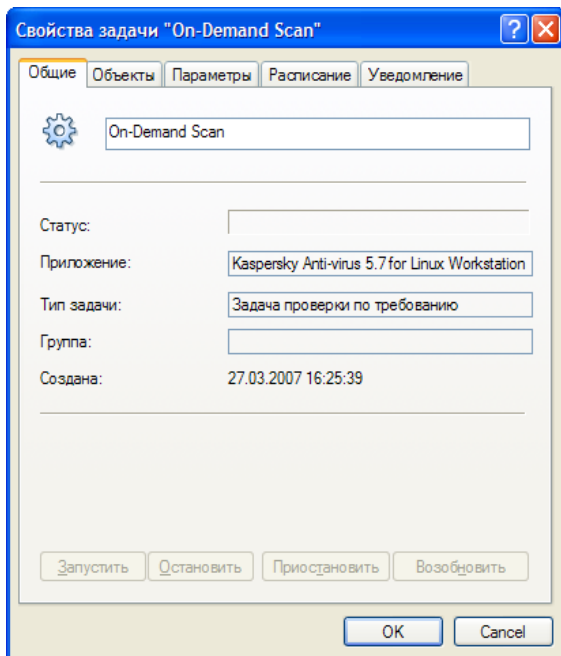


Рисунок 5. Настройка параметров задачи

6.2.2.1. Задача проверки по требованию

Для задачи проверки по требованию помимо параметров, заданных при создании задачи, можно произвести следующие настройки:

- указать типы проверяемых объектов;
- задать доверенную зону – объекты и маски имен файлов, исключенные из проверки (маски задаются в виде стандартных shell-масок),
- задать режим проверки файловых систем компьютера;
- задать режим рекурсивной проверки каталогов;
- указать, раскрывать ли символные ссылки на каталоги;
- задать режим полной проверки.

6.2.2.2. Задача обновления

Для задачи обновления антивирусных баз доступны следующие настройки:

- источник обновлений. В качестве источника обновлений может выступать либо сервер обновлений «Лаборатории Касперского», либо источник, указанный пользователем;
- региональные настройки. При выборе региона, в котором находится компьютер, процесс обновления в первую очередь будет производиться с серверов, принадлежащих выбранному региону;
- использование пассивного режима FTP;
- тайм-аут соединения, в сек.

Включить / отключить использование прокси-сервера и настроить его параметры можно в окне, открываемом по нажатию на гиперссылку **Настройка параметров прокси-сервера**.

6.2.3. Запуск и остановка задач

Запуск и остановка задач осуществляется автоматически, в соответствии с расписанием, а также вручную при помощи команд контекстного меню и из окна просмотра настроек задачи.



Для того чтобы запустить / остановить действие задачи вручную:

Выберите необходимую задачу в панели результатов, откройте контекстное меню и выберите команду **Запустить / Остановить** или воспользуйтесь аналогичными пунктами в меню **Действие**.

Аналогичные операции (для всех типов задач) вы можете инициировать из окна настройки задачи на закладке **Общие** (см. рис. 5) при помощи командной кнопки **Запустить, Остановить**.



Запуск задач на клиентском компьютере выполняется только в том случае, если запущено соответствующее приложение. При остановке приложения выполнение всех запущенных задач прекращается.

6.3. Управление политиками

Определение политик позволяет распространять единые настройки параметров приложения и задач на клиентские компьютеры, входящие в состав одной группы логической сети.

В данном разделе приведена информация о создании и настройке политики для Антивируса Касперского.

6.3.1. Создание политики




Чтобы создать политику для Антивируса Касперского, выполните следующие действия:

1. В папке **Группы** (см. рис. 1) выберите группу компьютеров, для которой нужно создать политику.
2. Выберите входящую в состав выбранной группы папку **Политики**, откройте контекстное меню и воспользуйтесь командой **Создать** → **Политику**. На экране появится окно создания новой политики.

Создание политики выполнено в виде мастера для Microsoft Windows (Windows Wizard) и состоит из последовательности окон (шагов), перемещение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы – при помощи кнопки **Готово**. Для прекращения работы мастера на любом шаге служит кнопка **Отмена**.



На каждом шаге создания политики (Шаг 3- Шаг 5), введенные параметры можно зафиксировать с помощью кнопки . Если замок на кнопке закрыт, то в дальнейшем при использовании политики на клиентских компьютерах будут использоваться значения, заданные создаваемой политикой.

Шаг 1. Ввод общих данных о политике

Первый шаг мастера - вводный. В первом окне мастера вам необходимо указать имя политики (поле **Имя**), во втором – выбрать приложение **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server** из раскрывающегося списка **Имя приложения**.

Шаг 2. Выбор статуса политики

В данном окне вам предлагается указать статус политики, для этого установите переключатель в нужное положение: активная политика, неактивная политика или политика для мобильных пользователей (вступает в силу после отключения компьютера от сети).



В группе для одного приложения может быть создано несколько политик, но действующей (активной) политикой может быть только одна из них.

Шаг 3. Настройка параметров политики

Настройки приложения разделены на две категории:

- общие параметры;
- область и объекты защиты.

В категорию **Общие параметры** входят следующие настройки:

- режим работы постоянной защиты;
- выбор действия над обнаруженными зараженными объектами (вы можете включить / отключить лечение зараженных объектов);
- использование эвристического анализатора и технологии iChecker.

В категорию **Область и объекты защиты** входят следующие настройки:


- доверенная зона (список каталогов, исключенных из проверки);
- исключение файлов по маске (маски задаются в виде стандартных shell-масок);
- выбор типа защищаемых объектов.

Списки каталогов и масок объектов разделяются двоеточиями.

Шаг 4. Завершение создания политики

Последнее окно мастера информирует об успешном завершении процесса создания политики.

По окончании работы мастера политика для Антивируса Касперского будет добавлена в папку **Политики** соответствующей группы и представлена в панели результатов.

Для созданной политики вы можете отредактировать ее настройки и установить ограничения на изменения ее параметров с помощью кнопки  для каждой группы настроек. Пользователь на клиентском компьютере не сможет изменить настройки, зафиксированные таким образом. Распространение политики на клиентские компьютеры будет осуществлено при первой синхронизации клиентов с сервером.

Вы можете копировать, переносить политики из одной группы в другую и удалять при помощи стандартных команд контекстного меню **Копировать / Вставить**, **Вырезать / Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**.

6.3.2. Просмотр и редактирование параметров политики

На этапе редактирования вы можете вносить изменения в политику, накладывая запрет на изменение параметров в политиках вложенных групп, в настройках приложения и настройках задач.

1. Выберите группу компьютеров в дереве консоли в папке **Группы**, для которой необходимо отредактировать настройки.
2. Выберите входящую в состав данной группы папку **Политики**, при этом в панели результатов будут отображены все политики, созданные для группы.
3. Выберите в списке политик нужную политику для **Антивируса Касперского 5.7 для Linux Workstation** (название приложения указано в поле **Приложение**).
4. Выберите в контекстном меню выбранной политики команду **Свойства**. Откроется окно настроек политики для приложения, содержащее несколько вкладок.

Закладки **Общие**, **Применение** и **События** являются стандартными для приложения Kaspersky Administration Kit (подробнее смотрите одноименное Руководство администратора).

Закладка **Параметры** (см. рис. 6) содержит разделы с настройками Антивируса Касперского. Описание каждого из разделов приведено ниже.

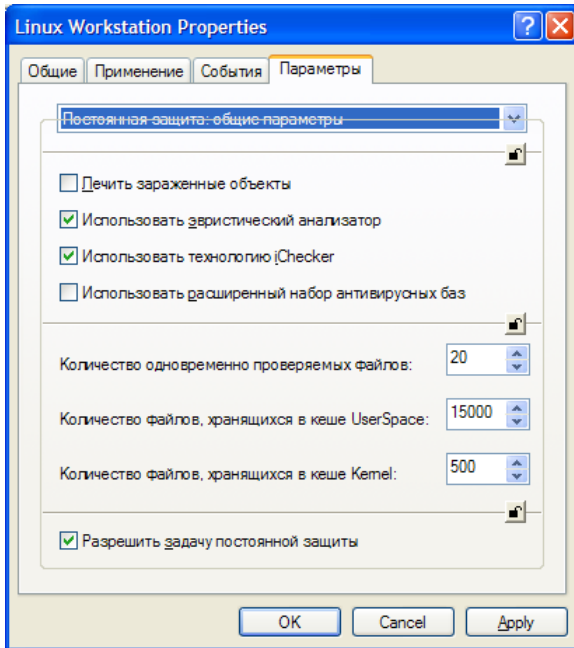



Рисунок 6. Настройка параметров политики



При редактировании параметров политики используйте кнопку  для того, чтобы зафиксировать введенные данные о политике. В дальнейшем, пользователь на клиентском компьютере не сможет редактировать настройки политики, которые были зафиксированы таким образом.

6.3.2.1. Настройка области защиты

На закладке **Параметры** в разделе **Постоянная защита: область и объекты защиты** вы можете:

- задать доверенную зону (список каталогов, исключенных из проверки);
- задать исключение файлов из проверки по маске (маски задаются в виде стандартных shell-масок);
- задать область проверки (список каталогов, подлежащих проверке).

Списки каталогов и масок объектов разделяются двоеточиями.

6.3.2.2. Определение типа проверяемых файлов

На закладке **Параметры** в разделе **Постоянная защита: область и объ-екты защиты** включить защиту:

- упакованных файлов;
- архивов;
- самораспаковывающихся архивов;
- почтовых баз;
- файлов почтовых форматов.

6.3.2.3. Настройка действий над объектами

На закладке **Параметры** в разделе **Постоянная защита: общие парамет-ры** вы можете:

- включить / отключить режим лечения зараженных объектов;
- включить / отключить постоянную защиту;
- включить / отключить использование эвристического анализатора;
- включить / отключить использование технологии iChecker;
- включить / отключить использование расширенного набора антивирусных баз.

6.3.2.4. Настройка дополнительных параметров

На закладке **Параметры** в разделе **Постоянная защита: общие парамет-ры** вы можете:

- задать число одновременно проверяемых файлов;
- задать число файлов, хранящихся в кеше UserSpace;
- задать число файлов, хранящихся в кеше Kernel.

ГЛАВА 7. УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Выполнение процедуры удаления Антивируса Касперского требует:

- Наличия прав привилегированного пользователя (**root**). Если на момент удаления приложения вы не обладаете такими правами, то вам необходимо войти в систему под пользователем **root**.
- Наличия файла отчета о процессе установки.
- Полного соответствия имен и размеров установленных файлов Антивируса Касперского приведенным в файле отчета об установке.
- Также перед началом процедуры удаления приложения необходимо остановить работу компонента **kavmonitor**. Для этого в командной строке введите:

```
# /etc/init.d/kav4ws stop
```

Затем необходимо деинсталлировать приложение и Агент Администрирования.



Если при инсталляции вы использовали rpm-пакеты Антивируса Касперского и Агента Администрирования, для запуска процедуры деинсталляции в командной строке введите:

```
# rpm -e <имя_пакета>
```




Если при инсталляции вы использовали deb-пакеты Антивируса Касперского и Агента Администрирования, для запуска процедуры деинсталляции в командной строке введите:

```
# dpkg -r <имя_пакета>
```

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

ГЛАВА 8. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ АНТИВИРУСА

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

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

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



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

Загрузить тестовый "вирус" можно с официального веб-сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

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

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

Таблица. Модификации тестового "вируса"

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

В первом столбце таблицы приведены префиксы, которые нужно добавить в начало строки стандартного тестового "вируса" (например:

```
CORR-X50!P#@P[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.

ПРИЛОЖЕНИЕ А.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ПРИЛОЖЕНИИ

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

А.1. Конфигурационный файл Антивируса Касперского

В поставку Антивируса Касперского включен конфигурационный файл **kav4ws.conf**, содержащий параметры функционирования приложения. В данном разделе мы подробно рассмотрим каждую секцию параметров файла. При описании параметров файла будут указаны значения по умолчанию, если таковые предусмотрены.

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

BasesPath – полный путь к антивирусным базам.

LicensePath – полный путь к каталогу расположения лицензионных ключей.

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

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

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



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

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



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

Секция **[network]** содержит настройки соединения сервиса *kavmiddleware*:



Значение данного параметра не следует менять в случае нормального функционирования приложения.

MiddlewareAddress=/var/run/kav4ws/kavmiddleware.socket – настройка соединения *kavmiddleware* с Агентом Администрирования и компонентом *kavmonitor*.

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

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

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

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

Packed=yes – режим проверки запакованных файлов. Для включения режима присвойте параметру значение **yes**.

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

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

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

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

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

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

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

FileCacheSize – размер файлового кеша (в записях).

KernelCacheSize – размер кеша, хранящегося антивирусным ядром (в записях).

CheckFileLimit=20 – максимальное количество одновременно проверяемых объектов.

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

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

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

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

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

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

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

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

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

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

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

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

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

Синтаксис параметра **действие** состоит из двух частей: непосредственно действия и его дополнительного параметра, разделяемых пробелом. Значение дополнительного параметра заключаются в кавычки. Например: `OnInfected=move "/tmp/infected"`

Действие может принимать одно из следующих значений:

- *move* <каталог> – переместить файл в <каталог>.
- *movePath* <каталог> – переместить файл в <каталог> рекурсивно (с абсолютным путем).
- *remove* – удалить файл.
- *exec* <параметр> – выполнить над объектом действие, определенное значением <параметр>.

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

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

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

ReportLevel=4 – уровень детализации отчета (см. п. 5.6 на стр. 46).

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента. Если параметру задано значение **syslog**, информация будет записана в системный журнал под категорией **daemon**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UseAVbasesSet=standard|extended – набор антивирусных баз, используемых приложением. Набор **extended** помимо записей, содержащихся в наборе **standard**, содержит также сигнатуры потен-

циально опасных программ, таких как: рекламные программы, программы удаленного администрирования и проч.

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

MaxLoadAvg – максимальная загрузка процессора. В случае превышения данного значения компонент *kavscanner* прекращает работу.

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

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

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента. Если параметру задано значение **syslog**, информация будет записана в системный журнал под категорией **daemon**.

ReportLevel=4 – уровень детализации отчета (см. п. 5.6 на стр. 46).

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

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

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

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

OnCorrupted=действие – действия в случае обнаружения поврежденного контейнера.

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

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

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

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

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

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

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

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

OnCorrupted=действие – действия в случае обнаружения поврежденного файла.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AVBasesTestPath – полный путь к каталогу хранения антивирусных баз.

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

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

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

ReportFileName – имя файла отчета, в котором фиксируются результаты работы компонента. Если параметру задано значение **syslog**, информация будет записана в системный журнал под категорией **daemon**.

ReportLevel=4 – уровень детализации отчета (см. п. 5.6 на стр. 46).

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

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

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

UseProxy – режим использования прокси-сервера при соединении с сервером обновлений «Лаборатории Касперского». Если значение

параметра **no**, прокси-сервер не используется. Если значение параметра **yes**, используется адрес прокси-сервера, определенный параметром **ProxyAddress**. Если значение параметра **ProxyAddress** не определено, будет использовано значение переменной окружения **http_proxy**. Если значение переменной окружения не определено, прокси-сервер не используется.

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

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

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

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

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

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

PassiveFtp=no режим использования для соединения passive FTP.

Секция **[middleware.options]** содержит настройки сервиса *kavmiddleware*:



Значения данных параметров не следует изменять в случае нормального функционирования приложения.

ScannerExe=/opt/kaspersky/kav4ws/bin/kav4ws-kavscanner – путь к исполняемому файлу компонента *kavscanner*.

Keepup2dateExe=/opt/kaspersky/kav4ws/bin/kav4ws-keepup2date – путь к исполняемому файлу компонента *keepup2date*.

LicensemanagerExe=/opt/kaspersky/kav4ws/bin/kav4ws-licensemanager – путь к исполняемому файлу компонента *licensemanager*.

MonitorInitdScript=/etc/init.d/kav4ws – путь к скрипту управления сервисом *kavmonitor*.

DirToStoreFiles=/var/opt/kaspersky/kav4ws/middleware – путь файлам сервиса *kavmiddleware*.

ReportLevel=0 – уровень детализации отчета (см. п. 5.6 на стр. 46).

ReportsDir=/var/log/kaspersky/kav4ws – путь к файлам отчета компонент.

A.2. Ключи командной строки компонента kavscanner

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

Опции помощи:

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

Опции конфигурации:

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

Опции проверки:

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

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

Опции формирования отчета:

-q	Не выводить на консоль сообщения;
-o <имя>	Задать имя файла, в который будет выводиться отчет о работе компонента; если имя файла не задано, то отчет формироваться не будет. Помимо файла, информация о работе компонента будет выведена на консоль. Для вывода информации в системный журнал задайте <code>syslog</code> в качестве значения параметра <имя> .
-j<число>	Задать уровень детализации отчета по объему содержащейся в нем информации. В качестве <опции> можно использовать следующие уровни детализации:
1	Выводить/не выводить сообщения о прочих ошибках;
2	Выводить/не выводить информационные сообщения;
3	Выводить/не выводить сообщения о проверке.

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

Опции файлов:

- p<опция>**
<имя_файла> Сохранить список объектов в заданный файл; сохранять каждый объект с полным путем с новой строки. В качестве **<опции>** могут быть:
- i** Сохранить в файл **<имя_файла>** список инфицированных объектов;
- s** Сохранить в файл **<имя_файла>** список подозрительных объектов;
- c** Сохранить в файл **<имя_файла>** список поврежденных объектов;
- w** Сохранить в файл **<имя_файла>** список объектов, код которых похож на код известных вирусов.

-@ <filelist.lst> Проверить объекты, путь к которым приведен в файле **<filelist.lst>**.

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

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

А.3. Коды возврата компонента kavscanner

В процессе работы компонент kavscanner может возвращать следующие коды:

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

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

A.4. Ключи командной строки компонента kavmonitor

Опции помощи:

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

Опции конфигурации:

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

А.5. Ключи командной строки компонента `licensmanager`

Опции помощи:

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

Опции работы с лицензионными ключами:

- s** Вывести на консоль информацию обо всех установленных лицензионных ключах;
- c** (**-C**) Использовать альтернативный конфигурационный файл `<путь_к_файлу>` `<путь_к_файлу_ключа>`;
- k <путь_к_файлу>** Отобразить на консоли информацию о ключе `<путь_к_файлу_ключа>`;
- a <путь_к_файлу>** Установить лицензионный ключ `<путь_к_файлу_ключа>`;
- d(a|r)** Удалить активный (опция **-da**) или дополнительный (опция **-dr**) лицензионный ключ.

А.6. Коды возврата компонента `licensmanager`

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

- 0** Компонент успешно загрузил информацию лицензионном ключе и завершил свою работу;
- 30** При работе компонента возникла системная ошибка;

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

A.7. Ключи командной строки компонента `keepup2date`

Опции помощи:

- v** Вывести на консоль версию приложения и завершить работу компонента;
- h** Вывести на консоль справочную информацию о ключах командной строки, поддерживаемых компонентом и завершить работу компонента;

Опции работы:

- r** Откат последнего обновления на предыдущую версию;
- s** Вывести на консоль список серверов обновлений;
- k** Не выполнять команду **PostUpdateCmd** после успешного завершения обновления антивирусных баз;
- q** Режим работы компонента, при котором на консоль не выводится никаких системных сообщений.
- e** Режим работы компонента, при котором на консоль выводятся только сообщения о критических системных ошибках.

- b <путь>** При обновлении создавать копию имеющихся анти-вирусных баз в каталоге <путь>.
- x <путь_к_файлу>** Копировать все обновления антивирусных баз в локальный каталог <путь_к_файлу>.
- t <путь>** Использовать каталог <путь> для хранения временных файлов.
- u <путь_к_файлу>** Копировать последнее обновление антивирусных баз в локальный каталог <путь_к_файлу>;
- c <путь_к_файлу>** Использовать альтернативный конфигурационный файл <путь_к_файлу>;
- g <URL>** Адрес для обновления антивирусных баз. При определении этого ключа обновление будет производиться с указанного адреса.
- d <путь_к_файлу>** Использование rid-файла компонента, расположенного в локальном каталоге <путь_к_файлу>.

Опции формирования отчета:

- l <путь_к_файлу>** Фиксировать результаты работы компонента в файле <путь_к_файлу>.

А.8. Коды возврата компонента keepup2date

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

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

А.9. Ключи командной строки компонента **kavmiddleware**

Опции помощи:

- v** Вывести на консоль версию приложения и завершить работу компонента;
- h** Вывести на консоль справочную информацию о ключах командной строки, поддерживаемых компонентом и завершить работу компонента;

ПРИЛОЖЕНИЕ В. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

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



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

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



Вопрос: Антивирус Касперского не проверяет файл повторно. Почему?

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

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



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

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

В отличие от других антивирусов, сокращающих время проверки путем исключения из антивирусных баз более сложных в обнаружении или более редких (например, в географическом отношении) вирусов, а также более сложных в анализе форматов файлов (например, pdf), «Лаборатория Касперского» считает, что задача Антивируса – обеспечивать реальную антивирусную безопасность пользователей.

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

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



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

Без лицензионного ключа Антивирус Касперского не работает.

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



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

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

При возникновении данной ситуации проинформируйте вашего системного администратора или обратитесь за продлением лицензии в компанию, где был приобретен Антивирус Касперского или непосредственно в ЗАО «Лаборатория Касперского».



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

Существует несколько вариантов решения этой проблемы.

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

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

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



Вопрос: мой Антивирус не работает. Что мне делать?

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

Также мы рекомендуем обратиться к фирме, где вы приобрели Антивирус Касперского или обратиться к разделу База Знаний на сайте «Лаборатории Касперского»: <http://support.kaspersky.ru>.



Вопрос: Зачем нужны ежедневные обновления?

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

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

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



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

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

Преимущества нового сервиса обновления:

- Дозагрузка файлов при разрыве соединения. *Теперь не нужно повторно скачивать уже полученные обновления после восстановления соединения.*
- Двукратное уменьшение размера кумулятивного обновления. Кумулятивное обновление содержит в себе всю антивирусную базу, поэтому размер кумулятива значительно превышает размер обычного обновления. В новом сервисе применена специальная технология, позволяющая использовать уже имеющиеся антивирусные базы для кумулятивного обновления.
- Ускорение загрузки из интернета. Антивирус Касперского выбирает сервер обновления «Лаборатории Касперского», расположенный в вашем регионе. Кроме того, нагрузка на сервера распределяется в соответствии с их производительностью, то есть вы не попадете на перегруженный сервер, в то время как другой сервер будет простаивать.
- Применение "черных списков" ключей. Это позволяют исключить обновление для пользователей, не имеющих лицензии на использование Антивируса Касперского. В результате лицензированные пользователи не страдают от перегруженности серверов обновлений.
- Для корпоративных продуктов реализована возможность создания локального сервера обновлений. Такая функция

востребована для организаций, где в одной локальной сети объединены компьютеры, защищенные приложениями «Лаборатории Касперского». В этом случае любой компьютер может быть превращен в сервер обновлений, который будет получать обновления из интернета, помещать их в локальный каталог и предоставлять к ним доступ другим компьютерам сети.



Вопрос: может ли злоумышленник подменить антивирусные базы?

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



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

Тестирование Антивируса Касперского версии 5.7 производилось на дистрибутивах RedHat, Debian, SUSE и Mandriva, и именно для них собирались дистрибутивы Антивируса Касперского.

О версиях поддерживаемых операционных систем см. п. 1.5 на стр. 9.

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



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

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



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

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



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

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

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

где:

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

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

Например:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-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*.



Вопрос: как просмотреть результаты работы приложения после запуска задачи с помощью Kaspersky Administration Kit?

По умолчанию запись результатов работы приложения при запуске задач из Administration Kit не ведется.

Для сохранения результатов работы задач в файл внесите следующие изменения в конфигурационный файл приложения:

- задайте уровень детализации отчета (см. п. 5.6 на стр. 46) с помощью параметра **ReportLevel** в секции **[middleware.options]**.
- задайте каталог хранения файла отчета.

По окончании выполнения задачи в указанном каталоге будет создан один из следующих файлов:

- *kavscanner_middleware.log* – после выполнения задачи проверки по требованию;
- *keepup2date_middleware.log* – после выполнения задачи обновления антивирусных баз.

ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

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

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

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

С.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

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

Новостной Агент также позволяет:

- визуализировать в системной панели состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

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

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

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

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется непосредственно в браузере. В рамках проверки пользователь может:

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

Антивирус Касперского® 6.0

Антивирус Касперского 6.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP – для исходящих) независимо от используемой почтовой программы, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно запустить анализ на присутствие вирусов только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе.* Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.
- *Наблюдение за процессами в оперативной памяти.* **Антивирус Касперского 6.0** своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.
- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.
- *Блокирование опасных макросов Visual Basic for Applications* в документах Microsoft Office.
- *Восстановление системы* после вредоносного воздействия программ-шпионов **за счет** фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 6.0

Kaspersky Internet Security 6.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;
- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы:* антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;
- *проактивную защиту:* программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

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

Kaspersky Internet Security 6.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На *основе заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим невидимости *предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Symbian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- *проверку по требованию* памяти мобильного устройства, карт памяти, отдельной папки либо конкретного файла. При обнаружении зараженного объекта он помещается на карантин или удаляется;
- *постоянную защиту*: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;
- *защиту от sms- и mms-спама*.

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare, Linux и Samba от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux Workstation.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени:* все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- *предотвращение вирусных эпидемий;*
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- *восстановление системы после заражения;*
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *соблюдение баланса загрузки системы;*
- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуются их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;

- *ведение детальных отчетов;*
- *автоматическое обновление баз программного продукта.*

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Программный продукт включает в себя четыре продукта:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это продукт для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама;*
- *проактивная защита от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *отмена вредоносных изменений в системе;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *проверка электронной почты и интернет-трафика в режиме реального времени;*

- *блокирование всплывающих окон и рекламных баннеров* при работе в интернете;
- *безопасная работа в сетях любого типа*, включая Wi-Fi;
- *средства для создания диска аварийного восстановления*, позволяющего восстановить систему после вирусной атаки;
- *развитая система отчетов* о состоянии защиты;
- *автоматическое обновление баз*;
- *полноценная поддержка 64-битных операционных систем*;
- *оптимизация работы программного продукта на ноутбуках* (технология Intel® Centrino® Duo для мобильных ПК);
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™).

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз*;
- *использование технологии iSwift* для исключения повторных проверок в рамках сети;
- *распределение нагрузки между процессорами сервера*;
- *изоляция подозрительных объектов* рабочих станций в специальном хранилище;
- *отмена вредоносных изменений в системе*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;

- *проверка электронной почты и интернет-трафика в режиме реального времени;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *защита при работе в беспроводных сетях Wi-Fi;*
- *технология самозащиты антивируса от вредоносных программ;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *автоматическое обновление баз.*

Kaspersky Enterprise Space Security

Программный продукт включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *защита рабочих станций и серверов от вирусов, троянских программ и червей;*
- *защита почтовых серверов Sendmail, Qmail, Postfix и Exim;*
- *проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *обработка сообщений, баз данных и других объектов серверов Lotus Domino;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *предотвращение массовых рассылок и вирусных эпидемий;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*

- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *безопасная работа в беспроводных сетях Wi-Fi*;
- *проверка интернет-трафика* в режиме реального времени;
- *отмена вредоносных изменений в системе*;
- *динамическое перераспределение ресурсов* при полной проверке системы;
- *изоляция подозрительных объектов* в специальном хранилище;
- *система отчетов* о состоянии системы защиты;
- *автоматическое обновление баз*.

Kaspersky Total Space Security

Решение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама* на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *защита почтовых серверов и серверов совместной работы*;
- *проверка интернет-трафика (HTTP/FTP)*, поступающего в локальную сеть, в режиме реального времени;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *блокирование доступа с зараженных рабочих станций*;

- *предотвращение вирусных эпидемий;*
- *централизованные отчеты о состоянии защиты;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *поддержка аппаратных прокси-серверов;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *использование технологии iSwift для исключения повторных проверок в рамках сети;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа пользователей в сетях любого типа, включая WiFi;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™);*
- *отмена вредоносных изменений в системе;*
- *технология самозащиты антивируса от вредоносных программ;*
- *полноценная поддержка 64-битных операционных систем;*
- *автоматическое обновление баз.*

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.

- Антивирус Касперского для Lotus Notes/Domino.
- Антивирус Касперского для Microsoft Exchange.
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *фильтрация нежелательной почтовой корреспонденции;*
- *проверка входящих и исходящих почтовых сообщений и вложений;*
- *антивирусная проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino;*
- *фильтрация сообщений по типам вложений;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления программным продуктом;*
- *предотвращение вирусных эпидемий;*
- *мониторинг состояния системы защиты с помощью уведомлений;*
- *система отчетов о работе приложения;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- [Kaspersky Administration Kit.](#)
- [Антивирус Касперского для Proxy Server.](#)
- [Антивирус Касперского для Microsoft ISA Server.](#)
- [Антивирус Касперского для Check Point FireWall-1.](#)

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *проверка интернет-трафика (HTTP/FTP) в режиме реального времени;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления;*
- *система отчетов о работе приложения;*
- *поддержка аппаратных прокси-серверов;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky® Anti-Spam

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

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

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

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

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

С.2. Наши координаты

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

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700, +7 (495) 645-79-39
Экстренная круглосуточная помощь:	+7 (495) 797-8707, +7 (495) 645-79-29
Поддержка пользователей персональных продуктов и Business Optimal:	+7 (495) 797-8707, +7 (495) 645-79-29 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка пользователей Corporate Suite:	Телефоны и электронный адрес предоставляются при покупке Corporate Suite в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)

Департамент продаж:	+7 (495) 797-8700, +7 (495) 645-79-39 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700, +7 (495) 645-79-39 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru