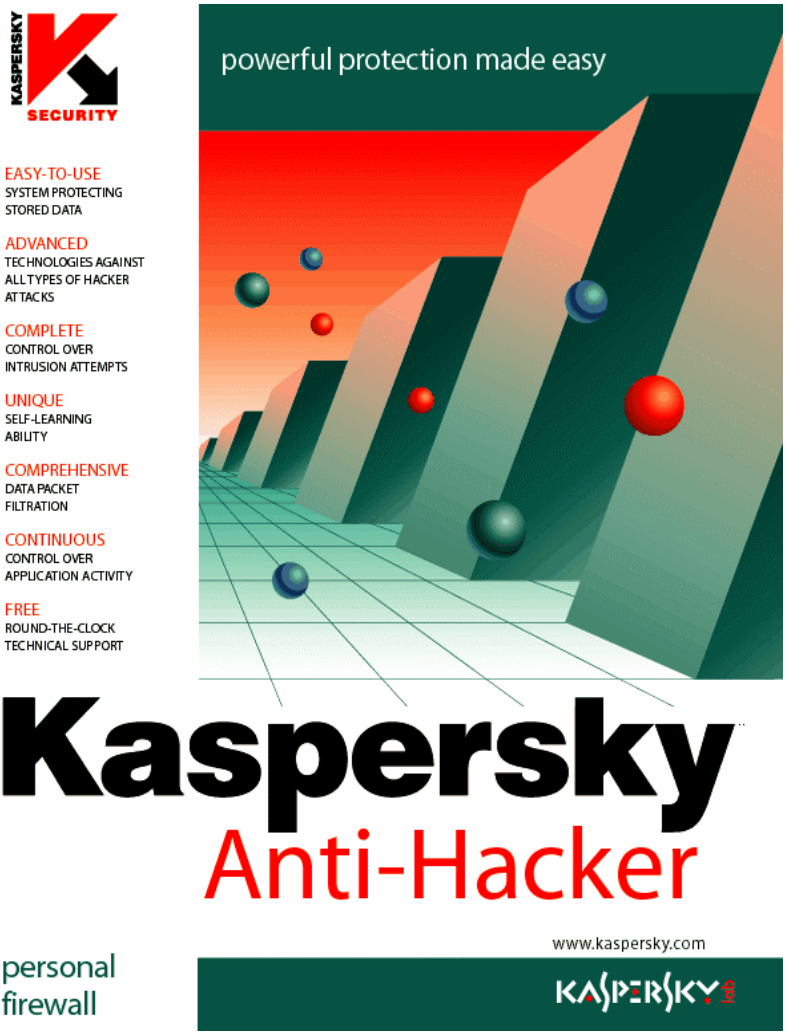
ЛАБОРАТОРИЯ КАСПЕРСКОГО



Kaspersky Anti-Hacker 1.5

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

KASPERSKY ANTI-HACKER 1.5

Руководство пользователя

Тел. +7 (095) 797-87-00 • Факс +7 (095)948-43-31
http://www.kaspersky.ru

Дата редакции: апрель 2004 года

Содержание

ГЛАВА 1. KASPERSKY ANTI-HACKER

1.1. Назначение программы и ее основные функции

Что такое Kaspersky Anti-Hacker?

Программа Kaspersky Anti-Hacker является персональным межсетевым экраном и предназначена для защиты компьютера, работающего под управлением операционной системы Windows, от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети или интернета.

Программа Kaspersky Anti-Hacker выполняет перечисленные ниже функции.

- Отслеживает сетевую активность по протоколу TCP/IP для всех приложений на вашем компьютере. При обнаружении подозрительных действий какого-либо приложения программа информирует вас об этом, и при необходимости блокирует сетевой доступ этому приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере. Например, если "троянская" программа пытается передать ваши данные по интернету злоумышленникам, Kaspersky Anti-Hacker блокирует ей сетевой доступ.

- Технология SmartStealth™ затрудняет обнаружение компьютера извне. В результате хакеры теряют объект для атаки, и все их попытки получить доступ к компьютеру обречены на провал. Кроме того, это помогает предотвратить любые типы DoS (Denial of Service) атак. В то же время, режим невидимости не оказывает никакого негативного влияния на вашу работу в интернете: программа обеспечивает стандартную прозрачность и доступность информации.

- Блокирует наиболее распространенные сетевые хакерские атаки посредством постоянной фильтрации входящего и исходящего трафика, а также предупреждает о них пользователя.

- Отслеживает попытки сканирования портов (такие попытки обычно предшествуют сетевой атаке) и запрещает дальнейшее взаимодействие с атакующим компьютером.

- Позволяет просматривать списки всех установленных соединений, открытых портов и активных сетевых приложений, и при необходимости позволяет разрывать нежелательные соединения.

- Позволяет работать с программой, не производя специализированной настройки. Программа поддерживает упрощенное администрирование по пяти режимам безопасности: Разрешить все, Низкий, Средний, Высокий, Запретить все. По умолчанию включается самообучающийся режим (Средний), который настраивает систему безопасности в зависимости от вашей реакции на различные события.

- Позволяет при необходимости гибко настроить систему защиты. В частности позволяет настроить систему фильтрации желательных и нежелательных сетевых операций, а также настроить детектор атак.

- Позволяет протоколировать определенные события, связанные с сетевой безопасностью, в специальных журналах. При необходимости можно настраивать уровень детализации записи событий в журналы.

Программа может использоваться как отдельный продукт или включаться в различные интегрированные решения **ЗАО "Лаборатория Касперского"**.

Внимание! Kaspersky Anti-Hacker не защищает ваш компьютер от вирусов и вредоносных программ, которые могут уничтожить или испортить ваши данные. Мы рекомендуем использовать Kaspersky Anti-Virus Personal для антивирусной защиты вашего компьютера.

1.2. Что нового в версии 1.5

Что изменилось в версии 1.5. Новые возможности

Новая версия программы:

- поддерживает работу с ADSL-модемами;

- полностью поддерживает работу **Режима невидимости** (пройдены тесты на www.pcflank.com);

- обнаруживает новые сетевые атаки: SmbDie, Helkern и Lovesan;

- позволяет задавать диапазон портов для правил фильтрации пакетов и правил для приложений;

- облегчает первоначальную настройку программы, не снижая при этом уровня защищенности компьютера: наиболее часто используемым приложениям по умолчанию разрешена сетевая активность в соответствии с их типом;

- обладает улучшенным интерфейсом: поддерживается XP-стиль под ОС Windows XP; списки работы с правилами допускают изменение размера; для добавления нового правила можно пользоваться клавишей <Ins>.

1.3. Комплект поставки

Что входит в комплект поставки.
Лицензионное соглашение.
Регистрационная карточка

1.3.1. Что входит в комплект поставки

В комплект поставки программного продукта входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;

- руководство пользователя;

- ключевая дискета или key-файл, записанный на установочный компакт-диск;

- регистрационная карточка (с указанием серийного номера продукта);

- лицензионное соглашение.

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

1.3.2. Лицензионное соглашение

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

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с Kaspersky Anti-Hacker дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с установочным компакт-диском (или с дискетами) должен оставаться запечатанным.

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

1.3.3. Регистрационная карточка

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

Если впоследствии у вас изменится почтовый/электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был 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 в течение срока подписки. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского", высылается информация о выходе новых программных продуктов.

1.4. Какие сведения содержатся в документации

Какие вопросы освещаются в данной документации

В настоящей документации содержатся сведения, необходимые для установки, настройки и эксплуатации программы Kaspersky Anti-Hacker.

Документация содержит следующие главы:

Название главы	**Краткое содержание**
Kaspersky Anti-Hacker	Начальная информация о продукте, описание комплекта поставки и структуры руководства
Установка и удаление программы	Системные требования, которым должна удовлетворять система. Описание процедуры установки и удаления
Начало работы	Как начать работать с программным продуктом. Пример создания системы защиты
Kaspersky Anti-Hacker – предотвращение хакерских атак при работе в интернете и локальных сетях	Принципы работы программного продукта. Описание основных терминов, основных решаемых задач
Запуск программы и ее интерфейс	Вызов главного окна программы и его интерфейс
Активизация защиты и настройка ее параметров	Активизация защиты. Настройка параметров защиты: правил для приложений и правил для фильтрации пакетов

Название главы	Краткое содержание
Просмотр результатов работы программы	Просмотр журналов сетевых атак, активности приложений и пакетной фильтрации. Просмотр списка открытых портов, установленных соединений и активных сетевых приложений
Приложение A. ЗАО Лаборатория Касперского	Основные сведения о ЗАО "Лаборатория Касперского". Контактная информация
Приложение B. Указатель	Глоссарий использующихся в документации терминов
Приложение C. Часто задаваемые вопросы	Ответы на распространенные вопросы, задаваемые пользователями

1.5. Принятые обозначения

Обозначение различных смысловых частей документации

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

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.
 Примечание.	Дополнительная информация, примечания.
 Внимание	Информация, на которую следует обратить особое внимание.

Оформление	Смысловое назначение
Чтобы запустить программу: 1. Шаг 1. 2. …	Описание последовательности выполняемых шагов и возможных действий.
Задача:	Постановка задачи в качестве примера реализации настроек, функциональности и т.д.
Решение	Решение поставленной задачи.

1.6. Сервис для зарегистрированных пользователей

Услуги, предоставляемые зарегистрированным пользователям

ЗАО "Лаборатория Касперского" предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования Kaspersky Anti-Hacker.

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

- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и электронной почте;

- оповещение о выходе новых программных продуктов Лаборатории Касперского и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского").

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

ГЛАВА 2. УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

2.1. Системные требования

Перечень требований к аппаратному и программному обеспечению

Для работы **Kaspersky Anti-Hacker** требуется:

- наличие компьютера с установленной на нем операционной системой Microsoft Windows версии 98/ME/NT 4.0/2000/XP;
- при установке на Microsoft Windows версии NT 4.0/2000/XP; необходимо обладать правами администратора;
- поддержка на компьютере установленного протокола TCP/IP;
- наличие локальной сети (Ethernet) или модемного соединения (стандартный или ADSL-модем);
- наличие Microsoft Internet Explorer версии 5.0 (минимум) или 5.5 (SP 2) или выше (рекомендуется);
- не менее 50 MB на диске для программных файлов, а также пространство, необходимое для хранения журналов желаемого размера;
- **При работе под ОС** Windows® 98/Me/NT 4.0 **требуется:**
    - Intel Pentium® 133MHz или выше для Windows 98 и Windows NT 4.0;
    - Intel Pentium® 150MHz или выше для Windows Me;
    - 32 MB RAM;
    - для Windows NT 4.0 Workstation наличие установленного Service Pack версии 6.0 или выше;

- **При работе под ОС** Windows 2000 **требуется:**
    - Intel Pentium 133MHz или выше;
    - 64 MB RAM;
- **При работе под ОС** Windows XP **требуется.**
    - Intel Pentium 300MHz или выше;
    - 128 MB RAM.

2.2. Установка программы

Процедура установки. Мастер установки

Для инсталляции программного продукта запустите программу Setup.exe на CD-диске. Программа установки работает в диалоговом режиме. Каждое диалоговое окно содержит определенный набор кнопок для управления процессом инсталляции. Кратко поясним назначение основных типов кнопок:

- **OK** – принятие действий;
- **Отмена** – отмена действий;
- **Далее** – переход на шаг вперед;
- **Назад** – переход на шаг назад.

Перед установкой программы Kaspersky Anti-Hacker на компьютер желательно закрыть все работающие на компьютере программы.

Шаг 1. Чтение общей информации

Первое диалоговое окно мастера установки (см. рис. 1) содержит общие сведения о пакете программ Kaspersky Anti-Hacker.

Шаг 2. Чтение лицензионного соглашения

Диалоговое окно **Лицензионное соглашение** (см. рис. 2) содержит текст лицензионного соглашения. Прочтите его, после чего, если вы согласны с условиями лицензионного соглашения, нажмите на кнопку **Да**. В противном случае нажмите на кнопку **Нет** и прервите процесс установки.

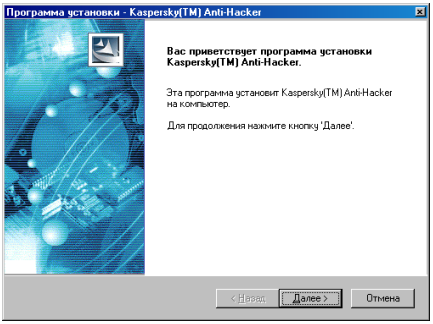


Рисунок 1. Первое диалоговое окно мастера установки

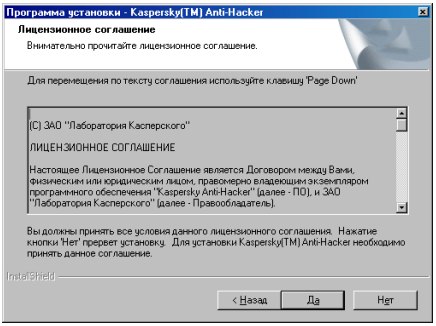


Рисунок 2. Диалоговое окно **Лицензионное соглашение**

Шаг 3. Ввод сведений о пользователе

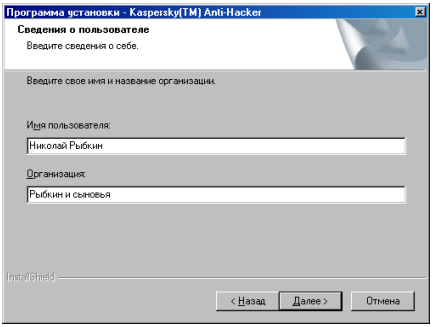


Рисунок 3. Диалоговое окно **Сведения о пользователе**

В диалоговом окне **Сведения о пользователе** (см. рис. 3) введите информацию о пользователе. В поле **Имя пользователя** введите имя пользователя, а в поле **Организация** — название организации. По умолчанию в этих полях находится информация, прописанная в реестре Windows.

Шаг 4. Выбор каталога для установки

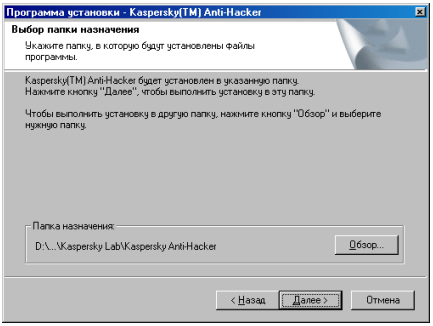


Рисунок 4. Диалоговое окно **Выбор папки назначения**

В диалоговом окне **Выбор папки назначения** (см. рис. 4) выберите каталоги для установки компонентов Kaspersky Anti-Hacker. В поле **Папка назначения** задается каталог для компонентов. Выбор каталога осуществляется с помощью кнопок **Обзор**.

Шаг 5. Ввод названия программной группы в меню Пуск\Программы (Start\Programs)

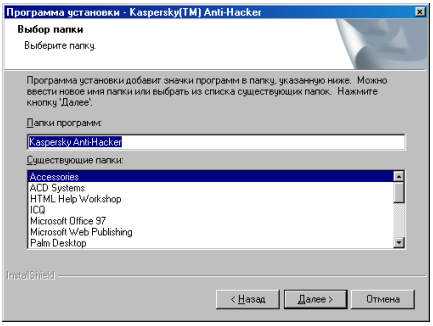


Рисунок 5. Диалоговое окно **Выбор папки**

В диалоговом окне **Выбор папки** (см. рис. 5) укажите имя папки в стандартном меню **Программы** (**Program**), в которой будет расположен значок для запуска программ пакета Kaspersky Anti-Hacker. Нажмите на кнопку **Далее**.

Шаг 6. Указание пути к ключевым файлам

В диалоговом окне **Ключевой файл** (см. рис. 6) необходимо указать имя файла-ключа (*.key файла) и путь к нему.

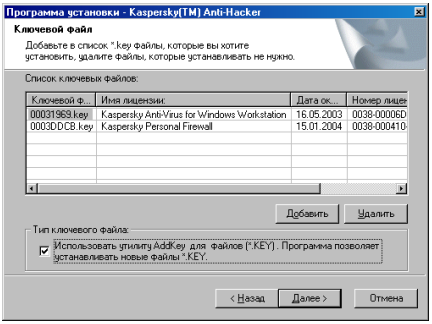


Рисунок 6. Диалоговое окно **Ключевой файл**

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 **Выбор ключевого файла** укажите нужные имя и путь. При необходимости одновременно можно использовать несколько файлов-ключей.

Рекомендуем вам установить флажок **Использовать утилиту AddKey для файлов**. В этом случае вы сможете устанавливать в систему новые key-файлы с помощью двойного щелчка мышью по их названию. Если вы оставите флажок снятым, то для установки нового ключа вам придется вручную копировать его в папку для общих файлов.

Файл-ключ является вашим личным "ключом", в котором находится вся служебная информация, необходимая для работы *Kaspersky Anti-Hacker*, а именно:

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

Шаг 7. Копирование файлов на диск

В диалоговом окне **Начало копирования файлов** (см. рис. 7) прочтите информацию об инсталляции. При необходимости внесения каких-либо изменений вернитесь к одному из предыдущих диалоговых окон, нажимая на кнопку **Назад**. Если вся информация введена правильно, нажмите на кнопку **Далее**. После этого начнется процесс копирования файлов на

жесткий диск компьютера, сведения о котором отображаются в диалоговом окне **Состояние установки** (рис. 8).

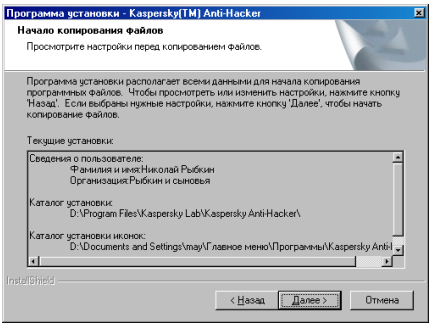


Рисунок 7. Диалоговое окно **Начало копирования файлов**

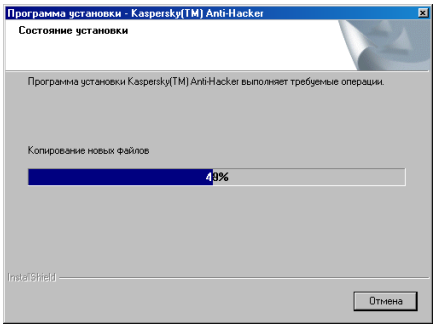


Рисунок 8. Диалоговое окно **Состояние установки**

Шаг 8. Завершение установки

После завершения установки пакета Kaspersky Anti-Hacker на экране отобразится окно **Завершение установки** (см. рис. 9).

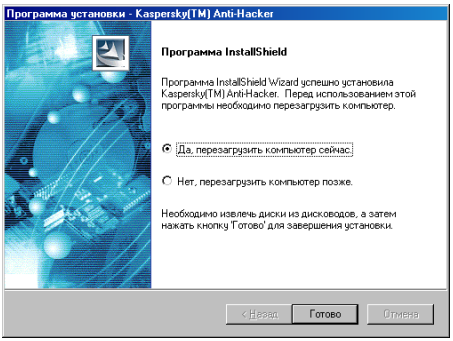


Рисунок 9. Диалоговое окно **Завершение установки**

Для корректного завершения процесса установки компьютер необходимо перезагрузить. Выберите вариант **Да, перезагрузить компьютер сейчас** для немедленной перезагрузки компьютера, или **Нет, перезагрузить компьютер позже**, если вы хотите перезагрузить компьютер позже. Нажмите на кнопку **Готово**.

2.3. Удаление программы

Удаление программы с компьютера

Для удаления программы Kaspersky Anti-Hacker выполните следующие действия:

1. Нажмите на кнопку **Пуск (Start)** в панели задач Windows **и в** появившемся меню **Windows** выберите пункт **Программы (Programs)**.

2. Затем выберите пункт, соответствующий программе Kaspersky Anti-Hacker. По умолчанию он называется **Kaspersky Anti-Hacker**, однако вы могли изменить название в процессе установки программы. В следующем меню выберите пункт **Kaspersky Anti-Hacker Uninstall**.

3. Если вы действительно хотите удалить Kaspersky Anti-Hacker, нажмите в диалоговом окне подтверждения на кнопку **Да**. Для отказа от удаления нажмите на кнопку **Нет**.

Вы можете удалить программу из окна **Установка и удаление программ**, которое можно вызвать из стандартной **Панели управления**.

ГЛАВА 3. НАЧАЛО РАБОТЫ

Начало работы с программой.
Пример создания системы безопасности

После установки программы и перезагрузки вашего компьютера система безопасности вступает в действие. Фактически, именно в этот момент Kaspersky Anti-Hacker уже отслеживает атаки на ваш компьютер, а также попытки взаимодействия приложений с локальной сетью или интернетом.

После входа в систему вы начинаете работать, как обычно. В отсутствии сетевых взаимодействий наличие программы на компьютере выдает только значок  в системной панели. Щелкнув по нему, вы можете открыть главное окно программы и просмотреть информацию о действующем режиме безопасности и изменить его (подробно главное окно рассматривается в п. 5.3. на стр. 32). По умолчанию программа работает в режиме **Средний**, который позволяет вам настроить систему защиты наиболее простым образом. В большинстве случаев вам не придется настраивать ее самостоятельно: наиболее часто используемым приложениям по умолчанию разрешена сетевая активность в соответствии с их типом. Однако, в некоторых ситуациях систему защиты понадобится настраивать вручную. Рассмотрим этот процесс более подробно.

Задача. Предположим, что ваш компьютер подключен к интернету; вы запустили Microsoft Internet Explorer и ввели адрес сайта www.kaspersky.com. После этого на экране вашего компьютера появится сообщение **Создать правило для IEXPLORER.EXE** (см. рис. 10).

В верхней части окна отображается значок, соответствующей программе Microsoft Internet Explorer, ее имя, адрес сайта www.kaspersky.com и номер порта, используемый для установки соединения. Вы можете просмотреть более подробную информацию о соединении, щелкнув мышью по подчеркнутой ссылке (см. рис. 11).

До тех пор, пока вы не укажете программе, как поступить, сетевое соединение установлено не будет. Вам необходимо среагировать на выданное программой сообщение.

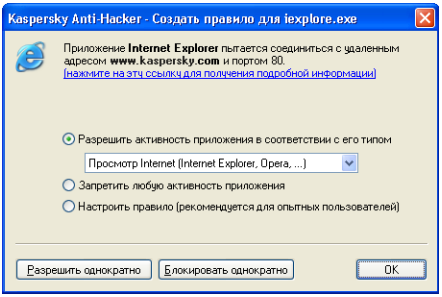


Рисунок 10. Окно самообучения системы безопасности

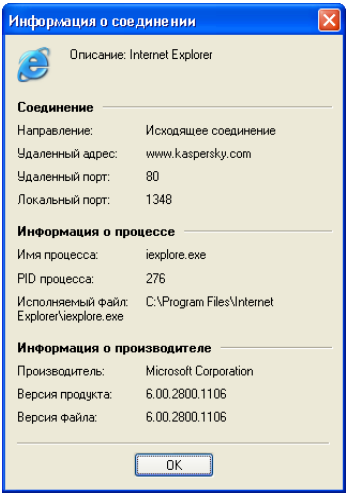


Рисунок 11. Информация о соединении

Выполните следующие действия.

1. Выберите кнопку **Разрешить активность приложения в соответствии с его типом** и в расположенном под ней раскрывающемся списке выберите значение **Просмотр Internet**.

2. Нажмите на кнопку **OK**.

После этого Kaspersky Anti-Hacker разрешает программе Microsoft Internet Explorer соединение. Кроме того, ей будут разрешены все дальнейшие соединения, обычные для веб-браузера.

Как вы могли заметить в ходе выполнения задачи, в окне **Создать правило для IEXPLORER.EXE** есть три варианта действий, которые мы перечисляем ниже.

- **Разрешить активность приложения в соответствии с его типом** (который вы выбрали в данном случае) – разрешить приложению, вызвавшему событие, любые сетевые взаимодействия в соответствии с типом приложения. Тип задается в расположенной под кнопкой выбора раскрывающемся списке. Вы можете разрешить приложению любую активность, задав значение **Разрешить все**.

- **Запретить любую активность приложения** – запретить вызвавшему событие приложению данную операцию, а также любые другие сетевые операции в дальнейшем.

- **Настроить правило** – разрешить приложению данную операцию и все такие же сетевые операции в дальнейшем. Условия сетевых операций понадобится подтвердить в мастере правил после нажатия на кнопку **ОК** (подробнее о мастере см. п. 6.3.2. на стр. 52).

Если Вы не уверены, какой из вариантов выбрать, вы можете нажать на кнопку **Разрешить однократно** или **Блокировать однократно** и посмотреть на дальнейшее поведение приложения, пытающегося получить сетевой доступ.

Если вы закроете окно обучения, нажав на кнопку  в его верхнем правом углу, спорная операция будет однократно запрещена.

Действуя таким образом, в процессе работы вы можете настроить систему безопасности на вашем компьютере оптимальным образом.

Вы можете увидеть список введенных правил, выбрав в меню **Сервис** пункт **Правила для приложений**, или нажав на кнопку  в панели инструментов.

Мы рекомендуем использовать режим **Средний** первые несколько недель после установки программы на компьютер. В процессе выполнения вами стандартных сетевых операций программа будет обучаться на основе ваших ответов. Создавайте на основе стандартных сетевых операций разрешающие правила.

После обучающего периода вы можете перевести программу в **Высокий** режим, таким образом обезопасив себя от любых несанкционированных сетевых событий и хакерских атак. Помните однако, что вновь устанавливаемые сетевые приложения по умолчанию не будут иметь доступа к интернету. Для обучения Kaspersky Anti-Hacker вам понадобится вновь перевести ее в режим **Средний** или создать правило для установленных приложений самостоятельно.

ГЛАВА 4. KASPERSKY ANTI-HACKER – ПРЕДОТВРАЩЕНИЕ ХАКЕРСКИХ АТАК ПРИ РАБОТЕ В ИНТЕРНЕТЕ И ЛОКАЛЬНЫХ СЕТЯХ

4.1. Принципы работы Kaspersky Anti-Hacker

Как работает Kaspersky Anti-Hacker? Правила для приложений. Правила фильтрации пакетов. Детектор атак

Kaspersky Anti-Hacker защищает ваш компьютер от сетевых атак, а также обеспечивает конфиденциальность ваших данных. Для этого Kaspersky Anti-Hacker осуществляет контроль всех сетевых операций на вашем компьютере. Сетевые операции бывают двух видов:

- Операции на уровне приложений (высокоуровневые). На этом уровне Kaspersky Anti-Hacker анализирует активность таких приложений, как веб-браузеры, почтовые программы, программы для передачи файлов и т.д.;

- Операции на уровне пакетов (низкоуровневые). На этом уровне Kaspersky Anti-Hacker анализирует непосредственно пакеты, передаваемые/получаемые вашей сетевой картой или модемом.

Настройка Kaspersky Anti-Hacker осуществляется путем задания правил фильтрации сетевых операций. Часть работы по фильтрации производится в автоматическом режиме детектором атак, который обнаруживает сканирование портов, DoS атаки и т.п., а также может блокировать

нападавшего. Также вы можете задать собственные правила фильтрации для усиления защиты вашего компьютера.

Для сетевых операций каждого из видов в Kaspersky Anti-Hacker предусмотрены специальные списки правил.

- *Правила для приложений*. Здесь вы можете выбрать конкретное приложение и разрешить специфичную для него активность. При необходимости вы можете задавать произвольное количество правил для каждого приложения. В случае обнаружения сетевых операций, отклоняющихся от заданного вами правила, вы будете предупреждены и сможете при необходимости блокировать нежелательные действия (в режиме **Средний**). Наиболее простой способ задать такое правило – это определить, к какому типу относится ваше приложение (список и описание типов см. п. 6.3.2.1. на стр. 52). Второй способ – это задание разрешенных удаленных служб и адресов для этого приложения.

- *Правила фильтрации пакетов* разрешают или блокируют сетевые пакеты, отправляемые или получаемые с вашего компьютера. Решение принимается на основе анализа заголовка сетевого пакета: используемого протокола, номеров портов, IP-адресов и пр. В правилах фильтрации пакетов вы задаете правила, которые применяются для всех без исключения приложений. Например, если вы заблокировали с помощью правила фильтрации пакетов какой-то IP адрес, все сетевые операции с ним будут полностью запрещены.

Приоритет правил фильтрации пакетов выше, чем у правил для приложений: правила фильтрации выполняются программой в первую очередь. Например, если вы задали правило блокирования всех входящих и исходящих пакетов, то при фильтрации ни одно правило для приложений учитываться не будет.

4.2. Режимы безопасности

Какие режимы безопасности обеспечивает Kaspersky Anti-Hacker?

Программа позволяет выбрать один из пяти режимов безопасности.

- **Разрешить все** – программа отключает защиту вашего компьютера. При работе в этом режиме допускается любая сетевая активность.

- **Низкий** – программа разрешает сетевую активность всех приложений, кроме явно запрещенных с помощью правил для приложений.

- **Средний** – программа уведомляет вас о сетевой активности приложений и позволяет настроить систему безопасности оптимальным образом. При попытке приложения выполнить сетевую операцию используется механизм обучения. На экран выдается информация о приложении и параметры сетевой операции. На ее основе вам предлагается принять решение: пропустить или блокировать данное событие однократно, запретить активность приложения полностью, разрешить активность приложения в соответствии с типом, или настроить дополнительные параметры сетевого взаимодействия. На основе вашего ответа программа может сформировать правило для данного приложения, которое будет использовать в дальнейшем автоматически.

- **Высокий** – программа разрешает доступ к сети только тем приложениям, которые явно разрешены с помощью правил. В этом режиме окно обучения не появляется, и все попытки несанкционированных соединений отклоняются.

Помните, что сетевые приложения, устанавливаемые после выбора этого режима, по умолчанию не будут иметь доступа к интернету.

- **Запретить все** – программа полностью блокирует доступ вашего компьютера к сети. Данный режим аналогичен физическому разъединению компьютера с интернетом и/или локальной сетью.

В режимах **Высокий**, **Средний** и **Низкий** вы сможете задать дополнительный режим – **Режим невидимости** (см. п. 5.6. на стр. 36). В этом режиме разрешена сетевая активность, инициатором которой выступил пользователь, вся остальная активность (удаленное подключение к вашему компьютеру, проверка с помощью утилиты ping и т.д.) запрещена, если только это явно не разрешено правилами.

Фактически это означает, что ваш компьютер становится "невидимым" для внешнего окружения. Хакеры теряют объект для атаки, и все их попытки получить доступ к компьютеру обречены на провал. Кроме того, режим невидимости помогает предотвратить любые типы DoS (Denial of Service) атак.

В то же время, режим невидимости не оказывают негативного влияния на вашу работу в интернете: Kaspersky Anti-Hacker разрешает сетевую активность, инициатором которой выступил ваш компьютер.

Обратите внимание! В случае, если вы задали разрешающие правила фильтрации пакетов, они будут выполнены, даже если включен режим невидимости.

Детектор атак активен для всех режимов безопасности, кроме **Разрешить все**. Однако, при желании вы можете его отключить (см. п. 6.5.1. на стр. 70).

4.3. Рекомендации по настройке

Как выбрать режим безопасности и как настроить правила в различных ситуациях?

Какими компонентами Kaspersky Anti-Hacker рекомендуется пользоваться и какой режим безопасности выбирать? Ответ на этот вопрос зависит от задачи, которая перед вами стоит.

Задача 1. Как обезопасить ваши данные от злоумышленников из интернета.

Существует два основных способа похищения или повреждения данных на компьютере пользователя злоумышленниками из интернета – это проникновение на компьютер через ошибки в программном обеспечении и заражение компьютера троянскими программами.

Если вам стало известно об ошибке в некоторой программе, установленной на вашем компьютере, создайте для нее запрещающее правило. Рекомендуем вам настроить сложное запрещающее правило (см. п. 6.3.2.1. на стр. 52), которое учитывало бы особенности этой ошибки.

Предположим, на ваш компьютер через дискету или по почте была занесена троянская программа, и она пытается отослать ваши данные по интернету. Kaspersky Anti-Hacker без труда обезопасит сохранность ваших данных либо запретив операцию (в режиме **Высокий**), либо выдав предупреждающее сообщение о ней (в режиме **Средний**).

Внимание!!! Kaspersky Anti-Hacker не защищает ваш компьютер от вирусов и полностью не защищает от вредоносных программ.

Например, "троянская" программа может воспользоваться для отправки ваших данных стандартной почтовой программой, тогда Kaspersky Anti-Hacker не сможет ей помешать. Кроме того, если на ваш компьютер попал вирус или вредоносная программа, ваши данные могут быть уничтожены, а компьютер стать источником дальнейшего распространения вирусов. Kaspersky Anti-Hacker в этом случае сможет лишь частично предотвратить последствия заражения. Для эффективной защиты от вирусов и вредоносных программ мы рекомендуем использовать в совокупности с Kaspersky Anti-Hacker антивирусную программу Kaspersky Anti-Virus Personal / Personal Pro. Кроме того, в списке правил для приложений рекомендуем присваивать приложениям категории, строго соответствующие операциям, которые разрешено выполнять этим приложениям. Таким образом риск выполнения на вашем компьютере несанкционированных сетевых операций будет минимизирован.

Предположим, вы обнаружили, что с некоторых удаленных компьютеров постоянно проводятся попытки атаковать ваш компьютер.

Задача 2. Как блокировать неблагонадежные адреса интернета.

Вы можете запретить взаимодействие вашего компьютера с удаленными адресами, задав соответствующие правила пакетной фильтрации. Например, на рис. 12 задано правило, позволяющее полностью блокировать адрес "111.111.111.111".

Для профилактики таких ситуаций рекомендуется держать постоянно включенным детектор атак, какой бы режим безопасности вы ни выбрали.

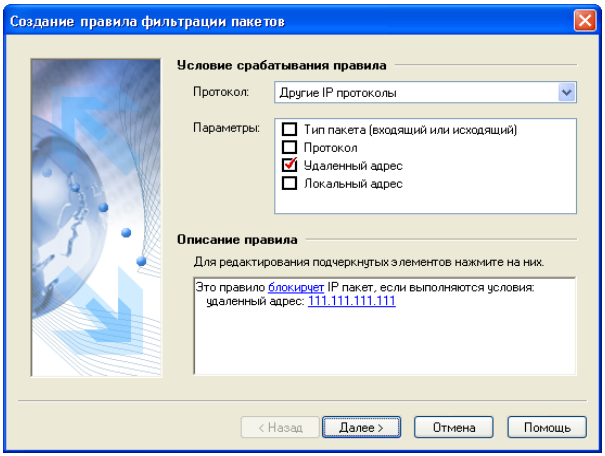


Рисунок 12. Правило для блокирования неблагонадежного адреса

В качестве интересного примера использования программы Kaspersky Anti-Hacker можно назвать блокирование показа баннеров на веб-страницах. Внесите в правила пакетной фильтрации запрет на соединение с интернет-сайтами, с которых качаются баннеры (например, **linkexchange.ru**).

Предположим, вы опасаетесь атак из локальной сети или хотите обезопасить себя от хищения личной информации.

Задача 3. Контроль операций локальной сети

Взаимодействия компьютера с локальной сетью производятся на уровне операционной системы, и не всегда возможно назвать выполняющее их приложение. В этом случае для обеспечения защиты вам необходимо задать правила пакетной фильтрации.

Программа Kaspersky Anti-Hacker предустанавливает некоторые разрешающие правила фильтрации пакетов, чтобы облегчить настройку системы безопасности. По умолчанию локальная сеть разрешена. Вы можете провести настройку установленных по умолчанию правил пакетной фильтрации самостоятельно, чтобы либо полностью запретить доступ из локальной сети, либо разрешить доступ только некоторым компьютерам.

ГЛАВА 5. ЗАПУСК ПРОГРАММЫ И ЕЕ ИНТЕРФЕЙС

Способы запуска программы. Интерфейс главного окна и его настройка. Выход из программы

5.1. Запуск программы

После входа в систему Kaspersky Anti-Hacker запускается автоматически. Если вы закрыли программу, то сможете запустить ее вновь самостоятельно.

Для того чтобы запустить программу Kaspersky Anti-Hacker,

1. Нажмите на кнопку **Пуск (Start)** в панели задач **Windows и в** появившемся меню **Windows** выберите пункт **Программы (Programs)**.

2. Затем выберите пункт, соответствующий программе Kaspersky Anti-Hacker. По умолчанию он называется **Kaspersky Anti-Hacker**, однако вы могли изменить название в процессе установки программы. В следующем меню выберите пункт **Kaspersky Anti-Hacker**.

3. Щелкните по появившемуся в панели задач значку  левой кнопкой мыши, либо щелкните по нему правой кнопкой мыши и выберите в открывшемся системном меню пункт **Открыть Kaspersky Anti-Hacker…**.

После этого на экране откроется главное окно программы Kaspersky Anti-Hacker (см. п. 5.3. на стр. 32).

Вы также можете запустить программу непосредственно из каталога, в котором она установлена. Для этого откройте каталог программы Kaspersky Anti-Hacker в проводнике (по умолчанию **C:\Program Files\Kaspersky Lab\Kaspersky Anti-Hacker**). Найдите файл ***KAVPF.exe***, затем два раза щелкните по значку файла мышью.

5.2. Системное меню

Значок в системной панели.
Системное меню

После запуска программы в системной панели (системной части панели задач) появится значок  .

Щелкнув по значку программы правой кнопкой мыши, вы можете открыть системное меню (см. рис. 13). Системное меню состоит из следующих пунктов:

Таблица 1

Пункт меню	Назначение
Открыть Kaspersky Anti-Hacker…	Вызов главного окна программы.
Режим безопасности	Выбор режима безопасности: **Запретить все**, **Высокий**, **Средний**, **Низкий**, **Разрешить все**. Подробнее о режимах безопасности см. п. 4.2. на стр. 25.
О программе	Вызов окна с информацией о версии программы и об используемых ключах.
Выход	Выгрузка программы из памяти.

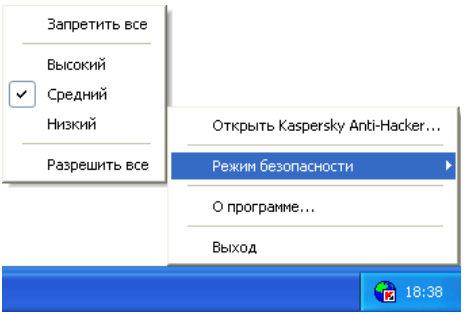


Рисунок 13. Системное меню

5.3. Главное окно

После запуска программы на экране откроется главное окно программы (см. рис. 14). Главное окно программы Kaspersky Anti-Hacker предназначено для выбора текущего режима безопасности, просмотра текущего статуса защиты, изменения настроек фильтрации пакетов и просмотра/настройки журналов.

Рисунок 14. Главное окно **Kaspersky Anti-Hacker**

В главном окне программы Kaspersky Anti-Hacker расположены:

- меню;
- панель инструментов;
- рабочая область;
- строка состояния.

5.4. Меню

В верхней части главного окна расположено *меню*. Вы можете перенести меню в любую часть главного окна или вынести за его пределы, потянув меню мышью.

Некоторые пункты меню продублированы кнопками в панели инструментов. Соответствие кнопок в панели инструментов пунктам меню приведено в п. 5.5. на стр. 35.

Таблица 2

Пункт меню	**Назначение**
Сервис ⟶ Правила для приложений	Вызвать окно настройки правил для приложений.
Сервис ⟶ Правила фильтрации пакетов	Вызвать окно настройки правил для фильтрации пакетов.
Сервис ⟶ Режим безопасности	Выбрать режим безопасности: • Запретить; • Высокий; • Средний; • Низкий; • Разрешить все. Вы также можете выбрать режим безопасности в рабочей области программы. Подробнее см. п. 4.2. на стр. 25.
Сервис⟶ Параметры	Вызвать окно для настройки параметров журналов, параметров активации защиты и параметров детектора атак.
Сервис ⟶ Выход	Выгрузить программу из памяти.

Пункт меню	Назначение
Вид ⟶ Панель инструментов	Настроить интерфейс программы: • **Стандартная панель инструментов** – показать/спрятать панель инструментов; • **Настроить** – вызвать диалоговое окно настройки интерфейса программы.
Вид ⟶ Панель состояния	Показать/спрятать строку состояния.
Вид ⟶ Журналы	Вызвать окно с журналами: • **Журнал сетевых атак**; • **Журнал сетевой активности приложений**; • **Журнал пакетной фильтрации**.
Вид ⟶ Показать	Вызвать окна просмотра с системной информацией: • **Активные сетевые приложения** – список запущенных сетевых приложений; • **Открытые порты** – список открытых портов; • **Активные соединения** – список активных соединений.
Справка ⟶ Оглавление	Вызвать справочную систему.
Справка ⟶ О программе…	Вызвать диалоговое окно с краткой информацией о версии программы и используемых ключах.
Справка ⟶ Kaspersky Anti-Hacker в Интернет	Открыть страницу ЗАО "Лаборатории Касперского"

5.5. Панель инструментов

Панель инструментов расположена под строкой меню. При желании вы можете поменять месторасположение панели в пределах главного окна или вынести за его пределы. Для этого просто потяните мышью за пустую часть панели инструментов.

В *панели инструментов* собраны кнопки, нажимая на которые вы можете инициировать те или иные действия. вы можете скрыть панель инструментов с экрана или отобразить ее вновь, выбрав пункт **Панель инструментов** меню **Вид**, и в открывшемся подменю щелкнув по пункту **Стандартная панель инструментов**.

Вы можете добавить на панель инструментов новые кнопки или убрать находящиеся на ней (см. п. 5.10. на стр. 38).

Таблица 3

Кнопка	Меню	Назначение
	Сервис ⟶ Режим безопасности	Выбрать режим безопасности: • Запретить; • Высокий; • Средний; • Низкий; • Разрешить все. Подробнее см. п. 4.2. на стр. 25.
	Сервис ⟶ Правила для приложений	Вызвать окно настройки правил для приложений.
	Сервис ⟶ Правила фильтрации	Вызвать окно настройки правил для фильтрации пакетов.
	Вид ⟶Журналы ⟶ Журнал сетевых атак	Вызвать окно с журналом сетевых атак.

Кнопка	Меню	Назначение
	Вид ⟶Показать ⟶ Активные сетевые приложения	Показать список запущенных сетевых приложений.
	Вид ⟶Показать ⟶ Открытые порты	Показать список открытых портов.
	Вид ⟶Показать ⟶ Активные соединения	Показать список активных соединений.
	Сервис ⟶ Параметры	Вызвать окно для настройки параметров журналов, параметров активации защиты и параметров детектора атак.
	Справка ⟶ Оглавление	Вызвать справочную систему.

5.6. Рабочая область

В рабочей области программы расположена *шкала режимов безопасности*, а также информация о текущем состоянии системы.

Шкала режимов безопасности позволяет выбрать один из пяти режимов:

- Запретить все;
- Высокий;
- Средний;
- Низкий;
- Разрешить все.

Вы можете сменить текущий режим безопасности, передвинув ползунок на шкале. После этого справа от ползунка появится описание нового режима безопасности. Новый режим вступает в силу немедленно.

В режимах **Высокий**, **Средний** и **Низкий** вы сможете установить дополнительный флажок – **Режим невидимости** (подробнее см. п. 4.2. на стр. 25).

Информация о текущем состоянии системы находится в нижней части рабочей области и содержит сведения о последней зарегистрированной хакерской атаке: ее дате, времени, типе и адресе атаковавшего компьютера, если его удалось определить.

5.7. Строка состояния

В нижней части главного окна расположена *строка состояния.* В ней отображается контекстная подсказка для выбранного в текущий момент элемента главного окна. Вы можете отобразить/скрыть строку состояния, выбрав пункт **Панель состояния** в меню **Вид**.

5.8. Контекстное меню

У диалоговых окон имеется *контекстное меню,* используя которое можно выполнять операции, применимые именно к этим окнам.

Чтобы вызвать контекстное меню окна, нажмите на правую клавишу мыши.

5.9. Мастера создания правил

Мастер создания/редактирования правил состоит из нескольких диалоговых окон. Каждое диалоговое окно содержит определенный набор кнопок для управления процессом добавления правила. Поясним назначение кнопок:

- **Готово** – создание правила;
- **Отмена** – отмена создания правила;
- **Далее** – переход на шаг вперед;
- **Назад** – переход на шаг назад.
- **Справка** – вызов справочной системы.

5.10. Изменение и сохранение настроек интерфейса

*Чтобы изменить настройки интерфейса, выберите пункт **Панель инструментов** в меню **Вид**, и в открывшемся подменю выберите пункт **Настроить**.*

На экране откроется диалоговое окно **Настройка** (см. рис. 15).

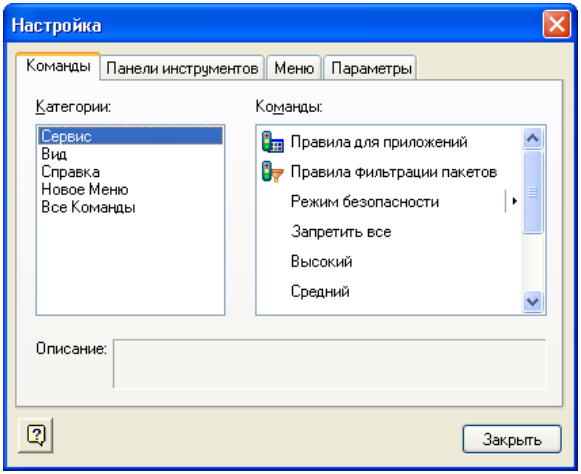


Рисунок 15. Диалоговое окно **Настройка**

Для работы с интерфейсом рекомендуется разместить окно **Настройка** таким образом, чтобы было видно панель инструментов и главное меню программы одновременно.

С помощью закладки **Команды** вы сможете изменить конфигурацию главного меню и панели инструментов. Для добавления новой команды вам необходимо потянуть мышью нужную команду из списка на меню или панель инструментов, а для ее удаления, наоборот, потянуть мышью команду с главного окна.

С закладок **Панели инструментов** и **Меню** вы можете вернуть исходный вид, соответственно, панели инструментов и меню.

На закладке **Параметры** Вы можете включить или отключить вывод всплывающих подсказок к кнопкам панели инструментов, выбрать размер кнопок, а также настроить порядок отображения пунктов меню.

При желании вы можете изменять названия пунктов главного меню и кнопок, показывать кнопки в виде текста или в виде значков.

Чтобы изменить название и/или другие свойства пункта главного меню или кнопки панели инструментов,

1. Не закрывая окно **Настройка**, выберите нужный пункт в главном меню или нужную кнопку в панели инструментов.

2. Нажмите на правую кнопку мыши. В открывшемся контекстном меню выберите желаемое действие:

   - **Удалить** – удалить пункт или кнопку;
   - **Свойства кнопки** – изменить название. В открывшемся одноименном диалоговом окне в поле **Текст** измените название пункта (см. рис. 16). Нажмите на кнопку **Применить**.
   - **Иконка** – отображать только значок;
   - **Текст** – отображать только текст;
   - **Иконка и текст** – отображать и значок, и текст;
   - **Начать группу** – поставить разделитель.

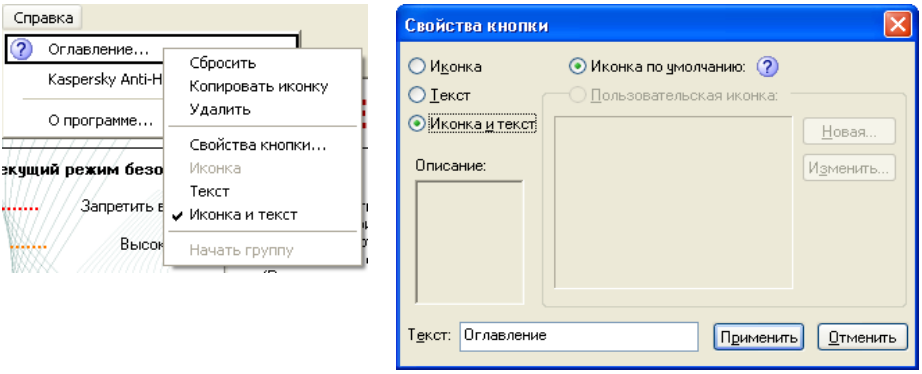


Рисунок 16. Редактирование параметров команд

Настройки интерфейса сохраняются автоматически, вступают в силу сразу после их изменения в текущем сеансе работе, и распространяются на все последующие сеансы работы.

5.11. Завершение работы с программой

Для выгрузки программы из памяти выберите пункт **Выход в** системном меню или в меню **Сервис** главного окна программы. Вы также можете закрыть главное окно с помощью кнопки  в правом верхнем углу программы.

Закрытие главного окна программы не приведет к ее выгрузке из памяти, если включен режим **Прятать главное окно программы в системной панели при его закрытии**. По умолчанию данный режим включен, при желании вы сможете его отключить (см. п. 6.1.1. на стр. 41). Наличие значка программы в системной панели свидетельствует о ее присутствии в памяти компьютера.

ГЛАВА 6. АКТИВИЗАЦИЯ ЗАЩИТЫ И НАСТРОЙКА ЕЕ ПАРАМЕТРОВ

6.1. Активизация защиты и выбор режима безопасности

Как активировать защиту компьютера с помощью Kaspersky Anti-Hacker? Как выбрать режим безопасности?

6.1.1. Активизация защиты

Защита компьютера от хакерских атак активизируется сразу после окончания инсталляции программы Kaspersky Anti-Hacker на компьютер и его перезагрузки. После запуска программы в системной панели появится значок  . По умолчанию программа работает в режиме **Средний**. При попытке приложения выполнить сетевую операцию используется специальный механизм обучения. На экран выдается информация о приложении, параметры сетевого события, и запрос действий: пропустить или блокировать данное событие, запретить активность приложения, разрешить активность приложения в соответствии с его типом, или настроить сложное правило для этого события. На основе вашего ответа программа может сформировать правило для данного приложения, которое будет использовать в дальнейшем автоматически.

По умолчанию Kaspersky Anti-Hacker защищает компьютер после входа пользователя в систему. Однако вы можете включить режим, при котором защита будет действовать сразу после старта ОС Windows.

Чтобы отключить/включить запуск Kaspersky Anti-Hacker сразу после загрузки ОС:

1. Выберите в меню **Сервис** пункт **Параметры**.

2. В открывшемся диалоговом окне **Параметры** (см. рис. 17) на закладке **Общие** снимите/установите флажок **Запускать модуль защиты сразу при старте системы**. Если вы установите флажок, программа запустится с пользовательскими настройками после загрузки ОС. Если программа настроена на запуск в режиме **Средний**, то, поскольку до входа пользователя в систему нет возможности отображать на экране окно обучения, все неизвестные сетевые взаимодействия будут разрешаться. В режимах **Низкий** и **Разрешить все** программа также будет разрешать неизвестную сетевую активность, при работе в остальных режимах она будет блокироваться.

Предположим, ваш компьютер включен в локальную сеть; вы установили активизацию защиты компьютера сразу после старта ОС, и в настройках Kaspersky Anti-Hacker указали режим **Запретить все**, либо в других режимах (кроме **Разрешить все**) установили правило фильтрации пакетов, блокирующее весь сетевой трафик. В этом случае вход в систему будет производиться дольше обычного, и после входа локальная сеть будет недоступна.

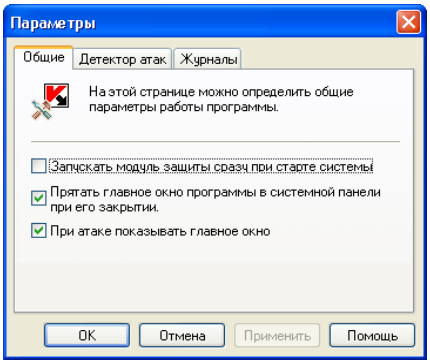


Рисунок 17. Диалоговое окно **Параметры**

Вы можете переопределить реакцию программы на нажатие кнопки в правом верхнем углу программы. По умолчанию в этом случае главное окно программы закрывается, но выгрузки программы из памяти не происходит.

Чтобы задать режим работы, при котором при закрытии главного окна программы происходит ее выгрузка из памяти,

1. Выберите в меню **Сервис** пункт **Параметры**.

2. В открывшемся диалоговом окне **Параметры** (см. рис. 17) на закладке **Общие** снимите флажок **Прятать главное окно программы в системной панели при его закрытии**.

По умолчанию при обнаружении атаки на ваш компьютер на экране появляется главное окно с ее описанием.

Чтобы главное окно не отображалось всякий раз при обнаружении атаки,

1. Выберите в меню **Сервис** пункт **Параметры**.

2. В открывшемся диалоговом окне **Параметры** (см. рис. 17) на закладке **Общие** снимите флажок ☑ **При атаке показывать главное окно**.

6.1.2. Выбор режима безопасности

Выбор режима безопасности осуществляется с помощью ползунка шкалы режимов безопасности на главном окне программы или с помощью пункта **Режим безопасности** меню **Сервис**. Вы также можете выбрать режим с помощью одноименного пункта в системном меню.

Вы можете выбрать один из следующих пяти вариантов защиты:

- **Запретить все**;
- **Высокий**;
- **Средний**;
- **Низкий**;
- **Разрешить все**.

В режимах **Высокий**, **Средний** и **Низкий** вы сможете задать дополнительный режим, установив флажок **Режим невидимости**.

Режимы вступают в силу немедленно после их выбора.

Подробные рекомендации по использованию режимов приведены в п. 4.2. на стр. 25.

6.1.3. Окно уведомления о сетевом событии

Если при создании правила вы установили флажок **Уведомлять пользователя** (см. п. 6.3.2.3. на стр. 61, п. 6.4.2.2. на стр. 69), то при срабатывании этого правила на экране открывается окно уведомления (см. рис. 18).

На рисунке 18 приведен пример уведомления, которое появляется при срабатывании правила фильтрации пакетов. В тексте уведомления указывается удаленный и локальный адреса, а также порты соединения.

Вы можете просмотреть сработавшее правило в соответствующем мастере, нажав на подчеркнутую ссылку.

Вы также можете отменить вывод уведомления в дальнейшем, установив флажок **Не выводить больше сообщений для этого правила**.

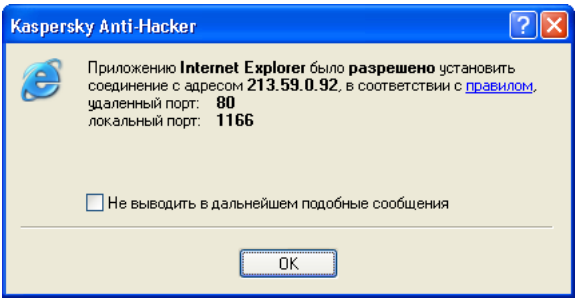


Рисунок 18. Уведомление о произошедшем событии

При создании правила вы можете включить флажок **Занести событие в журнал**, чтобы запись о произошедшем сетевом событии появлялась в журнале..

6.1.4. Окно обучения

В режиме **Средний** при возникновении события, реакция на которое не была определена правилами, программа выдает *окно обучения* (см. рис. 19) .

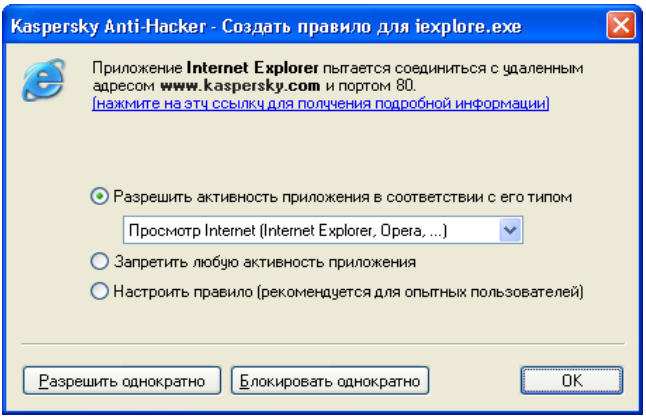


Рисунок 19. Диалоговое окно **Создать правило…**

В верхней части окна отображается значок и имя приложения, пытающегося соединиться с удаленным компьютером, адрес этого компьютера, и номера портов. При желании вы можете просмотреть более детальную информацию о запрашиваемом соединении, нажав на подчеркнутую ссылку.

Вы можете нажать на кнопку **Разрешить однократно** или **Блокировать однократно** для, соответственно, разрешения или запрета конкретной операции.

Если вы закроете окно обучения, нажав на кнопку в его верхнем правом углу, спорная операция будет однократно запрещена.

Чтобы задать правило для дальнейшей обработки событий, вызываемых этим приложением, выберите одно из ниже перечисленных действий и нажмите на кнопку **ОК**. После этого в список правил для приложений будет добавлено новое правило.

- **Разрешить активность приложения в соответствии с его типом** – разрешить приложению, вызвавшему событие, любые сетевые операции в соответствии с типом приложения. Тип следует выбрать из раскрывающегося списка (подробнее см. п. 6.3.2.1. на стр. 52).

- **Запретить любую активность приложения** – запретить вызвавшему событие приложению данную операцию, а также любые другие сетевые операции.

- **Настроить правило** – разрешить или запретить приложению сетевые операции, если они удовлетворяют некоторым условиям, кото-

рые понадобится задать в мастере правил после нажатия на кнопку **ОК** (подробнее о мастере см. п. 6.3.2. на стр. 52).

Если вы настроили правило, которое не позволяет программе среагировать на возникшую ситуацию, появляется соответствующее предупреждение (см. рис. 20). Нажмите на кнопку **Да,** если вы хотите сохранить созданное правило, или на кнопку **Нет**, если вы создали правило по ошибке. В обоих случаях вам будет предложено продолжить выбор действия в окне обучения.

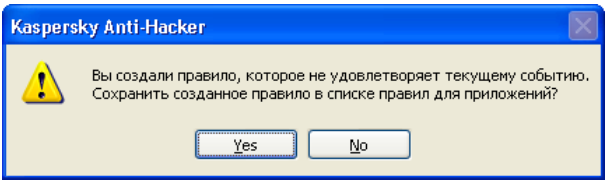


Рисунок 20. Предупреждение о несоответствии созданного правила и ситуации

Обратите внимание, в случае, когда на вашем компьютере в течение короткого промежутка времени несколько программ пытаются выполнить сетевые операции, реакция на которые еще не определена правилами, образуется *очередь запросов* на создание новых правил. Данные запросы будут последовательно выводиться в окне обучения: сначала вам придется определить реакцию на действия первой сетевой программы, затем второй и т.д.. Все программы, до которых очередь еще не дошла, будут ожидать вашей реакции.

6.1.5. Предупреждение о подмене исполняемого модуля

Kaspersky Anti-Hacker защищает сетевые приложения от подмены оригинальных исполняемых файлов. В случае обнаружения подмены Kaspersky Anti-Hacker выдает предупреждение (см. рис. 21).

Вы можете выбрать один из следующих вариантов:

- **Запретить данному приложению дальнейшую сетевую активность** – все последующие сетевые операции для приложения будут запрещены: в начало списка правил для приложений будет добавлено запрещающее правило, а все ранее созданные для приложения правила будут отключены. Рекомендуем вам запустить антивирусную программу для данного приложения, либо восстановить приложение из архива, или переустановить его заново. После восстановления приложения удалите в списке правил запрещающее правило

для данного приложения, а также включите все созданные для него правила. Kaspersky Anti-Hacker может вновь показать предупреждение о подмене исполняемого модуля. В этом случае выберите описанный ниже вариант и продолжите работу.

- **Я знаю, что файл был изменен, и продолжаю доверять данному приложению** – все существующие для данного приложения правила будут продолжать действовать для измененного файла.

Нажмите на кнопку **ОК**.

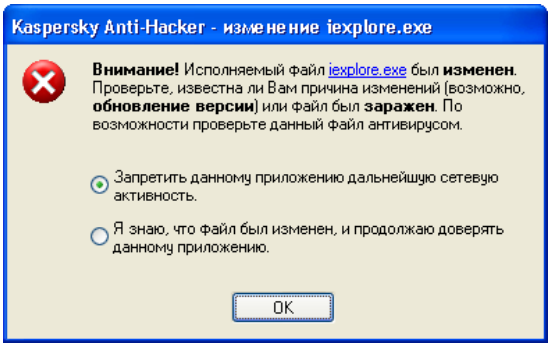


Рисунок 21. Предупреждение о подмене исполняемого файла приложения

6.2. Действия программы в случае атаки

Что происходит при обнаружении хакерской атаки?

При обнаружении хакерской атаки из системной панели разворачивается главное окно программы (если установлен флажок **При атаке показывать главное окно** – см. п. 6.1.1. на стр. 41). Обратите внимание на информацию о произошедшей хакерской атаке в нижней части рабочей области: программа отображает дату, время и тип атаки (см. рис. 24).

Атака будет заблокирована, а также будет заблокирован атакующий компьютер на время, которое определено в настройках (см. п. 6.5. на стр. 70).

Рисунок 22. Сообщение об обнаруженной хакерской атаке

Предположим, вы обнаружили, что с некоторых удаленных компьютеров постоянно проводятся попытки взлома. Вы можете запретить взаимодействие вашего компьютера с удаленными, задав соответствующие правила пакетной фильтрации (см. п. 6.4. на стр. 62).

При частом повторении атак рекомендуем вам выбрать режим **Запретить все** и обратиться к администратору или интернет-провайдеру.

6.3. Настройка правил для приложений

Как настроить правила для приложений? Мастер создания правил для приложений

6.3.1. Работа со списком правил

Чтобы вызвать на экран окно работы со списком правил для приложений,

выберите пункт **Правила для приложений** в меню **Сервис** программы.

После этого на экране откроется диалоговое окно **Правила для приложений** (см. рис. 23).

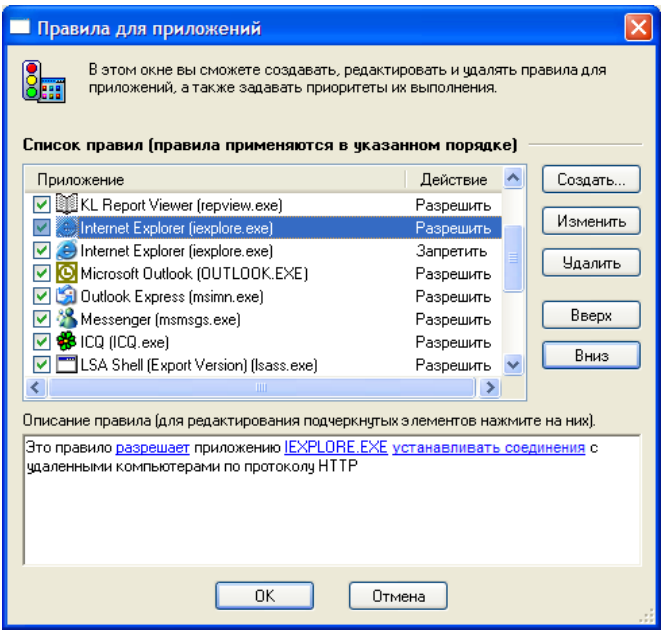


Рисунок 23. Диалоговое окно **Правила для приложений**

В левой верхней части диалогового окна находится список правил для приложений. В колонке "Приложение" отображается значок приложения, его название, а также флажок, показывающий, включено или отключено данное правило. В колонке "Действие" отображается краткая характеристика правила: **Разрешить** – если правило разрешающее, **Запретить** – если правило запрещающее.

Правила располагаются в порядке убывания приоритета их выполнения: первым выполняется правило, стоящее в списке первым, затем выполняется второе по списку правило и т.д. При попытке приложением выполнить сетевую операцию список правил перебирается сверху вниз до тех пор, пока не найдется правило, разрешающее или запрещающее данную операцию, либо пока не кончится список. Если правило не найдено, применяется действие по умолчанию (см. п. 4.2. на стр. 25). Таким образом, если вы хотите запретить приложению только часть операций, необходимо создать два правила - одно, расположенное в списке выше, должно разрешать часть операций, а другое, расположенное ниже, должно запрещать все операции для приложения. В этом случае при попытке приложения выполнить разрешенную операцию Kaspersky Anti-Hacker при переборе правил списка найдет разрешающее правило, а при возникновении любой другой операции найдет запрещающее правило.

Например, на рисунке 23 третье правило запрещает Internet Explorer любую сетевую активность, однако второе правило разрешает Internet Explorer доступ к интернету по HTTP-протоколу. Поскольку второе правило имеет приоритет выше, чем третье, Internet Explorer сможет соединяться с удаленными HTTP-серверами (и только с ними).

Обратите внимание, выполняются только правила с установленным флажком слева от названия. Например, на рисунке 23 четвертое и пятое правила отключены.

Чтобы временно включить/исключить правило из списка выполняемых,

установите/снимите соответствующий ему флажок в списке правил.

Справа от списка правил расположены кнопки управления, с помощью которых вы можете:

- **Создать** – создать новое правило. При нажатии на кнопку появляется мастер создания/редактирования правил для приложений;
- **Изменить** – редактировать правило, выбранное в списке. При нажатии на эту кнопку появляется мастер правил, который позволит вам изменить параметры выбранного правила;
- **Удалить** – удалить правило, выбранное в списке;

- **Вверх** – переместить выбранное в списке правило на одну строку выше, т.е. повысить его приоритет;

- **Вниз** – переместить выбранное в списке правило на одну строку ниже, т.е. понизить его приоритет.

Для изменения выбранного в списке правила вы можете нажать на клавишу **<ENTER>** или дважды щелкнуть по правилу мышью. Для удаления выбранного в списке правила вы можете нажать на клавишу **<DEL>**, а для добавления нового правила – нажать на клавишу **<INS>**.

Работать со списком правил можно также с помощью контекстного меню, которое содержит следующие пункты:

- **Изменить** – редактировать выбранное в списке правило;

- **Удалить** – удалить выбранное в списке правило;

- **Создать копию** – создать копию выбранного в списке правила. Созданная копия будет помещена под выбранным правилом.

Под списком правил расположено окно с кратким описанием правила, выделенного в списке. Такое же окно вы будете видеть в мастере создания и редактирования правила, поэтому расскажем о нем подробнее.

В окне описания правила черным цветом написан текст правила, который изменить нельзя, а синим цветом и подчеркиванием выделены параметры правила, поддающиеся изменению. Если параметр выделен жирным начертанием, это означает, что его значение необходимо ввести.

Чтобы ввести или изменить параметр правила,

1. В окне описания правила щелкните по параметру мышью.

2. В открывшемся диалоговом окне выберите нужный параметр (подробнее назначения параметров и соответствующие им диалоговые окна приведены в следующих пунктах).

В нижней части диалогового окна **Правила для приложений** расположены следующие кнопки:

- **ОК** – закрыть окно, сохранив все сделанные изменения;

- **Отмена** – закрыть окно без сохранения изменений.

Все изменения списка правил вступают в силу немедленно после их сохранения.

6.3.2. Добавление нового правила

Чтобы вызвать мастер правил для приложений,

нажмите на кнопку **Создать** в диалоговом окне **Правила для приложений** (см. рис. 23).

6.3.2.1. Шаг 1. Настройка правила

После вызова мастера на экране появится окно, показанное на рис. 24.

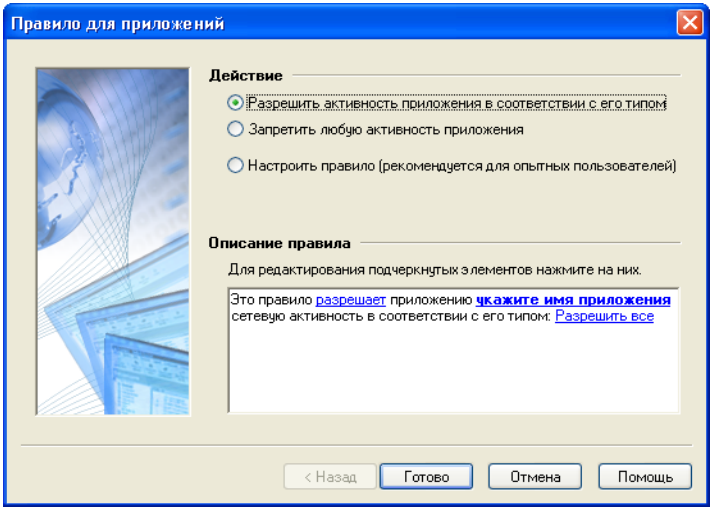
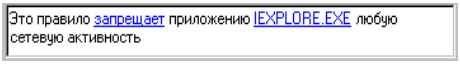


Рисунок 24. Первое окно мастера создания правила для приложений

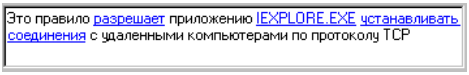
В группе **Действие** вы можете выбрать один из трех вариантов:

Действие	Описание правила
• **Разрешить активность приложения в соответствии с его типом**;	Это правило разрешает приложению IEXPLORE.EXE сетевую активность в соответствии с его типом: Просмотр Internet (Internet Explorer, Opera, ...)

- **Запретить любую активность приложения**;



- **Настроить правило**.



При выборе варианта **Настроить правило** на следующем шаге мастера возможно уточнение дополнительных параметров:

- тип интернет-приложения (клиент или сервер);
- протокол;
- удаленный адрес;
- удаленный порт;
- локальный порт.

Чтобы задать правило, разрешающее приложению сетевые взаимодействия в соответствии его с типом,

1. Выберите в группе **Действие** кнопку **Разрешить активность приложения** в соответствии с его типом.

2. Щелкните по строке "Укажите имя приложения" в поле **Описание правила**. В открывшемся окне **Выбор приложения** укажите имя приложения, к которому необходимо применить правило.

3. Тип приложения также указывается в поле **Описание правила**. По умолчанию указан тип "Разрешить все", который не ограничивает действий приложения никаким образом. Чтобы изменить тип, щелкните по нему мышью. В открывшемся диалоговом окне **Тип приложения** (см. рис. 25) выберите нужное значение в раскрывающемся списке и нажмите на кнопку **ОК**.

    - Просмотр Internet – для Internet browser, Netscape Navigator, и других веб-браузеров. Разрешается работа по протоколам HTTP, HTTPS, FTP и через стандартные прокси-серверы.

    - Передача файлов – для Reget, Gozilla и прочих подобных программ. Разрешается работа по протоколам HTTP, HTTPS, FTP, TFTP и через стандартные прокси-серверы.

- Электронная почта – для MS Outlook, MS Outlook Express, the Bat и прочих почтовых программ. Разрешается работа по протоколам SMTP, NNTP, POP3, IMAP4.

- Новости – для Forte Agent и других программ получения новостей. Разрешается работа по протоколам SMTP, NNTP.

- Обмен сообщениями – для ICQ, AIM и прочих chat-программ. Разрешается работа через стандартные прокси-серверы, а также непосредственное соединение вашего компьютера с компьютером собеседника.

- Конференции IRC – для mIRC и подобных программ. Разрешается стандартная аутентификация пользователей для сетей IRC и доступ к портам IRC-сервера.

- Бизнес-конференции – для MS NetMeeting и подобных программ. Разрешается работа по протоколам HTTP, HTTPS, через стандартные прокси-серверы, а также поддерживается работа в локальной сети (LDAP и др.).

- Удаленное управление – для Telnet и т.п.. Разрешается работа по протоколам Telnet и SSH.

- Синхронизация времени – для Timehook и подобных программ. Разрешается соединение с time и daytime-серверами.

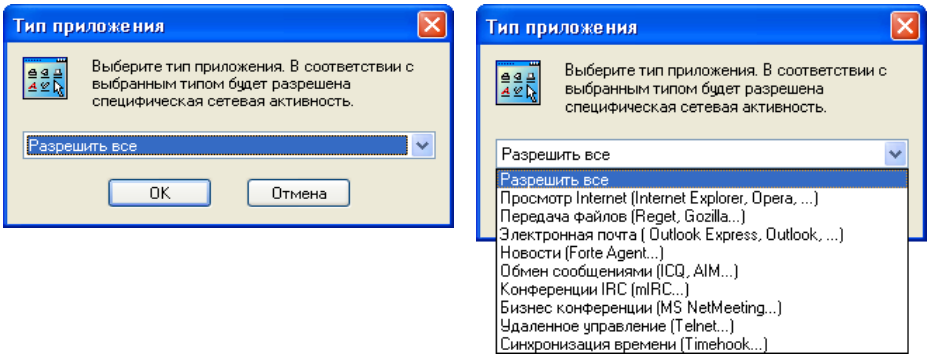


Рисунок 25. Выбор типа приложения

Чтобы запретить приложению любые сетевые взаимодействия,

1. Выберите в группе **Действие** кнопку **Запретить любую активность приложения**.

2. Щелкните по строке "Укажите имя приложения" в поле **Описание правила**. В открывшемся окне **Выбор приложения** укажите имя приложения, к которому необходимо применить запрещающее правило.

Если перечисленные выше возможности настройки правил недостаточны, например, вы хотите устанавливать соединение только с определенным IP-адресом, задайте дополнительные параметры правила.

Чтобы настроить дополнительные параметры правила,

1. Выберите в группе **Действие** кнопку **Настроить правило**.

2. Щелкните по строке "Укажите имя приложения" в поле **Описание правила**. В открывшемся окне **Выбор приложения** укажите имя приложения, к которому необходимо применить правило.

3. Щелкните по строке "Разрешает" в поле **Описание правила**. В открывшемся диалоговом окне **Выбор действия** (см. рис. 26) укажите нужное действие, и нажмите на кнопку **ОК**:

   - **Запретить**;

   - **Разрешить**.

4. Укажите, на какую активность приложения должно реагировать данное правило: установку (по умолчанию) или прием соединений. Чтобы сменить значение по умолчанию, щелкните по строке "устанавливать соединения" в поле **Описание правила**. В открывшемся диалоговом окне **Выбор типа активности приложения** (см. рис. 27) укажите нужный вариант активности **Прием входящих сетевых соединений с удаленных компьютеров** и нажмите на кнопку **ОК**.

После завершения работы с первым окном мастера нажмите на кнопку **Далее**.

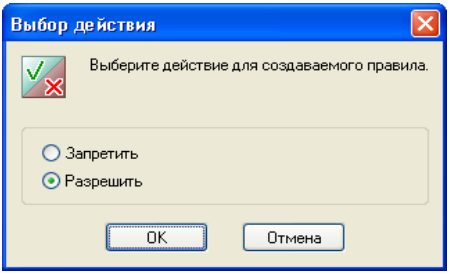


Рисунок 26. Выбор действия

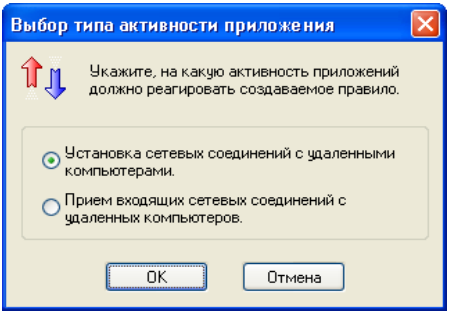


Рисунок 27. Выбор типа активности приложения

Если вы нажмете на кнопку **Далее**, не выбрав приложения, на экране появится предупреждение о необходимости продолжить работу в текущем окне мастера.

6.3.2.2. Шаг 2. Условия выполнения правила

Окно для ввода условий выполнения правила появляется только в случае, если вы выбрали в группе **Действие** кнопку **Настроить правило**.

В этом окне вы можете уточнить протокол, адрес удаленного компьютера и порты.

В раскрывающемся списке **Протокол** находится ряд предустановленных названий протоколов и соответствующих им номеров портов:

- HTTP;
- IMAP;
- SMTP;
- NNTP;
- POP3;
- DNS.

Если вы хотите задать другой номер порта, выберите значение:

- Другой протокол, базирующийся на TCP – для служб, основанных на TCP-протоколе;
- Другой протокол, базирующийся на UDP – для служб, основанных на UDP протоколе.

В группе **Параметры** отображается список дополнительных параметров, состав которого зависит от выбранного протокола.

Удаленный адрес – адрес удаленного компьютера, с которым происходит обмен данными. Для ввода адреса следует щелкнуть мышью по строке "Укажите адрес" в поле **Описание правила**. Если вы хотите задать список адресов, щелкните мышью, удерживая клавишу **<CTRL>**. Подробнее см. п. 6.3.2.2.1. на стр. 57.

Удаленный порт – номер удаленного порта. Для ввода порта следует щелкнуть мышью по строке "Укажите порт", расположенной справа от строки "Удаленный порт" в поле **Описание правила**. Если вы хотите задать список портов, щелкните мышью, удерживая клавишу **<CTRL>**. Подробнее см. п. 6.3.2.2.2. на стр. 60.

Локальный порт – номер локального порта. Для ввода порта следует щелкнуть мышью по строке "Укажите порт", расположенной справа от строки "Локальный порт" в поле **Описание правила**. Если вы хотите задать список портов, щелкните мышью, удерживая клавишу **<CTRL>**. Подробнее см. п. 6.3.2.2.2. на стр. 60.

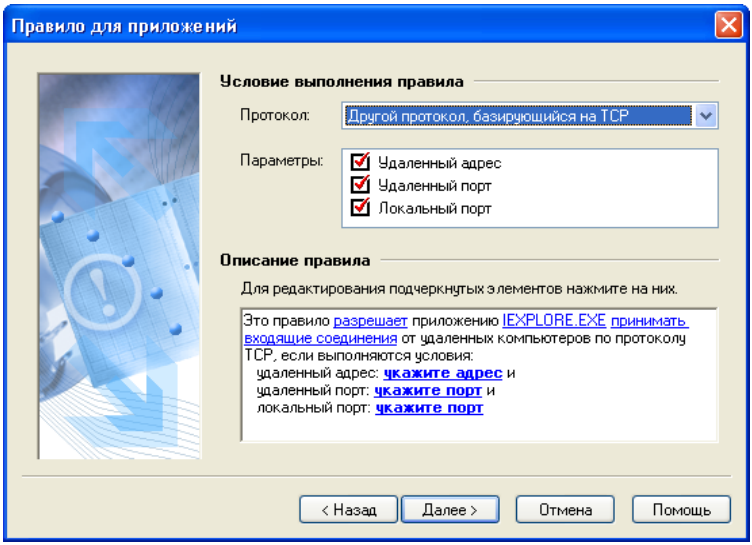


Рисунок 28. Ввод условий выполнения правила

6.3.2.2.1. Ввод адреса или диапазона адресов

Ввод адресов осуществляется с помощью двух диалоговых окон.

Диалоговое окно **Укажите адрес или диапазон адресов** (см. рис. 29) появляется, когда в мастере правил вы щелкаете мышью по строке с названием параметра-адреса, удерживая при этом клавишу **<CTRL>**,

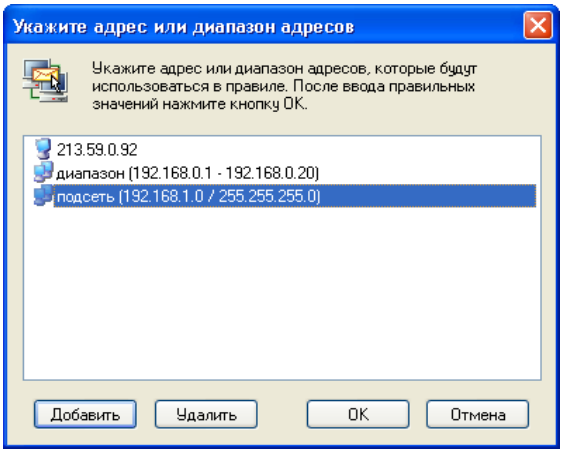


Рисунок 29. Диалоговое окно **Укажите адрес или диапазон адресов**

В расположенный в окне список вы можете добавлять произвольное количество адресов, диапазонов адресов и адресов сетей с помощью кнопок **Добавить** и **Удалить**. После окончания формирования списка адресов нажмите на кнопку **OK** для возврата к мастеру правил.

По кнопке **Добавить**. из окна **Укажите адрес и диапазон адресов** появляется окно **Адрес** (см. рис. 30). Это же окно появляется, когда вы щелкаете мышью по строке с названием параметра-адреса напрямую из мастера правил.

Диалоговое окно **Адрес** предназначено для ввода адреса, или диапазона адресов, или адреса сети, который будут использовать в правиле (см. рис. 30).

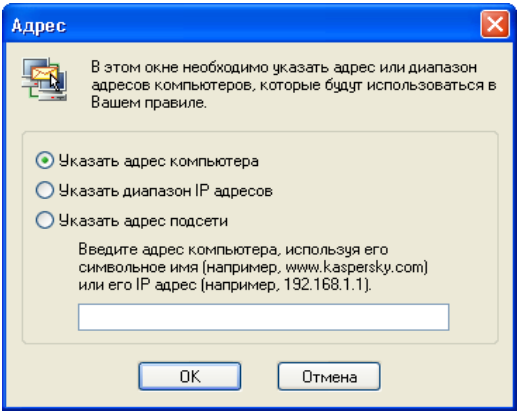


Рисунок 30. Диалоговое окно **Адрес**. Ввод адреса компьютера

Вы можете выбрать один из трех вариантов:

- **Указать адрес компьютера** – в поле ввода указывается символьное имя компьютера (например, `www.kaspersky.com`) или его IP адрес (например, `192.68.1.1`);

- **Указать диапазон IP адресов** – в поле **Стартовый адрес** указывается IP адрес начала диапазона адресов, а в поле **Конечный адрес** – IP адрес конца диапазона (см. рис. 31);

- **Указать адрес подсети** – в поле **Адрес подсети** указывается адрес подсети, а в поле **Маска подсети** – ее маска (см. рис. 32).

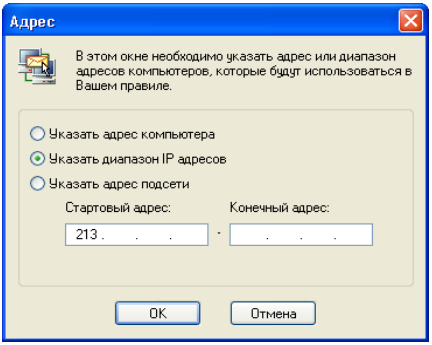


Рисунок 31. Ввод диапазона адресов

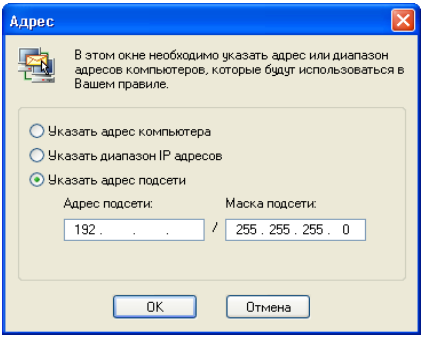


Рисунок 32. Ввод адреса подсети

После ввода адреса нажмите на кнопку **ОК**.

6.3.2.2.2. Ввод порта

Ввод номеров портов осуществляется с помощью двух диалоговых окон.

Диалоговое окно **Укажите порт или диапазон портов** (см. рис. 33) появляется, когда в мастере правил вы щелкаете мышью по строке с названием параметра-порта, удерживая при этом клавишу **<CTRL>**,

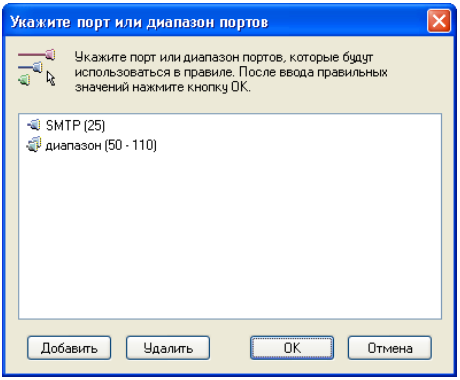


Рисунок 33. Диалоговое окно **Укажите порт или диапазон портов**

В расположенный в окне список вы можете добавлять произвольное количество номеров и диапазонов номеров портов с помощью кнопок **Добавить** и **Удалить**. После окончания формирования списка портов нажмите на кнопку **ОК** для возврата к мастеру правил.

По кнопке **Добавить** из окна **Укажите порт и диапазон портов** появляется окно **Порт** (см. рис. 30). Это же окно появляется, когда вы щелкаете мышью по строке с названием параметра-порта напрямую из мастера правил.

Диалоговое окно **Порт** предназначено для ввода номера порта или диапазона номеров портов, которые будут использоваться в правиле (см. рис. 34).

Вы можете выбрать один из двух вариантов:

- **Указать номер порта** – в редактируемом раскрывающемся списке вы можете выбрать одно из предустановленных значений или ввести номер порта вручную.

- **Указать диапазон портов** – в первом поле укажите номер начала диапазона портов, а во втором поле – номер конца диапазона (см. рис. 35).

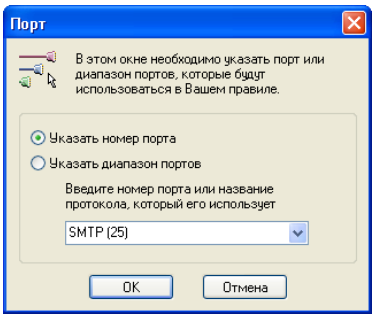


Рисунок 34. Диалоговое окно **Порт**

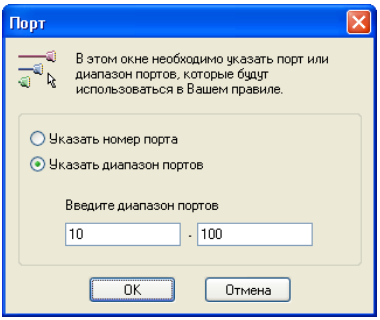


Рисунок 35. Ввод адреса подсети

После ввода номеров портов нажмите на кнопку **ОК**.

6.3.2.3. Шаг 3. Дополнительные действия

В качестве дополнительных действий вы можете включить флажки **Занести событие в журнал**, чтобы запись о произошедшем событии появлялась в журнале, а также флажок **Уведомить пользователя**, чтобы при возникновении события на экран выводилось предупреждение (см. рис. 18).

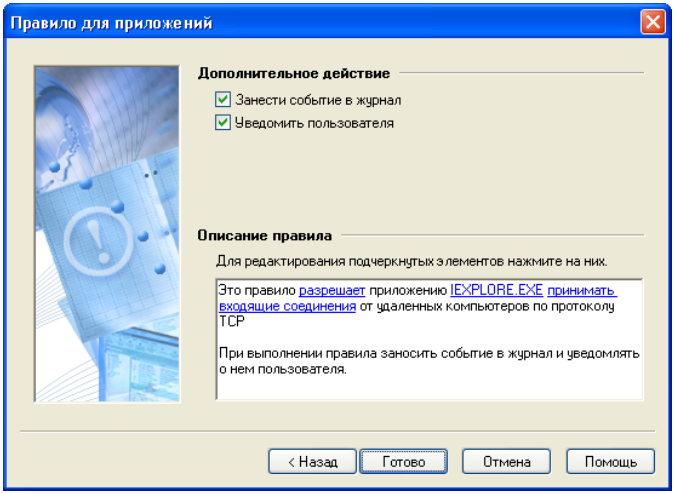


Рисунок 36. Дополнительные действия

6.4. Настройка правил фильтрации пакетов

Как настроить правила фильтрации пакетов? Мастер создания правил фильтрации пакетов

6.4.1. Работа со списком правил

Работа с правилами фильтрации пакетов происходит аналогично работе с правилами для приложений.

Чтобы вызвать на экран окно работы со списком правил фильтрации пакетов,

выберите пункт **Правила фильтрации пакетов** в меню **Сервис** программы.

После этого на экране откроется диалоговое окно **Правила фильтрации пакетов** (см. рис. 37).

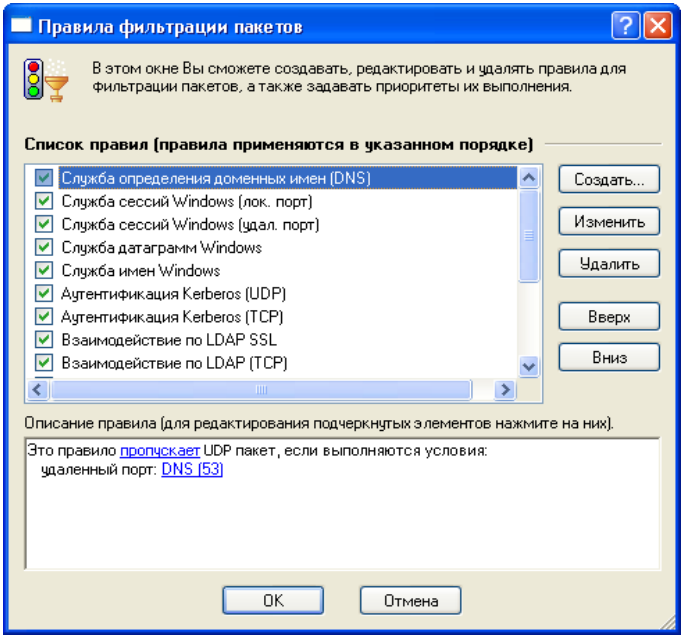


Рисунок 37. Диалоговое окно **Правила фильтрации пакетов**

В левой верхней части диалогового окна находится список правил фильтрации пакетов. В каждой строке перед названием правила находится флажок, показывающий его статус: включено или отключено.

Правила располагаются в порядке убывания приоритета их выполнения: первым выполняется правило, стоящее в списке первым, затем выполняется второе по списку правило и т.д. Обратите внимание, выполняются только правила с установленным флажком слева от названия.

Чтобы включить/исключить правило из списка выполняемых,

установите/снимите соответствующий ему флажок в списке правил.

Справа от списка правил расположены кнопки управления, с помощью которых вы можете:

- **Создать** – создать новое правило. При нажатии на кнопку появляется мастер создания нового правила фильтрации пакетов;

- **Изменить** – редактировать правило, выбранное в списке. При нажатии на кнопку появляется мастер редактирования правила фильтрации пакетов;

- **Удалить** – удалить правило, выбранное в списке;

- **Вверх** – переместить выбранное в списке правило на одну строку выше, т.е. повысить его приоритет;

- **Вниз** – переместить выбранное в списке правило на одну строку ниже, т.е. понизить его приоритет.

Для изменения выбранного в списке правила вы можете нажать на клавишу **<ENTER>** или дважды щелкнуть по правилу мышью. Для удаления выбранного в списке правила вы можете нажать на клавишу **<DEL>**, а для добавления нового правила – нажать на клавишу **<INS>**.

Работать со списком правил можно также с помощью контекстного меню, которое содержит следующие пункты:

- **Изменить** – редактировать выбранное в списке правило;

- **Удалить** – удалить выбранное в списке правило;

- **Создать копию** – создать копию выбранного в списке правила. Созданная копия будет помещена под выбранным правилом.

Под списком правил расположено окно с кратким описанием правила, выделенного в списке. Такое окно вы будете видеть также в мастере создания и редактирования правила, поэтому расскажем о нем подробнее.

В окне описания правила черным цветом написан текст правила, который изменить нельзя, а синим цветом и подчеркиванием выделены параметры правила, поддающиеся изменению. Если параметр выделен жирным начертанием, это означает, что его значение необходимо ввести.

Чтобы ввести или изменить параметр правила,

1. В окне описания правила щелкните по параметру мышью.

2. В открывшемся диалоговом окне выберите нужный параметр (подробнее назначения параметров и соответствующие им диалоговые окна приведены в следующих пунктах).

В нижней части диалогового окна **Правила фильтрации пакетов** расположены следующие кнопки:

- **ОК** – закрыть окно, сохранив все сделанные изменения;
- **Отмена** – закрыть окно без сохранения изменений.

Все изменения списка правил вступают в силу немедленно после их сохранения.

Правила пакетной фильтрации имеют более высокий приоритет, чем правила для приложений, и исполняются первыми.

6.4.2. Добавление нового правила

Мастер добавления правил фильтрации пакетов аналогичен мастеру добавления правил для приложений и состоит из двух шагов.

6.4.2.1. Шаг 1. Ввод условий срабатывания правила

На первом шаге определения правила фильтрации правила вы можете задать:

- используемый протокол (TCP, UDP, ICMP, другие IP протоколы);
- адрес назначения пакетов;
- направление трафика (исходящий, входящий);
- специфичные для протокола значения (для протоколов TCP и UDP – порты, для протокола ICMP – типы сообщений, для других IP протоколов – номер протокола);
- действие (разрешить/запретить).

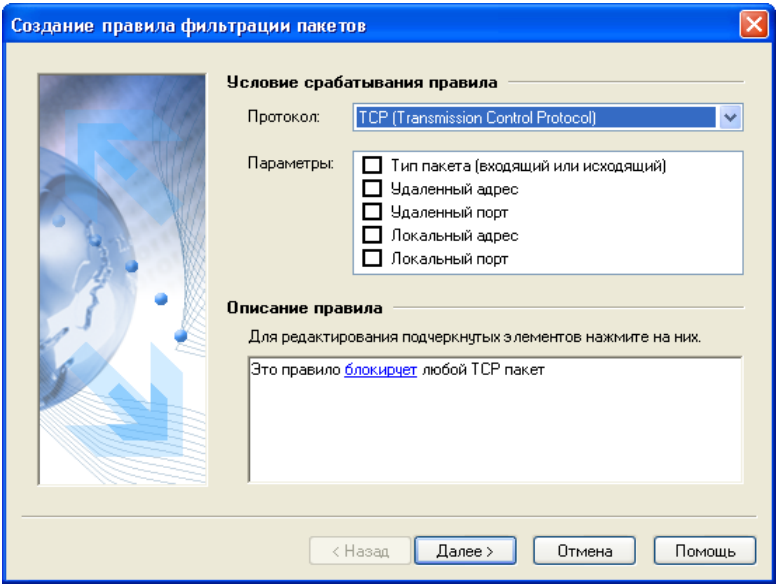


Рисунок 38. Первое окна мастера создания правил фильтрации пакетов

Чтобы задать правило фильтрации,

1. Выберите протокол, который будет фильтроваться, в раскрывающемся списке **Протокол**: Возможные варианты протоколов: **TCP (Transmission Control Protocol)**, **UDP (User Datagram Protocol)**, **ICMP (Internet Control Message Protocol)**, **Другие IP протоколы**. По умолчанию выбран пункт TCP.
2. В группе флажков **Параметры** задайте

Тип пакета (входящий или исходящий) – направление передачи пакетов. По умолчанию флажок отключен, что соответствует контролю трафика в обоих направлениях. Если вы хотите, чтобы программа контролировала только входящий, или только исходящий трафик, включите флажок, и задайте направление трафика в поле **Описание правила**. Для ввода направления трафика следует щелкнуть мышью по строке с указанием направления. В открывшемся диалоговом окне **Направление передачи пакетов** выберите нужный вариант и нажмите на кнопку **ОК**.

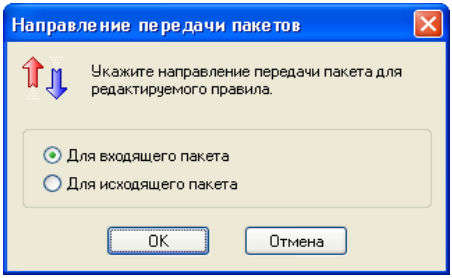


Рисунок 39. Диалоговое окно **Направление передачи пакетов**

3. В группе флажков **Параметры** отображается также список дополнительных параметров, состав которого зависит от выбранного протокола.

   - Для протоколов TCP, UDP можно указать **Удаленный порт** и **Локальный порт**.
   - Для протокола ICMP можно указать **Тип ICMP сообщения**.
   - Для других протоколов, базирующихся на IP, можно указать **Протокол**.

   Удаленный адрес – адрес удаленного компьютера (для всех протоколов).

   Локальный адрес – адрес локального компьютера (для всех протоколов).

   Для ввода адреса следует щелкнуть мышью по строке "Укажите адрес", расположенной справа от строки "Удаленный адрес" или, соответственно, "Локальный адрес" в поле **Описание правила**. Если вы хотите задать список адресов, щелкните мышью, удерживая клавишу **<CTRL>**. Подробнее см. п. 6.3.2.2.1. на стр. 57.

   Удаленный порт – номер порта удаленного компьютера (для протоколов TCP и UDP).

   Локальный порт – номер порта локального компьютера (для протоколов TCP и UDP).

   Для ввода порта следует щелкнуть мышью по строке "Укажите порт", расположенной справа от строки "Удаленный порт" или, соответственно, "Локальный порт" в поле **Описание правила**. Если вы хотите задать список портов, щелкните мышью, удерживая клавишу **<CTRL>**. Подробнее см. п. 6.3.2.2.2. на стр. 60.

Тип ICMP сообщения – тип ICMP сообщения (только для протокола ICMP). Для ввода типа следует щелкнуть мышью по строке "Укажите тип сообщения" в поле **Описание правила**. В открывшемся диалоговом окне **Тип ICMP сообщения** (см. рис. 40) в раскрывающемся списке выберите нужное значение и нажмите на кнопку **OK**.

- Echo request;
- Echo reply;
- Trace route (TTL exceed);
- Net unreachable;
- Host unreachable;
- Protocol unreachable;
- Port unreachable;
- Redirect for host;
- Redirect for net;
- Redirect for TOS and net;
- Redirect for TOS and host.

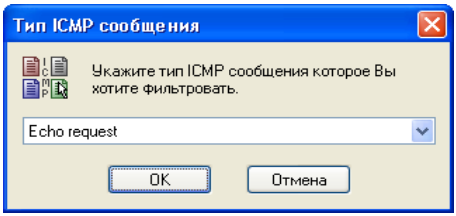


Рисунок 40. Диалоговое окно **Тип ICMP сообщения**

Протокол – название или номер протокола (только для IP-протоколов). Если вы не установите данный флажок, будет производиться фильтрация всех IP протоколов. Для ввода определенного протокола установите флажок и щелкните мышью по строке "Укажите протокол" в поле **Описание правила**. В открывшемся диалоговом окне **Укажите протокол** (см. рис. 41) в раскрывающемся списке выберите нужное значение и нажмите на кнопку **OK**. В приведенном ниже списке протоколов в скобках приводится соответствующий номер протокола.

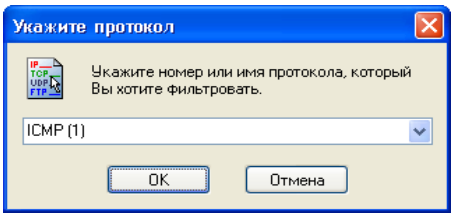


Рисунок 41. Диалоговое окно **Укажите протокол**

- ICMP(1);
- IGMP,RGMP(2);
- GGP(3);
- IP in IP encupsulation(4);
- TCP(6);
- IGRP(9);
- UDP(17);
- GRE(47);
- ESP(50);
- AH(51);
- IP with encryption(53).

4. Задайте действие, которое программе следует выполнять при обнаружении пакета, удовлетворяющего вышеперечисленным условиям: блокировать или разрешать. По умолчанию предлагается блокировать такие пакеты. Чтобы изменить значение, щелкните по нему в поле **Описание правила**. В открывшемся окне Выбор действия выберите нужный вариант и нажмите на кнопку **ОК** (см. рис. 42).

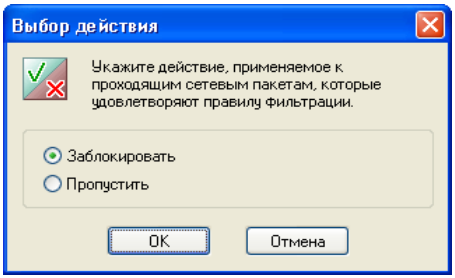


Рисунок 42. Диалоговое окно **Выбор действия**

6.4.2.2. Шаг 2. Ввод названия правила и дополнительных действий

На втором шаге создания правила фильтрации пакетов необходимо ввести его название в поле **Название правила**. Название правила отображается в списке правил и помогает их идентифицировать. По умолчанию предлагается уникальное имя правила вида: "Правило фильтрации #<номер правила>". Рекомендуем вам ввести название, отражающее специфику правила.

В качестве дополнительных действий вы можете включить флажки **Занести событие в журнал**, чтобы запись о произошедшем событии появлялась в

журнале, а также флажок **Уведомить пользователя**, чтобы при возникновении события на экран выводилось предупреждение (см. рис. 18).

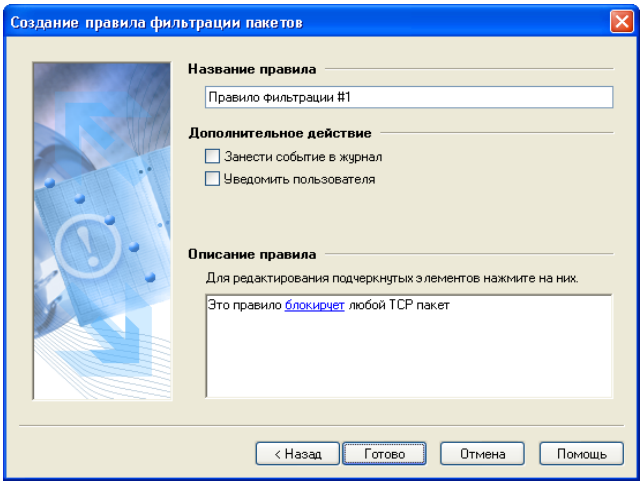


Рисунок 43. Ввод названия правила и дополнительных действий

6.5. Детектор атак

Как настроить детектор атак оптимальным образом?

6.5.1. Окно настройки детектора атак

Чтобы открыть окно настройки детектора атак,

выберите в меню **Сервис** пункт **Параметры** и переключитесь на закладку **Детектор атак** (см. рис. 44).

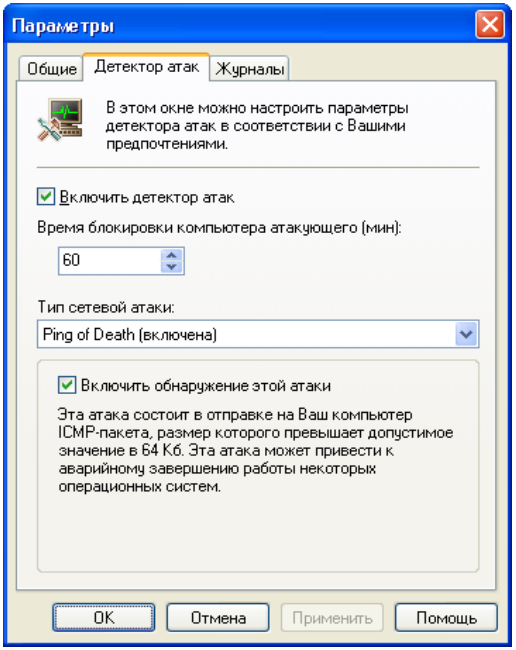


Рисунок 44. Закладка **Детектор атак** диалогового окна **Параметры**

Расположенный в верхней части закладки флажок ☑ **Включить детектор атак** рекомендуем вам держать включенным постоянно. Именно он отвечает за включение и отключение детектора атак на вашем компьютере.

Ниже расположено числовое поле **Время блокировки атакующего**, которое определяет, на сколько минут будет полностью блокирован атакующий компьютер, если его адрес удалось определить. Данный параметр является общим для всех типов атак.

Изменение параметра **Время блокировки атакующего** вступает в силу немедленно после нажатия на кнопку **ОК** или **Применить** в окне **Параметры**, и действует для всех вновь обнаруживаемых атак. Для компьютеров, заблокированных в результате уже произошедших атак, время блокировки не меняется.

Расположенная в нижней части окна группа полей меняется в зависимости от названия атаки, которая выбрана в раскрывающемся списке **Тип сетевой атаки**.

Установите флажок **Включить обнаружение этой атаки**, если вы хотите, чтобы атаки выбранного типа были обнаружены. Для принятия решения вам сможет помочь описание атаки, которое расположено под этим флажком.

6.5.2. Список обнаруживаемых хакерских атак

Kaspersky Anti-Hacker обнаруживает наиболее распространенные DoS атаки (*SYN Flood, UDP Flood, ICMP Flood*), атаки *Ping of death, Land, Helkern, Lovesan u SmbDie*, а также отслеживает сканирование портов, которое обычно предшествует более мощной атаке:

- *Атака Ping of death* состоит в посылке ICMP-пакета, размер которого превышает допустимое значение в 64Кб. Эта атака может привести к аварийному завершению работы некоторых операционных систем.

- *Атака Land* заключается в передаче на открытый порт вашего компьютера запроса на установление соединения с самим собой. Атака приводит к зацикливанию компьютера, в результате чего сильно возрастает загрузка процессора и возможно аварийное завершение работы операционной системы.

- *Сканирование TCP портов* заключается в попытке обнаружить открытые TCP-порты на вашем компьютере. Атака используется для поиска слабых мест в компьютерной системе и обычно предшествует более мощной атаке. Для этой атаки вы можете задать **Количество портов** – число портов, которые пытается открыть удаленный компьютер, и **Время** – период времени, в течение которого это происходит.

- *Сканирование UDP портов* аналогично сканированию TCP-портов и заключается в попытке обнаружить открытые UDP-порты на вашем компьютере. Наличие атаки определяется по количеству UDP-пакетов, отправленных на различные порты компьютера за некоторый промежуток времени. Атака используется для поиска слабых мест в компьютерной системе и обычно предшествует более мощной атаке. Для этой атаки вы можете задать **Количество портов** – число портов, которые пытается открыть удаленный компьютер, и **Время** – период времени, в течение которого это происходит.

- *Атака SYN Flood* заключается в отправке на ваш компьютер большого количества запросов на установку ложного соединения. Система резервирует определенные ресурсы для каждого из таких соединений, в результате чего тратит свои ресурсы полностью и перестает реагировать на другие попытки соединения. Для этой атаки вы можете задать **Количество соединений** – число соединений, которые пытается установить удаленный компьютер, и **Время** – период времени, в течение которого это происходит.

- *Атака UDP Flood* заключается в отправке UDP-пакета, который за счет своей структуры бесконечно пересылается от вашего компьютера на произвольный доступный компьютеру адрес и обратно. В результате атаки тратятся ресурсы обоих машин и увеличивается нагрузка на канал связи. Для этой атаки вы можете задать **Количество UDP пакетов** – число входящих UDP пакетов, и **Время** – период времени, в течение которого это происходит.

- *Атака ICMP Flood* заключается в отправке на ваш компьютер большого количества ICMP-пакетов. Атака приводит к тому, что компьютер вынужден отвечать на каждый поступивший пакет, в результате чего сильно возрастает загрузка процессора. Для этой атаки вы можете задать **Количество ICMP пакетов** – число входящих ICMP пакетов, и **Время** – период времени, в течение которого это происходит.

- *Атака Helkern* заключается в отправке на ваш компьютер UDP-пакетов специального вида, способных выполнить вредоносный код. Атака приводит к замедлению работы интернета.

- *Атака Lovesan* заключается в попытке обнаружения на вашем компьютере бреши в сервисе DCOM RPC операционных систем Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server 2003. При наличии бреши на компьютер отправляется вредоносная программа, позволяющая производить любые манипуляции на вашем компьютере.

- *Атака SmbDie* заключается в попытке установить соединение по SMB-протоколу; в случае успеха на компьютер отправляется пакет особого вида, который пытается переполнить буфер. Результатом является перезагрузка компьютера. Атаке подвержены ОС Windows 2k/XP/NT.

ГЛАВА 7. ПРОСМОТР РЕЗУЛЬТАТОВ РАБОТЫ ПРОГРАММЫ

7.1. Просмотр текущего состояния

Сетевая активность всех приложений, установленных на вашем компьютере, постоянно регистрируется программой Kaspersky Anti-Hacker. Вы можете просматривать информацию о текущей сетевой активности в следующем виде:

- **Список активных сетевых приложений**. Вся сетевая активность группируется по приложениям, ее инициирующим. Для каждого приложения приводится список портов и соединений, которыми владеет данное приложение.

- **Список активных соединений**. Отображаются все входящие и исходящие соединения, адреса удаленных компьютеров и номера портов.

- **Список открытых портов**. Отображаются открытые на вашем компьютере порты.

7.1.1. Список активных сетевых приложений

Если вы хотите узнать, какие сетевые приложения активны на вашем компьютере в данный момент,

выберите в меню **Вид** пункт **Показать**, и в открывшемся подменю укажите пункт **Активные сетевые приложения** (см. рис. 45). Вы также можете нажать на кнопку  в панели инструментов.

После этого на экране появится диалоговое окно **Список активных сетевых приложений**.

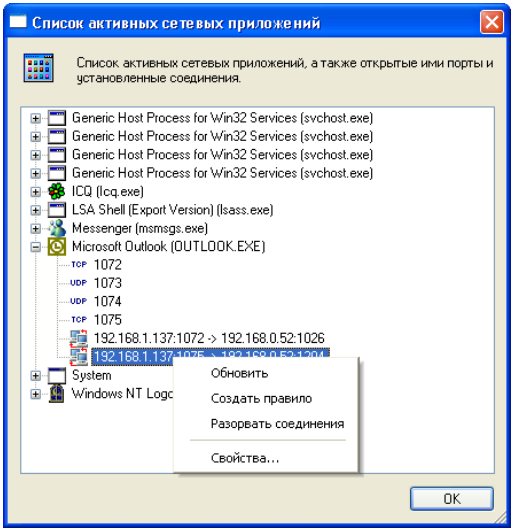


Рисунок 45. Диалоговое окно **Список активных сетевых приложений**

С помощью этого диалогового окна вы можете просмотреть список активных приложений и принадлежащих им сетевых ресурсов. Приложения упорядочены по именам, что упрощает навигацию по списку. Слева от названия каждого приложения находится его значок.

Раскрыв строку с названием приложения вы можете просматривать список открытых портов и установленных соединений для конкретного приложения:

- Открытый порт обозначается значком **TCP** или **UDP** в зависимости от типа порта. Справа от него отображается номер порта.

- Соединение обозначается значком  , если инициатором соединения является ваш компьютер, или значком  , если это соединение установлено извне. Справа от значка приводятся параметры соединения:
  `<адрес инициатора>:<порт инициатора>` → `<адрес назначения>:<порт назначения>`

Список активных сетевых приложений обновляется автоматически два раза в секунду.

Список имеет контекстное меню, состоящее из нескольких пунктов.

- **Обновить** – принудительно обновить информацию об активных сетевых приложениях.

- **Создать правило** – создать правило на основе выбранного в списке порта или соединения. Программа вызовет мастер создания правил для приложений, заполнив его сведениями о выбранном вами номере порта или соединении.

- **Разорвать соединение** – разорвать установленное соединение, выбранное в списке (пункт появляется только при выборе соединений).

Внимание! При принудительном разрыве соединения некоторые приложения могут начать работать некорректно.

- **Свойства** – показать более детальную информацию о выбранном в списке элементе: приложении (см. рис. 46), соединении (см. рис. 48) или порте (см. рис. 50).

Таблица может содержать строки с одинаковыми названиями приложений. Это означает, что одно и то же приложение запущено несколько раз. Обратите внимание, что открыв строки с одинаковыми названиями, вы можете увидеть разные списки открытых портов и установленных соединений.

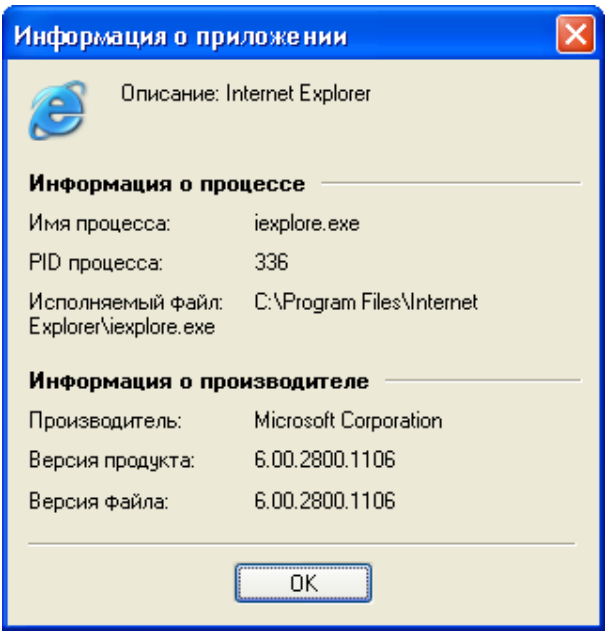


Рисунок 46. Диалоговое окно **Информация о приложении**

В верхней части диалогового окна **Информация о приложении** расположена секция **Информация о процессе**:

- **Имя процесса** – название исполняемого файла;
- **PID процесса** – идентификатор процесса;
- **Исполняемый файл** – полный путь к исполняемому файлу;

В нижней части таблицы сведений находится секция **Информация о производителе**:

- **Производитель** – информация о фирме, выпустившей программу;
- **Версия продукта** – номер версии программы;
- **Версия файла** – номер версии исполняемого файла.

7.1.2. Список установленных соединений

Чтобы просмотреть список установленных соединений,

выберите в меню **Вид** пункт **Показать**, и в открывшемся подменю выберите пункт **Активные соединения** (см. рис. 47). Вы также можете нажать на кнопку  в панели инструментов.

После этого на экране появится диалоговое окно **Список активных соединений**.

Каждая строка списка соответствует одному соединению. Соединение обозначается значком  , если инициатором соединения является ваш компьютер, или значком  , если это соединение установлено извне.

Для каждого соединения приводятся следующие параметры:

- **Удаленный адрес** – адрес и порт удаленного компьютера, с которым установлено соединение;
- **Локальный адрес** – адрес и порт вашего компьютера;

- **Процесс** – инициировавший соединение процесс.

Вы можете отсортировать список по любому из перечисленных параметров.

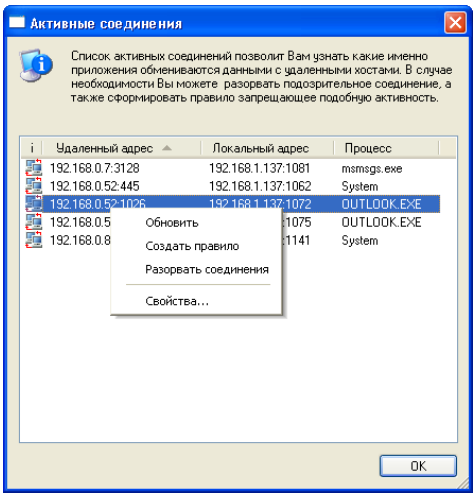


Рисунок 47. Диалоговое окно **Активные соединения**

Список активных соединений обновляется автоматически два раза в секунду.

При необходимости вы можете разорвать нежелательные соединения и/или создать правила, запрещающие подобные соединения в дальнейшем. Используйте для этого контекстное меню:

- **Обновить** – принудительно обновить информацию о текущих соединениях;

- **Создать правило** – создать правило на основе выбранного в списке соединения. Программа вызовет мастер создания правил для приложений, заполнив его сведениями о выбранном вами соединении;

- **Разорвать соединение** – разорвать выбранное в списке соединение;

Внимание! При принудительном разрыве соединения некоторые приложения могут начать работать некорректно.

- **Свойства** – показать более детальную информацию о выбранном в списке соединении (см. рис. 48).

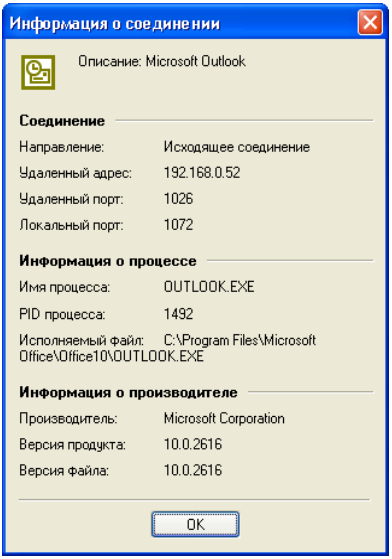


Рисунок 48. Диалоговое окно **Информация о соединении**

В секции **Соединение** диалогового окна **Информация о соединении** содержатся следующие сведения:

- **Направление** – является соединение входящим или исходящим;
- **Удаленный адрес** – символьное имя или IP-адрес удаленного компьютера;
- **Удаленный порт** – номер удаленного порта;
- **Локальный порт** – номер локального порта;

Ниже расположены секции **Информация о процессе** и **Информация о производителе** (см. п. 7.1.1. на стр. 74).

7.1.3. Список открытых портов

Чтобы просмотреть список открытых портов,

выберите в меню **Вид** пункт **Показать**, и в открывшемся подменю пункт **Открытые порты** (см. рис. 49). Вы также можете нажать на кнопку в панели инструментов.

После этого на экране появится диалоговое окно **Открытые порты**.

Каждая строка списка соответствует одному открытому порту. Порт обозначается значком **TCP** или **UDP** в зависимости от его типа.

Для каждого открытого порта приводятся следующие параметры:

- **Локальный порт** – номер порта;
- **Процесс** – открывший порт процесс;
- **Путь** – полный путь к исполняемому модулю.

Вы можете отсортировать список по любому из перечисленных параметров.

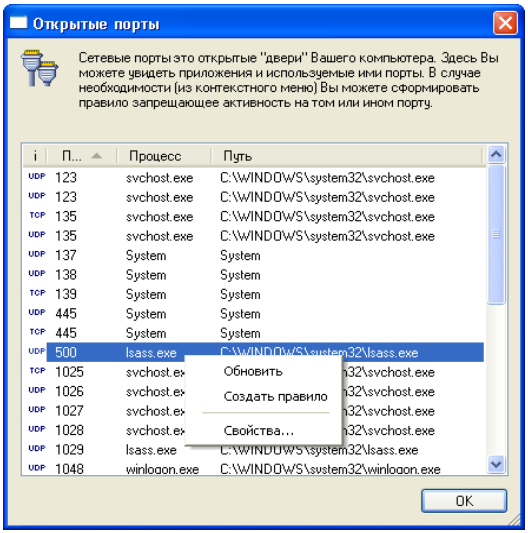


Рисунок 49. Диалоговое окно **Открытые порты**

Список открытых портов обновляется автоматически два раза в секунду.

При необходимости вы можете создать правило, запрещающее в дальнейшем соединения на выбранный порт. Используйте для этого контекстное меню:

- **Обновить** – принудительно обновить информацию об открытых портах;

- **Создать правило** – создать правило на основе выбранного в списке порта. Программа вызовет мастер создания правил для приложений, заполнив его сведениями о выбранном вами номере порта;

- **Свойства** – показать более детальную информацию о выбранном в списке порте (см. рис. 50).

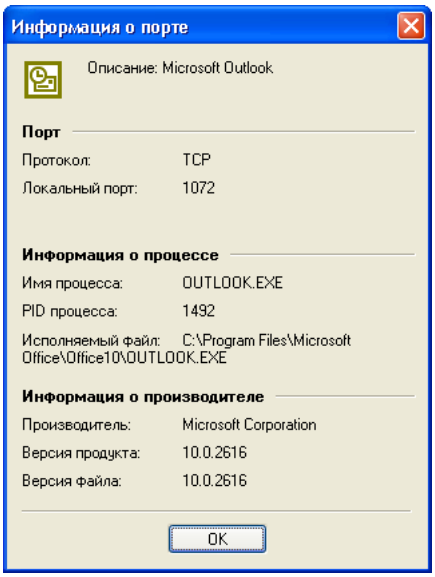


Рисунок 50. Диалоговое окно **Информация о порте**

Секция **Порт** диалогового окна **Информация о порте** содержит следующие данные:

- **Протокол** – имя протокола;

- **Локальный порт** – номер локального порта.

Ниже расположены секции **Информация о процессе** и **Информация о производителе** (см. п. 7.1.1. на стр. 74).

7.2. Работа с журналами

Сетевые события, происходящие на вашем компьютере, заносятся и хранятся в *журналах*. Для разных событиях предусмотрены журналы трех типов:

- **Сетевых атак**. В этом журнале хранится информация о последних атаках на ваш компьютер (см. п. 6.5. на стр. 70);
- **Активности сетевых приложений**. В этот журнал заносятся события, протоколировать которые вы указали в мастере создания правил для приложений (см. п. 6.3.2.3. на стр. 61);
- **Пакетной фильтрации**. В этот журнал заносятся события, протоколировать которые вы указали в мастере создания правил фильтрации пакетов (см. п. 6.4.2.2. на стр. 69).

Для работы со всеми журналами предназначено единственное окно (*окно журналов*).

Размер журналов может быть ограничен, также вы можете задать режим очистки журнала каждый раз при запуске программы или хранить результаты нескольких сессий работы (см. п. 7.2.4. на стр. 87).

При желании вы можете дать команду принудительно очистить журнал.

Вы также можете сохранить журнал в файле на жестком диске.

7.2.1. Вызов окна журналов

Чтобы открыть окно журналов,

выберите в меню **Вид** пункт **Журналы**, и в открывшемся меню выберите пункт, соответствующий нужному типу.

После этого на экране откроется окно журналов (см. рис. 51).

7.2.2. Интерфейс окна журналов

Окно журнала состоит из нескольких частей:

- главное меню;
- таблица отчета;
- ярлыки закладок, позволяющие выбрать отчет нужного типа.

7.2.2.1. Главное меню

В верхней части главного окна расположено *главное меню*.

Таблица 4

Пункт меню	**Назначение**
Файл ⟶ Сохранить в файл	Сохранить текущий журнал в файле
Справка ⟶ Справка по Kaspersky Anti-Hacker	Вызов справочной системы
Справка ⟶ Kaspersky Anti-Hacker в Интернет	Показать страницу Лаборатории Касперского в интернете
Справка ⟶ О программе	Показать справочную информацию о программе

7.2.2.2. Таблица отчета

В таблице отчета отображается журнал выбранного типа. Вы можете просматривать его, пользуясь полосой прокрутки справа.

Таблица отчетов обладает контекстным меню, которое по умолчанию состоит из двух пунктов, и расширяется в зависимости от выбранного журнала:

- **Очистить журнал** – очистить выбранный журнал;
- **Показывать последнюю запись** – в видимой области таблицы отчета всегда показывать запись о последнем событии;
- **Отключить протоколирование этого события** – больше не заносить в журнал записи о выделенном событии. Пункт доступен для всех журналов, кроме журнала хакерских атак;

- **Создать правило** – создать правило на основе выделенного события. При создании правила оно помещается в список правил как наиболее приоритетное.

7.2.2.3. Ярлыки закладок

Ярлыки закладок предназначены для выбора нужного журнала:

- Сетевые атаки;
- Активность приложений;
- Пакетная фильтрация.

7.2.3. Выбор журнала

7.2.3.1. Журнал сетевых атак

Вы можете просматривать журнал сетевых атак, в котором отображается список всех обнаруженных попыток атаковать ваш компьютер (см. п. 6.5. на стр. 70).

Чтобы открыть журнал сетевых атак,

выберите в меню **Вид** пункт **Журналы**, и в открывшемся подменю пункт **Журнал сетевых атак**.

После этого на экране откроется окно **Журналы** на странице **Сетевые атаки** (см. рис. 51). В журнале отображается:

- **Дата и время** – дата и время произошедшей попытки атаковать ваш компьютер;
- **Описание события** – описание сетевой атаки: ее название и адрес атаковавшего компьютера, если его удалось определить.

Список с событиями можно сортировать только по дате и времени.

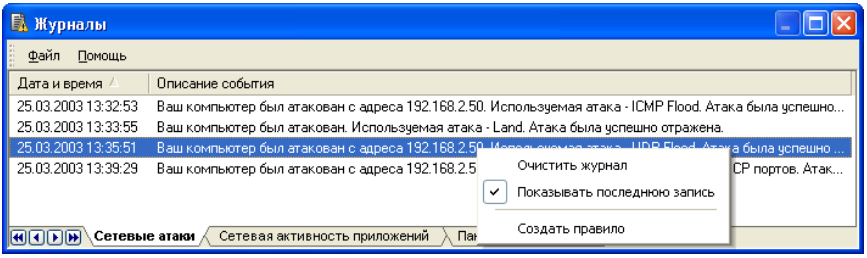


Рисунок 51. Журнал сетевых атак

7.2.3.2. Журнал активности приложений

Вы можете просматривать журнал активности приложений, для которых задан режим протоколирования в правилах для приложений (см. п. 6.3.2.3. на стр. 61).

Чтобы открыть журнал активности приложений,

выберите в меню **Вид** пункт **Журналы**, и в открывшемся подменю пункт **Журнал сетевой активности приложений**.

После этого на экране откроется окно **Журналы** на странице **Активность приложений** (см. рис. 52). В журнале отображается:

- **Дата и время** – дата и время произошедшего события;
- **Интернет приложение** – название приложения и путь к исполняемому файлу;
- **Описание активности** – что именно произошло;
- **Локальный адрес** – локальный адрес;
- **Удаленный адрес** – удаленный адрес.

Список с событиями можно сортировать только по дате и времени.

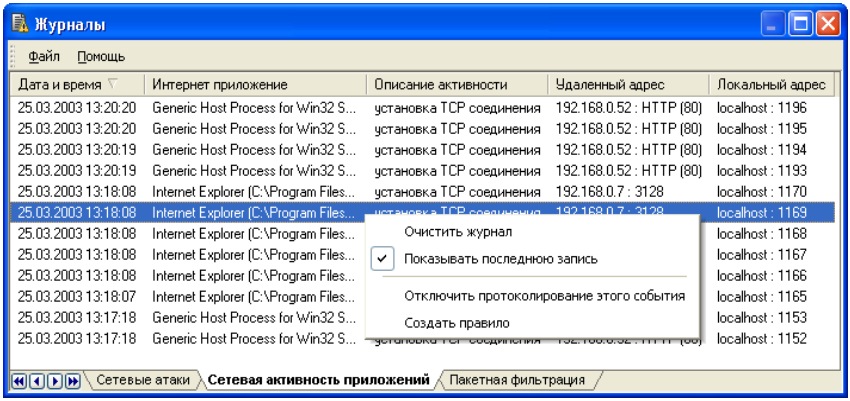


Рисунок 52. Журнал активности приложений

7.2.3.3. Журнал пакетной фильтрации

Вы можете просматривать журнал активности на пакетном уровне, которую указали протоколировать в правилах фильтрации пакетов (см. п. 6.4.2.2. на стр. 69).

Чтобы открыть журнал активности приложений,

выберите в меню **Вид** пункт **Журналы**, и в открывшемся подменю пункт **Журнал пакетной фильтрации**.

После этого на экране откроется окно **Журналы** на странице **Пакетная фильтрация** (см. рис. 53). В журнале отображается:

- **Дата и время** – дата и время произошедшего события;
- **Направление** – входящий или исходящий пакет;
- **Протокол** – название протокола;
- **Локальный адрес** – локальный адрес;
- **Удаленный адрес** – удаленный адрес;
- **Используемое правило** – имя сработавшего правила.

Черным цветом отображаются разрешенные пакеты и красным цветом – запрещенные.

Список с событиями можно сортировать только по дате и времени.

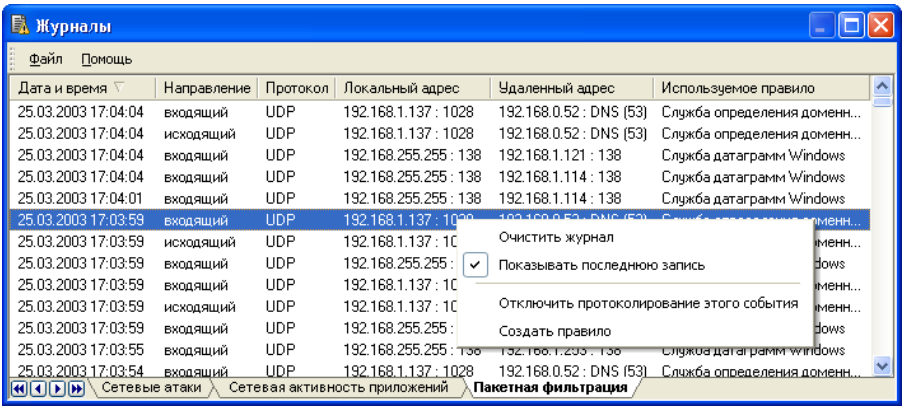


Рисунок 53. Журнал пакетной фильтрации

7.2.4. Настройка параметров журнала

Чтобы настроить параметры журнала,

выберите в меню **Сервис** пункт **Параметры** и переключитесь на закладку **Журналы** (см. рис. 54).

Вы можете задать два следующих параметра.

- **Очищать журналы при старте программы** – при запуске программы очищать все три журнала.
- **Ограничить размер журналов (Кб)** – установить максимальный размер файла-журнала, равным указанному в расположенном ниже поле ввода значению. При достижении максимального размера в журнал будет добавляться новое сообщение и удаляться наиболее старое.

Обратите внимание, с помощью данного поля вы определяете размер не всех трех, а только ОДНОГО журнала. При расчете места на жестком диске, необходимого для нормальной работы программы, следует умножить введенное значение на три.

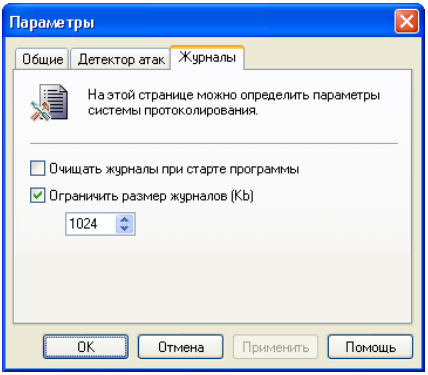


Рисунок 54. Закладка **Журналы** диалогового окна **Параметры**

7.2.5. Сохранение журнала в файле на диске

*Чтобы сохранить журнал, выбранный в окне **Журналы**,*

выберите в меню **Файл** пункт **Сохранить в файл**. В открывшемся диалоговом окне введите имя файла. Журнал будет сохранен в текстовом виде.

ПРИЛОЖЕНИЕ А. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

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

ЗАО "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, веб-серверах, почтовых шлюзах и межсетевых экранах. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей.

А.1. Другие разработки "Лаборатории Касперского"

Антивирус Касперского® Lite

Программа является самым простым в использовании антивирусным продуктом "Лаборатории Касперского", предназначенным для защиты

компьютера домашнего пользователя, работающего под управлением операционных систем Windows 95/98/Me, Windows 2000/NT Workstation, Windows XP.

В состав Антивируса Касперского® Lite входят:

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

Антивирус Касперского® Personal/Personal Pro

Пакет разработан специально для полномасштабной антивирусной защиты домашних компьютеров, работающих под управлением операционных систем Windows 95/98/ME, Windows 2000/NT, Windows XP с бизнес-приложениями из состава MS Office 2000, а также почтовыми программами Outlook, Outlook Express. Антивирус Касперского Personal/Personal Pro включает программу загрузки ежедневных обновлений через интернет, интегрированный модуль управления и автоматизации антивирусной защиты. Уникальная система эвристического анализа данных второго поколения сможет эффективно нейтрализовать неизвестные вирусы. Простой и удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского Personal включает:

- **антивирусный сканер** для проведения полной проверки локальных и сетевых дисков по требованию пользователя;
- **антивирусный монитор**, автоматически проверяющий все используемые файлы в масштабе реального времени;
- **почтовый фильтр**, осуществляющий проверку всех входящих и исходящих почтовых сообщений в фоновом режиме;
- **центр управления**, выполняющий автоматический запуск Антивируса Касперского по расписанию, централизованный контроль за программой, автоматическую рассылку предупреждений о вирусных атаках.

Антивирус Касперского® Personal Pro, кроме перечисленных компонент, включает в себя две дополнительные:

- **ревизор изменений**, который надежно следит за всеми изменениями на диске и по требованию восстанавливает модифицированные файлы и загрузочные секторы;
- **поведенческий блокиратор**, гарантирующий 100% защиту от макро-вирусов.

Kaspersky® Security для PDA

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

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

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

Антивирус Касперского® Business Optimal

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

Антивирус Касперского® Business Optimal включает полномасштабную антивирусную защиту:

- рабочих станций под управлением Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux;
- файловых серверов и серверов приложений под управлением Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD;
- почтовых шлюзов MS Exchange Server 5.5/2000, Lotus Notes/Domino, sendmail, Postfix, Qmail, Exim.

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- рабочих станций под управлением Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux, OS/2;
- файловых серверов и серверов приложений под управлением Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi; OpenBSD;
- почтовых шлюзов MS Exchange Server 5.5/2000, Lotus Notes/Domino, sendmail, Postfix; Exim, Qmail;
- CVP-совместимых межсетевых экранов;
- веб-серверов;
- персональных компьютеров (PDA), работающих под управлением Palm OS.

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

Kaspersky® Anti-Spam

Kaspersky™ Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая RBL-списки и формальные признаки письма) и

уникальный набор сервисов, которые позволяют пользователям распознать и уничтожить до 95% нежелательного трафика.

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

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

A.2. Наши координаты

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

Адрес:	Россия, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700, 948-4331, 948-8350	
Экстренная круглосуточная помощь	+7 (095) 797-8707, 495-0300	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	
Антивирусная лаборатория	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)	
Департамент продаж	+7 (095) 797-8700 +7 (095) 948-4331 +7 (095) 948-8350	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (095) 948-5650	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.com	

ПРИЛОЖЕНИЕ В. УКАЗАТЕЛЬ

ПРИЛОЖЕНИЕ C. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

При выполнении некоторой задачи на вашем компьютере возникают ошибки, и вы хотите проверить, вызваны ли они работой программы Kaspersky Anti-Hacker.

Включите на некоторое время режим **Разрешить все** или выгрузите Kaspersky Anti-Hacker из памяти компьютера. Проверьте, изменилась ли ситуация. Если возникает та же ошибка, это значит, что она не связана с работой Kaspersky Anti-Hacker. Если ошибка не возникает, свяжитесь со специалистами компании Лаборатория Касперского.