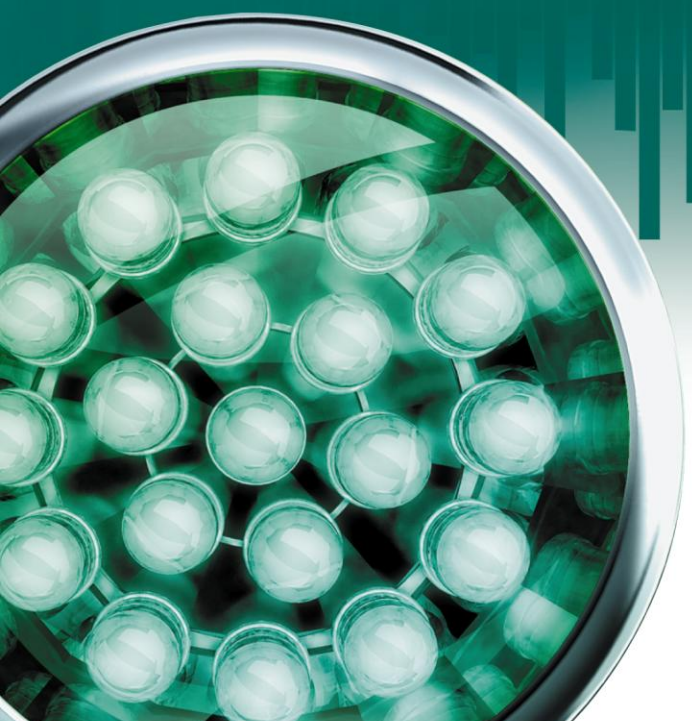
Антивирус Касперского 8.0 для Linux File Server

РУКОВОДСТВО ПО УСТАНОВКЕ

ВЕРСИЯ ПРОГРАММЫ: 8.0



KASPERSKY lab

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 18.11.2010

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Это руководство описывает установку программы Антивирус Касперского 8.0 для Linux File Server (далее – *Антивирус Касперского* или *программа*).

Все примеры команд, приведенные далее в этом документе, указаны для Linux-систем.

В ЭТОМ РАЗДЕЛЕ

НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа Антивирус Касперского 8.0 для Linux File Server предназначена для антивирусной защиты файловых серверов, работающих под управлением операционных систем Linux и FreeBSD.

Антивирус Касперского позволяет:

- осуществлять постоянную защиту файловой системы сервера от вредоносного кода – перехватывать обращения к файлам; анализировать их; лечить или удалять зараженные объекты;
- проверять объекты на сервере по требованию – искать зараженные и подозрительные файлы в заданных областях проверки; анализировать их; лечить или удалять зараженные объекты;
- помещать зараженные и подозрительные объекты на карантин;
- создавать копии зараженных объектов в резервном хранилище перед лечением и удалением в целях возможного восстановления объектов, которые представляют информационную ценность;
- обновлять базы (ресурсом для обновления баз служат серверы обновлений или Сервер администрирования «Лаборатории Касперского»; существует также возможность настроить Антивирус Касперского на обновление баз из локальной директории);
- управлять программой и настраивать параметры ее работы с помощью утилиты управления, Kaspersky Administration Kit и Web Management Console.

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ

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

- Минимальные аппаратные требования:
  - процессор Intel Pentium® II 400 МГц или выше;

- 512 МБ оперативной памяти;
- раздел подкачки объемом не менее 1 ГБ;
- 2 ГБ на жестком диске для установки Антивируса Касперского и хранения временных файлов и файлов журналов.

- Программные требования:
  - для 32-битной платформы – одна из следующих операционных систем:
    - Red Hat Enterprise Linux 5.5 Server;
    - Red Hat Enterprise Linux 6 Server;
    - Fedora 13;
    - CentOS-5.5;
    - SUSE Linux Enterprise Server 10 SP3;
    - SUSE Linux Enterprise Server 11 SP1;
    - Novell Open Enterprise Server 2 SP2;
    - openSUSE Linux 11.3;
    - Mandriva Enterprise Server 5.1;
    - Ubuntu 10.04 LTS Server Edition;
    - Debian GNU/Linux 5.0.5;
    - FreeBSD 7.3, 8.1.
  - для 64-битной платформы одна из следующих операционных систем:
    - Red Hat Enterprise Linux 5.5 Server;
    - Red Hat Enterprise Linux 6 Server;
    - Fedora 13;
    - CentOS-5.5;
    - SUSE Linux Enterprise Server 10 SP3;
    - SUSE Linux Enterprise Server 11 SP1;
    - Novell Open Enterprise Server 2 SP2;
    - openSUSE Linux 11.3;
    - Ubuntu 10.04 LTS Server Edition;
    - Debian GNU/Linux 5.0.5;
    - FreeBSD 7.3, 8.1.
  - один из следующих веб-браузеров (для управления с помощью Web Management Console):

  - Microsoft Internet Explorer 7;
  - Microsoft Internet Explorer 8;
  - Mozilla FireFox 3.x.
- Интерпретатор языка Perl версии 5.0 или выше http://www.perl.org
- Установленные пакеты для компиляции программ (gcc, binutils, glibc (для 64-битных операционных систем используется 32-битная версия glibc), glibc-devel, make, ld), а также установленный исходный код ядра операционной системы – для компиляции модулей Антивируса Касперского.

Получение информации об Антивирусе Касперского

«Лаборатория Касперского» предоставляет различные источники информации об Антивирусе Касперского. Выберите наиболее удобный для себя в зависимости от важности и срочности вопроса.

Если вы уже приобрели Антивирус Касперского, обратитесь в Службу технической поддержки. Если вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме по адресу http://forum.kaspersky.com.

Источники информации для самостоятельного поиска

В вашем распоряжении находятся следующие источники информации об Антивирусе Касперского:

- страница Антивируса Касперского на веб-сайте «Лаборатории Касперского»;
- документация;
- manual pages.

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/anti-virus-linux-file-server

На этой странице вы получите общую информацию о приложении, его возможностях и особенностях. Приобрести Антивирус Касперского или продлить срок его использования можно в нашем электронном магазине.

Документация

Руководство по установке описывает назначение Антивируса Касперского, требования к аппаратному и программному обеспечению для установки и работы Антивируса Касперского, инструкции по его установке, проверке его работоспособности и первоначальной настройке.

Руководство администратора содержит информацию о том, как управлять Антивирусом Касперского с помощью утилиты командной строки, Kaspersky Web Management Console и Kaspersky Administration Kit.

Эти документы в формате PDF входят в комплект поставки Антивируса Касперского. Также вы можете загрузить документы со страницы Антивируса Касперского на сайте «Лаборатории Касперского».

Manual pages

Вы можете просматривать следующие файлы manual pages для получения информации об Антивирусе Касперского:

- управление Антивирусом Касперского с помощью командной строки:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-control.1.gz*;
  - для FreeBSD – */usr/local/man/man1/kav4fs-control.1.gz;*
- настройка общих параметров Антивируса Касперского:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs.conf.5.gz;*
- настройка задачи постоянной защиты:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-oas.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-oas.conf.5.gz;*
- настройка задач проверки по требованию:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-ods.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-ods.conf.5.gz;*
- настройка задач обновления:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-update.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-update.conf.5.gz;*
- настройка параметров хранилища объектов на карантине и объектов, зарезервированных перед лечением или удалением:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-quarantine.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-quarantine.conf.5.gz;*
- настройка уведомлений:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-notifier.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-notifier.conf.5.gz;*
- настройка параметров SNMP-агента:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-snmp.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-snmp.conf.5.gz;*
- настройка параметров хранилища событий:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-events.conf.5.gz*;
  - для FreeBSD – */usr/local/man/man5/kav4fs-events.conf.5.gz;*
- описание утилиты, изменяющей пароль пользователя Web Management Console:
  - для Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-wmconsole-passwd.1.gz*;
  - для FreeBSD – */usr/local/man/man1/kav4fs-wmconsole-passwd.1.gz;*

- описание утилиты, изменяющей параметры соединения с Сервером администрирования Kaspersky Administration Kit:
  - для Linux – */opt/kaspersky/klnagent/share/man/man1/klmover.1.gz*;
- описание утилиты, проверяющей параметры соединения с Сервером администрирования Kaspersky Administration Kit:
  - для Linux – */opt/kaspersky/klnagent/share/man/man1/klnagchk.1.gz.*

Обращение в Службу технической поддержки

Если вы уже приобрели Антивирус Касперского, информацию о нем можно получить у специалистов Службы технической поддержки по телефону или через интернет.

Прежде чем обратиться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами ее оказания (http://support.kaspersky.ru/support/rules).

Электронный запрос в Службу технической поддержки

Вы можете задать вопрос специалистам Службы технической поддержки, заполнив веб-форму системы обработки клиентских запросов (http://support.kaspersky.ru/helpdesk.html).

Запрос можно отправить на русском, английском, немецком, французском или испанском языках.

Чтобы отправить электронный запрос, вам нужно указать в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

Если вы еще не являетесь зарегистрированным пользователем приложений «Лаборатории Касперского», вы можете заполнить регистрационную форму (https://support.kaspersky.com/ru/personalcabinet/registration/form/). При регистрации укажите имя файла ключа.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (https://support.kaspersky.com/ru/PersonalCabinet) и по электронному адресу, который вы указали в запросе.

В веб-форме запроса как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Выберите тему, наиболее точно соответствующую характеру возникшей проблемы, например, «Проблема установки / удаления продукта» или «Проблема поиска / удаления вирусов».
- **Название и номер версии Антивируса Касперского**.
- **Текст запроса**. Подробно опишите возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы всегда можете позвонить в Службу технической поддержки в вашем городе. Обращаясь к сотрудникам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, не забудьте предоставить им информацию об Антивирусе Касперского (http://support.kaspersky.ru/support/details), чтобы наши специалисты могли помочь вам как можно быстрее.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

Если ваш вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме по адресу http://forum.kaspersky.com.

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Что нового в версии 8.0

Рассмотрим подробнее нововведения Антивируса Касперского 8.0 для Linux File Server.

Новое в защите:

- Антивирус Касперского 8.0 объединяет возможности предыдущих версий программы, Антивируса Касперского 5.7 для Linux File Server и Антивируса Касперского 5.5 для Samba Servers, за счет использования перехватчиков файловых операций двух типов: перехватчика уровня ядра (kernel module) и перехватчика Samba;
- Расширены возможности карантина / резервного хранилища:
  - объекты хранятся в зашифрованном виде;
  - новые возможности администрирования позволяют:
    - добавлять объекты на карантин вручную;
    - искать объекты на карантине (по значениям атрибутов объектов);
    - удалять найденные объекты;
    - восстанавливать найденные объекты;
    - повторно проверять объекты;
    - сохранять часть карантина / резервного хранилища в архив (для уменьшения занимаемого объема);
    - импортировать объекты в карантин/резервное хранилище из архива;
  - появилась возможность управлять карантином / резервным хранилищем посредством Web Management Console.

Новое в управлении работой Антивируса Касперского:

- Централизованное управление жизненным циклом Антивируса Касперского и выполнением задач проверки по требованию, постоянной защиты и обновления баз Антивируса Касперского.
- Централизованное хранение параметров работы Антивируса Касперского.
- Параметры работы Антивируса Касперского больше не хранятся в текстовых конфигурационных файлах. Текстовые файлы используются только во время сохранения и получения настроек из центрального хранилища параметров.
- Существует возможность указания нескольких областей проверки для одной задачи. При этом:

- параметры проверки можно задавать для каждой области отдельно;
- область проверки может быть задана:
  - полным путем в файловой системе;
  - именем устройства;
  - типом сетевого доступа (Shared, Mounted);
  - протоколом сетевого доступа (SMB / CIFS, NFS);
  - именем сетевого ресурса (Samba share name, NFS shared folder);
- в описании области проверки поддерживаются регулярные выражения стандарта POSIX Extended;

- Для области проверки можно задавать список пользователей / групп, файловые операции от имени которых проверяются задачей постоянной защиты.
- Предусмотрена возможность задавать несколько правил исключения для одной области проверки.
- Возможно удаленное управление с помощью Kaspersky Administration Kit.
- Можно задавать действия над объектами в зависимости от типа обнаруженной угрозы.
- Существует возможность подробно настраивать расписания запуска / остановки задач.

Новое в средствах мониторинга, отчетов и статистики работы Антивируса Касперского:

- Расширены следующие возможности мониторинга работы Антивируса Касперского:
  - средства получения следующих категорий информации:
    - общая информация о приложении;
    - информация о версии баз Антивируса Касперского;
    - информация о состоянии лицензии;
    - информация о статусе компонентов Антивируса Касперского;
    - информация о результатах работы задач;
    - информация о состоянии карантина/резервного хранилища;
  - средства уведомления администраторов защищаемого сервера о событиях, связанных с работой Антивируса Касперского, например:
    - устаревание баз Антивируса Касперского;
    - окончание срока действия лицензии;
    - нарушение условий лицензионного соглашения;
    - возникновение критических ошибок в работе Антивируса Касперского;
  - средства ретроспективного анализа работы Антивируса Касперского, позволяющие осуществлять:
    - сбор, подсчет и хранение статистической информации о работе Антивируса Касперского;

  - отображение статистической информации о работе Антивируса Касперского, собранной за указанный пользователем промежуток времени;
  - поиск событий на основе критериев, заданных пользователем;
  - аудит следующих аспектов работы Антивируса Касперского: создания / запуска / остановки задач, изменения параметров работы программы, действий пользователя над объектами в карантине / резервном хранилище и т. д.;
- средства создания отчетов о работе Антивируса Касперского на основе собранной статистики, средства экспорта отчетов (поддерживаются форматы HTML, PDF и XLS);
- мониторинг работы Антивируса Касперского и вирусной активности. Информация находится в централизованном хранилище событий Антивируса Касперского. Антивирус Касперского предоставляет собственные средства для поиска, отображения и анализа данных о своей работе, а также возможность использования внешних средств.

СОСТАВ ДИСТРИБУТИВА

Состав дистрибутива Антивируса Касперского приведен в таблице ниже.

Таблица 1. Пакеты Антивируса Касперского

Пакет	Назначение
kav4fs-<номер_версии>.i386.rpm **kav4fs_<номер_версии>_i386.deb** **kav4fs-<номер_версии>.tgz**	Содержит основные файлы Антивируса Касперского. Пакет может быть установлен как на 32-, так и на 64-битные операционные системы.
klnagent-<номер_версии>.i386.rpm **klnagent_<номер_версии>_i386.deb**	Содержит Агент Администрирования (утилиту связи Антивируса Касперского с Kaspersky Administration Kit).
kav4fs-rpm.tar.gz **kav4fs-deb.tar.gz**	Содержит файлы kav4fs.kpd и akinstall.sh, используемые в процедуре удаленной установки Антивируса Касперского с помощью Kaspersky Administration Kit.
klnagent-rpm.tar.gz **klnagent-deb.tar.gz**	Содержит файлы klnagent.kpd и akinstall.sh, используемые в процедуре удаленной установки Агента Администрирования с помощью Kaspersky Administration Kit.

В основной пакет Антивируса Касперского входит компонент Web Management Console.

УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

Антивирус Касперского распространяется в пакетах форматов *.tgz*, *.deb* и *.rpm*.

Процесс установки включает несколько этапов:

1. Установка пакета Антивируса Касперского.
2. Установка пакета Агента администрирования (установка этого пакета необходима для управления Антивирусом Касперского с помощью Kaspersky Administration Kit).

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Установка пакета Антивируса Касперского

Перед установкой Антивируса Касперского 8.0 для Linux File Server удалите Антивирус Касперского 5.5 для Samba Servers или Антивирус Касперского 5.7 для Linux File Server, установленные на сервере.

Запускать процесс установки пакета Антивируса Касперского необходимо с правами учетной записи **root**.

До установки Антивируса Касперского необходимо установить пакет glibc (для 64-битных операционных систем требуется 32-битная версия glibc).

- *Чтобы установить Антивирус Касперского из .rpm-пакета, выполните следующую команду:*

  ```
  # rpm -i kav4fs-<номер_версии>.i386.rpm
  ```

- *Чтобы установить Антивирус Касперского из .deb-пакета, выполните следующую команду:*

  ```
  # dpkg -i kav4fs_<номер_версии>_i386.deb
  ```

- *Чтобы установить Антивирус Касперского из .deb-пакета на 64-битную операционную систему, выполните следующую команду:*

  ```
  # dpkg -i --force-architecture kav4fs_<номер_версии>_i386.deb
  ```

- *Чтобы установить Антивирус Касперского на сервер, работающий под управлением операционной системы FreeBSD, выполните следующую команду:*

  ```
  # pkg_add kav4fs-<номер_версии>.tgz
  ```

- *Чтобы включить автоматический запуск служб Антивируса Касперского и Web Management Console после установки на сервер, работающий под управлением операционной системы FreeBSD, добавьте в конфигурационный файл* /etc/rc.conf *следующие строки:*

  ```
  kav4fs_supervisor_enable="YES"
  kav4fs_wmconsole_enable="YES"
  ```

После запуска команды дальнейший процесс установки будет выполнен автоматически.

По завершении установки Антивируса Касперского из rpm-пакета необходимо запустить (см. стр. 24) скрипт постинсталляционной настройки Антивируса Касперского.

Шаг 2. Установка Агента администрирования

Установка Агента администрирования требуется, если вы планируете управлять Антивирусом Касперского с помощью Kaspersky Administration Kit.

Запускать процесс установки Агента администрирования необходимо с правами учетной записи **root**.

- *Чтобы установить Агент администрирования из .rpm-пакета, выполните следующую команду:*

  ```
  # rpm -i klnagent-<номер_версии>.i386.rpm
  ```

- *Чтобы установить Агент администрирования из .deb-пакета, выполните следующую команду:*

  ```
  # dpkg -i klnagent_<номер_версии>_i386.deb
  ```

- *Чтобы установить Агент администрирования из .deb-пакета на 64-битную операционную систему, выполните следующую команду:*

  ```
  # dpkg -i --force-architecture klnagent_<номер_версии>_i386.deb
  ```

После запуска команды дальнейший процесс установки будет выполнен автоматически.

По завершении установки Агента администрирования из rpm-пакета следует запустить (см. стр. 30) скрипт постинсталляционной настройки.

УДАЛЕННАЯ УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

Вы можете установить Антивирус Касперского удаленно через Консоль администрирования Kaspersky Administration Kit. Для удаленной установки Антивируса Касперского создайте задачу удаленной установки (см. раздел «Создание задачи удаленной установки» на стр. 16) для набора компьютеров.

Установка программы осуществляется методом *форсированной установки* (см. Руководство по внедрению Kaspersky Administration Kit 8.0). Форсированная установка позволяет провести удаленную установку программного обеспечения на конкретные клиентские компьютеры логической сети. При запуске задачи Сервер администрирования копирует из папки общего доступа набор файлов для установки программы на каждый клиентский компьютер во временную папку и производит запуск программы установки на каждом из них.

Связь Сервера администрирования с клиентскими компьютерами обеспечивает компонент Агент администрирования. Поэтому он должен быть установлен и настроен (см. стр. 30). Для успешного завершения удаленной установки Агент администрирования должен быть запущен на защищаемом сервере.

При создании задач удаленной установки используются инсталляционные пакеты (см. раздел «Создание инсталляционного пакета» на стр. 20). Инсталляционный пакет представляет собой набор файлов, необходимых для установки программы, и содержит параметры, касающиеся как самого процесса установки, так и первоначальной настройки (см. стр. 24) устанавливаемой программы. Инсталляционный пакет можно сформировать перед созданием задачи удаленной установки или во время ее создания. Один и тот же инсталляционный пакет может быть использован многократно.

Обратите внимание, что для операционных систем, использующих dpkg, инсталляционный пакет должен быть сформирован на основе deb-пакета, а для операционных систем, использующих RPM – на основе rpm-пакета.

Все сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Хранилища** → **Инсталляционные пакеты**.

В ЭТОМ РАЗДЕЛЕ

СОЗДАНИЕ ЗАДАЧИ УДАЛЕННОЙ УСТАНОВКИ

Чтобы создать задачу удаленной установки для набора компьютеров с помощью метода форсированной установки, выполните следующие действия:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли папку **Задачи для наборов компьютеров**.

3. Откройте контекстное меню и выберите пункт **Создать** → **Задачу** или выберите аналогичный пункт в меню **Действие**.

В результате откроется мастер создания задачи. Следуйте его указаниям.

Шаги мастера

Шаг 1. Определение имени задачи

Введите имя задачи в поле **Имя**.

Шаг 2. Выбор типа задачи

В узле **Kaspersky Administration Kit** выберите тип задачи **Удаленная установка программы**.

Шаг 3. Выбор инсталляционного пакета

Укажите инсталляционный пакет, установка которого будет проводиться при выполнении данной задачи. Выберите нужный из числа пакетов, сформированных для данного Сервера администрирования, либо создайте новый инсталляционный пакет при помощи кнопки **Новый**. Создание нового инсталляционного пакета (см. раздел «Создание инсталляционного пакета» на стр. 20) выполняется с помощью мастера создания инсталляционного пакета.

Шаг 4. Выбор метода удаленной установки

Выберите вариант **Форсированная установка**.

Шаг 5. Определение параметров задачи

На этом шаге вам предлагается определить, нужно ли переустанавливать программу, если она уже установлена на клиентском компьютере. Установите флажок **Не устанавливать программу, если она уже установлена**, чтобы повторная установка программы на компьютеры не проводилась.

Шаг 6. Выбор инсталляционного пакета для совместной установки

Если вы хотите совместно с программой установить Агент администрирования, установите флажок **Установить Агент администрирования совместно с данной программой**, а затем выберите нужный инсталляционный пакет.

- *Чтобы создать новый инсталляционный пакет Агента администрирования,*

  нажмите на кнопку **Создать**.

В результате откроется мастер создания инсталляционного пакета (см. раздел «Создание инсталляционного пакета» на стр. 20). Следуйте его указаниям.

Шаг 7. Настройка параметров перезагрузки компьютеров

Определите действия, которые следует предпринять, если после установки программы потребуется перезагрузка сервера. Доступны следующие варианты:

- **Не перезагружать компьютер**;
- **Перезагрузить компьютер** – при выборе этого варианта операционная система будет перезагружена только в случае необходимости;
- **Спросить у пользователя** – при выборе этого варианта вам следует настроить параметры уведомления пользователя о перезагрузке.

Выберите вариант **Не перезагружать компьютер**.

Шаг 8. Определение способа выбора компьютеров

Определите способ выбора компьютеров, для которых будет создана задача:

- **На основании данных, полученных в ходе опроса Windows-сети** – в этом случае клиентские компьютеры для установки выбираются на основании данных, получаемых Сервером администрирования при опросе сети предприятия;
- **На основании адресов (IP-адрес, NetBIOS- или DNS-имя), вводимых вручную** – в этом случае имена или IP-адреса клиентских компьютеров нужно выбирать или вводить вручную.

Шаг 9. Выбор клиентских компьютеров

Если компьютеры выбираются на основании данных, полученных в ходе опроса сети, то формирование списка производится в окне мастера. Для выбора установите флажки рядом с именами клиентских компьютеров из состава групп администрирования (узел **Управляемые компьютеры**) и компьютеров, не включенных в их состав (узел **Нераспределенные компьютеры**).

Если выбор компьютеров проводится вручную, то список адресов формируется за счет ввода NetBIOS- или DNS-имен, IP-адресов (или диапазона IP-адресов) компьютеров, либо путем импорта списка из txt-файла, в котором

каждый адрес должен быть указан с новой строки. Сформируйте список адресов нажатием на кнопки **Добавить**, **Удалить** и **Добавить IP-интервал**, либо импортируйте список из текстового файла, нажав на кнопку **Импортировать**. В качестве адреса сервера можно использовать IP-адрес (или диапазон IP-адресов), NetBIOS- или DNS-имя. Для импорта списка из файла необходимо указать txt-файл с перечнем адресов добавляемых серверов.

Шаг 10. Выбор учетной записи для запуска задачи

Так как копирование файлов на клиентские компьютеры выполняет Агент администрирования, то учетную запись задавать не нужно. Все операции по копированию и установке файлов Агент администрирования будет выполнять с правами учетной записи **Локальная система**.

Шаг 11. Формирование расписания запуска задачи

Составьте расписание запуска задачи.

- В раскрывающемся списке **Запуск по расписанию** выберите нужный режим запуска задачи:
  - **Вручную**;
  - **Каждый N час**;
  - **Ежедневно**;
  - **Еженедельно**;
  - **Ежемесячно**;
  - **Один раз** – в этом случае запуск задачи удаленной установки на компьютерах будет осуществлен только один раз независимо от того, с каким результатом закончится ее выполнение;
  - **Немедленно** – сразу после создания задачи, по завершению работы мастера;
  - **По завершении другой задачи** – в этом случае задача удаленной установки будет запускаться только после завершения работы указанной задачи.
- Проведите настройку параметров расписания в группе полей, соответствующих выбранному режиму.
- Настройте дополнительные параметры запуска задачи (их состав зависит от выбранного режима запуска). Для этого выполните следующие действия:
  - Задайте порядок запуска задачи, если в заданное расписанием время клиентский компьютер недоступен (выключен, отключен от сети и т. п.) или программа не запущена.
  - Установите флажок **Запускать пропущенные задачи**, чтобы попытка запуска задачи предпринималась при очередном запуске программы на данном клиентском компьютере. Для вариантов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления компьютера в сети.
  - Если данный флажок не установлен, запуск задачи на клиентских компьютерах будет производиться только по расписанию, а для вариантов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских компьютерах. По умолчанию флажок не установлен.

Шаг 12. Завершение создания задачи

По окончании работы мастера сформированная задача удаленной установки будет добавлена в папку **Задачи для наборов компьютеров** и представлена в панели результатов. В случае необходимости вы можете вносить изменения в ее параметры (см. стр. 20).

Запуск задачи удаленной установки

Чтобы вручную запустить на выполнение задачу удаленной установки для набора компьютеров, выполните следующие действия:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли папку **Задачи для наборов компьютеров**.
3. В панели результатов выберите в списке нужную задачу.
4. Откройте контекстное меню и выберите пункт **Запустить** или выберите аналогичный пункт в меню **Действие**.

Просмотр и настройка параметров задачи удаленной установки

Чтобы просмотреть свойства задачи удаленной установки и изменить ее параметры, выполните следующие действия:

1. Выберите в дереве консоли папку **Задачи для наборов компьютеров**.
2. В панели результатов выберите в списке нужную задачу.
3. Откройте контекстное меню и выберите пункт **Свойства** или выберите аналогичный пункт в меню **Действие**.

В результате откроется окно **Свойства <Имя задачи>**, состоящее из закладок: **Общие**, **Уведомление**, **Клиентские компьютеры**, **Расписание**, **Параметры**, **Учетная запись** и **Перезагрузка ОС**.

Настройка задачи удаленной установки осуществляется так же, как и настройка свойств любой из задач. Рассмотрим подробнее специфичные для данного типа задачи параметры, представленные на закладке **Параметры**. На этой закладке вы можете определить:

- способ доставки необходимых для установки программы файлов на клиентские компьютеры и указать максимальное количество одновременных соединений;
- количество попыток провести установку при запуске задачи по расписанию;
- нужно ли переустанавливать программу, если она уже установлена на клиентском компьютере;
- нужно ли закрывать работающие программы перед началом установки;
- следует ли до начала установки программы проверять версию операционной системы на соответствие требованиям к системе.

Создание инсталляционного пакета

Перед созданием инсталляционного пакета необходимо выполнить подготовку дистрибутива Антивируса Касперского.

- *Чтобы подготовить дистрибутив Антивируса Касперского к установке, выполните следующие действия:*

  1. Распакуйте архив kav4fs-rpm.tar.gz или kav4fs-deb.tar.gz (в зависимости от менеджера пакетов, используемого в операционной системе защищаемого сервера) в папку, доступную для Сервера администрирования Kaspersky Administration Kit.

  2. Скопируйте в ту же папку пакет kav4fs-<номер_версии>.i386.rpm или kav4fs_<номер_версии>_i386.deb (в зависимости от менеджера пакетов, используемого в операционной системе защищаемого сервера).

- *Чтобы создать инсталляционный пакет, выполните следующие действия:*

  1. Подключитесь к нужному Серверу администрирования.

  2. Выберите в дереве консоли папку **Хранилища** → **Инсталляционные пакеты**.

  3. Откройте контекстное меню и выберите пункт **Создать** → **Инсталляционный пакет** или выберите аналогичный пункт в меню **Действие**.

В результате откроется мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаги мастера

Шаг 1. Определение имени инсталляционного пакета

Введите имя инсталляционного пакета в поле **Имя**.

Шаг 2. Выбор дистрибутива программы

На данном шаге вам предлагается указать программу для установки.

В раскрывающемся списке выберите вариант: **Создать инсталляционный пакет для программы «Лаборатории Касперского»**. Нажмите на кнопку **Выбрать** и выберите файл с расширением .kpd. В результате автоматически заполняются поля с именем программы и номером версии.

Параметры инсталляционного пакета создаются по умолчанию и соответствуют программе, выбранной для установки. Вы можете их изменить (см. стр. 23) после создания пакета в окне его свойств.

Шаг 3. Загрузка инсталляционного пакета

Для загрузки сформированного инсталляционного пакета на Сервер администрирования нажмите на кнопку **Далее**.

Шаг 4. Настройка параметров задачи постоянной защиты

На данном шаге вам предлагается запустить компиляцию модуля ядра операционной системы. При этом компилируется модуль, необходимый для работы задачи постоянной защиты. Вы можете выбрать один из следующих вариантов:

- **Не компилировать модуль постоянной защиты**;
- **Компилировать модуль, автоматически искать исходные коды** – при выборе этого варианта исходные коды ядра будут найдены автоматически;
- **Компилировать модуль, указать путь к исходным кодам** – при выборе этого варианта вам следует вручную указать полный путь к исходным кодам ядра операционной системы (например, */lib/modules/2.6.27.39-0.2-default*). Нажмите на кнопку **Дополнительно**, чтобы указать полный путь к исходным кодам ядра.

Ниже на данном шаге вам предлагается определить параметры интеграции с сервером Samba. Вы можете выбрать один из следующих вариантов:

- **Не устанавливать перехватчик Samba**;
- **Автоматическая интеграция с сервером Samba** – при выборе этого варианта интеграция Антивируса Касперского с сервером Samba будет производиться автоматически;
- **Интеграция с сервером Samba, указать параметры вручную** – при выборе этого варианта вам следует вручную указать параметры интеграции с сервером Samba. Нажмите на кнопку **Дополнительно**, чтобы задать следующие параметры интеграции с сервером Samba:
  - полный путь к конфигурационному файлу Samba-сервера (например, */etc/samba/smb.conf*);
  - директорию для VFS-модулей Samba (например, */usr/lib/samba/vfs*);
  - имя устанавливаемого VFS-модуля (например, */opt/kaspersky/kav4fs/lib/samba/kav4fs-smb-vfs21.so*).

Установите флажок **Запустить задачу постоянной защиты после установки**, если вы хотите, чтобы задача была запущена сразу после установки.

Шаг 5. Настройка параметров задачи обновления

На данном шаге вам предлагается указать параметры задачи обновления. Вы можете выбрать один из следующих источников обновлений:

- **Не изменять**;
- **Сервер администрирования Kaspersky Administration Kit**;
- **Серверы обновлений Лаборатории Касперского**;
- **Другие источники обновлений**.

  Если вы выбрали этот вариант, нажмите на кнопку **Дополнительно**, чтобы настроить пользовательский источник обновлений. Источником обновлений могут быть HTTP- или FTP-серверы, локальные или сетевые папки.

Установите флажок **Запустить обновление после установки**, если вы хотите, чтобы сразу после установки была запущена задача обновления.

Шаг 6. Завершение создания инсталляционного пакета

В результате инсталляционный пакет будет сформирован и представлен в панели результатов в папке **Хранилища** → **Инсталляционные пакеты**. Вы можете изменять параметры инсталляционного пакета в окне его свойств.

Просмотр и настройка параметров инсталляционного пакета

Чтобы просмотреть свойства инсталляционного пакета и изменить его параметры, выполните следующие действия:

1. В дереве консоли перейдите в папку **Хранилища** → **Инсталляционные пакеты**.
2. В панели результатов выберите нужный инсталляционный пакет.
3. Откройте контекстное меню и выберите пункт **Свойства** или выберите аналогичный пункт в меню **Действие**.
4. В результате откроется окно **Свойства <Имя инсталляционного пакета>**, состоящее из закладок: **Общие**, **Постоянная защита**, **Обновление** и **Лицензия**.

Закладка **Общие** содержит общую информацию о пакете. В ее состав входят следующие данные:

- Название инсталляционного пакета (вы можете его изменить).
- Имя и версия программы, для установки которой сформирован пакет.
- Размер пакета.
- Дата создания.
- Путь к папке размещения инсталляционного пакета.

Закладка **Постоянная защита** содержит параметры задачи постоянной защиты: параметры компиляции модуля ядра операционной системы, необходимого для работы задачи постоянной защиты, и параметры интеграции с сервером Samba. Данные параметры настраиваются на этапе формирования инсталляционного пакета (см. раздел «Создание инсталляционного пакета» на стр. 20). В случае необходимости вы можете их изменить.

Закладка **Обновление** содержит параметры задачи обновления: выбор источника обновлений и настройка пользовательского источника обновлений. Данные параметры настраиваются на этапе формирования инсталляционного пакета (см. раздел «Создание инсталляционного пакета» на стр. 20). В случае необходимости вы можете их изменить.

Закладка **Лицензия** содержит общую информацию о лицензии, соответствующей программе, для установки которой сформирован инсталляционный пакет. На этой закладке вы можете добавлять или изменять файл ключа.

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА АНТИВИРУСА КАСПЕРСКОГО

По завершении установки Антивируса Касперского на сервер нужно выполнить первоначальную настройку Антивируса Касперского.

Если процедура первоначальной настройки Антивируса Касперского не выполнялась, антивирусная защита сервера не будет работать.

Процесс первоначальной настройки представляет собой последовательность шагов, которая для удобства пользователя реализована в виде скрипта. Скрипт первоначальной настройки запускается автоматически, когда завершается установка приложения на компьютер. Если менеджер пакетов, используемый в операционной системе, не допускает использования интерактивных скриптов, скрипт первоначальной настройки нужно запустить вручную.

По завершении процесса первоначальной настройки запускается задача постоянной защиты. Необходимым условием этого является выполнение следующих действий:

- установка файла ключа,
- загрузка баз Антивируса Касперского,
- компиляция модулей ядра.

Чтобы запустить скрипт первоначальной настройки Антивируса Касперского вручную, выполните следующую команду:

для Linux:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-setup.pl
```

Действия, требуемые для запуска задачи постоянной защиты, вы можете выполнить с помощью средств управления Антивирусом Касперского. Для получения подробной информации обратитесь к «Руководству администратора» Антивируса Касперского 8.0 для Linux File Server.

В этом разделе

Шаг 1. Просмотр текста лицензионного соглашения

На данном этапе вам необходимо принять или отклонить условия лицензионного соглашения.

Просмотр текста осуществляется с помощью утилиты *less*. Для перемещения по тексту используйте клавиши управления курсором или клавиш **b** (для перемещения назад на один экран) и **f** (для перемещения вперед на один экран). Для получения справки используйте клавишу **h**. Для завершения просмотра используйте клавишу **q**.

После выхода из режима просмотра введите **yes** (или **y**), чтобы согласиться с условиями лицензионного соглашения. Если вы не согласны с условиями лицензионного соглашения, введите **no** (или **n**).

Если вы не согласны с условиями лицензионного соглашения, процесс настройки Антивируса Касперского завершается.

Шаг 2. Выбор локали

На данном этапе необходимо задать обозначение локали, которая будет использоваться при работе Антивируса Касперского.

Локаль задается в формате, определенном в RFC 3066.

- *Чтобы получить полный список обозначений локалей, воспользуйтесь следующей командой:*

```
# locale -a
```

По умолчанию вам предлагается использовать локаль **en_US.utf8**.

Шаг 3. Установка файла ключа

На данном этапе необходимо установить файл ключа. Файл ключа содержит сведения, на основании которых проверяется наличие прав на использование Антивируса Касперского и определяется срок его использования.

- *Чтобы установить файл ключа,*

  укажите полный путь к файлу ключа или путь к директории, содержащей файлы ключей.

Если в указанной директории находятся несколько файлов ключа, установлен будет первый файл, подходящий для Антивируса Касперского 8.0 для Linux File Server.

Если лицензия не установлена, Антивируса Касперского не будет обеспечивать антивирусную защиту сервера.

Вы можете установить файл ключа без использования скрипта первоначальной настройки. Для получения информации об установке файла ключа обратитесь к разделу «Управление лицензиями» «Руководства администратора» Антивируса Касперского 8.0 для Linux File Server.

Шаг 4. Настройка параметров прокси-сервера

На данном этапе укажите параметры прокси-сервера. Это необходимо сделать в том случае, если для доступа к интернету используется прокси-сервер. Подключение к интернету необходимо для загрузки баз Антивируса Касперского с серверов обновлений.

- *Чтобы настроить параметры прокси-сервера, выполните следующие действия:*

  - Если при подключении к интернету используется прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:

    - `IP_адрес_прокси_сервера:порт`, если при подключении к прокси-серверу не требуется аутентификация;

    - `имя_пользователя:пароль@IP_адрес_прокси_сервера:порт`, если при подключении к прокси-серверу необходима аутентификация.

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

По умолчанию предлагается ответ **no**.

Вы можете настроить параметры прокси-сервера без использования скрипта первоначальной настройки. Для получения информации о настройке параметров прокси-сервера обратитесь к разделу «Обновление Антивируса Касперского» «Руководства администратора» Антивируса Касперского 8.0 для Linux File Server.

Шаг 5. Загрузка баз Антивируса Касперского

На данном этапе вам предлагается загрузить на сервер базы Антивируса Касперского. Защита информации на сервере обеспечивается на основании баз данных, содержащих описания сигнатур угроз и методов борьбы с ними. Антивирус Касперского использует их при поиске и обезвреживании опасных объектов. Базы регулярно пополняются записями о новых угрозах и способах борьбы с ними.

- *Чтобы загрузить базы Антивируса Касперского на сервер,*

  введите в качестве ответа **yes**.

Если вы хотите отказаться от загрузки баз сейчас, введите **no**.

По умолчанию предлагается ответ **yes**.

Если базы Антивируса Касперского не были загружены, Антивирус Касперского не будет обеспечивать антивирусную защиту сервера.

Вы можете запустить обновление баз Антивируса Касперского без использования скрипта. Для получения информации о запуске обновления баз Антивируса Касперского обратитесь к разделу «Обновление Антивируса Касперского» «Руководства администратора» Антивируса Касперского 8.0 для Linux File Server.

Шаг 6. Включение автоматического обновления баз

На данном шаге вы можете включить автоматическое обновление баз Антивируса Касперского.

- *Чтобы включить автоматическое обновление баз,*

  введите **yes**.

По умолчанию базы Антивируса Касперского обновляются каждые 30 минут.

Вы можете включить автоматическое обновление баз Антивируса Касперского без помощи скрипта первоначальной настройки. Для получения информации о настройке расписания обновления баз Антивируса Касперского см. разделы «Изменение параметров расписания задачи. -T --set-schedule» и «Параметры расписания» «Руководства администратора» Антивируса Касперского 8.0 для Linux File Server.

Шаг 7. Компиляция модуля ядра

На данном этапе вам предлагается запустить компиляцию модуля ядра. При этом компилируется модуль, необходимый для работы задачи постоянной защиты.

Если скрипт обнаруживает исходные коды ядра операционной системы в директории по умолчанию, найденный путь будет использоваться по умолчанию. В противном случае вам будет предложено указать путь к исходным кодам ядра.

Вы можете выполнить компиляцию модуля ядра, не повторяя предыдущие шаги скрипта.

- *Чтобы выполнить компиляцию модуля ядра, не запуская процесс первоначальной настройки, выполните следующую команду:*

```
# /opt/kaspersky/kav4fs/bin/kav4fs-setup.pl \

--build=<путь к исходным кодам ядра>
```

Если компиляция модуля ядра не производилась, задача постоянной защиты не будет обрабатывать операции над локальными или смонтированными объектами файловой системы сервера.

Шаг 8. Интеграция с сервером Samba

На данном этапе проводится интеграция с сервером Samba. При этом выполняются следующие действия:

- поиск установленного сервера Samba и проверка его версии на соответствие программным требованиям;
- поиск и изменение конфигурационного файла сервера Samba;
- проверка конфигурационного файла сервера Samba на наличие VFS-модулей.

Если в конфигурационном файле сервера Samba на момент установки Антивируса Касперского заданы VFS-модули, эти модули будут отключены.

Скрипт первоначальной настройки производит поиск установленных серверов Samba. После этого вам будет предложено настроить защиту найденных серверов автоматически или вручную. Введите **Y**, чтобы настроить защиту сервера Samba автоматически. Этот режим используется по умолчанию. Введите **N**, если сервер Samba обнаружен неверно, или если вы хотите настроить защиту сервера Samba вручную.

Чтобы настроить защиту сервера Samba вручную, выполните следующие действия:

Если вы введете пустую строку в ответ на запрос скрипта первоначальной настройки, процесс настройки защиты сервера Samba прерывается.

1. Укажите путь к директории, содержащей файл *smbd*.
2. Укажите путь к директории, содержащей конфигурационный файл сервера Samba (*smb.conf*).
3. Укажите путь к директории, содержащей VFS-модули сервера Samba.

По окончании интеграции вручную перезапустите службу сервера Samba.

Если задача постоянной защиты была остановлена после интеграции с сервером Samba, доступ к ресурсам Samba будет заблокирован.

Чтобы избежать блокирования доступа к ресурсам Samba после остановки задачи постоянной защиты,

добавьте в секцию `[global]` конфигурационного файла */etc/samba/smb.conf* следующую строку:

```
kavsamba:access_on_error = yes
```

Вы можете выполнить интеграцию с сервером Samba, не повторяя предыдущие шаги скрипта.

Чтобы выполнить интеграцию с сервером Samba, не запуская процесс первоначальной настройки, выполните следующую команду:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-setup.pl --samba
```

Шаг 9. Назначение пароля доступа к Web Management Console

На этом этапе вам предлагается задать пароль для доступа к Web Management Console.

Чтобы задать пароль для доступа к Web Management Console, выполните следующие действия:

1. Введите **yes**.
2. Задайте и подтвердите пароль.

Если вы не задали пароль для доступа к Web Management Console на данном этапе, вы можете сделать это в дальнейшем с помощью утилиты /opt/kaspersky/kav4fs/bin/kav4fs-wmconsole-passwd.

По умолчанию предлагается ответ **no**.

Шаг 10. Запуск задачи постоянной защиты

На данном этапе запускается задача постоянной защиты, если были выполнены следующие действия:

- установка лицензии;
- загрузка баз Антивируса Касперского;
- компиляция модулей ядра или интеграция с сервером Samba.

Для получения информации об управлении задачей обратитесь к разделу «Управление задачами» «Руководства администратора» Антивируса Касперского 8.0 для Linux File Server.

Шаг 11. Управление службой Web Management Console

Для управления службой Web Management Console необходимо зарегистрироваться в системе с правами учетной записи **root**.

В состав Антивируса Касперского входит компонент удаленного управления Web Management Console. По умолчанию служба Web Management Console не запускается при старте операционной системы или во время запуска Антивируса.

Чтобы запустить службу Web Management Console, выполните команду:

```
# /etc/init.d/kav4fs-wmconsole start
```

Чтобы остановить службу Web Management Console, выполните команду:

```
# /etc/init.d/kav4fs-wmconsole stop
```

Для настройки автоматического запуска службы Web Management Console воспользуйтесь утилитой **chkconfig** (на RPM-системах) или утилитой **update-rc.d** (на DEB-системах).

Шаг 12. Доступ к веб-интерфейсу Web Management Console

Управление Антивирусом Касперского с помощью Web Management Console осуществляется через веб-интерфейс этого компонента.

- *Чтобы открыть веб-интерфейс Web Management Console, выполните следующие действия:*

1. Запустите веб-браузер.
2. Введите в адресную строку веб-браузера следующий URL:

   `http://DNS_имя_или_IP_адрес_защищаемого_сервера:9080`

3. Введите пароль пользователя, заданный во время первоначальной настройки Антивируса Касперского.

Web Management Console обращается к защищаемому серверу с правами учетной записи **kluser**.

Шаг 13. Настройка параметров Агента администрирования

Если вы планируете управлять Антивирусом Касперского с помощью Kaspersky Administration Kit, следует настроить параметры Агента администрирования. Процесс настройки реализован в виде скрипта.

- *Чтобы запустить скрипт настройки Агента администрирования, выполните следующую команду:*

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

В процессе работы скрипта вам будет предложено выполнить следующие действия:

1. Указать DNS-имя или IP-адрес Сервера администрирования.
2. Указать номера порта Сервера администрирования или использовать порт по умолчанию (14000).
3. Указать номер SSL-порта Сервера администрирования или использовать порт по умолчанию (13000).
4. Указать, использовать ли SSL-соединение для передачи данных. По умолчанию SSL-соединение включено.

Для получения подробной информации о настройке Агента администрирования обратитесь к «Руководству Администратора» Kaspersky Administration Kit.

Запуск автоматической первоначальной настройки

Первоначальную настройку Антивируса Касперского можно выполнять в автоматическом режиме.

- *Чтобы запустить первоначальную настройку в автоматическом режиме, выполните следующую команду:*

для Linux:

```
/opt/kaspersky/kav4fs/bin/kav4fs-setup.pl \
--auto-install=<полный путь к конфигурационному файлу первоначальной настройки>
```

для FreeBSD:

```
/usr/local/bin/kav4fs-setup.pl \
--auto-install=<полный путь к конфигурационному файлу первоначальной настройки>
```

Параметры конфигурационного файла первоначальной настройки приведены в таблице ниже.

Таблица 2. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр. Согласие с условиями лицензионного соглашения	**yes**
SERVICE_LOCALE	Локаль, используемая при работе Антивируса Касперского	Локаль в формате, определенном в RFC 3066
INSTALL_KEY_FILE	Полный путь к файлу ключа	
UPDATER_SOURCE	Источник обновлений	• **AKServer** – использовать в качестве источника обновлений Сервер администрирования Kaspersky Administration Kit; • **KLServers** – использовать в качестве источника обновлений серверы ЗАО «Лаборатория Касперского»; • URL источника обновлений;
UPDATER_PROXY	Адрес прокси-сервера, используемого для подключения к интернету	• URL прокси-сервера; • **no** – не использовать прокси-сервер;
UPDATER_EXECUTE	Запуск задачи обновления баз во время процедуры настройки	• **yes** – запускать задачу обновления; • **no** – не запускать задачу обновления;
UPDATER_ENABLE_AUTO	Включение / отключение автоматического запуска задачи обновления баз	• **yes** – включить автоматический запуск задачи обновления; • **no** – отключить автоматический запуск задачи обновления;
RTP_BUILD_KERNEL_MODULE	Обязательный параметр. Запуск компиляции модуля ядра	• **yes** – компилировать модуль ядра; • **no** – не компилировать модуль ядра;
RTP_BUILD_KERNEL_SRCS	Путь к исходным кодам ядра	• **auto** – автоматический поиск; • путь к исходным кодам;
RTP_SAMBA_ENABLE	Обязательный параметр. Интеграция с сервером Samba	• **yes** – проводить интеграцию с использованием значений параметров RTP_SAMBA_CONF, RTP_SAMBA_VFS, RTP_SAMBA_VFS_MODULE; • **no** – не проводить интеграцию; • **auto** – автоматически определять пути к компонентам Samba-сервера;
RTP_SAMBA_CONF	Полный путь к конфигурационному файлу сервера Samba (*smb.conf*)	

Параметр	Описание	Возможные значения
RTP_SAMBA_VFS	Полный путь к директории, содержащей VFS-модули сервера Samba	
RTP_SAMBA_VFS_MODULE	Полный путь к VFS-модулю Антивируса Касперского, который будет установлен в качестве модуля-обработчика	
RTP_START	Запуск задачи постоянной защита по завершении настройки	• **yes** – запускать задачу постоянной защиты; • **no** – не запускать задачу постоянной защиты;

Вводите значения параметров в формате **имя параметра=значение** (пробелы между именем параметра и его значением не обрабатываются).

Настройка разрешающих правил в системах SELinux и AppArmor

Установите пакет policycoreutils-python перед использованием утилиты audit2allow.

Чтобы создать модуль SELinux с правилами, необходимыми для работы Антивируса Касперского, выполните следующие действия:

1. Переведите SELinux в разрешающий режим:

   ```
   # setenforce Permissive
   ```

2. Проверьте работоспособность задачи постоянной защиты (см. стр. 37).

3. Создайте модуль правил на основе блокирующих записей:

   ```
   # audit2allow -l -M kav4fs –i\ /var/log/audit/audit.log
   ```

   Убедитесь, что созданный список содержит только правила, относящиеся к Антивирусу Касперского.

4. Загрузите полученный модуль правил:

   ```
   # semodule -i kav4fs.pp
   ```

5. Переведите SELinux в принудительный режим:

   ```
   # setenforce Enforcing
   ```

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

Чтобы обновить файл модуля правил, выполните следующие команды:

```
# audit2allow -l -M kav4fs –i /var/log/audit/audit.log

# semodule –u kav4fs.pp
```

Дополнительная информация приведена в следующих руководствах:

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

Чтобы обновить профили AppArmor, необходимые для работы Антивируса Касперского, выполните следующие действия:

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

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

   # /etc/init.d/apparmor reload
   ```

2. Перезапустите kav4fs:

   ```
   # /etc/init.d/kav4fs-supervisor restart
   ```

3. Проверьте работоспособность задачи постоянной защиты (см. стр. 37).

4. Запустите утилиту обновления профилей:

   ```
   # aa-logprof
   ```

5. Перезагрузите правила AppArmor:

   ```
   # /etc/init.d/apparmor reload
   ```

6. Переведите все правила для приложений в «принудительный» режим:

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

   # /etc/init.d/apparmor reload
   ```

В случае появления новых audit-сообщений, связанных с Антивирусом Касперского, следует повторить шаги, описанные в п. 3 и 4.

Дополнительная информация приведена в следующих руководствах:

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

УДАЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Если вы хотите восстановить файлы, которые находятся на карантине, сделайте это до удаления Антивируса Касперского. В противном случае восстановить файлы из карантина будет невозможно.

- *Чтобы удалить Антивирус Касперского, установленный из rpm-пакета, выполните следующую команду:*

  ```
  # rpm -e kav4fs
  ```

- *Чтобы удалить Антивирус Касперского, установленный из deb-пакета, выполните следующую команду:*

  ```
  # dpkg -r kav4fs
  ```

- *Чтобы удалить Антивирус Касперского установленный на сервере, работающем под управлением операционной системы FreeBSD, выполните следующую команду:*

  ```
  # pkg_delete kav4fs
  ```

При этом все задачи Антивируса Касперского будут остановлены.

- *Чтобы удалить Агент администрирования, установленный из rpm-пакета, выполните следующую команду:*

  ```
  # rpm -e klnagent
  ```

- *Чтобы удалить Агент администрирования, установленный из deb-пакета, выполните следующую команду:*

  ```
  # dpkg -r klnagent
  ```

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

УДАЛЕННАЯ ДЕИНСТАЛЛЯЦИЯ АНТИВИРУСА КАСПЕРСКОГО

Удаленная деинсталляция Антивируса Касперского с помощью Kaspersky Administration Kit осуществляется путем запуска задачи удаленной деинсталляции.

- *Чтобы создать задачу удаленной деинсталляции Антивируса Касперского, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли папку **Задачи для наборов компьютеров**.
3. Откройте контекстное меню и выберите пункт **Создать** → **Задачу** или выберите аналогичный пункт в меню **Действие**.

   В результате откроется мастер создания задачи.
4. В окне **Имя задачи** введите имя задачи в поле **Имя**.
5. В окне **Тип задачи** в узле **Kaspersky Administration Kit** раскройте вложенную папку **Дополнительно** и выберите **Удаленная деинсталляция программы**.
6. В окне **Параметры** укажите программу, которую нужно удалить. Для этого в раскрывающемся списке **Удалить программу, поддерживаемую Kaspersky Administration Kit** выберите вариант **Антивирус Касперского 8.0 для Linux File Server**.
7. В окне **Метод удаленной деинсталляции** выберите вариант **Форсированная деинсталляция**.
8. В окне **Параметры** в блоке параметров **Форсировать загрузку утилиты деинсталляции** установите флажок **С помощью Агента администрирования**.
9. Завершите формирование задачи аналогично задаче удаленной установки (см. стр. 16).

Сформированная вами задача будет запускаться на выполнение в соответствии со своим расписанием.

- *Чтобы вручную запустить задачу удаленной деинсталляции Антивируса Касперского, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли папку **Задачи для наборов компьютеров**.
3. В панели результатов выберите в списке нужную задачу.
4. Откройте контекстное меню и выберите пункт **Запустить** или выберите аналогичный пункт в меню **Действие**.

ДЕЙСТВИЯ ПОСЛЕ УДАЛЕНИЯ АНТИВИРУСА КАСПЕРСКОГО

После удаления Антивируса Касперского (см. стр. 34) на сервере остается следующая информация:

- базы Антивируса Касперского;
- базы данных хранилища лицензий;
- базы данных хранилища событий;
- базы данных параметров работы Антивируса Касперского;
- файлы в резервном хранилище и карантине;
- файлы журнала.

В состав Антивируса Касперского входят скрипты, которые удаляют файлы и директории, оставшиеся после деинсталляции Антивируса Касперского на сервере.

Чтобы запустить эти скрипты, выполните следующие действия:

1. Выполните следующую команду:
   - для Linux: `# /var/opt/kaspersky/kav4fs/cleanup.sh`
   - для FreeBSD: `# /var/db/kaspersky/kav4fs/cleanup.sh`
2. Подтвердите удаление информации, оставшейся после удаления Антивируса Касперского, введя **yes**. Чтобы отказаться от удаления информации и остановить работу скрипта, введите **no**.

ПРОВЕРКА РАБОТЫ ЗАДАЧ ПОСТОЯННОЙ ЗАЩИТЫ И ПРОВЕРКИ ПО ТРЕБОВАНИЮ

После установки и первоначальной настройки Антивируса вы можете убедиться в том, что задачи постоянной защиты и проверки по требованию настроены должным образом.

В ЭТОМ РАЗДЕЛЕ

ПРОВЕРКА РАБОТЫ ЗАДАЧИ ПОСТОЯННОЙ ЗАЩИТЫ

В этом разделе описано, как убедиться в том, что с помощью задачи постоянной защиты Антивирус обнаруживает зараженные и подозрительные объекты при доступе к ним и выполняет над ними указанные в задаче действия.

Чтобы проверить работу задачи постоянной защиты, выполните следующие действия:

1. Загрузите файл *eicar.com* со страницы сайта EICAR http://www.eicar.org/anti_virus_test_file.htm. Сохраните его на защищаемом сервере.

   Если вы хотите проверить, как Антивирус обнаруживает подозрительные объекты, добавьте к текстовой строке в файле префикс SUSP- (подробнее читайте в разделе «Тестовый вирус EICAR и его модификации»).

2. Если задача постоянной защиты была остановлена, запустите ее с помощью следующей команды:

   ```
   # /opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 8
   ```

3. Откройте файл *eicar.com* на чтение с помощью следующей команды:

   ```
   # cat <полный_путь_к_eicar.com>
   ```

4. Антивирус перехватит обращение к файлу, проверит его и заблокирует доступ к нему. При этом на консоли отображается следующее сообщение:

   ```
   "cat: <полный_путь_к_eicar.com>: Permission denied"
   ```

5. Выполните следующую команду:

   ```
   # echo $?
   ```

   Задача постоянной защиты успешно обрабатывает обращение к файлу *eicar.com*, если результатом выполнения этой команды является ненулевое значение.

Проверка работы задачи проверки по требованию

В этом разделе описано, как убедиться в том, что Антивирус обнаруживает в указанной в задаче проверки по требованию области проверки зараженные и подозрительные объекты и выполняет над ними указанные в задаче действия.

Вы можете проверить функцию «Проверка по требованию» при выполнении как предустановленной задачи **Полная проверка компьютера**, так и другой, пользовательской, задачи проверки по требованию.

Вам нужно сохранить на защищаемом сервере файл *eicar.com*.

Чтобы проверить работу задачи проверки по требованию, выполните следующее действие:

1. Остановите задачу постоянной защиты с помощью следующей команды:

   ```
   # /opt/kaspersky/kav4fs/bin/kav4fs-control --stop-task 8
   ```

2. Загрузите файл *eicar.com* со страницы сайта EICAR http://www.eicar.org/anti_virus_test_file.htm и сохраните его на защищаемом сервере.

   При проверке Антивирус присвоит файлу статус **Зараженный**, если вы оставите файл eicar.com без изменений. Антивирус присвоит файлу статус **Подозрительный**, если вы добавите к текстовой строке в файле *eicar.com* префикс SUSP- (подробнее читайте в разделе «Тестовый вирус EICAR и его модификации» (см. стр. 38)).

3. Создайте задачу проверки по требования с помощью следующей команды:

   ```
   # /opt/kaspersky/kav4fs/bin/kav4fs-control \

   --create-task <имя_задачи> --use-task-type=ODS
   ```

   ID созданной задачи будет отображено в консоли.

4. Добавьте директорию, содержащую файл *eicar.com*, в область проверки созданной задачи с помощью следующей команды:

   ```
   # /opt/kaspersky/kav4fs/bin/kav4fs-control \

   --set-settings <ID_созданной_задачи> \

   ScanScope.AreaPath.Path=<путь_к_директории_содержащей_eicar.com>
   ```

5. Запустите созданную задачу с помощью следующей команды:

   ```
   # /opt/kaspersky/kav4fs/bin/kav4fs-control \

   --start-task <ID_созданной_задачи> -W
   ```

6. Просмотрите результаты работы задачи в консоли.

Задача проверки по требованию настроена должным образом, если файл *eicar.com* удален с защищаемого сервера (при условии, что в параметрах задачи указано действие над зараженными объектами **Лечить, если не возможно, удалять**).

Тестовый вирус EICAR и его модификации

Тестовый вирус предназначен для проверки работы антивирусных приложений. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вредоносной программой. Он не содержит программного кода, который может нанести ущерб вашему серверу, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Вы можете загрузить его со страницы http://www.eicar.org/anti_virus_test_file.htm официального сайта организации EICAR.

Перед сохранением файла в директории на сервере убедитесь, что постоянная защита файлов в этой директории отключена.

Файл eicar.com содержит текстовую строку. При проверке файла Антивирус обнаруживает в этой текстовой строке «угрозу», присваивает файлу статус **Зараженный** и выполняет над ним указанное в задаче действие.

Вы также можете использовать файл eicar.com, чтобы проверить реакцию Антивируса при обнаружении объектов других типов. Для этого откройте файл с помощью текстового редактора, добавьте к содержимому файла один из префиксов, перечисленных в следующей таблице, и сохраните файл под новым именем.

Таблица 3. Префиксы

Префикс	Статус файла после проверки и действие Антивируса
Без префикса	Антивирус присваивает объекту статус **Зараженный**.
WARN-	Антивирус присваивает объекту статус **Предупреждение** (код объекта частично совпадает с кодом известной угрозы).
ERRO–	При проверке объекта возникла ошибка. Антивирус Касперского не смог получить доступ к объекту: нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе).
SUSP-	Антивирус присваивает объекту статус **Подозрительный** (обнаружен с помощью эвристического анализатора).
CURE-	Антивирус присваивает объекту статус **Зараженный** и пытается вылечить его. Если лечение успешно, тело вируса заменяется словом «CURE».
CORR–	Антивирус присваивает объекту статус **Поврежденный**.

СХЕМА РАСПОЛОЖЕНИЯ ФАЙЛОВ АНТИВИРУСА КАСПЕРСКОГО

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

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

bin/ – каталог исполняемых файлов всех компонентов Антивируса Касперского:

kav4fs-control – исполняемый файл компонента управления Антивирусом Касперского;

kav4fs-setup.pl – скрипт постинсталляционной настройки Антивируса Касперского;

kav4fs-wmconsole-passwd – исполняемый файл утилиты для изменения пароля доступа к Web Management Console.

lib/ – каталог хранения дополнительных модулей Антивируса Касперского:

samba/ – каталог хранения скомпилированных модулей Samba.

lib64/ – каталог хранения дополнительных 64-битных модулей Антивируса Касперского:

samba/ – каталог хранения скомпилированных 64-битных модулей Samba.

libexec/ – каталог хранения служебных файлов Антивируса Касперского;

src/ – каталог хранения исходного кода модулей Антивируса Касперского:

kernel/ – каталог хранения библиотек модуля антивирусного ядра Антивируса Касперского;

samba/ – каталог хранения библиотек Samba-модуля Антивируса Касперского.

/opt/kaspersky/kav4fs/share/doc/ – файлы документации Антивируса Касперского:

LICENSE – лицензионное соглашение.

LICENSE.GPL – лицензионное соглашение для модулей ядра и Samba.

/opt/kaspersky/kav4fs/share/man/ – каталог хранения man-файлов.

/opt/kaspersky/kav4fs/share/snmp-mibs/ – каталог хранения mib-файлов Антивируса Касперского.

/etc/init.d/ – директория, содержащая скрипты управления службами Web Management Console и Kaspersky Lab Framework:

kav4fs-wmconsole – скрипт управления службой Web Management Console;

kav4fs-supervisor – скрипт управления службой Kaspersky Lab Framework.

/etc/opt/kaspersky/ – каталог, содержащий конфигурационные файлы Web Management Console и Kaspersky Lab Framework

kav4fs-wmconsole.conf – конфигурационный файл Web Management Console;

kav4fs-supervisor.conf – конфигурационный файл Kaspersky Lab Framework.

/var/opt/kaspersky/kav4fs/ – каталог данных Антивируса Касперского:

db/ – базы данных Антивируса Касперского;

update/ – каталог хранения обновлений Антивируса Касперского;

quarantine/ – хранилище карантина.

/var/log/kaspersky/kav4fs/ – каталог хранения лог-файлов Антивируса Касперского;

/var/run/kav4fs/ – каталог хранения служебных файлов Антивируса Касперского.

Для подключения справочной системы Антивируса Касперского (manual pages) добавьте в конфигурационный файл оболочки следующие строки:

```
MANPATH="$MANPATH:/opt/kaspersky/kav4fs/share/man/:"

export MANPATH
```

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

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

kav4fs-control – исполняемый файл компонента управления Антивирусом Касперского;

kav4fs-setup.pl – скрипт постинсталляционной настройки Антивируса Касперского;

kav4fs-wmconsole-passwd – исполняемый файл утилиты для изменения пароля доступа к Web Management Console.

/usr/local/lib/kaspersky/kav4fs/ – каталог хранения дополнительных модулей Антивируса Касперского:

samba/ – каталог хранения скомпилированных модулей Samba.

lib64/ – каталог хранения дополнительных 64-битных модулей Антивируса Касперского:

samba/ – каталог хранения скомпилированных 64-битных модулей Samba.

libexec/ – каталог хранения служебных файлов Антивируса Касперского;

src/ – каталог хранения исходного кода модулей Антивируса Касперского:

kernel/ – каталог хранения библиотек модуля антивирусного ядра Антивируса Касперского;

samba/ – каталог хранения библиотек Samba-модуля Антивируса Касперского.

/usr/local/share/doc/kav4fs/ – файлы документации Антивируса Касперского:

LICENSE – лицензионное соглашение.

LICENSE.GPL – лицензионное соглашение для модулей ядра и Samba.

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

/usr/local/share/kav4fs/snmp-mibs/ – каталог хранения mib-файлов Антивируса Касперского.

/usr/local/etc/rc.d/ – директория, содержащая скрипты управления службами Web Management Console и Kaspersky Lab Framework:

kav4fs-wmconsole – скрипт управления службой Web Management Console;

kav4fs-supervisor – скрипт управления службой Kaspersky Lab Framework.

/usr/local/etc/kaspersky/ – каталог, содержащий конфигурационные файлы Web Management Console и Kaspersky Lab Framework

kav4fs-wmconsole.conf – конфигурационный файл Web Management Console;

kav4fs-supervisor.conf.default – конфигурационный файл Kaspersky Lab Framework.

/var/db/kaspersky/kav4fs/ – каталог данных Антивируса Касперского:

db/ – базы данных Антивируса Касперского;

update/ – каталог хранения обновлений Антивируса Касперского;

quarantine/ – хранилище карантина.

/var/log/kaspersky/kav4fs/ – каталог хранения лог-файлов Антивируса Касперского;

/var/run/kav4fs/ – каталог хранения служебных файлов Антивируса Касперского.

Для подключения справочной системы Антивируса Касперского (manual pages) добавьте в конфигурационный файл /etc/manpath.config следующие строки:

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

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. 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 тысячи 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. Основной продукт 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 мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), 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 технической поддержкой на нескольких языках.

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.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)