ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского для FIREWALL Версия 4.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

АНТИВИРУС КАСПЕРСКОГО ДЛЯ FIREWALL

Руководство пользователя

Тел. (095)797-87-00 • Факс (095)797-87-00
Посетите наш WEB-сайт: http://www.kaspersky.ru/

Дата редакции: март 2002

Содержание

Уважаемый покупатель!

Мы благодарим Вас за то, что Вы выбрали Антивирус Касперского — эффективную защиту компьютера от вирусов. Лучшие в мире эксперты долго работали над этим продуктом, чтобы удовлетворить взыскательным требованиям пользователей. Выбирая наше программное обеспечение, Вы получаете непревзойденную антивирусную защиту.

Наша компания всегда думает о том, чтобы сделать программные продукты проще и доступнее для наших клиентов, не снижая при этом их функциональность. Высокий уровень антивирусной защиты, эвристический анализатор кода, возможность проверки всех известных почтовых форматов, проверка упакованных файлов, удобные инструменты управления компонентами — лишь немногие преимущества, которые предоставляет Антивирус Касперского. Плюс к этому: круглосуточная техническая поддержка, информационное обеспечение, персональный подход к каждому клиенту, а также незамедлительная реакция на появление новых вирусов.

Мы высоко ценим доверие, которое Вы оказали нашим антивирусным продуктам, и надеемся, что Вы найдете их высокоэффективными и полезными.

Лаборатория Касперского

Глава

1

1. Антивирус Касперского для Firewall

Что такое Антивирус Касперского для Firewall?
Комплект поставки.

1.1. Назначение и основные функции

Антивирус Касперского для Firewall является специальным встраиваемым модулем, осуществляющим централизованную антивирусную фильтрацию данных, которые проходят через брэндмауэры, поддерживающие протокол обмена данных CVP (Content Vectoring Protocol).

Антивирус Касперского для Firewall создан на основе антивирусного ядра, использующегося в других продуктах компании. Применение Антивируса Касперского для Firewall позволяет защитить рабочие места пользователей от заражения вирусами, поступающими через сетевой шлюз из Интернета.

Антивирус Касперского для Firewall устанавливается на любом компьютере, на котором установлена одна из следующих ОС: Windows NT Server, Windows 2000 Server, Windows 2000 Advansed Server, Windows NT Workstation, Windows 2000 Professional, и работает с брэндмауэрами CheckPoint независимо от операционной системы, в которой они работают. Поступающие данные передаются от брэндмауэра в программу Антивирус Касперского для Firewall по протоколу TCP/IP, сортируются по протоколам SMTP, FTP и HTTP, проходят проверку на присутствие в них вирусов и возвращаются в брэндмауэр с флагом, отражающим результат проверки. Если необходимо ускорить работу, для сканирования трафиков SMTP, FTP и HTTP можно использовать разные рабочие станции.

Программа Антивирус Касперского для Firewall позволяет:

- В масштабе реального времени обнаруживать и удалять все типы вредоносных кодов из трафика, проходящего через Ваш брэндмауэр по протоколам HTTP, FTP и SMTP.
- Проверять на наличие вирусов архивированные и упакованные файлы, электронную почту.
- Эвристический анализатор кода и функция избыточного сканирования позволяют защитить локальную сеть от проникновения даже неизвестных вирусов.
- Указать в настройках специальную карантинную директорию, куда будут помещаться все зараженные и подозрительные объекты, обнаруженные в потоке данных из Интернета. Обо всех попытках проникновения вирусов в сеть Антивирус Касперского для Firewall будет сообщать на указанный адрес электронной почты.
- Вести и при необходимости просматривать подробный отчет обо всех действиях программы, а также статистику обнаруженных вирусных атак.

- Менять любые настройки программы без ее дополнительной перезагрузки. Все изменения вступают в силу сразу же после их подтверждения.

🗁 Протокол обмена CVP (Content Vectoring Protocol) был создан компанией Check Point Software Technologies в рамках открытой платформы безопасности для предприятий OPSEC (Open Platform for Secure Enterprise Connectivity. Протокол обмена CVP позволяет «состыковать» брэндмауэр с другими программами.

Программа разработана для брэндмауэра Check Point Firewall-1 версии 3.0, 4.0, 4.1.

1.2. Антивирус Касперского для Firewall: защита локальной сети от проникновения вирусов

В настоящее время все большее число крупных, средних и малых предприятий обеспечивают своих сотрудников доступом к Интернету. Это приводит, в частности, к тому, что вероятность занесения компьютерного вируса из глобальной сети в корпоративную растет день ото дня. По данным International Computer Security Association (ICSA), практически все средние и крупные предприятия подвергались вирусным атакам (1998 Virus Prevalence Survey); закономерно, что самым распространенным посредником при заражении системы вирусами являются сообщения электронной почты.

Сегодня основной точкой входа в корпоративную сеть для компьютерных вирусов является Интернет-шлюз корпорации. Большинство администраторов заботится о защите вверенных им файл-серверов и рабочих станций, но выходы в Интернет они часто оставляют незащищенными, надеясь на то, что от вирусов их предохранит брэндмауэр. К сожалению, брэндмауэры обращают внимание только на то, от-

куда поступил тот или иной файл, что делает их слабо вооруженными против вирусов. Однако интеграция антивирусного продукта типа Kaspersky Anti-Virus с архитектурой OPSEC позволяет компаниям определить такую внутреннюю политику безопасности, при которой вирусы останавливаются прежде, чем они успевают добраться до рабочих мест пользователей.

Для защиты от вирусов используется онлайновый сканер Антивирус Касперского для Firewall. Поступающие из Интернета данные передаются от брэндмауэра в Антивирус Касперского для Firewall по протоколу TCP/IP, проходят проверку на предмет наличия вирусов и возвращаются в брэндмауэр с флагом, отражающим результат сканирования.

Антивирус Касперского для Firewall использует все возможности брэндмауэра Firewall-1 для регистрации событий, а также ведет свои журналы, где регистрирует результаты сканирования. Эти данные представляют собой важнейшую информацию, необходимую для определения источника вирусов. С их помощью можно повысить степень защиты, например запретив все попытки загрузить файлы с такого «проблемного узла».

Разные серверы нуждаются в различных средствах антивирусной защиты. Так, HTTP является носителем элементов ActiveX и Java-аплетов. Они могут содержать вирусы, которые необходимо удалить, прежде чем они достигнут браузера. Для защиты электронной почты (SMTP) сканирующая программа должна открывать каждую базу данных и искать любые скрытые вирусы, присоединенные к сообщению, до того как получатель прочтет или переадресует его. Наконец, FTP представляет собой способ загрузки приложений, которые могут быть поражены вирусом. Антивирус Касперского для Firewall обеспечивает серверы разного типа требуемыми для них средствами защиты.

Антивирус Касперского для Firewall сочетает в себе такие качества, как высокая скорость сканирования и надежность полученного результата. Последнее качество гарантируется возможностью регулярного обновления через Интернет базы данных вирусов; обновление осуществляется одним нажатием кнопки.

1.3. Что нового

В данной версии программы пользователям предоставлена возможность оптимизировать работу Антивируса Касперского для Firewall с проверяемыми файлами (процент от общего размера файла, передаваемый пользователю без проверки).

Кроме того, в новой версии добавилась возможность просматривать количество одновременно запущенных сессий и принудительно завершать в случае необходимости.

В комплект нововой версии входит также модуль Kaspersky Anti-Virus for Firewall Agent, позволяющий в случае сбоя в работе Антивируса Касперского для Firewall вызывать какую-либо вспомогательную программу или перезапускать Антивирус Касперского для Firewall.

1.4. Комплект поставки

1.4.1. Что входит в комплект поставки

В комплект поставки программного продукта входит следующее:

- лицензионное соглашение;
- запечатанный конверт с установочным CD-диском, на котором записана программа;
- руководство пользователя;
- регистрационная карточка.

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

1.4.2. Лицензионное соглашение

Лицензионное соглашение — это юридическое соглашение между Вами и ЗАО "Лаборатория Касперского", в котором указано, на каких условиях Вы можете пользоваться купленным Вами продуктом.

🗁 Внимательно прочитайте лицензионное соглашение!

Если Вы не согласны с условиями лицензионного соглашения, Вы можете вернуть коробку с Антивирусом Касперского для Firewall дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с дискетами должен оставаться запечатанным.

Открывая запечатанный пакет с дискетами, Вы принимаете все условия лицензионного соглашения.

1.4.3. Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью); телефон, адрес электронной почты, и пошлите ее дистрибьютору, у которого Вы приобрели продукт.

Если у Вас изменится почтовый/электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отослан 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 и получение обновлений в течение срока подписки. Кроме того, зарегистри-

рованным пользователям высылается информация о выходе новых программных продуктов ЗАО "Лаборатория Касперского".

1.5. Сервис для зарегистрированных пользователей

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

Приобретя подписку, Вы получаете статус зарегистрированного пользователя программы и в течение срока ее действия получаете следующие услуги:

- еженедельное обновление антивирусных баз;
- предоставление новых версий данного продукта;
- консультации по вопросам, связанным с эксплуатацией данного продукта, оказываемые по телефону, электронной почте и в нашем офисе;
- оповещение о выходе новых продуктов Лаборатории Касперского и о новых вирусах, появляющихся в мире.

🗁 Дополнительная информация о сервисных услугах приведена в файле README.TXT.

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

1.6. Какие сведения содержатся в документации

В настоящей документации содержатся сведения, необходимые для установки и эксплуатации продукта. Описаны концепции, заложенные в основу программы, и способ ее применения. Приведены рекомендации по настройке.

Глава

2

2. Установка программы

Процедура установки программы.
*Файл *.KEY.*

2.1. Системные требования

Для корректной работы Антивируса Касперского для Firewall требуется:

- IBM PC или стопроцентно-совместимый компьютер, процессор Pentium 133 МГц;
- 64 Мб оперативной памяти;
- 100 Мб на жестком диске (для эффективной работы сервера рекомендуется иметь 500 Мб на жестком диске);
- CD-ROM (если комплект поставляется на CD-дисках, а не на дискетах);

- Одна из следующих ОС: Windows NT Server, Windows 2000 Server, Windows NT Workstation, Windows 2000 Professional, Windows 2000 Advanced Server.

Антивирус Касперского для Firewall устанавливается на любом компьютере, входящем в данную сеть и работает с брэндмауэрами Check Point Firewall-1, независимо от ОС, в которой они работают. Если нужно этот сервер разгрузить, для сканирования трафиков SMTP, FTP и HTTP можно использовать отдельный компьютер.

2.2. Процедура установки

2.2.1. Первая установка

☞ **Чтобы установить программу Антивирус Касперского для Firewall на компьютер,**

1. Вставьте CD-ROM с программой в устройство чтения компакт-дисков.

2. Запустите программу установки `setup.exe`.

3. После этого будет запущена процедура установки (рис. 1). Внимательно следуйте ее инструкциям.

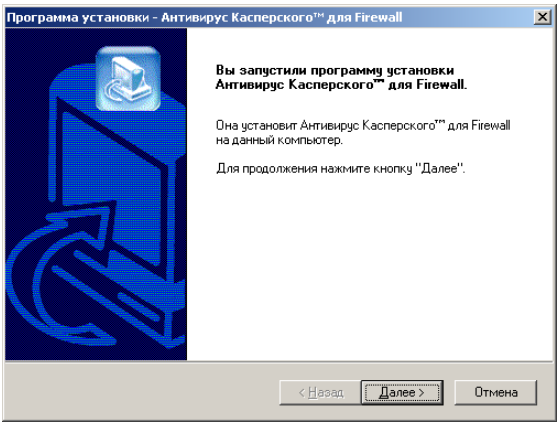

Рисунок 1. Диалоговое окно запуска программы установки

4. Ознакомившись с этим диалоговым окном, нажмите на кнопку **Далее**. После этого на экране отобразится диалоговое окно **Лицензионное соглашение** (рис. 2).

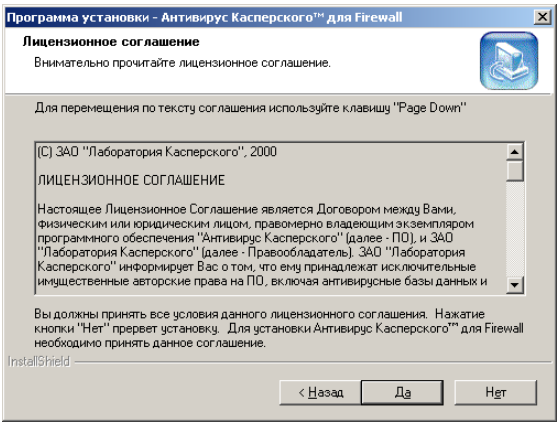

Рисунок 2. Диалоговое окно **Лицензионное соглашение**

5. Прочтите лицензионное соглашение, после чего, если Вы согласны с условиями лицензионного соглашения, нажмите на кнопку **Да**. В противном случае нажмите на кнопку **Нет** и прервите процесс установки. После нажатия на кнопку **Да** на экране отобразится диалоговое окно **Сведения о пользователе** (рис. 3).

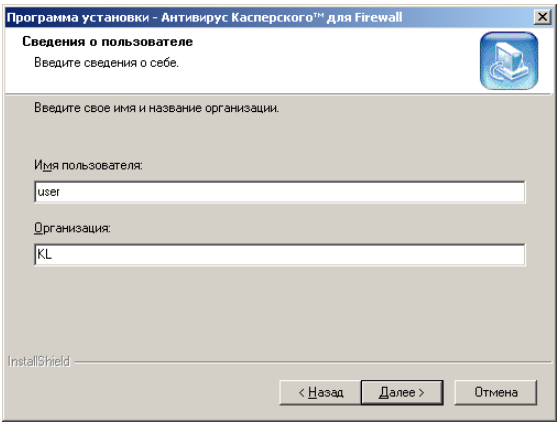

Рисунок 3. Диалоговое окно **Сведения о пользователе**

6. В поле **Имя пользователя** введите имя пользователя, а в поле **Организация** — название организации. После заполнения этих полей нажмите на кнопку **Далее**. На экране отобразится диалоговое окно **Выбор папки назначения** (рис. 4).

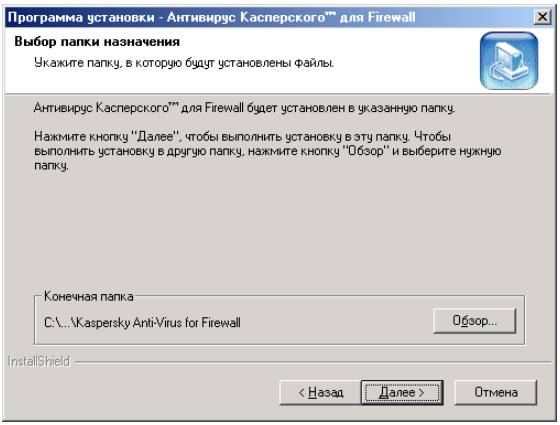

Рисунок 4. Диалоговое окно **Выбор папки назначения**

7. В этом диалоговом окне выберите каталог для установки Антивируса Касперского для Firewall:

   - Для этого нажмите на кнопку **Обзор** и в появившемся на экране стандартном диалоговом окне **Выбор папки** (рис. 5) укажите путь к нужной папке.
   - Нажмите на кнопку **ОК**.
   - В появившемся вновь на экране диалоговом окне **Выбор папки назначения** нажмите на кнопку **Далее**.

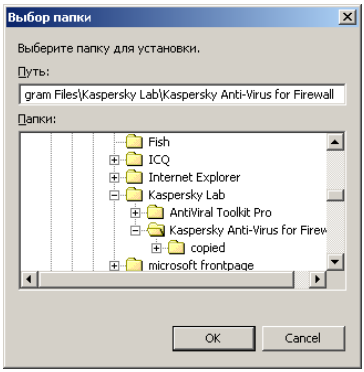

Рисунок 5. Диалоговое окно **Выбор папки**

8. В появившемся после этого на экране диалоговом окне **Выбор папки** (рис. 6) укажите имя папки в стандартном меню **Программы**, в которой будет расположен значок для запуска Антивируса Касперского для Firewall. Нажмите на кнопку **Далее**.

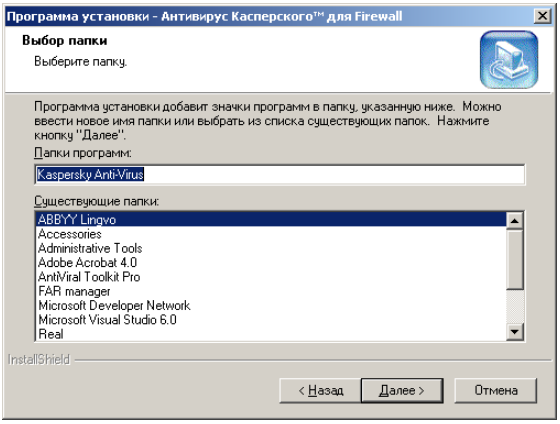

Рисунок 6. Диалоговое окно **Выбор папки**

9. После этого на экране отобразится диалоговое окно **Вид установки** (рис. 7). В этом диалоговом окне выберите:

   - **Выборочная** — если необходимо выбрать устанавливаемые компоненты из пакета Антивирус Касперского для Firewall;
   - **Обычная** — если необходимо установить все компоненты программы. При этом будет пропущен шаг 11 и 12 данной процедуры.

10. Нажмите на кнопку **Далее**.

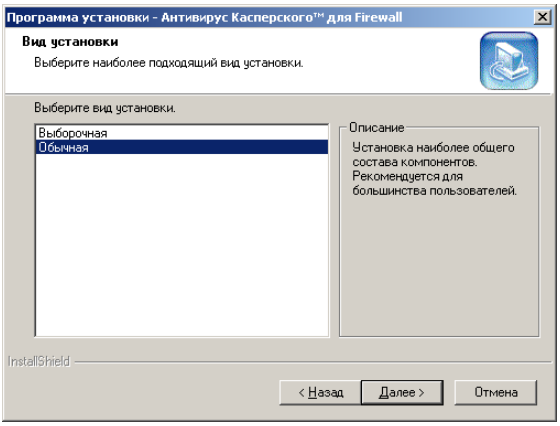

Рисунок 7. Диалоговое окно **Вид установки**

11. Если на предыдущем шаге был выбран режим выборочной инсталляции, на экране отобразится диалоговое окно **Выбор компонентов** (рис. 8). В этом диалоговом окне можно выбрать компоненты, которые необходимо установить. По умолчанию выбраны все компоненты. Для того чтобы включить/исключить какой-либо из компонентов, достаточно щелкнуть мышью по соответствующей строке. После выбора всех компонентов, которые необходимо установить, нажмите на кнопку **Далее**.

Если из установки будет исключен компонент Kaspersky Anti-Virus for Firewall, то в процессе установки будут пропущены шаги 13 и 14.

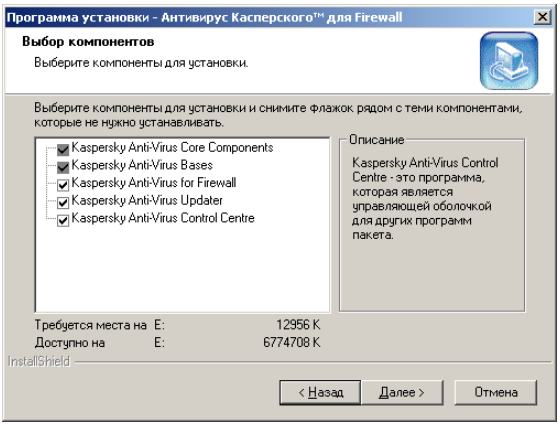

Рисунок 8. Диалоговое окно **Выбор компонентов**

12. После этого на экране отобразится диалоговое окно **Выбор папки назначения** (рис. 9). В этом диалоговом окне выберите каталог, в котором будут располагаться файлы с отчетами о работе Антивируса Касперского для Firewall:

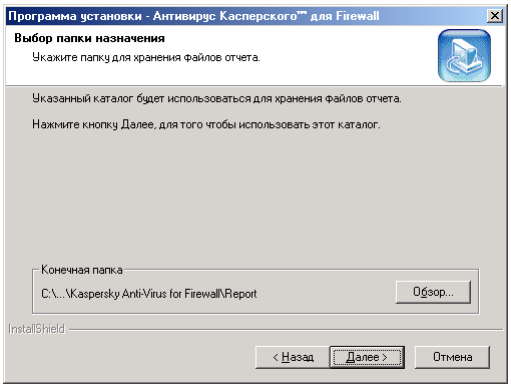

Рисунок 9. Диалоговое окно **Выбор папки назначения**

13. После этого на экране отобразится диалоговое окно **Начало копирования файлов** (рис. 10). Прочтите информацию об инсталляции. Для продолжения инсталляции нажмите на кнопку **Далее**. После этого начнется процесс копирования файлов на жесткий диск компьютера (рис. 11).

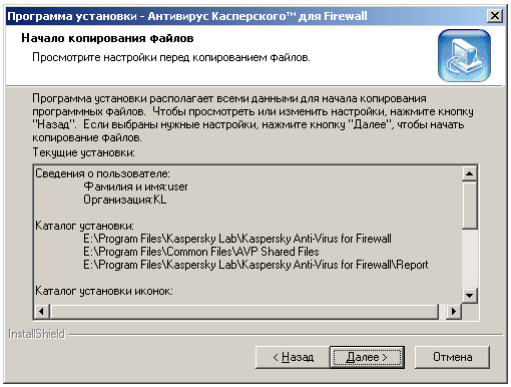

Рисунок 10. Диалоговое окно **Начало копирования файлов**

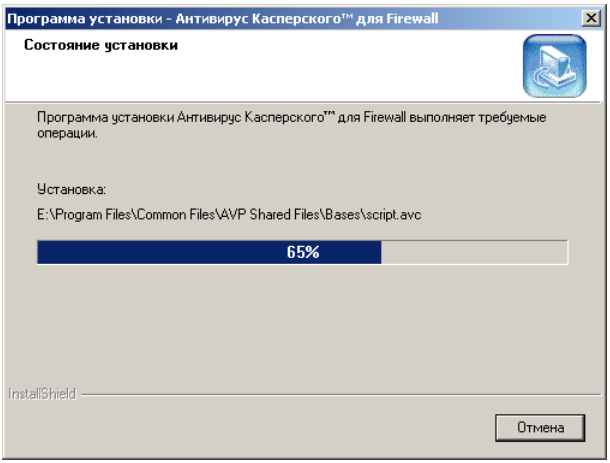

Рисунок 11. Диалоговое окно **Состояние установки**

14. После завершения процедуры установки на экране отобразится диалоговое окно **Конфигурация** (рис. 12). В поле **Локальный IP адрес** этого диалогового окна следует указать локальный IP-адрес компьютера, на который производится установка. В поле **CVP порт** — номер соответствующего порта.
    Если при работе с брэндмауэром необходима дополнительная аутентификация, необходимо установить во включенное положение переключатель **Аутентификация**, а в поле **Аутентификационный CVP порт** указать необходимый номер порта. Для продолжения инсталляции нажмите на кнопку **Далее**.

Все поля данного диалогового окна не обязательны для заполнения, по умолчанию будут использоваться соответствующие параметры из настроек рабочей станции.

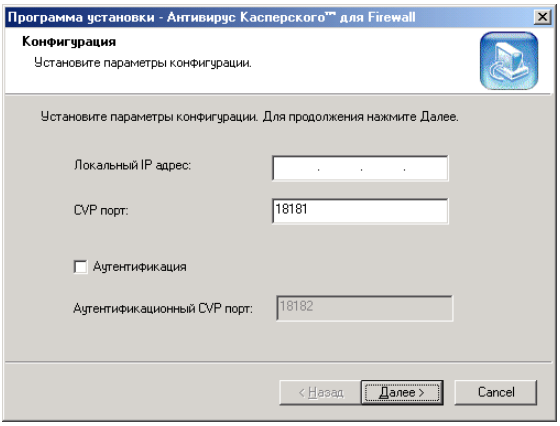

Рисунок 12. Диалоговое окно **Конфигурация**

15. В появившемся после этого на экране диалоговом окне **Выбор папки назначения** (рис. 13) необходимо указать папку, в которой будут храниться временные файлы, создаваемые в процессе работы Антивируса Касперского для Firewall. Нажмите на кнопку **Далее**.

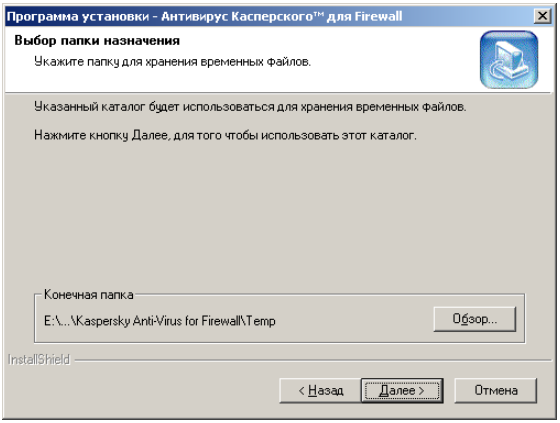

Рисунок 13. Диалоговое окно **Выбор папки назначения**

16. В появившемся после этого на экране диалоговом окне **Ключевой файл** (рис. 14) необходимо указать имя файла-ключа (см. п. 2.3) и путь к нему. Если этот файл располагается в папке, из которой производится установка, он автоматически отобразится в списке **Список ключевых файлов**. Если файл-ключ расположен в какой-либо другой папке, нажмите на кнопку **Добавить** и в появившемся на экране стандартном диалоговом окне укажите имя и путь к файлу-ключу. При необходимости одновременно можно использовать несколько файлов-ключей. После того как в список будут внесены все необходимые файлы-ключи, нажмите на кнопку **Далее**.

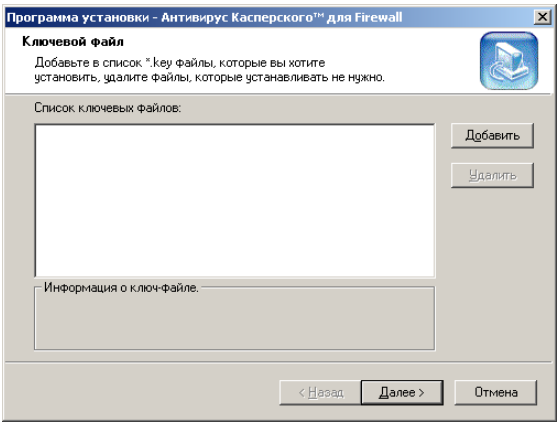

Рисунок 14. Диалоговое окно **Ключевой файл**

17. После завершения установки программы на экране отобразится диалоговое окно **Завершение установки** (рис. 15). Установите во включенное состояние переключатели, соответствующие компонентам, которые необходимо запустить непосредственно после завершения установки, и нажмите на кнопку **Готово**.

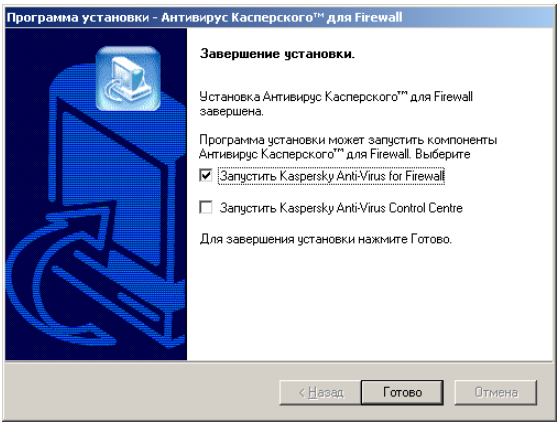

Рисунок 15. Диалоговое окно **Завершение установки**

2.2.2. Повторная установка

Если в начале процесса установки программа обнаружит на компьютере ранее установленную версию программы Антивирус Касперского для Firewall, на экране отобразится диалоговое окно **Добро пожаловать** (рис. 16), в котором можно выбрать один из следующих режимов:

- **Изменить** — добавить новые компоненты программы к ранее установленным;
- **Исправить** — переустановить все компоненты программы;
- **Удалить** — деинсталлировать программу Антивирус Касперского для Firewall с компьютера (см. п. 2.2.3).

Для того чтобы выбрать одно из этих действий, необходимо установить во включенное состояние соответствующую кнопку выбора и нажать на кнопку **Далее**.

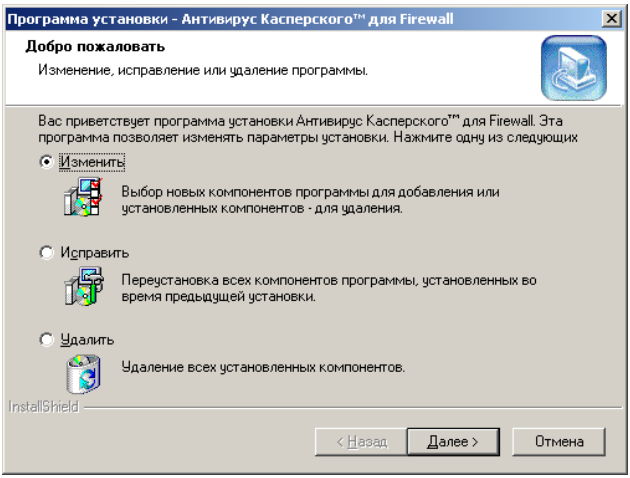

Рисунок 16. Диалоговое окно **Добро пожаловать**

Если был выбран режим **Изменить**, после нажатия на кнопку **Далее** на экране отобразится диалоговое окно **Выбор компонентов** (рис. 17), в котором можно выбрать необходимые компоненты, установив соответствующие им переключатели во включенное состояние.

После выбора необходимых компонентов нажмите на кнопку **Далее**. На экране последовательно отобразятся диалоговые окна **Состояние установки** (см. рис. 11) и **Завершение установки** (см. рис. 15).

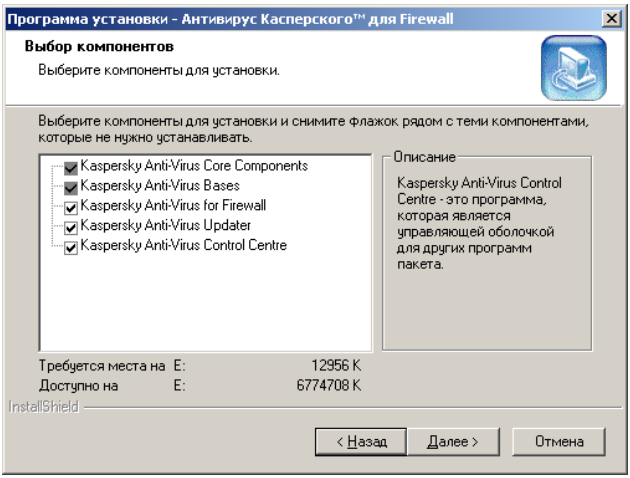

Рисунок 17. Диалоговое окно **Выбор компонентов**

Если был выбран режим **Исправить**, после нажатия на кнопку **Далее** на экране отобразится диалоговое окно **Подтверждение переустановки файлов** (рис. 18), в котором можно выбрать способ переустановки:

- **OK** — обновление ранее установленных компонентов;
- **Cancel** — отказ от переустановки.

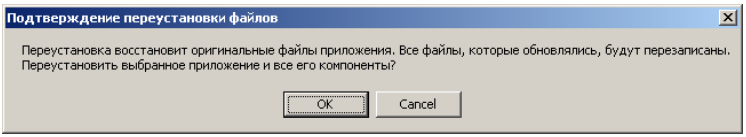

Рисунок 18. Диалоговое окно **Подтверждение переустановки файлов**

2.2.3. Удаление программы

Если по каким-либо причинам необходимо деинсталлировать программу Антивирус Касперского для Firewall, в диалоговом окне **Добро пожаловать** (см. рис. 16) выберите режим **Удалить** и нажмите на кнопку **Далее**.

После этого на экране отобразится диалоговое окно подтверждения удаления. Для того чтобы запустить процедуру деинсталляции, нажмите на кнопку **ОК**. После этого начнется процесс удаления файлов программы с жесткого диска компьютера.

Если в процессе деинсталляции программа обнаружит файлы, которые могут использоваться другими программами, на экране отобразится диалоговое окно подтверждения удаления файла. Для того чтобы удалить данный файл, нажмите на кнопку **Да**.

2.3. Файл *.KEY

Файл *.KEY является Вашим личным "ключом", в котором находится вся служебная информация, необходимая для работы Антивируса Касперского для Firewall, а именно:

- координаты продавца данной версии (название фирмы, адреса, телефоны);
- информация о поддержке (кто осуществляет и где можно ее получить);
- дата выпуска продукта;
- подтверждение, что данная версия является зарегистрированной;
- срок действия данной лицензии.

- При отсутствии этого файла программа будет работать как демонстрационная версия (в ней будет отсутствовать возможность лечения зараженных файлов).

- Следует особо следить за сохранностью файла *.KEY. Для этого, например, рекомендуется создать его резервную копию.

Глава

3

3. Подготовка программы к работе

Настройка брэндмауэра CheckPoint для работы с Антивирусом Касперского для Firewall

3.1. Связывание брэндмауэра и Антивируса Касперского для Firewall

Для того чтобы обеспечить совместную работу Антивируса Касперского для Firewall и программы-брэндмауэра в последней необходимо произвести настройку соответствующих параметров.

3.2. Добавление CVP-сервера

В первую очередь необходимо создать новый CVP-сервер.

☞ **Для того чтобы добавить CVP-сервер,**

1. В меню **Manage** программы-брэндмауэра выберите пункт **Servers**. После этого откроется диалоговое окно **Servers** (рис. 19), в котором отражены существующие на данный момент CVP-серверы.

2. Нажмите на кнопку **New**, чтобы добавить новый CVP-сервер. В раскрывающемся списке выделите пункт **CVP** (рис. 20).

3. Для того чтобы новый CVP-сервер начал корректно работать, необходимо заполнение реквизитов добавляемого сервера.
   В диалоговом окне **CVP Server Properties** (рис. 21) введите в поле **Name** любое понятное для Вас название для добавляемого сервера. Желательно также, чтобы это название отражало функциональную нагрузку добавленного сервера, так что в случае Вашего отсутствия другой сотрудник, решивший изменить установки, смог легко опознать его по названию. В раскрывающемся списке **Host** выберите название компьютера, на котором установлен Антивирус Касперского для Firewall. В раскрывающемся списке **Service** выделите пункт с названием **FW1_cvp**. Нажмите на кнопку **OK**.

4. Результат добавления CVP-сервера перед Вами.
   В диалоговом окне **Servers** появится новый сервер с тем названием, которое Вы задали (рис. 22). Нажмите на кнопку **Close**.

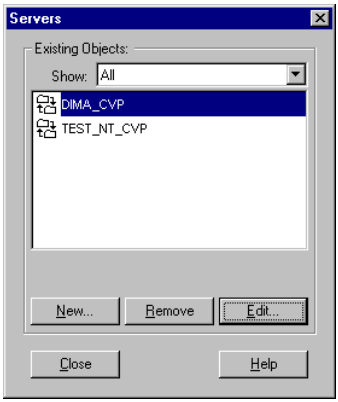

Рисунок 19. Диалоговое окно **Servers**

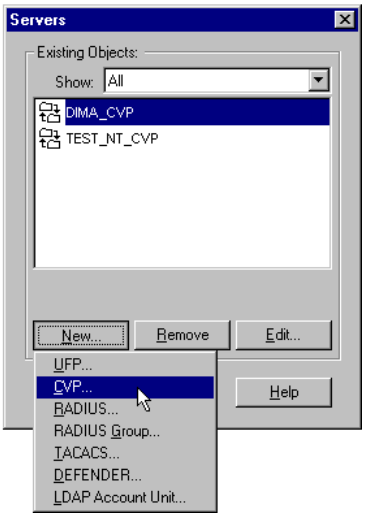

Рисунок 20. Добавление нового сервера в диалоговом окне **Servers**

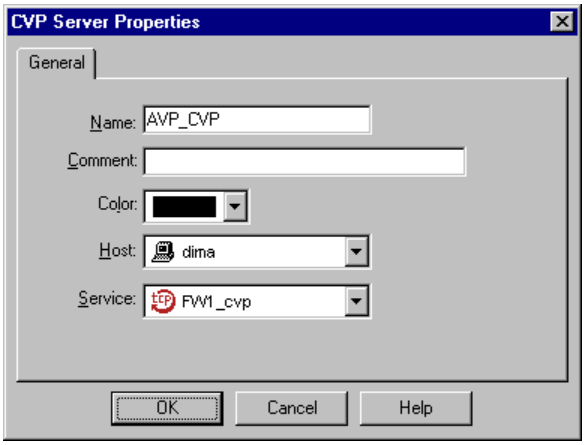

Рисунок 21. Диалоговое окно **CVP Servers Properties**

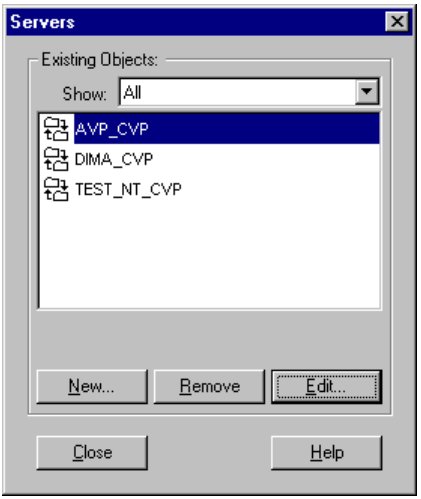

Рисунок 22. Результат добавления CVP-сервера

3.3. Добавление ресурсов

Программа Антивирус Касперского для Firewall может отслеживать информационные потоки, передаваемые по трем протоколам: HTTP, SMTP и FTP. По Вашему усмотрению Вы можете включить проверку по всем этим протоколам либо выборочно.

3.3.1. Добавление HTTP-ресурса

☞ **Для того чтобы добавить HTTP-ресурс,**

1. В меню **Manage** программы-брэндмауэра выберите пункт **Resources**, появится диалоговое окно **Resources** (рис. 23).

2. В появившемся диалоговом окне **Resources** нажмите на кнопку **New**. В раскрывающемся списке выделите пункт **URL** (рис. 24).

3. В появившемся диалоговом окне **URL Defition** (рис. 25) при активной закладке **General** введите в поле **Name** любое имя, например `KAV_HTTP`. Желательно, чтобы это имя было содержательным, что облегчит работу Вам и другим сотрудникам.

4. Переключитесь на закладку **Match** и в разделе **Schemes** установите переключатель **HTTP** во включенное состояние (рис. 26). Тем самым Вы подтверждаете, что введенное ранее имя ресурса является именем HTTP-ресурса.

5. Переключитесь на закладку **Action**. В группе полей CVP в раскрывающемся списке Server выберите название добавленного Вами CVP-сервера (`KAV_CVP`), поскольку Вы создаете установки конкретно для него.
   У Вас есть возможность установить одну из кнопок выбора — **None**, **Read Only**, **Read/Write** — во включенное состоя-

ние (рис. 27). Каждая кнопка выбора дает следующие возможности: **None** — ничего не делать, т.е. ничего не отдавать для антивирусной проверки серверу KAV_CVP; **Read Only** — давать только на чтение; **Read/Write** — позволять изменять переданные серверу KAV_CVP-пакеты (т.е. позволять заменять зараженные файлы на вылеченные). Установите кнопку выбора **Read/Write** во включенное состояние. Нажмите на кнопку **OK**.

Если у Вас возникли проблемы с маршрутизацией информации (какая-то информация не приходит или не отправляется), Вы можете проверить, происходит ли это в результате работы Антивируса Касперского для Firewall. Для этого выберите **None** в качестве режима работы сервера (для всех протоколов). Если проблема осталась, то Антивирус Касперского для Firewall не имеет к ней отношения. Если в результате эта проблема исчезла, необходимо обратиться в службу технической поддержки Лаборатории Касперского.

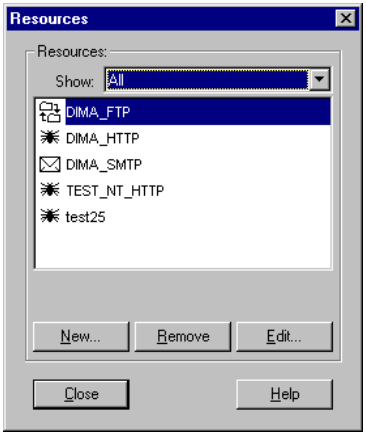

Рисунок 23. Диалоговое окно **Resources**

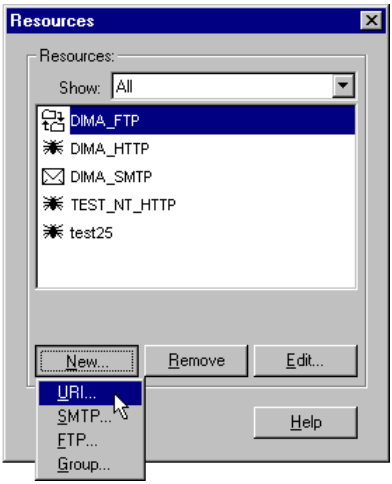

Рисунок 24. Добавление HTTP-ресурса

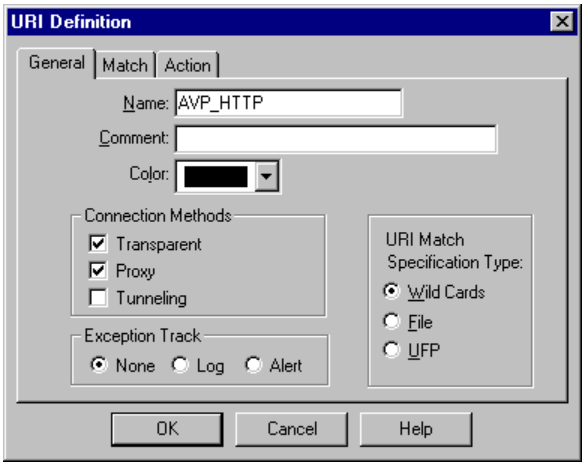

Рисунок 25. Диалоговое окно **URL Definition**

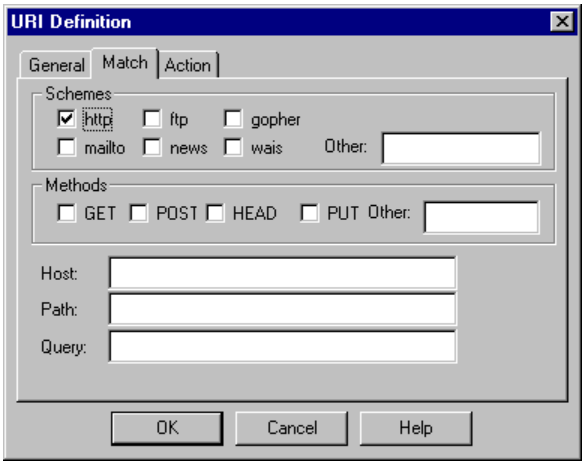

Рисунок 26. Включение переключателя HTTP

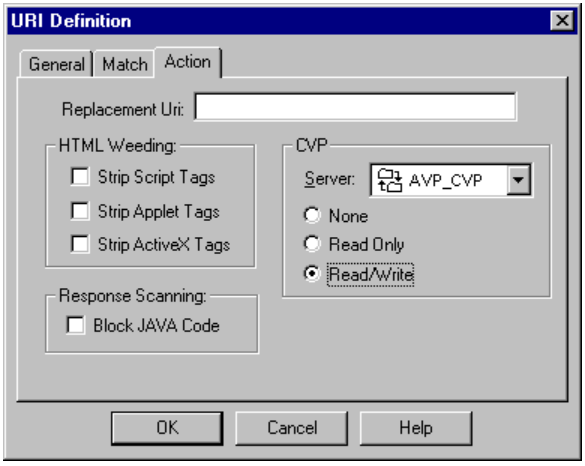

Рисунок 27. Определение режима прохождения информации через Антивирус Касперского для Firewall

3.3.2. Добавление SMTP-ресурса

☞ **Для того чтобы добавить SMTP-ресурс,**

1. В меню **Manage** программы-брэндмауэра выберите пункт **Resources**, появится диалоговое окно **Resources** (рис. 28).

2. В появившемся диалоговом окне **Resources** нажмите на кнопку **New** и в раскрывающемся списке выделите пункт **SMTP**. Откроется диалоговое окно **SMTP Definition** (рис. 29). При активной закладке **General** в поле **Name** введите любое имя, например `KAV_SMTP`.

3. Переключитесь на закладку **Match** (рис. 30) и задайте нужные Вам параметры в полях **Sender** и **Recipient**.

4. Переключитесь на закладку **Action1** (рис. 31) и задайте нужные Вам параметры в полях **Sender**, **Recipient**, **Field** и **Contents**.

5. Переключитесь на закладку **Action2** (рис. 32). В группе полей CVP в раскрывающемся списке Server выделите название добавленного Вами CVP-сервера (`KAV_CVP`). Установите кнопку выбора **Read/Write** во включенное состояние. Нажмите на кнопку **OK**.

Из поля Strip MIME of Type следует удалить значение, присваиваемое ему по умолчанию, и оставить его пустым. В противном случае может происходить утеря файлов, присоединенных к входящим письмам.

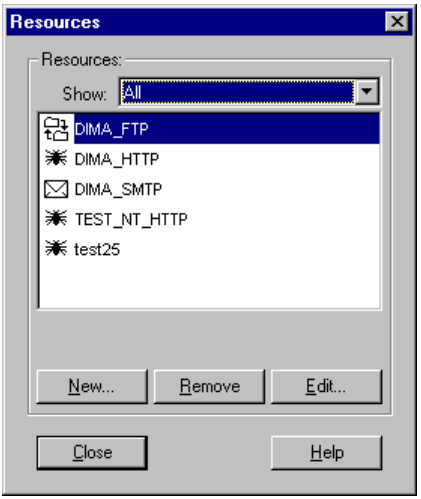

Рисунок 28. Диалоговое окно **Resources**

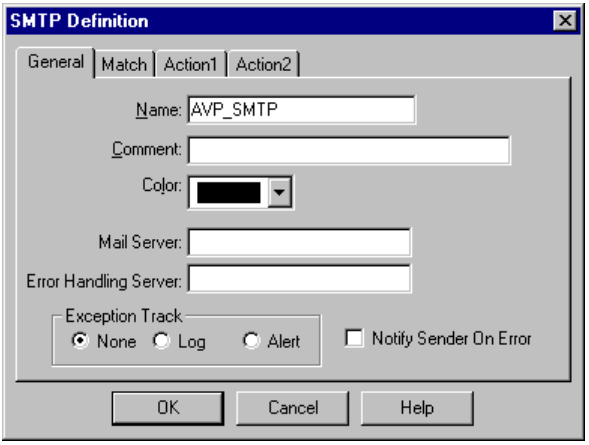

Рисунок 29. Диалоговое окно **SMTP Definition**

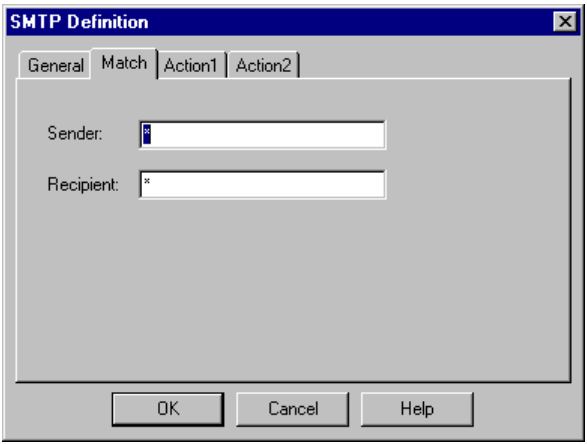

Рисунок 30. Закладка **Match** диалогового окна **SMTP Definition**

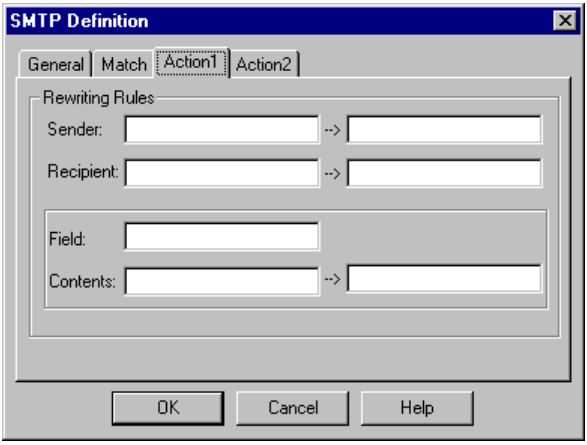

Рисунок 31. Закладка **Action1** диалогового окна **SMTP Definition**

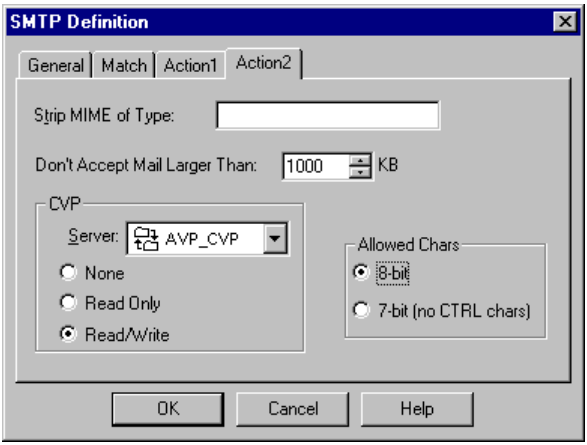

Рисунок 32. Закладка **Action2** диалогового окна **SMTP Definition**

3.3.3. Добавление FTP-ресурса

☞ **Для того чтобы добавить FTP-ресурс,**

1. В меню **Manage** программы-брэндмауэра выберите пункт **Resources**, появится диалоговое окно **Resources** (рис. 33).
2. В появившемся диалоговом окне **Resources** нажмите на кнопку **New** и в раскрывающемся списке выберите пункт **FTP**. Откроется диалоговое окно **FTP Definition** (рис. 34). При активной закладке **General** в поле **Name** введите любое имя, например `KAV_FTP`.
3. Переключитесь на закладку **Match** (рис. 35) и установите переключатели **GET** и **PUT** в нужное Вам положение.
4. Переключитесь на закладку **Action** (рис. 36). В группе полей CVP в раскрывающемся списке Server выделите пункт с названием добавленного Вами CVP-сервера. Установите кнопку выбора **Read/Write** во включенное состояние. Нажмите на кнопку **OK**.

В появившемся диалоговом окне **Resources** Вы можете убедиться в правильности сделанных изменений (рис. 44).

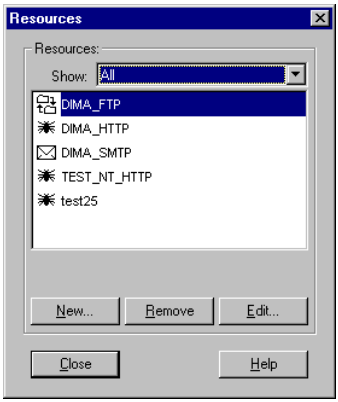

Рисунок 33. Диалоговое окно **Resources**

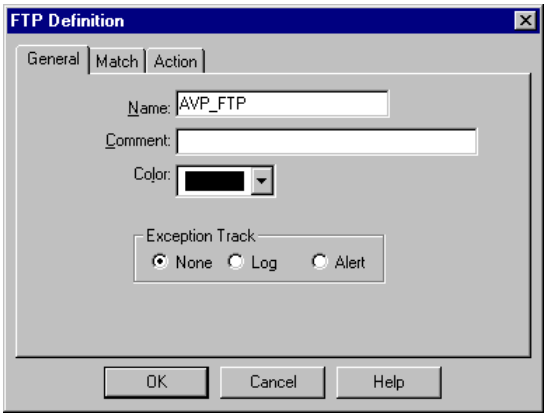

Рисунок 34. Диалоговое окно **FTP Definition**

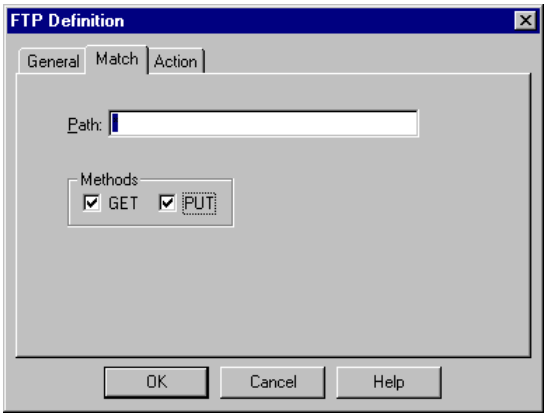

Рисунок 35. Закладка **Match** диалогового окна **FTP Definition**

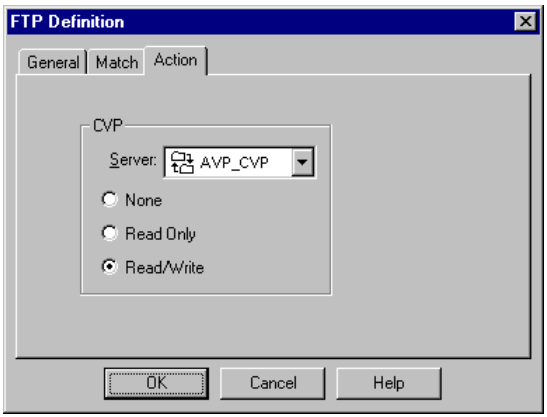

Рисунок 36. Закладка **Action** диалогового окна **FTP Definition**

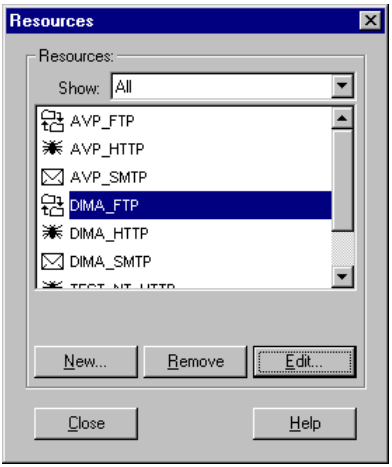

Рисунок 37. Диалоговое окно **Resources** с результатами изменений

3.4. Создание правил

Для того чтобы добавленные ресурсы начали влиять на прохождение информационных потоков, администратор сети должен добавить или отредактировать существующие правила для программы-брэндмауэра.

Ниже приводится пример создания трех правил для трех протоколов (FTP, HTTP, SMTP).

Для того чтобы создать новое правило, нужно щелкнуть правой кнопкой мыши на номере существующего правила. В появившемся динамическом меню необходимо выбрать пункт **Insert rule above** (как в нашем случае) или **Add rule below**.

Рисунок 38. Добавление нового правила

Для того чтобы добавить в правило ранее созданный Вами новый ресурс (см. пп. 3.3.1, 3.3.2, 3.3.3), достаточно просто щелкнуть правой кнопкой мыши в строке нужного правила по ячейке **Service** и в появившемся динамическом меню выбрать пункт **Add With Resource**.

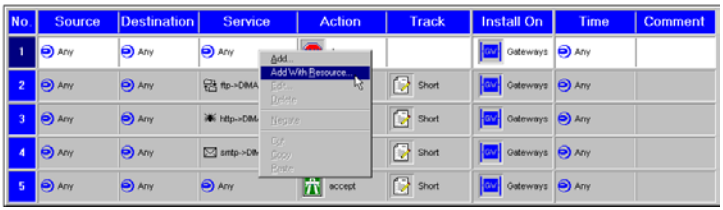

Рисунок 39. Добавление в правило нового ресурса

В появившемся диалоговом окне **Service with Resource** выберите пункт с названием нужного Вам ресурса, в данном случае KAV_FTP. Не забудьте нажать на кнопку **OK**.

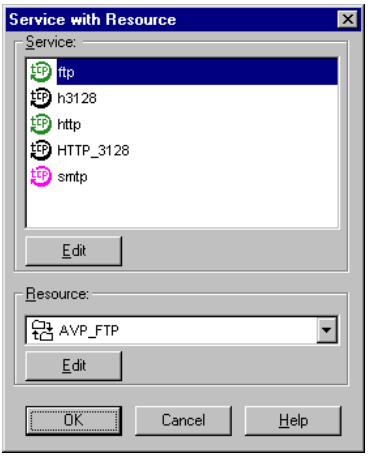

Рисунок 40. Диалоговое окно **Service with Resource**

После добавления в правило какого-либо ресурса, нужно указать программе-брэндмауэру, какие действия проводить с информацией, проходящей по протоколу данного ресурса. Для того чтобы выбрать конкретное действие, нужно щелкнуть правой кнопкой мыши по ячейке **Action**. Если Вы хотите, чтобы данные, проверенные (и, может быть, вылеченные) программой Антивирус Касперского для Firewall продолжили свое движение, то в появившемся динамическом меню выделите пункт **Accept**.

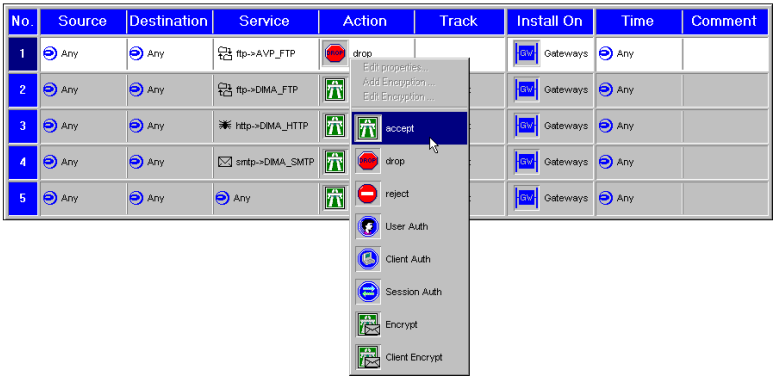

Рисунок 41. Выбор действия

Совершенно аналогично происходит настройка правил для остальных протоколов.

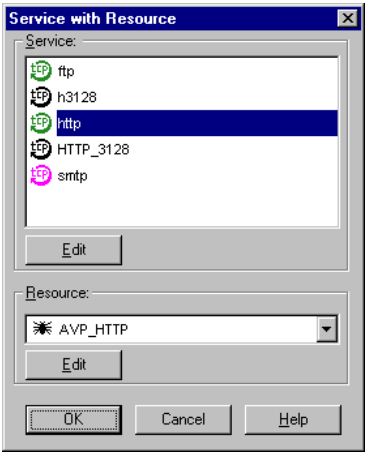

Рисунок 42. Добавление в правило HTTP-ресурса

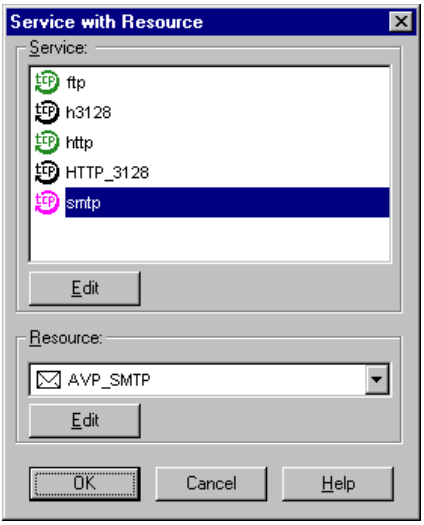

Рисунок 43. Добавление в правило SMTP-ресурса

В окне программы-брэндмауэра отразились сделанные Вами изменения.

Рисунок 44. Результаты добавления правил и ресурсов

3.5. Сохранение настроек

Созданные Вами настройки необходимо сохранить, для того чтобы они вступили в действие.

Для этого в меню **Policy** программы-брэндмауэра выберите пункт **Install**.

Глава

4

4. Запуск и остановка программы

Различные варианты запуска программы Антивирус Касперского для Firewall. Использование ключей.

4.1. Способы запуска программы

4.1.1. Запуск и остановка программы с помощью меню Пуск

Запустить Антивирус Касперского для Firewall можно из группы **Kaspersky Anti-Virus for Firewall**, которая создается при инсталляции программы в стандартном меню MS Windows.

☞ **Чтобы запустить программу Антивирус Касперского для Firewall,**

1. В меню **Пуск** (стандартном меню Windows) выберите пункт **Программы**.

2. В открывшемся меню выберите пункт с названием папки, в которую при инсталляции Вы поместили программу (по умолчанию Kaspersky Anti-Virus for Firewall).

3. В открывшемся меню выберите пункт **Start (Restart) Kaspersky Anti-Virus for Firewall**.

☞ **Чтобы остановить программу Антивирус Касперского для Firewall,**

1. В меню **Пуск** (стандартном меню Windows) выберите пункт **Программы**.

2. В открывшемся меню выберите пункт с названием папки, в которую при инсталляции Вы поместили программу (по умолчанию Kaspersky Anti-Virus for Firewall).

3. В открывшемся меню выберите пункт **Stop Kaspersky Anti-Virus for Firewall**.

4.1.2. Запуск Антивируса Касперского для Firewall из командной строки. Использование ключей

При запуске Антивируса Касперского для Firewall из командной строки существует возможность задавать дополнительные ключи. При этом командная строка может выглядеть так:

```
[Путь к файлу]KAWALL [ключ1] [ключ2]… [ключN]
```

Для запуска используйте команду `KAWALL /START`.

Для остановки — команду `KAWALL /DOWN`, если Вы хотите перед остановкой программы дождаться завершения обработки проверяемых

файлов, и KAWALL /STOP, если Вы хотите остановить программу, прервав обработку проверяемых файлов.

Возможные ключи:

/INSTALL — инсталлировать или переинсталлировать Антивирус Касперского для Firewall в список служб Windows NT.

/REMOVE — деинсталлировать Антивирус Касперского для Firewall из списка служб Windows NT.

/START — запустить или перезапустить Антивирус Касперского для Firewall.

/DOWN[=time, min] — завершить проверку обрабатываемых файлов и остановить работу.

/STOP — остановить работу Антивируса Касперского для Firewall.

/CONFIG[=filename] — перезагрузить файл конфигурации, если новые настройки необходимо загрузить не из файла, используемого по умолчанию; в ключе следует указать имя нового файла.

/RELOAD — перезагрузить антивирусные базы данных.

/STAT — отобразить статистику работы программы.

/RESET — обновить статистику программы.

/INFO — отобразить информацию о программе.

/PURGE — очистить файл отчета программы (см. п. 7.2).

/PLIST — показать список сессий.

/PKILL=<номер> — завершить сессию <номер>.

4.1.3. Запуск Антивируса Касперского для Firewall из Центра Управления

Антивирус Касперского для Firewall, как и все программы, входящие в пакет Kaspersky Anti-Virus, может быть запущен из Центра управления. В Центре Управления можно настроить автоматический запуск Антивируса Касперского для Firewall в нужное время каждый день или через определенные промежутки времени.

Глава

5

5. Настройка параметров работы программы

Настройки программы Антивирус Касперского для Firewall. Задание параметров проверки. Настройки протоколов.

5.1. Параметры проверки

Если Вы хотите изменить параметры работы программы Антивирус Касперского для Firewall, Вы можете произвести ее настройку, то есть указать объекты, которые Вы хотели бы проверить, действия, которые надо совершать с объектами, дополнительные режимы сканирования и т. д.

Настройка может быть осуществлена с помощью Центра Управления или путем редактирования файла конфигурации `kawall.cfg`.

Вы можете использовать различные настройки, сохраняя их в различных файлах настроек. Это может пригодиться, если Вы конфигурируе-

те Антивирус Касперского для Firewall из командной строки. В этом случае впоследствии Вам не придется тратить время на повторную настройку программы, достаточно будет лишь загрузить один из подходящих в данный момент файлов настройки, указав его в ключе `/CONFIG`. Например, `KAWALL/CONFIG[=<filename>]`, где `<filename>` — имя загружаемого файла настройки.

5.2. Способы настройки

5.2.1. Настройка с помощью Центра Управления

☞ **Для того чтобы отобразить на экране диалоговое окно настройки Антивируса Касперского для Firewall с помощью Центра Управления следует,**

1. В главном окне Kaspersky Anti-Virus Control Centre переключитесь на закладку **Задачи**.

2. В списке задач щелкните правой кнопкой мыши по строке с именем задачи, которая была создана Вами на основе Антивируса Касперского для Firewall.

3. В появившемся динамическом меню выберите пункт **Свойства**. После этого откроется диалоговое окно **Свойства задачи**.

4. Нажмите на кнопку **Настройка компоненты**.

В появившемся диалоговом окне **Настройка компоненты**, переключившись на закладку **Параметры**, Вы можете настроить общие параметры проверки (см. п. 5.3), а также установить необходимые параметры проверки для каждого протокола в отдельности (см. п. 5.4).

5.2.2. Настройка с помощью текстового файла

Настройку программы Антивирус Касперского для Firewall к работе можно осуществить при помощи редактирования файла `kapwall.cfg`. Файл `kapwall.cfg` находится в том же каталоге, куда Вы установили программу.

Изменить настройки, хранящиеся в файлах конфигурации, можно с помощью любого текстового редактора.

`kapwall.cfg` — это файл обычного текстового формата (ASCII). Он состоит из нескольких секций, в которых расположены названия параметров и соответствующие им значения. Секция имеет следующий вид:

```
[Название_секции]
Название_параметра_1=Значение_параметра_1
Название_параметра_2=Значение_параметра_2
...
```

В начале секции приводится ее название, заключенное в квадратные скобки. Далее следуют строки определения значений параметров. Слева от знака равенства — название очередного параметра, справа — его значение. У некоторых параметров значения могут отсутствовать. В этом случае параметрам присваиваются значения, принятые в Антивирусе Касперского для Firewall по умолчанию.

Строки файла конфигурации, начинающиеся с символа `;`, рассматриваются программой Антивирус Касперского для Firewall как комментарий, и настройки, содержащиеся в этих строках, системой не используются.

О настройке файла конфигурации более подробно будет рассказано в соответствующих пунктах руководства (см. пп. 5.3, 5.4).

5.3. Настройка общих параметров

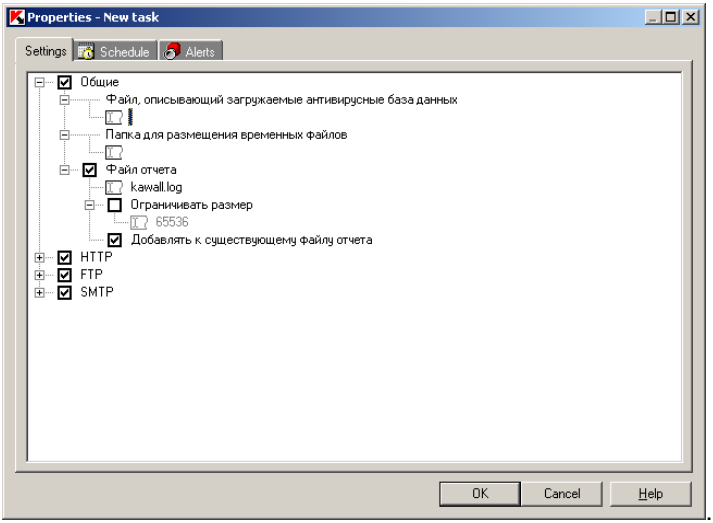

Рисунок 45. Настройки общих параметров путем редактирования полей пункта **Общие**

5.3.1. Режим проверки

Если переключатель пункта **Общие** установлен в выключенное состояние, то Антивирус Касперского для Firewall не будет осуществлять проверку информации, проходящей через брэндмауэр.

Этот переключатель соответствует параметру `Enable` в группе `[Commons]` файла `kapwall.cfg` (см. п. 5.2.2).

5.3.2. Файл, описывающий загружаемые антивирусные базы

В поле ввода пункта **Файл, описывающий загружаемые антивирусные базы** должен быть указан путь к файлу, содержащему описание антивирусных баз, и имя этого файла.

По умолчанию указывается путь к файлу с базами, установленному при установке Антивируса Касперского для Firewall (см. п. 2.2).

Это поле соответствует параметру `DatabasesSetFile` в группе `[Commons]` файла `kapwall.cfg` (см. п. 5.2.2).

5.3.3. Каталог для хранения временных файлов

В поле ввода пункта **Папка для размещения временных файлов** должен быть указан каталог, в котором будут создаваться временные файлы, необходимые для работы Антивируса Касперского для Firewall. По умолчанию используется значение `.\TEMP` относительно каталога, где находится программа.

Это поле соответствует параметру `TempFolder` в группе `[Commons]` файла `kapwall.cfg` (см. п. 5.2.2).

5.3.4. Файл отчета

В поле ввода пункта **Файл отчета** указывается имя файла, в котором будут сохраняться результаты проверки протоколов (см. п. 7.2).

По умолчанию используется файл `kawall.log`.

Если переключатель пункта установлен в выключенное состояние, то результаты проверки протоколов сохраняться не будут.

Кроме того, в поле **Ограничивать размер** Вы можете установить максимальный размер файла отчета.

☞ **Для того чтобы установить максимальный размер файла отчета,**

1. Установите переключатель **Ограничивать размер** во включенное состояние.
2. В поле ввода **Ограничивать размер** укажите максимальный размер файла отчета в килобайтах.

При установке переключателя **Добавлять к существующему отчету** во включенное состояние результаты каждой новой сессии будут добавляться в конец файла отчета, в противном случае информация о предыдущих сессиях сохраняться не будет.

Эти настройки соответствуют параметрам, собранным в группе `[LogFile]` файла `kapwall.cfg` (см. п. 5.2.2).

5.3.5. Редактирование общих параметров в файле конфигурации

Для редактирования общих настроек Антивируса Касперского для Firewall найдите в файле конфигурации секции `[Commons]` и `[LogFile]`.

Эти секции включают в себя следующие параметры:

`Enable` — включить/отключить проверку файлов, проходящих по всем протоколам. Может принимать значение `Yes` или `No` (см. п. 5.3.1).

`TempFolder` — содержит имя каталога для хранения временных файлов Антивируса Касперского для Firewall (см. п. 5.3.3).

`DatabasesSetFile` — содержит полное имя SET-файла Антивируса Касперского для Firewall (см. п. 5.3.2).

`Enable` — включить/отключить ведение файла отчета. Может принимать значение `Yes` или `No` (см. п.5.3.4).

`FileName` — имя файла отчета (см. п. 5.3.4).

`LimitSize` — ограничение размера файла отчета. Может принимать значение `Yes` или `No` (см. п. 5.3.4).

`LimitSizeKB` — предельный размер файла отчета (см. п. 5.3.4).

`Append` — добавлять/обновлять файл отчета. Может принимать значение `Yes` или `No` (см. п. 5.3.4).

5.4. Настройка параметров проверки протоколов

Антивирус Касперского для Firewall позволяет произвести раздельную настройку проверки объектов, поступающих по протоколам HTTP, FTP и SMTP.

Так как параметры настройки для всех протоколов практически идентичны, в дальнейшем в качестве примера будет использоваться настройка проверки протокола HTTP (рис. 46).

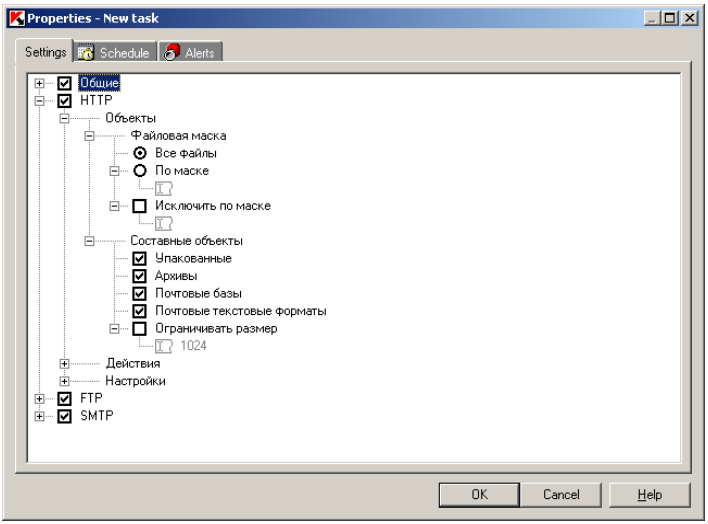

Рисунок 46. Диалоговое окно в процессе настройки проверки протоколов

5.4.1. Режим проверки

☞ **Для того чтобы Антивирус Касперского для Firewall осуществлял проверку объектов, поступающих через брэндмауэр по протоколу HTTP, необходимо установить переключатель HTTP во включенное состояние.**

Этот переключатель соответствует параметру `Enable` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2).

5.4.2. Объекты для проверки

Выбор объектов проверки осуществляется в пункте **Объекты**.

В группе **Файловая маска** Вы можете установить маску файлов, которые будут проверяться системой.

При установке во включенное состояние:

- кнопки выбора **Все файлы** — будет производиться проверка всех файлов;
- кнопки выбора **По маске** — будет производиться проверка файлов по маске, указанной Вами в поле ввода **По маске**. Вы можете задать несколько масок через разделитель (запятую, точку с запятой или пробел).

Кроме того, Вы можете указать маску файлов, которые не должны проверяться системой.

☞ **Для того чтобы исключить из процесса сканирования некоторые файлы,**

1. Установите переключатель **Исключить по маске** во включенное состояние.

2. В поле ввода этого пункта укажите маски или имена файлов, которые должны быть исключены из процесса сканирования.

При помощи переключателей в группе **Составные объекты** Вы можете настраивать проверку *сложных объектов*, т. е. файлов, включающих в себя, кроме текста, графические материалы, базы данных и данные из других приложений.

Установите во включенное состояние переключатели:

Упакованные — если хотите, чтобы проверялись упакованные исполняемые модули;

Архивы — если хотите, чтобы проверялись заархивированные файлы;

Почтовые базы — если Вы хотите проверять почтовые базы данных следующих форматов:

- Microsoft Outlook, Microsoft Exchange (файлы *.PST и *.PAB, тип архива MS Mail);
- Microsoft Internet Mail (файлы *.MBX, тип архива MS Internet Mail).

В режиме сканирования почтовых баз данных Антивирус Касперского для Firewall будет проверять каждую запись в базах электронной почты, сканировать на вирусы присоединенные файлы. При этом поддерживаются форматы: UUEncode; XXEncode; btoa (до 5.0); btoa 5.*; BinHex 4.0; ship; NETRUN 3.10; NETSEND 1.0 (неупакованный); NETSEND 1.0C (упакованный); MIME base64.

Почтовые текстовые форматы — если хотите проверять файлы почтовых текстовых форматов:

- Eudora Pro & Lite;
- Pegasus Mail;
- Netscape Navigator Mail;
- JSMail SMTP/POP3 server (базу данных по пользователям).

Кроме того, Вы можете ограничить максимальный размер сложных объектов, которые будет проверять Антивирус Касперского для Firewall.

Для того чтобы ограничить максимальный размер сложных объектов, проверяемых Антивирусом Касперского для Firewall,

1. Установите переключатель **Ограничивать размер** во включенное состояние.
2. В поле ввода этого пункта укажите максимальный размер файла (в килобайтах).

Эти настройки соответствуют параметрам: `FileMask`, `UserDefined`, `ExcludeMask`, `ExcludeDefined`, `CompoundPacked`, `CompoundArchives`, `CompoundMailDatabases`, `CompoundPlainMail`, `CompoundLimitSize`, `CompoundLimitSizeKB` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2).

5.4.3. Действия с зараженными, подозрительными и непроверенными объектами

Антивирус Касперского для Firewall позволяет устанавливать различные настройки для зараженных, подозрительных и непроверенных объектов.

Настройка действий с зараженными, подозрительными и непроверенными файлами производится в пункте **Действия** (рис. 47).

Действия, которые Антивирус Касперского для Firewall должен совершать с зараженными файлами, определяются в пункте **Инфицированные**.

☞ **Для того чтобы Антивирус Касперского для Firewall попыталась вылечить зараженный файл, установите переключатель Пытаться лечить во включенное состояние.**

Если Вы хотите, чтобы инфицированные файлы были сохранены на Вашем жестком диске, установите переключатель **Копировать** во включенное состояние, а в соответствующем поле ввода укажите каталог, в котором система должна сохранять эти файлы, а в поле **Ограничивать размер** — при необходимости задайте соответственно максимальный и минимальный размер файлов, подлежащих копированию.

По умолчанию для этого используется каталог **Infected**, созданный при установке Антивируса Касперского для Firewall.

Кроме того, Вы можете настроить действия Антивируса Касперского для Firewall с зараженными файлами, которые не удалось вылечить:

- если установить во включенное состояние кнопку выбора **Пропускать**, зараженные файлы будут без изменений переданы брэндмауэру;
- если установить во включенное состояние кнопку выбора **Отказывать**, зараженные файлы будут отвергнуты Антивирусом Касперского для Firewall.

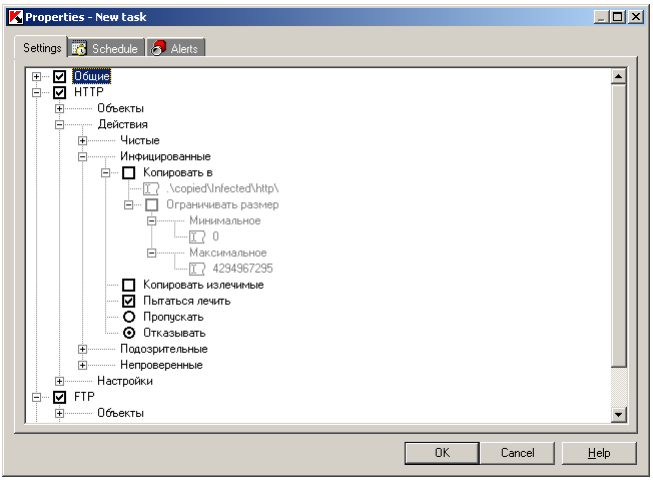

Рисунок 47. Пункт **Действия**

Таким же образом могут быть настроены действия с *подозрительными* (пункт **Подозрительные**) и *непроверенными* объектами (пункт **Непроверенные**) за тем исключением, что эти объекты не могут быть вылечены Антивирусом Касперского для Firewall.

Непроверенными являются объекты, которые Антивирус Касперского для Firewall по каким-либо причинам не смогла проверить (например, архивы, закрытые паролем).

Эти настройки соответствуют параметрам: `InfectedAction`, `InfectedCopyT`, `InfectedCopyFolder`, `InfectedCopyLimitSize`, `InfectedCopyLimitMinSizeKB`, `InfectedCopyLimitMaxSizeKB`, `InfectedCopyCurable`, `InfectedTryToCure` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2).

5.4.4. Дополнительные режимы проверки

Настройка дополнительных режимов проверки производится в пункте **Настройки** (рис. 48).

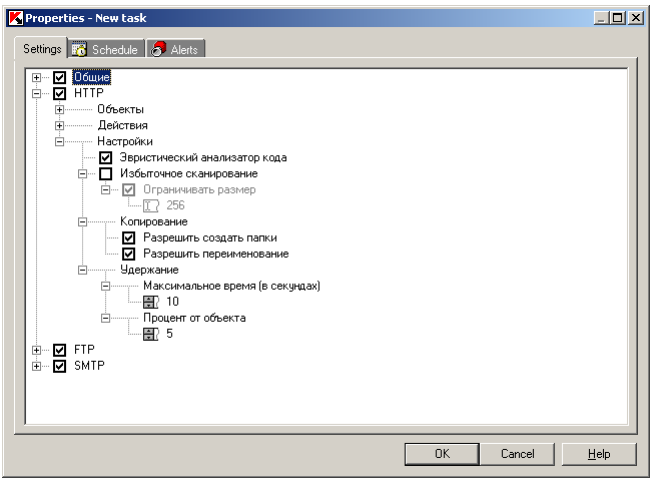

Рисунок 48. Пункт **Настройки**

5.4.4.1. Эвристический анализатор

Вы можете включать *эвристическое сканирование* файлов на вирусы, установив во включенное состояние переключатель **Эвристический анализатор кода**.

Эвристический анализатор (Code Analyzer) проверяет коды файлов на наличие вирусоподобных инструкций. Если эвристический анализатор обнаруживает комбинацию команд, таких как открытие или запись в файл, перехват векторов прерываний и т. д., то проверяемый файл считается «подозрительным», о чем выдается соответствующее сообщение в файл отчета.

Этот переключатель соответствует параметру `CodeAnalyser` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2)

5.4.4.2. Избыточное сканирование

Вы можете включать *избыточное сканирование* файлов на вирусы с помощью переключателя **Избыточное сканирование**.

Избыточное сканирование представляет собой полное сканирование содержимого исследуемых файлов вместо стандартной обработки только «точек входа» (т. е. тех мест, где начинается обработка программ системой). Этот механизм позволяет определить присутствие вируса в том случае, когда произошло некорректное заражение файла вирусом, или файл является «недолеченным», т.е. файл восстановлен, но вирус не отсечен.

Эти настройки соответствуют параметрам: `Redundant`, `RedundantLimitSize`, `RedundantLimitSizeKB` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2).

5.4.4.3. Правила копирования

В группе **Копирование** можно задать следующие параметры:

Разрешить создавать папки — разрешить создание новых папок при копировании.

Разрешить переименование — разрешить переименование файлов.

Эти настройки соответствуют параметрам: `CopyMakeSubFolder`, `CopyRenameFile` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2)

5.4.4.4. Параметры удержания

Важнейшим отличием новой версии Антивируса Касперского для Firewall является предоставление пользователю возможности задавать параметры *удержания* проверяемых файлов.

Дело в том, что при скачивании по какому-либо протоколу файлов большого размера, процедура скачивания иногда обрывалась по тайм-ауту, так как Антивирус Касперского для Firewall затрачивал значительное количество времени на проверку таких файлов.

Теперь в группе **Удержание** пользователь может самостоятельно определять:

Процент от объема — процент от объема, который Антивирус Касперского для Firewall может удерживать при проверке. Если установить значение 100, то Антивирус Касперского для Firewall будет удерживать проверяемые файлы целиком. Если установить 0 — проверка производиться не будет.

Эти настройки соответствуют параметрам: `HoldTimeSEC`, `HoldFilePER` в группе `[HTTP Scan]` файла `kapwall.cfg` (см. п. 5.2.2).

5.4.5. Редактирование параметров проверки протокола в файле конфигурации

Для редактирования параметров проверки протокола HTTP системой Антивируса Касперского для Firewall найдите в файле конфигурации секцию `[HTTP Scan]`.

Эта секция включает в себя следующие параметры:

`Enable` — включить/отключить проверку HTTP. Может принимать значение `Yes` или `No` (см. п. 5.4.1).

`FileMask` — задает тип маски проверяемых объектов (см. п. 5.4.2). Может принимать следующие значения:

`0` — соответствует пункту **All files**;

`1` — соответствует пункту **User defined**.

`UserDefined` — содержит установленные пользователем маски проверки. Используется только если переменной `FileMask` присвоено значение `1` (см. п. 5.4.2).

`ExcludeMask` — включает/выключает (значения `Yes` или `No`) использование маски для файлов, которые не будут проверяться Антивирусом Касперского для Firewall (см. п. 5.4.2).

`ExcludeDefined` — содержит установленные пользователем маски для файлов, которые не будут проверяться Антивирусом Касперского для Firewall. Используется, только если переменной `ExcludeMask` присвоено значение `Yes` (см. п. 5.4.2).

Следующие переменные:

CompoundPacked, CompoundArchives, CompoundMailDatabases и CompoundPlainMail могут принимать значение Yes или No в зависимости от того, хотите ли Вы, чтобы Антивирус Касперского для Firewall проверяла соответствующие сложные объекты (см. п. 5.4.2).

CompoundLimitSize — может принимать значение Yes или No в зависимости от того, хотите ли Вы ограничить размер проверяемых сложных объектов (см. п. 5.4.2).

CompoundLimitSizeKB — содержит числовое значение, соответствующее максимально допустимому размеру проверяемого сложного объекта. Используется, только если переменной CompoundLimitSize присвоено значение Yes (см. п. 5.4.2).

Следующие группы переменных описывают действия, которые система должна совершить с чистыми, зараженными, подозрительными и несканированными файлами.

InfectedAction — может принимать значение 0 или 1 в зависимости от того, что следует делать системе с зараженными файлами (0 — передать брэндмауэру без изменений, 1 — отвергнуть).

InfectedCopyTo — может принимать значение Yes или No в зависимости от того, хотите ли Вы, чтобы зараженные файлы были скопированы в отдельный каталог.

InfectedFolder — путь к каталогу, в который должны быть скопированы зараженные файлы. Используется, только если переменной InfectedCopyTo присвоено значение Yes.

Переменные InfectedCopyLimitSize, InfectedCopyLimitMinSizeKB и InfectedCopyLimitMaxSizeKB задают необходимость, а также минимальный и максимальный размер зараженных файлов, которые система должна копировать в каталог, указанный в переменной CleanFolder.

InfectedTryToCure — может принимать значение Yes или No в зависимости от того, хотите ли Вы, чтобы система Антивирус Касперского для Firewall попыталась вылечить зараженные файлы.

Аналогичным образом в файле конфигурации могут быть настроены действия, которые система должна производить с подозрительными и непроверенными файлами.

`CodeAnalyser` — может принимать значение `Yes` или `No` в зависимости от того, хотите ли Вы включить эвристический анализатор (см. п. 5.4.4.1).

`Redundant` — может принимать значение `Yes` или `No` в зависимости от того, хотите ли Вы включить режим избыточного сканирования (см. п. 5.4.4.2).

`RedundantLimitSize` — может принимать значение `Yes` или `No` в зависимости от того, хотите ли Вы ограничить размер файлов для избыточного сканирования (см. п. 5.4.4.2).

`RedundantLimitSizeKB` — содержит конкретное числовое значение, соответствующее максимально допустимому размеру файла для избыточного сканирования. Используется, только если переменной `RedundantLimitSize` присвоено значение `Yes` (см. п. 5.4.4.2).

`CopyMakeSubFolder` — может принимать значение `Yes` или `No` в зависимости от того, хотите ли Вы разрешить создание папок при копировании (см. п. 5.4.4.3).

`CopyRenameFile` — может принимать значение `Yes` или `No` в зависимости от того, хотите ли Вы разрешить переименование файлов при копировании (см. п. 5.4.4.3).

`HoldTimeSEC` — содержит конкретное числовое значение, соответствующее максимально допустимому времени удержания объекта.

`HoldFilePER` — — содержит конкретное числовое значение, соответствующее максимально допустимому проценту от размера объекта, удерживаемому Антивирусом Касперского для Firewall (см. п. 5.4.4.4).

Глава

6

6. Действия программы при обнаружении вируса

Действия Антивируса Касперского для Firewall при обнаружении вируса при работе с различными протоколами.

При обнаружении файлов, содержащих какой-либо вирус, Kaspersky Anti-Virus for Firewall удерживает процент от каждого инфицированного файла (количество удерживаемых таким образом процентов задается в настройках для каждого протокола в отдельности (см. п. 5.4.4.4)) .

В результате пользователь не получает файл целиком, что предотвращает, в большинстве случаев, запуск этого вируса на машине пользователя.

При этом процедура обработки немного отличается в зависимости от протокола (в случае если установлена опция не пропускать зараженные объекты):

- Протокол SMTP позволяет удержать 100% от проверяемого файла, т. е. в случае обнаружения в нем вируса, пользователь вообще не получит ничего.

- Протоколы HTTP и FTP не позволяют осуществить удержание 100% от файла. При попытке скачать зараженный файл по одному из этих протоколов пользователь получит лишь фрагмент подобного файла.

Глава

7

7. Отчеты о результатах работы Антивирусом Касперского для Firewall

Информация и статистика работы Антивируса Касперского для Firewall. Способы просмотра отчетов.

7.1. Просмотр отчета из Центра Управления

При помощи Kaspersky Anti-Virus Control Centre Вы в любой момент можете просмотреть статистику работы Антивируса Касперского для Firewall, а также его текущее состояние.

☞ **Для того чтобы просмотреть статистику работы Антивируса Касперского для Firewall,**

1. В главном окне Kaspersky Anti-Virus Control Centre переключитесь на закладку **Задачи**.

2. В списке справа щелкните мышью по пункту с именем задачи, созданной на основе Антивируса Касперского для Firewall.

В правой части экрана в табличной форме отобразится статистика работы данной задачи (рис. 50). Здесь можно узнать общее количество проверенных файлов отдельно по каждому протоколу.

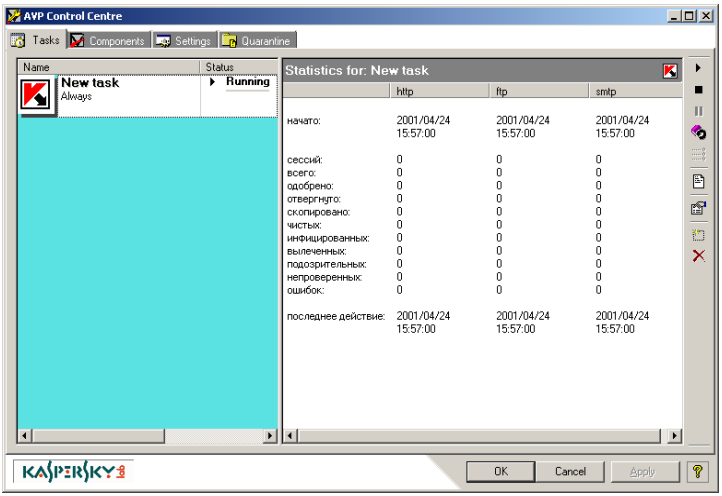

Рисунок 49. Статистика работы Антивируса Касперского для Firewall

Возможность оперативного просмотра отчетов о работе компонент пакета Антивирус Касперского для Firewall упрощает анализ и сравнение отчетов, позволяя тем самым своевременно предотвратить заражение.

Кроме того, просмотреть статистику можно из командной строки, набрав `kawall.exe -stat`.

☞ **Для того чтобы просмотреть более подробную информацию о работе Антивируса Касперского для Firewall,**

1. В главном окне Kaspersky Anti-Virus Control Centre переключитесь на закладку **Задачи**.
2. Выберите в списке задачу, созданную на основе Антивируса Касперского для Firewall, щелкнув мышью по ее названию или значку.
3. Нажмите на правую клавишу мыши и в появившемся динамическом меню выберите пункт **Отчет**.

В окне отчета в табличном виде представлена информация о дате и времени проверки, об объекте проверки и ее результатах.

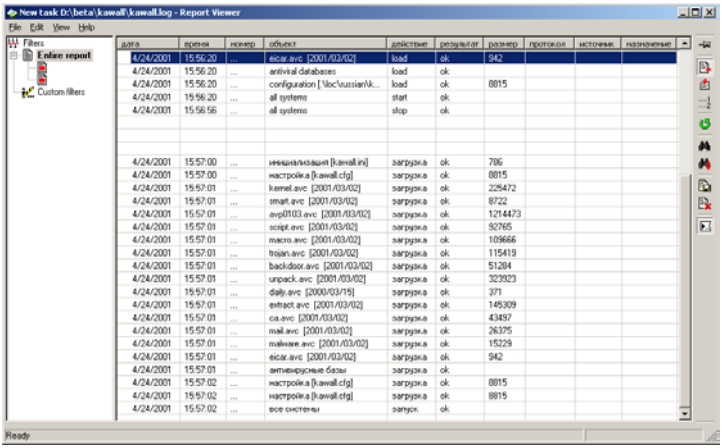

Рисунок 50. Пример отчета

Просмотреть статистику можно также из командной строки, набрав `kawall.exe -info`.

7.2. Файл отчета

В процессе работы формируется *файл отчета* (если в п. 6.3.4 эта опция не была отключена). Вы можете просмотреть его в текстовом редакторе или электронной таблице.

7.3. Предупреждения, отправляемые Центром Управления администратору

Если в диалоговом окне **Свойства** переключиться на закладку **Уведомления**, на экране отобразится перечень диагностических сообщений, которые задача формирует при наступлении тревожных событий (рис. 51). Если программа Kaspersky Anti-Virus Control Centre работает в составе программного комплекса Kaspersky Administration Kit, предупреждения могут быть переданы по электронной почте сетевому администратору.

Предупреждения, которые может отправлять Kaspersky Anti-Virus Control Centre при обнаружении программой Антивирус Касперского для Firewall, приведены на рисунке ниже.

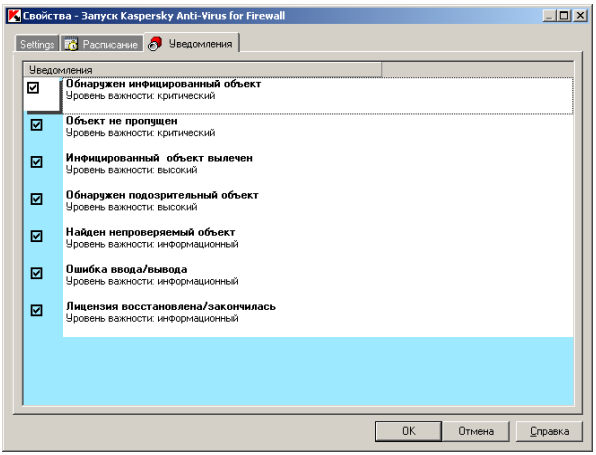

Рисунок 51. Закладка **Уведомления** диалогового окна **Свойства**

Отправка предупреждения администратору локальной сети может быть подавлена либо активизирована.

Для этого достаточно установить соответствующий предупреждению переключатель во включенное или выключенное состояние.

Настройка электронных адресов, на которые будут отправлены предупреждения, описывается в документации к Kaspersky Anti-Virus Control Centre.

В качестве темы сообщения задается строка, содержащая имя рабочей станции, имя компоненты, от которой пришло предупреждение, а также текст этого предупреждения. Обратным адресом сообщения служит адрес самого сервера. В тексте сообщения находится та же информация, что и в его теме, но в более подробном виде.

```
Alert number: <НОМЕР_ПРЕДУПРЕЖДЕНИЯ>
Alert priority: <ПРИОРИТЕТ_ПРЕДУПРЕЖДЕНИЯ>
Alert name: <ИМЯ_ПРЕДУПРЕЖДЕНИЯ>
From KAV component: <ИМЯ_КОМПОНЕНТЫ>
From computer: <ИМЯ_КОМПЬЮТЕРА>
```

```
Date: <ДАТА>
Time: <ВРЕМЯ>
```

где <НОМЕР_ПРЕДУПРЕЖДЕНИЯ> — порядковый номер предупреждения в списке всех предупреждений, формируемых Антивирусом Касперского для Firewall;

<ПРИОРИТЕТ_ПРЕДУПРЕЖДЕНИЯ> — приоритет предупреждения;

<ПРЕДУПРЕЖДЕНИЕ> — текст предупреждения;

<ИМЯ_КОМПОНЕНТЫ> — название компоненты пакета Kaspersky Anti-Virus, которой было сформировано предупреждение, а именно: Антивирусом Касперского для Firewall;

<ИМЯ_КОМПЬЮТЕРА> — имя компьютера, с которого было отправлено предупреждение;

<ДАТА>, <ВРЕМЯ> — соответственно дата и время, когда программой Антивирус Касперского для Firewall, установленной на компьютере <ИМЯ_КОМПЬЮТЕРА>, было сформировано предупреждение <ПРЕДУПРЕЖДЕНИЕ>.

Глава

8

8. Kaspersky Anti-Virus for Firewall Agent

Программа Kaspersky Anti-Virus for Firewall Agent.

8.1. Общие сведения

Программа Kaspersky Anti-Virus for Firewall Agent, входящая в комплект поставки Антивируса Касперского для Firewall, предназначена для автоматического отслеживания корректности работы Антивируса Касперского для Firewall и запуска какой-либо вспомогательной программы в случае сбоя в работе Антивируса Касперского для Firewall (или ее перезапуска).

8.2. Настройка Kaspersky Anti-Virus for Firewall Agent

Настрйка параметров работы Kaspersky Anti-Virus for Firewall Agent производится в файле `.AGENT\kawallag.ini`.

Для того чтобы в случае какого-либо сбоя в работе Антивируса Касперского для Firewall запускалась какая-либо вспомогательная команда, в этом файле наобходимо установить следующие значения у параметров:

```
Enable=Yes

RunOnStop=Yes

RunOnStopProgram=<Полный_путь_к_программе>
```

Приложение А. ЗАО "Лаборатория Касперского"

"Лаборатория Касперского" является крупнейшим российским разработчиком антивирусных систем безопасности. Более половины российских пользователей выбрали качество и надежность наших продуктов. Как независимое юридическое лицо компания была основана летом 1997 г. Разработка и коммерческое распространение основного продукта "Лаборатории Касперского" — Антивируса Касперского началась в 1989 г.

"Лаборатория Касперского" — признанный лидер в антивирусных технологиях. Многие функциональные особенности практически всех современных антивирусов были впервые разработаны именно в нашей компании. Ряд крупных западных производителей антивирусного программного обеспечения использует в своих продуктах антивирусное ядро Антивируса Касперского. Исключительные надежность и качество Антивируса Касперского подтверждаются многочисленными наградами и сертификатами российских и зарубежных компьютерных изданий, независимых тестовых лабораторий.

Антивирусы — основная сфера деятельности "Лаборатории Касперского", на которой сконцентрированы главные усилия компании. Предлагаемый спектр продуктов ориентирован как на домашние компьютеры, так и на корпоративные сети любого масштаба. Антивирусные решения "Лаборатории Касперского" обеспечивают надежный контроль над всеми потенциальными источниками проникновения компьютерных вирусов: они используются на рабочих станциях, файловых серверах, WEB-серверах, почтовых системах и межсетевых экранах. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей.

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, 123363, Москва, ул. Героев Панфиловцев, 10	
Телефон:	+7 (095) 797-8700 +7 (095) 948-4331 +7 (095) 948-8350	отдел продаж
	+7 (095) 797-8707	отдел технической поддержки
	+7 (095) 948-5650	отдел маркетинга и рекламы
Факс:	+7 (095) 797-8700, 948-4331, 948-8350	
BBS:	+7 (095) 948-6333, +7 (095) 948-3601 (24 часа)	
E-Mail:	sales@kaspersky.com	отдел продаж
	support@kaspersky.com	отдел технической поддержки
	newvirus@kaspersky.com	антивирусная лаборатория (только для посылки новых вирусов в архивированном виде)
	info@kaspersky.com	отдел маркетинга и рекламы
WWW:	http://www.kaspersky.ru http://www.viruslist.com	

Приложение B. Часто задаваемые вопросы

Вопрос. KAWALL работает корректно, но когда я пытаюсь открыть какую-либо страницу в Internet Explorer, страница не грузится. При этом, если смотреть с помощью Netscape, все отображается корректно.

Ответ. Эта проблема связана не с KAWALL, она касается сервера безопасности HTTP. Скорее всего Ваш сервер не поддерживает HTTP1.1 и не открывает страницы.

Многие источники советуют в данной ситуации добавить определенный код в файл $FWDIR/conf/objects.C, но это не поможет.

Есть несколько способов обойти эту проблему:

1. Установить SP5, если Вы используете версию 4.0.

2. Установить версию 4.1 с SP1 (проблема также существует с версией 4.1 build 41439).

3. Наиболее простое решение — настроить соответствующим образом Internet Explorer (пример дан для v. 5.x):

   - для английской версии:
     Tools=>Internet Options=>Advanced=>
     HTTP 1.1 Settings=>снять галочку с пункта **Use HTTP 1.1**;

   - для русской версии:
     Сервис=>Настройки обозревате-

ля=>Дополнительно=>
Настройка HTTP 1.1=> снять галочку с пункта **Использовать HTTP 1.1**.

Вопрос. В логи Firewall-1 записывается много данных о результатах аутентификации между KAWALL и Firewall-1. Как можно заблокировать запись этой информации?

Ответ. Проблема заключается в том, что firewall-модули по умолчанию ожидают данных аутентификации от CVP-сервера.

Вы можете изменить файл firewall-модуля $FWDIR/conf/fwopsec.conf

Удалите в этом файле следующую строку:

```
server <IP address> 18181 AUTH_OPSEC
```

Затем перезагрузите firewall.

Вопрос. Когда я скачиваю файл, скачивание идет гораздо медленнее и, где-то после 50% скачивания, все обрывается. Почему так происходит?

Ответ. Для начала следует пояснить принцип работы KAWall.

1. Когда пользователь качает файл, данные сначала проходят от брэндмауэра (Firewall Check Point) к CVP-серверу (KAWALL) и затем от CVP-сервера к пользователю. Этот двойной трансфер и объясняет падение скорости передачи данных.

2. При передаче пакетов данных KAWALL удерживает часть данных (обычно конец файла), отдавая остальную часть брэндмауэру, и, если в этой части обнаружен вирус, трансфер файла прерывается.

Компромисс между безопасностью и удобством пользователя определяется процентом данных, удерживаемых CVP-сервером.

Данная опция настраивается в новой версии KAWALL.

Русская версия:
**Параметры=>HTTP (SMTP/FTP)=>Настройки=>
Удержание=>Процент от объекта**.

Английская версия:

**Parameters=>HTTP (SMTP/FTP)=>Options=>
Hold=>Percent**.

Либо в файле конфигурации kawall.cfg (параметр HoldFilePER=).

Вопрос. После установки KAWall письма приходят без вложений (вложения отсекаются). Как это можно исправить?

Ответ. Для решения проблемы нужно сделать следующее: в настройках брендмауэра (**SMTP Definition**), на закладке **Action2** поле **Strip MIME of Type** сделать пустым (по умолчанию, туда заносится строка message/partial – ее нужно удалить).

Вопрос. Если возникает проблема с маршрутизацией пакетов, как проверить, связано ли это с KAWall, можно следующим образом:

Ответ. Для этого необходимо:

1. В меню **Manage** брендмауэра выбрать пункт **Resources**.

2. В этом окне выбрать окно настройки брендмауэра для соответствующего протокола (с которым возникли проблемы) и открыть его в режиме правки.

3. В этом окне в разделе **CVP** (настройки CVP-сервера для конкретного протокола) поставьте галочку на **None** вместо **Read Only** или **Read/Write**.

Если проблема сохранится — она не связана с KAWALL. Если проблема исчезнет — обратитесь в службу технической поддержки Лаборатории Касперского.

Вопрос. Что необходимо указать при обращении в службу технической поддержки?

Ответ. Для передачи проблемы разработчику в информации о проблеме должны быть указаны:

1. Версия Firewall Check Point.
2. Какие SP для Firewall Check Point установлены.
3. Сколько машин работают через Firewall Check Point.
4. Версия KAWALL.