OUTPOST

Outpost

Personal Firewall

Руководство пользователя

Содержание

1. Введение

1

Содержание

1.1. Сеть Интернет и опасности при работе в сети

Идея обмена данными между компьютерами возникла еще на заре компьютерной цивилизации. Объединение находящихся в непосредственной близости друг от друга компьютеров с помощью специальных кабелей и программ поддержки соединения принято называть *локальной сетью* (рис. 1).

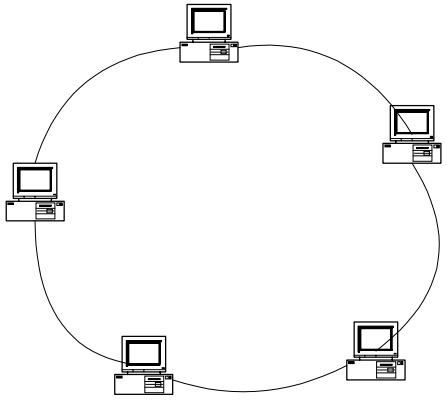

Рисунок 1. Пример локальной компьютерной сети

Соединение компьютеров, разделенных большими расстояниями, принято называть *глобальной сетью*. Например, глобальную сеть какой-либо компании, имеющей филиал (филиалы) в других городах, можно представить как объединение локальных сетей, как показано на рис. 2.

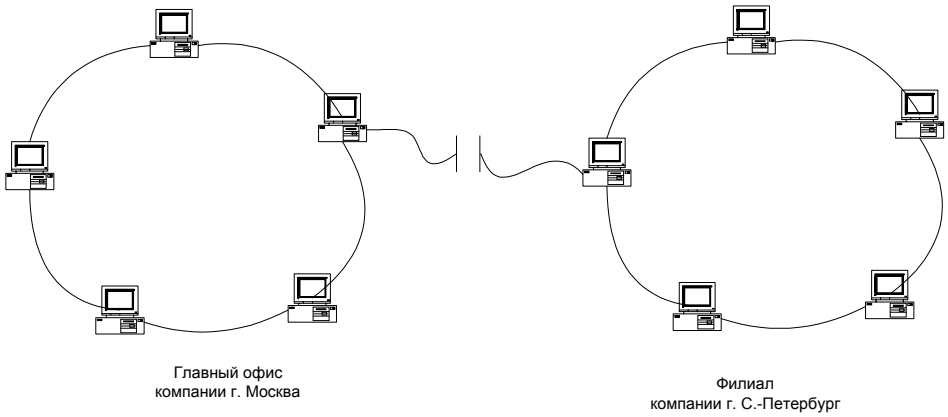

Рисунок 2. Пример глобальной компьютерной сети

Подобное соединение двух и более сетей является типичным. Фактически этот тип связи формирует основу мировой глобальной сети Интернет. Интернет — это *мегасеть*, т. е. объединение многих компьютерных сетей. Взаимодействие узлов в этой сети не зависит от типа компьютеров, их архитектуры и операционных систем, а также от физической реализации связи между ними (рис. 3).

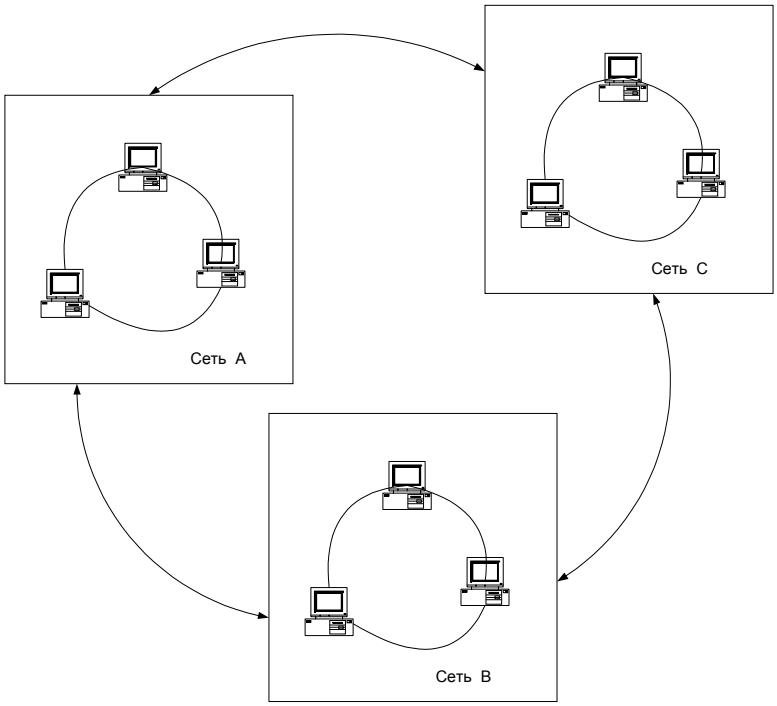

Рисунок 3. Связи между сетями и Интернет

Обмен информацией между узлами сети осуществляется с помощью специальных протоколов. Сетевые протоколы создаются в первую очередь для того, чтобы скрыть технологические различия между сетями, сделав соединение независимым от используемого оборудования. Приложения обмениваются информацией через Интернет, опираясь на все или некоторые из этих протоколов.

При работе в Интернете Вы получаете возможности:

- получения доступа к многочисленным архивам документов, связанных перекрестными ссылками;
- посылать и принимать сообщения на любой компьютер в любой точке мира с помощью электронной почты (e-mail);
- получения и передачи файлов через сеть (с помощью *FTP-протокола*) и т. д.

Однако использование Интернета, наряду с несомненными достоинствами (к которым, в частности, относится доступ к огромному количеству самой разнообразной информации), таит в себе и определенные опасности, связанные с безопасностью информации на Вашем компьютере. Главная причина возникновения проблемы безопасности связана с тем, что, получая доступ к ресурсам многих тысяч и миллионов компьютеров в Интернете, Вы одновременно предоставляете доступ (в той или иной степени) к ресурсам Вашего компьютера со стороны других компьютеров сети.

При работе в сети:

- на Вашем компьютере могут начать исполняться (например, при отображении на активных Web-страницах, содержащих ActiveX или Java апплеты) поступившие извне программы , которые в принципе могут выполнять на Вашем компьютере любые действия, например передавать файлы с Вашей частной информацией другим компьютерам в сети, причем управлять работой этих компьютеров Вы не имеете возможности;

- другие компьютеры в сети могут получить или попытаться получить доступ к файлам Вашего компьютера;
- на Вашем компьютере может размещаться информация (*Cookie* или *referrers*), по которой другие компьютеры сети смогут определить, к какой информации Вы обращались и кто, в свою очередь, обращался к Вашему компьютеру;
- на Вашем компьютере могут быть без Вашего ведома размещены *«троянские кони»*, т. е. программы, передающие приватную информацию (например, пароли доступа в Интернет или номера кредитных карточек) с Вашего компьютера на компьютер-злоумышленник. Основным отличием «троянца» от программ-вирусов является именно то, что вирус, попавший на Ваш компьютер, никак не связан со своим создателем, а «троянец» как раз и предназначен для последующего взаимодействия с пославшим его злоумышленником;
- вместе с запрашиваемой, в компьютер загружается и ненужная информация — *баннеры* и иная реклама. Хотя сами по себе эти объекты, как правило, не могут вызвать потерю или искажение информации на Вашем компьютере, однако они существенно увеличивают время загрузки страниц, особенно при работе через модем;
- на Вашем компьютере могут быть без Вашего ведома размещена spyware, то есть программа, которая передает своему разработчику информацию владельце компьютера и его пристрастиях (например, информацию о получаемых из сети файлах).

1.2. Персональный брандмауэр Outpost Firewall. Обзор возможностей

Для защиты информации на локальных компьютерах или в локальных сетях широко применяются программы, называемые *брандмауэрами* (firewall). Эти программы играют роль фильтра, ограждающего локальный компьютер или локальную компьютерную сеть от несанкционированного доступа из сети. Персональный брандмауэр устанавливается на локальном компьютере и предназначен для защиты персональной информации (рис. 4).

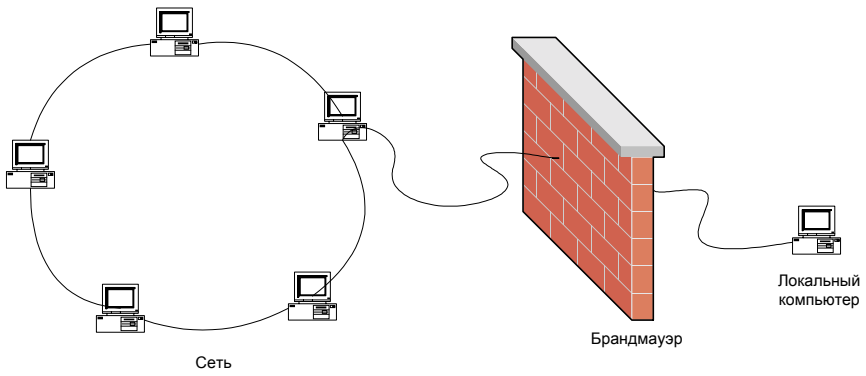

Рисунок 4. Персональный брандмауэр

Система **Outpost Firewall** относится к разряду персональных брандмауэров и обладает следующими основными свойствами:

- возможностью использования сразу же после установки без необходимости предварительной настройки;

- возможностью легко и быстро создать безопасную конфигурацию при работе в сети, используя приглашающие сообщения системы и настройки по умолчанию;
- простым пользовательским интерфейсом, позволяющим даже сложные настройки формировать одним или несколькими нажатиями кнопок;
- возможностями использования большого количества настроек для ограничения доступа из сети и выхода в сеть работающих приложений и работы служебных протоколов (для опытных, «продвинутых» пользователей или при наличии особых требований к безопасности);
- возможностью создания «невидимого» режима работы, при котором остальные компьютеры в сети не в состоянии обнаружить Ваш компьютер;
- модульной организацией системы, позволяющей встраивать в систему новые защитные модули (даже созданные сторонними разработчиками);
- совместимостью со всеми версиями системы Windows 95/98/2000/ME/NT и низкими системными требованиями.

Для успешного применения брандмауэра **Outpost Firewall** Вам необязательно уметь пользоваться всеми возможностями системы. Система способна эффективно работать с настройками, установленными по умолчанию. Многие дополнительные возможности, например такие, как ограничение поступления или отправки ICMP-сообщений определенных типов, будут применяться лишь немногими из пользователей системы.

Новым подходом при разработке персональных брандмауэров, реализованным при разработке системы **Outpost Firewall**, является модульный принцип организации. Это означает, что значительная часть возможностей по защите компьютера реализована в виде подключаемых модулей, представляющих собой файлы с расширением **.dll**. Эти модули никак не связаны друг с другом. Создав новые модули, Вы можете легко добавить их в уже установленную систему. Более подробно о подключаемых модулях см. п. 6.5.1.

Говоря конкретнее, при использовании системы **Outpost Firewall** Вы можете:

- Ограничить список приложений, получающих доступ в сеть; при этом для каждого из этих приложений указать список допустимых протоколов, портов, направлений обращения.
- Запретить или ограничить поступление на локальный компьютер незатребованной информации, в частности:
  - баннерной рекламы;
  - всплывающих окон в Web-страницах;
  - данных с определенных Web-страниц.
- Ограничить или запретить использование программных компонент, встроенных в Интернет-страницы, таких как Java-апплеты и программы на языке JavaScript, ActiveX и т. д.
- Ограничить или запретить использование cookie.

- Определить зону «дружественных» IP-адресов (например, адресов локальной сети, в которой установлен данный компьютер). В этой зоне Outpost Firewall не осуществляет контроль и не ограничивает сетевой обмен.
- Осуществлять проверку поступающих по электронной почте присоединенных файлов.
- Выдавать предупреждение при попытке атаковать Ваш компьютер из сети и предотвращать такие попытки.

1.3. Терминология и условные обозначения

Предполагая, что Вы уже знакомы со средой Windows, мы не приводим ее описание, но уточняем используемые в документации термины. Термины, применяющиеся при описании диалоговых окон, описаны в табл. 1.

Таблица 1. Термины, применяющиеся при описании диалоговых окон

Элемент интерфейса	Термин
Свернуть в панель задач	Переключатель во включенном состоянии
Свернуть при закрытии	Переключатель в выключенном состоянии
входящее	Кнопка выбора во включенном состоянии
исходящее	Кнопка выбора в выключенном состоянии
Общие Приложения	Закладка
Ширина 100	Поле ввода
OK	Кнопка

У ряда объектов, в частности у значков файлов и значка системы **Outpost Firewall**, имеется *динамическое меню* (рис.5), с помощью которого пользователь может выполнять те или иные операции, применимые к таким объектам.

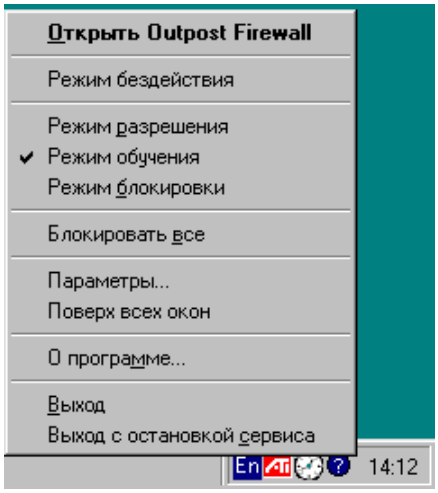

Рисунок 5. Динамическое меню системы Outpost Firewall

Для того чтобы вызвать динамическое меню:

1. Установите курсор мыши на объект, динамическое меню которого Вы хотите вызвать.
2. Щелкните правой клавишей мыши.

Некоторые объекты можно перемещать, буксируя их с помощью мыши.

Для того чтобы отбуксировать объект:

1. Установите курсор мыши на объект, который Вы хотите отбуксировать.
2. Нажмите на левую клавишу мыши и, не отпуская ее, переместите курсор мыши к тому месту, куда Вы хотите перенести объект.
3. Отпустите левую клавишу мыши.

В данной документации для выделения различных смысловых частей текста используются специальные обозначения, приведенные в табл. 2.

Таблица 2. Условные обозначения

Обозначение	**Смысл**
Троянский конь	Определяемый термин или термин, первый раз встретившийся в тексте
Режим обучения	Название какого-либо элемента системы: меню, пунктов меню, диалоговых окон, элементов диалоговых окон и т. п.
Encoding	Строка, вводимая пользователем или выводимая системой
Tab	Обозначение клавиш или комбинаций клавиш
Чтобы выполнить...	Описание выполняемой пользователем последовательности действий
1. Нажмите на кнопку	Шаг процедуры, выполняемой пользователем
• Перечисление	Пункт перечисления
 Предупреждение	Предупреждение об опасности получения неверных данных, потери информации и т. п.
 Замечание	Информация, на которую мы рекомендуем обратить внимание
 Совет	Рекомендация для пользователя

2. Установка и первичная настройка

2

Содержание

2.1. Установка системы Outpost Firewall

Процедура установки системы **Outpost Firewall** подобна установке большинства программ, работающих под управлением системы Windows.

Если Вы хотите установить систему **Outpost Firewall**, на котором она уже была установлена, то предварительно необходимо деинсталлировать старую версию.

Для того чтобы запустить программу установки системы Outpost Firewall:

1. Нажмите на кнопку **Пуск** на панели задач Windows.
2. Выберите в меню пункт **Выполнить…**.
3. В открывшемся диалоговом окне **Запуск программы** в поле **Открыть:** введите полный путь к исполняемому файлу программы установки; например (если программа устанавливается с диска **D**) строку **D:\outpost.exe**
4. Нажмите на кнопку **OK**.

Поскольку по завершении процедуры установки система **Outpost Firewall** начнет работать только после перезагрузки компьютера, то перед выполнением этой процедуры рекомендуется завершить работу всех задач и закрыть все приложения.

После этого на экране появится диалоговое окно: будет выдано предупреждение о начале процесса установки и начнется собственно установка системы.

Процедура установки состоит из последовательности шагов, о выполнении каждого из которых сообщает соответствующее диалоговое окно. Вы можете перейти к следующему шагу процедуры (если это возможно), нажав на кнопку **Дальше**, вернуться к предыдущему шагу (если это возможно), нажав на кнопку **Назад**, или прервать выполнение процедуры установки, нажав на кнопку **Отмена**.

1. Диалоговое окно выбора языка, на котором будет производиться процесс установки (но не языка интерфейса самой системы). Это окно показано на рис. 6.

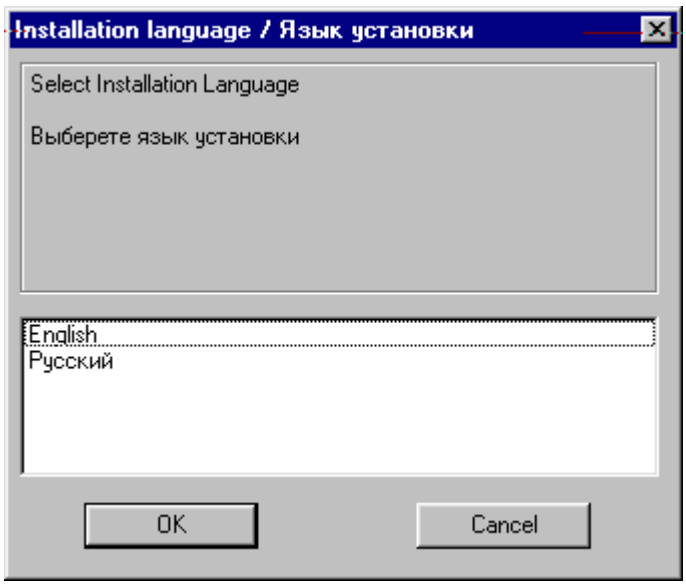

Рисунок 6. Диалоговое окно выбора языка установки

2. После выбора языка (русского или английского) нажмите на кнопку **ОК**, после чего на экране появится диалоговое окно ознакомления с Лицензионным Соглашением, показанное на рис. 7.

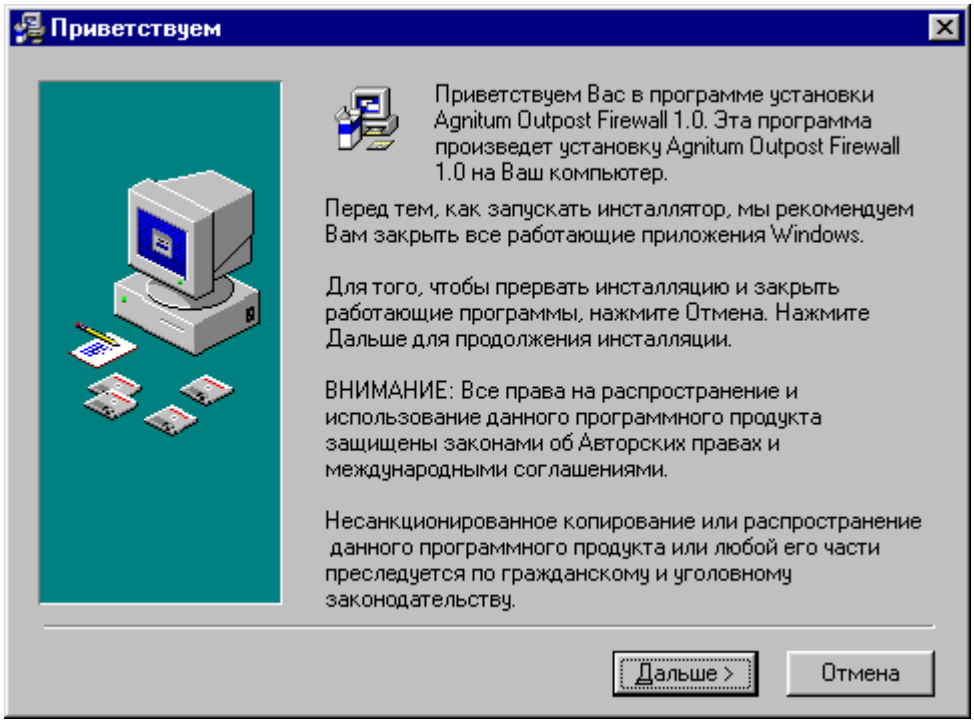

Рисунок 7. Диалоговое окно ознакомления с Лицензионным Соглашением

3. После нажатия на кнопку **Дальше** на экране появится диалоговое окно, описывающее Ваши действия, если у Вас была установлена предыдущая версия системы **Outpost Firewall** (это окно показано на рис. 8).

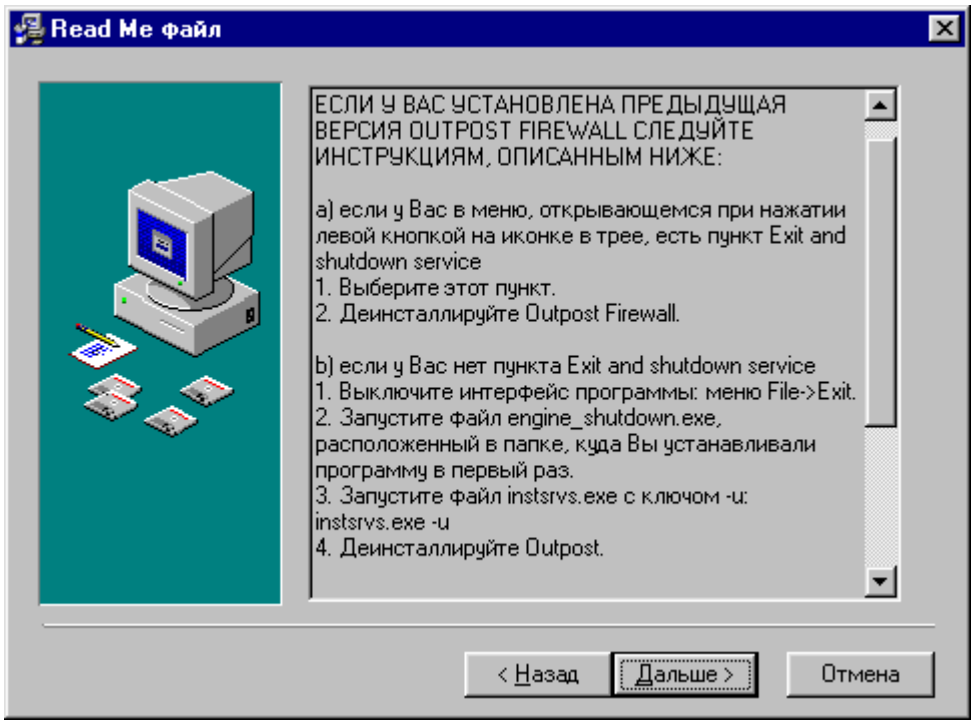

Рисунок 8. Диалоговое окно описания удаления предыдущей версии системы

4. При необходимости выполните действия, указанные в этом окне, и снова запустите процесс установки системы. Если никаких действий, указанных в данном диалоговом окне, выполнять не надо, то нажмите на кнопку **Дальше**, после чего на экране появится диалоговое окно задания каталога для установки системы, показанное на рис. 9.

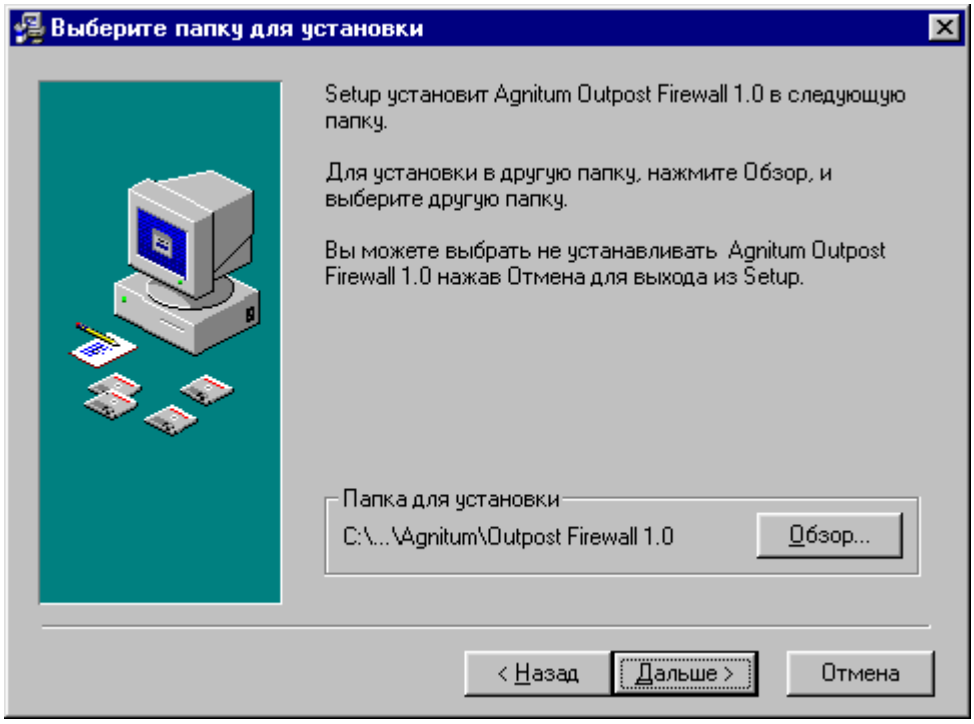

Рисунок 9. Диалоговое окно задания каталога для установки системы

5. В этом диалоговом окне укажите каталог, в котором будут размещаться компоненты системы **Outpost Firewall**. Имя этого каталога, задаваемое по умолчанию, указано в области **Папка для установки** диалогового окна.

Для того чтобы изменить заданное по умолчанию имя каталога, нажмите на кнопку **Обзор...** диалогового окна, после чего на экране появится диалоговое окно выбора каталога. В этом диалоговом окне выберите нужный каталог (или введите полный путь), после чего нажмите на кнопку **OK**.

Если Вы введете имя каталога, которого нет на соответствующем устройстве, то каталог с этим именем будет создан.

6. После того как Вы указали имя каталога, нажмите на кнопку **Дальше**. На экране появится диалоговое окно для выбора устанавливаемых компонент, показанное на рис. 10.

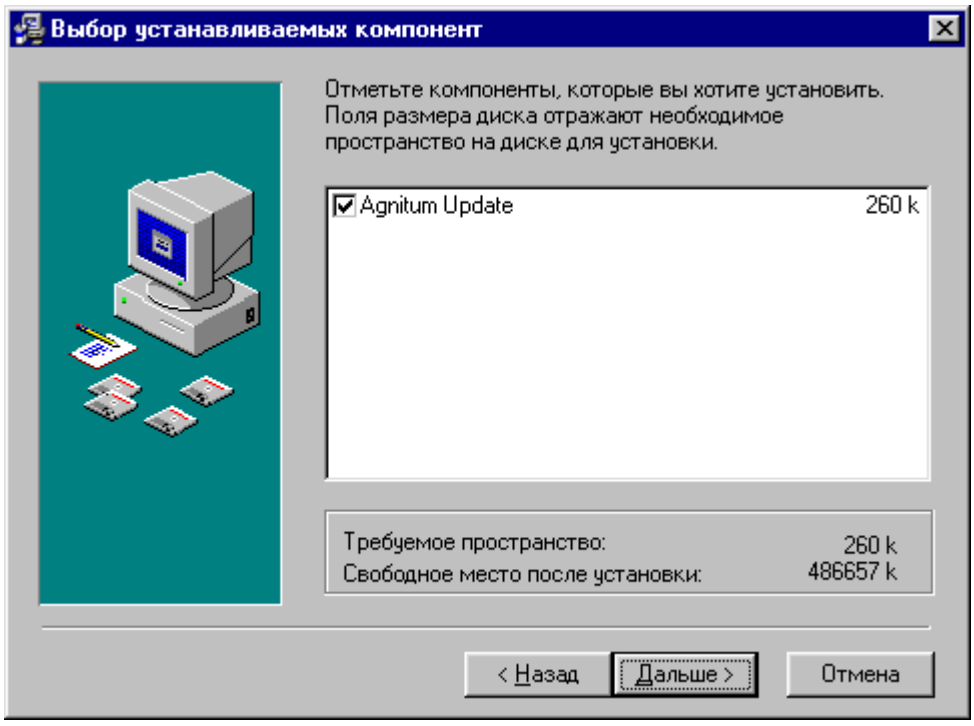

Рисунок 10. Диалоговое окно выбора устанавливаемых компонент системы

7. После того как Вы нажали на кнопку **Дальше**, на экране появится диалоговое окно готовности к процессу установки. После нажатия на кнопку **Дальше** в этом диалоговом окне начнется собственно процесс установки компонент.
8. После этого начнется процесс установки компонент, по окончании которого на экране появится диалоговое окно завершения установки.
9. После нажатия на кнопку **Finish** процедура установки завершается и на экране появляется диалоговое окно с предупреждением о необходимости перезагрузки компьютера для начала работы системы **Outpost Firewall**, показанное на рис. 11.

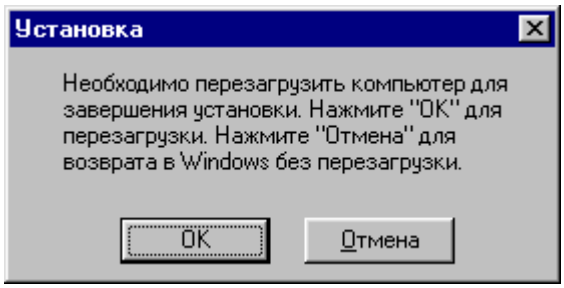

Рисунок 11. Диалоговое окно предупреждения о необходимости перезагрузки компьютера

Поскольку система Outpost Firewall может начать работу только после перезагрузки компьютера, то рекомендуется нажать на кнопку **OK**.

2.2. Системные требования и техническая поддержка

Система **Outpost Firewall** нормально функционирует на процессоре начиная с Intel Pentium 166 с общим объемом оперативной памяти не менее 16 Мб при наличии на Вашем компьютере операционной системы Windows 9x, или Windows 2000, или Windows NT 4.0 и старше, а также Windows Internet Explorer, версия 3.0 или более поздней, не менее 4Мб свободной памяти на жестком диске.

Система для своего нормального функционирования не предъявляет требований к параметрам сетевой карты и используемого Вами модема.

Если в ходе работы системы возникли ошибочные ситуации, то Вы можете сообщить о них в службу технической поддержки по адресу, указанному на домашней Web-странице системы **Outpost Firewall** (www.agnitum.com/products/outpost).

Для того чтобы обнаруженная Вами ошибочная ситуация была устранена в кратчайшие сроки, желательно максимально подробно сообщить в службу технической поддержки следующую информацию.

Определите версию используемого системой **Outpost Firewall** драйвера. Файлы драйвера располагаются в подкаталоге **\Kernel** того каталога, куда Вы установили систему **Outpost Firewall** для Windows 95/98, или Windows NT, или в подкаталоге **\Kernel\2000** для Windows 2000. Используются следующие файлы:

- filt95.vxd (при работе с Windows 95/98);
- filtnt.sys (при работе с Windows NT);
- 2000\filtnt.sys (при работе с Windows 2000).

Для того чтобы посмотреть номер версии, выберите в главном окне системы (см. п. 3.2) **Outpost Firewall** пункт меню **Справка**, а в следующем меню — **О программе Outpost Firewall**. В открывшемся диалоговом окне посмотрите значение поля **Version** для драйвера, соответствующего используемой Вами системе Windows. В этом же окне определите версию **Interface Library** (она указывается в верхней части диалогового окна).

Максимально подробно опишите условия, при которых возникла ошибочная ситуация работы системы.

Если прекратилось функционирование системы Windows (синий экран монитора в текстовом режиме), то желательно переслать в службу технической поддержки выводимую на экран информацию, а также (после перезагрузки) файлы с расширением **log** из подкаталога **\log** того каталога, в который Вы установили систему **Outpost Firewall**.

Если в ходе работы системы **Outpost Firewall** появилось диалоговое окно отладки (диалоговое окно с именем **Outpost Firewall debug window**), то нажмите на кнопку **Update log** и перешлите в службу технической поддержки файлы с расширением **log** из подкаталога **\log** того каталога, в который Вы установили систему **Outpost Firewall**.

Если в ходе работы системы отображаются браузером фрагменты Web-страницы, которые должны быть заблокированы (см. п. 6.5.3.1), то перешлите, пожалуйста, в службу технической поддержки:

- URL страницы, на которой не блокируется реклама;
- описание места в странице, где видна реклама (верх, низ, справа и т. д.);
- URL рекламной картинки и ссылки;
- название и версию браузера;
- разрешена ли поддержка Java и Javascript в браузере;
- конфигурацию прокси-сервера.

Более детально эту информацию можно посмотреть по адресу **www.agnitum.com/products/outpost/bugs.phtml**.

2.3. Первичная настройка

Сразу после установки система **Outpost Firewall** готова к работе. Однако Вы можете настроить систему так, чтобы она в наибольшей степени удовлетворяла Вашим запросам. Полностью настройки системы **Outpost Firewall** описаны в п. 6. В настоящей главе приводятся краткие сведения, позволяющие настроить систему перед началом работы с ней.

Одной из наиболее важных характеристик системы **Outpost Firewall** является политика работы с сетью. Политики системы показаны в табл. 3.

Таблица 3. Политики системы Outpost Firewall

Название	Значок системы	Описание
Блокировать все (Запрещать)		Запрещены все сетевые взаимодействия
Режим блокировки (Блокировать)		Запрещены все сетевые взаимодействия, за исключением явно разрешенных

Название	Значок системы	Описание
Режим обучения (Обучение)		Первое сетевое взаимодействие приложения сопровождается предупреждением, что предоставляет Вам возможность определить, каким образом данное приложение будет работать с сетью
Режим разрешения (Разрешать)		Разрешены все сетевые взаимодействия, кроме явно запрещенных
Режим бездействия (Отключать)		Разрешены все сетевые взаимодействия

Сразу после установки, поскольку никаких явно разрешенных сетевых взаимодействий не задано, политика **Режим блокировки** аналогична политике **Блокировать все**.

Сразу после установки, несмотря на то что никаких явно запрещенных сетевых взаимодействий нет, политика **Режим разрешения** отличается от политики **Режим бездействия**. Это отличие заключается в том, что в **Режиме бездействия** не выполняются подключаемые модули системы и, соответственно, они также не ничего блокируют.

Описание способов изменения политики работы системы **Outpost Firewall** приведено в п. 6.2.

Сразу после установки система **Outpost Firewall** работает в **Режиме обучения**. Этот режим позволит Вам выявить все приложения, взаимодействующие с сетью, и поможет Вам принять решение о допустимости сетевых взаимодействий для этих приложений. Если приложение может общаться с сетью, то работа в **Режиме обучения** облегчит Вам, при необходимости, задание правил, определяющих конкретные параметры сетевых соединений для данного приложения (протоколы, порты и т. д.). Работа в **Режиме обучения** означает, что при первой попытке получить или передать информацию через сеть на экране появится диалоговое окно предупреждения о сетевом взаимодействии, показанное на рис. 12.

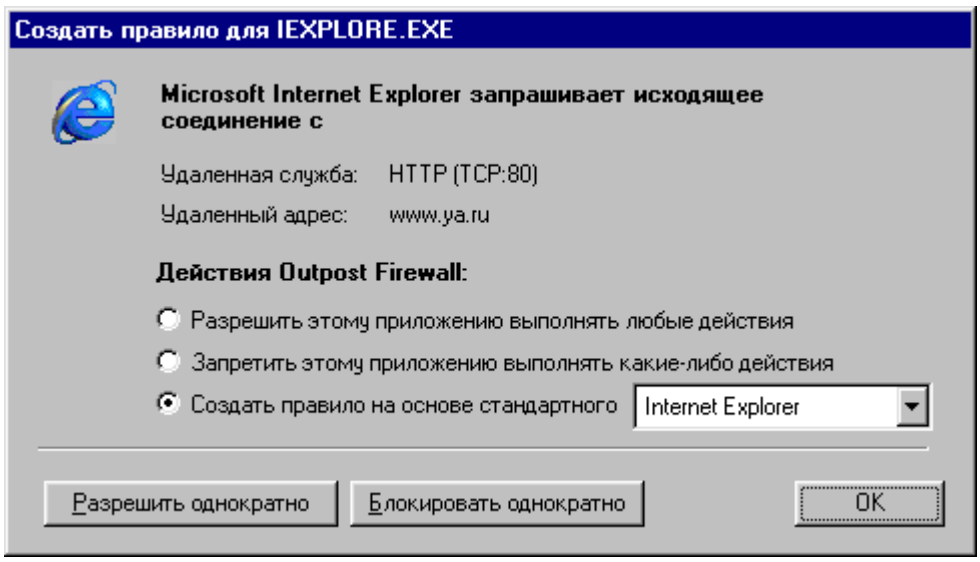

Рисунок 12. Окно предупреждения о сетевом взаимодействии

В этом диалоговом окне Вы получаете информацию о том, какое приложение (в данном примере — **Microsoft Internet Explorer**) пытается установить связь и основные параметры этой связи. После появления этого диалогового окна Вы можете определить правила выхода в сеть для данного приложения, как показано в табл. 4.

Таблица 4. Варианты действий пользователя при работе в Режиме обучения

Выбранное действие	**Для каких приложений**	**Что произойдет**
Кнопка выбора **Разрешить этому приложению выполнять любые действия** установлена во включенное состояние	Для тех приложений, которым Вы полностью доверяете	Разрешить все виды сетевых действий для данного приложения. Приложение попадает в список **Доверенные приложения**, расположенный на закладке **Приложения** диалогового окна **Параметры** (см. п. 6.3)
Кнопка выбора **Запретить этому приложению выполнять какие-либо действия** установлена во включенное состояние	Для приложений, которые не должны получать выхода в сеть	Все виды сетевых действий для данного приложения запрещены. Данное приложение попадает в список **Запрещенные приложения**, расположенный на закладке **Приложения** диалогового окна **Параметры** (см. п. 6.3)

Выбранное действие	Для каких приложений	Что произойдет
Кнопка выбора **Создать правило на основе стандартного** установлена во включенное состояние и в располагающемся справа от этой кнопки списке выбран тип приложения, для которого должно быть сформировано правило (см. п. 6.3)	Для приложений, которые могут выходить в сеть по определенным протоколам, через определенные порты и т. д.	Сформируйте правило (правила), определяющие возможности выхода данного приложения в сеть, как описано в п. 6.3. Это приложение попадет в список **Пользовательский уровень безопасности**, расположенный на закладке **Приложения** диалогового окна **Параметры**
Нажать на кнопку **Разрешить однократно**	Для приложений, для которых Вы еще не приняли окончательного решения о возможностях работы в сети	Это сетевое соединение будет разрешено. При следующей попытке данного приложения создать сетевое соединение на экране опять появится диалоговое окно предупреждения о сетевом соединении. Никакого правила для данного приложения не создается
Нажать на кнопку **Блокировать однократно**	Для приложений, для которых Вы еще не приняли окончательного решения о возможностях работы в сети	Это сетевое соединение будет запрещено. При следующей попытке данного приложения создать сетевое соединение на экране опять появится диалоговое окно предупреждения о сетевом соединении. Никакого правила для данного приложения не создается

По умолчанию в этом диалоговом окне включена кнопка выбора **Создать правило на основе стандартного**, а в качестве типа правила выбран тип, определенный системой **Outpost Firewall**.

С точки зрения системы **Outpost Firewall** все приложения делятся на три группы. К первой группе относятся приложения, которым разрешены все сетевые соединения. Ко второй группе принадлежат приложения, для которых явно, в виде специальных правил (см. п. 6.3), указаны те протоколы, порты и направления, с которыми сетевые соединения разрешены или запрещены. В состав третьей группы входят те приложения, которым запрещены все сетевые соединения.

Для первого знакомства с системой рекомендуется пользоваться значениями, задаваемыми по умолчанию, т. е. придерживаться следующей стратегии: оставить систему **Outpost Firewall** работать в режиме обучения и принимать решение отдельно для каждого сетевого соединения. В случае если Вы не можете определить причину сетевого соединения для данного приложения, рекомендуется это соединение запретить. Для остальных приложений лучше воспользоваться правилами по умолчанию, предлагаемыми системой, а для абсолютно надежных приложений, в корректном «поведении» которых Вы уверены, разрешить любые сетевые взаимодействия. В дальнейшем, после детального изучения возможностей системы, Вы можете изменить те или иные настройки.

После работы в течение некоторого времени (порядка 30 минут — 1 часа) система выявит большинство приложений, регулярно обращающихся к сети, и поможет Вам определить возможности сетевых обращений со стороны этих приложений. После этого Вы можете воспользоваться политикой **Режим блокировки**.

Однако Вы вправе использовать и другие стратегии, например запретить все сетевые соединения и далее последовательно разрешать только те из них, которые необходимы для работы.

2.4. Автоматическое обновление

Система **Outpost Firewall** предусматривает возможность обновления компонент системы через Интернет. При использовании средств автоматического обновления будут заменены только те компоненты системы, последняя версия которых отличается от установленной на Вашем компьютере.

Поскольку система **Outpost Firewall** сама определяет, нужно ли выполнять обновление компонент (эта проверка выполняется раз в день), то от пользователя не требуется запускать процедуру обновления. Если пользователь все же запустит процедуру автоматического обновления, а версия системы, установленная на Вашем компьютере, является последней, то никакие изменения в системе производиться не будут.

Для того чтобы запустить процедуру автоматического обновления системы Outpost Firewall:

1. Вызовите меню задач системы Windows, нажав на кнопку **Пуск** в панели задач системы.
2. В открывшемся меню выберите пункт **Программы**.
3. В следующем меню выберите пункт **Agnitum**.
4. В следующем меню выберите пункт **Outpost Firewall 1.0**.
5. В следующем меню выберите пункт **Agnitum Update**.

Вы можете запустить процедуру автоматического обновления системы из главного окна, нажав на кнопку панели инструментов главного окна системы **Outpost Firewall**, если главное окно системы открыто.

Поскольку после обновления системы желательно произвести перезагрузку компьютера, то перед выполнением этой процедуры рекомендуется завершить работу на компьютере всех задач и закрыть все приложения.

После вызова процедуры автоматического обновления будет вызван мастер обновления системы **Outpost Firewall**. Мастер обновления построен таким образом, чтобы максимально облегчить и автоматизировать процедуру обновления. Вам следует только следовать рекомендациям мастера обновления. Сама процедура обновления состоит из последовательности шагов, каждому из которых соответствует диалоговое окно, в котором описаны действия, выполняемые на данном шаге. Вы можете перейти к следующему шагу процедуры (если это возможно), нажав на кнопку **Далее**, вернуться к предыдущему шагу (если это возможно), нажав на кнопку **Назад**, или прервать выполнение процедуры обновления, нажав на кнопку **Отмена**.

После запуска процедуры автоматического обновления на экране появится диалоговое окно выбора типа обновления системы, показанное на рис. 13.

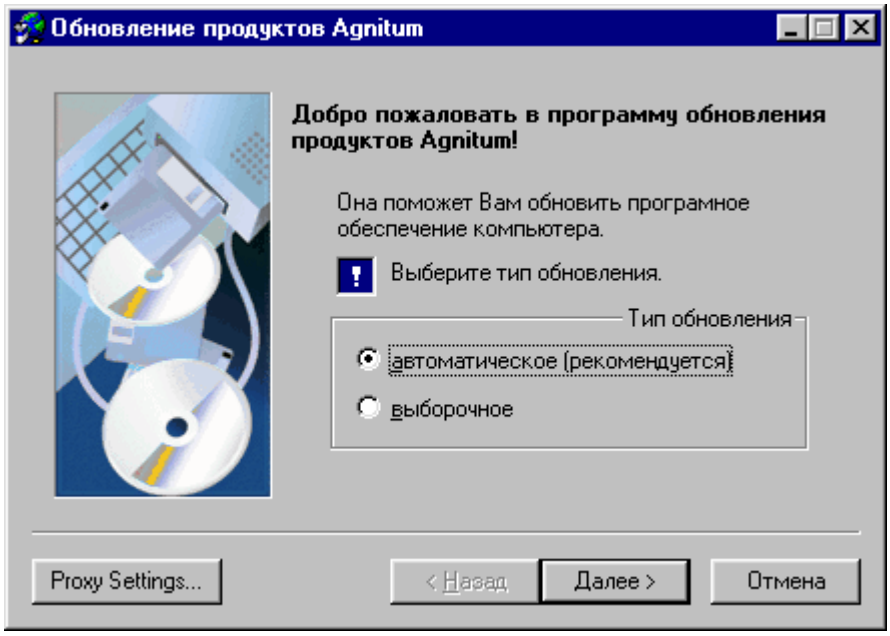

Рисунок 13. Диалоговое окно выбора типа обновления системы

В этом диалоговом окне Вы можете включить либо кнопку выбора **автоматическое** (после чего система сама определит, какие именно компоненты необходимо обновить),

либо кнопку выбора **выборочное**, а затем указать, какие именно компоненты Вы хотите обновить.

Тип обновления **выборочное** означает, что для невыбранных компонент обновление производиться не будет, а для выбранных будет выполнено только в том случае, если последняя версия этих компонент отличается от установленной на данном компьютере.

Рекомендуется включить кнопку выбора **автоматическое**, тип обновления **выборочное** рекомендуется использовать только при возникновении каких-либо проблем.

В этом же диалоговом окне Вы можете определить, будет ли система в процессе обновления использовать для приема данных из сети прокси-сервер и если да, то какой именно.

Для того чтобы задать настройки прокси-сервера:

1. Нажмите на кнопку **Proxy Settings** в диалоговом окне выбора типа обновления системы (см. рис. 13), после чего на экране появится диалоговое окно параметров прокси-сервера (рис. 14).

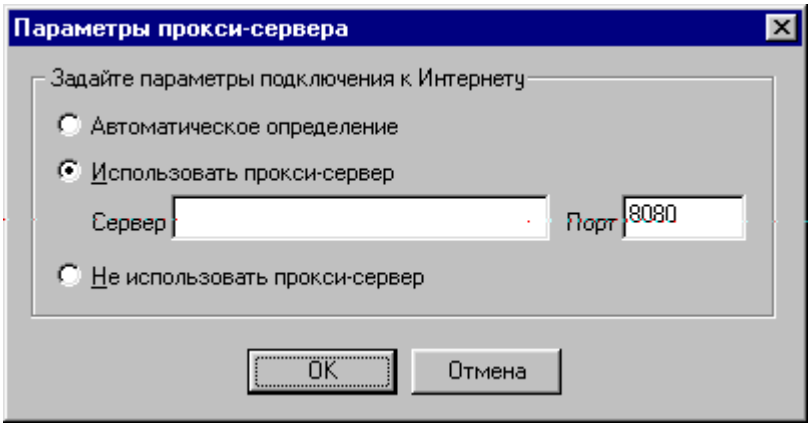

Рисунок 14. Диалоговое окно установки параметров прокси-сервера

2. В этом диалоговом окне установите одну из кнопок выбора:

   - **Автоматическое определение**, чтобы при получении информации из сети использовались настройки прокси-сервера, заданные в Microsoft Internet Explorer;
   - **Использовать прокси-сервер**, если Вы хотите явно задать параметры того прокси-сервера, который будет использовать программа автоматического обновления. В этом случае станут видимыми поля **Сервер** и **Порт**, в которых надо задать имя и порт прокси-сервера (по умолчанию используется порт 8080);
   - **Не использовать прокси-сервер**, если Вы не хотите использовать в процессе автоматического обновления прокси-сервер.

3. Нажмите на кнопку **OK**, после чего Вы снова вернетесь в диалоговое окно выбора типа обновления системы.

После выполнения всех действий нажмите на кнопку **Далее**.

Если Вы включили кнопку выбора **выборочное**, то на экране появится диалоговое окно выбора обновляемых компонент, показанное на рис. 15.

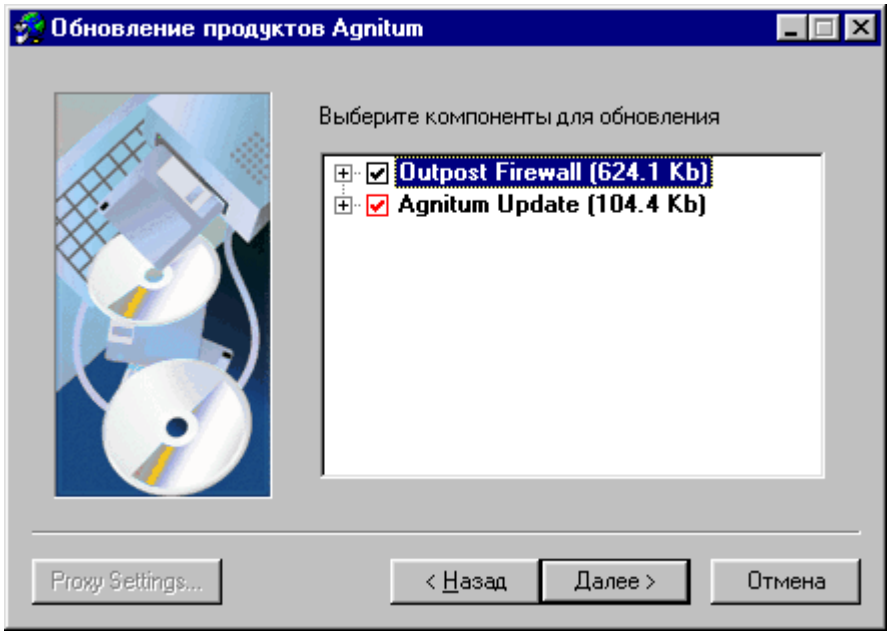

Рисунок 15. Диалоговое окно выбора обновляемых компонент системы

В этом диалоговом окне пометьте символом ☑ те компоненты, которые Вы хотите обновить. Все остальные компоненты должны быть помечены символом ☐.

При появлении диалогового окна выбора обновляемых компонент системы на экране все компоненты помечены символом ☑.

Для того чтобы какую-либо из компонент пометить символом ☐, щелкните правой клавишей мыши на символе ☑, расположенный слева от этой компоненты.

Если символ ☑ слева от какой-либо компоненты выделен красным цветом, то это означает, что обновление для этой компоненты обязательно.

После выбора всех компонент, которые следует обновить, нажмите на кнопку **Далее**.

После указания обновляемых компонент и нажатия на кнопку **Далее** начнется собственно процесс обновления компонент системы (если Вы включили кнопку выбора **автоматическое** в окне выбора типа обновления системы, то процесс обновления компонент системы начнется сразу после закрытия этого окна).

Во время процесса обновления компонент системы на экране будут появляться диалоговые окна, показывающие ход этого процесса. Большую часть времени на экране будет находиться диалоговое окно обновления компонент системы **Outpost Firewall**, показанное на рис. 16.

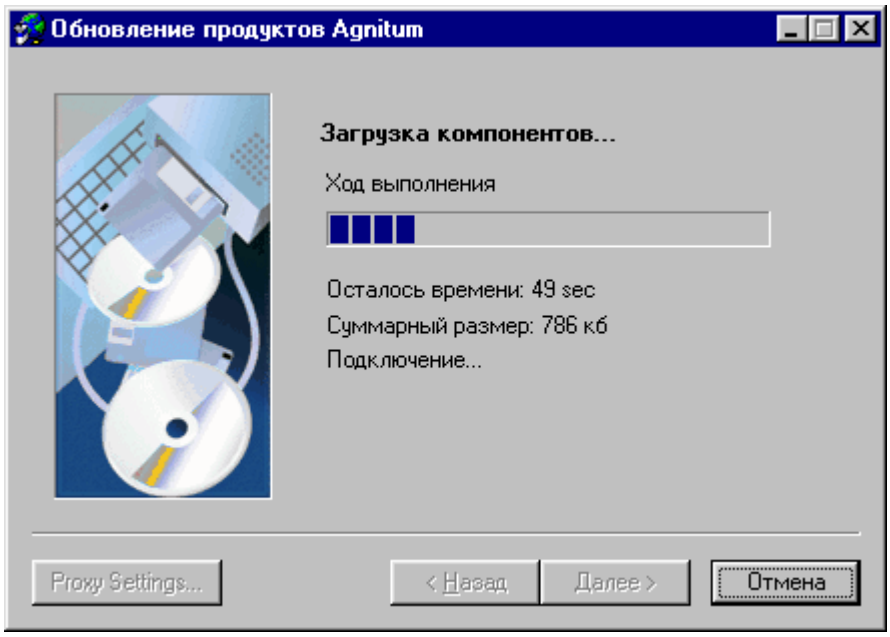

Рисунок 16. Диалоговое окно обновления компонент системы

После завершения процедуры обновления компонент на экране появится диалоговое окно завершения процесса обновления компонент системы **Outpost Firewall**, показанное на рис. 17.

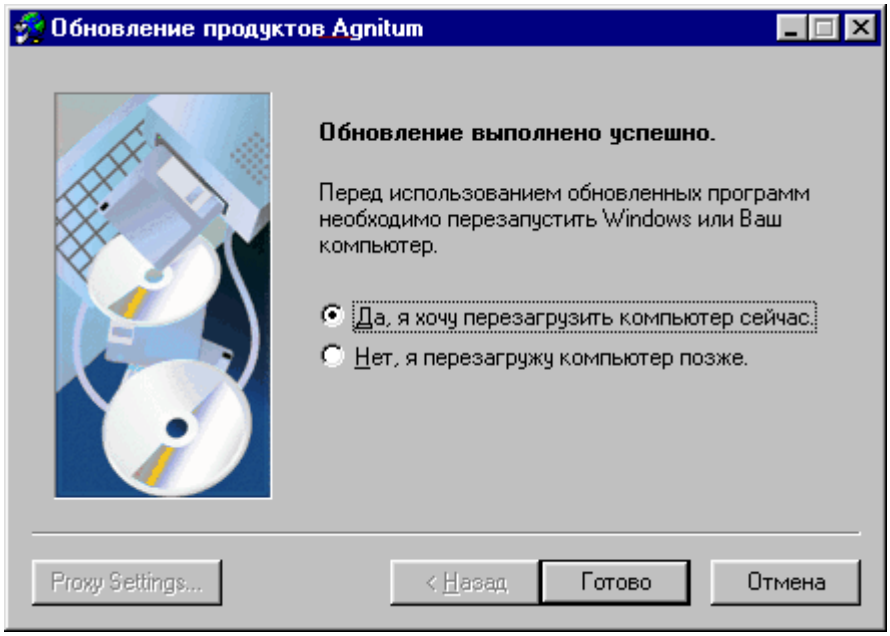

Рисунок 17. Диалоговое окно завершения процесса обновления компонент системы

В этом диалоговом окне включите:

- кнопку выбора **Да, я хочу перезагрузить компьютер сейчас**, в случае если после завершения процедуры установки Вы хотите перезагрузить компьютер;
- кнопку выбора **Нет, я перезагружу компьютер позже**, в случае если перезагрузку компьютера производить не нужно.

Поскольку обновление системы вступит в силу только после перезагрузки компьютера, то рекомендуется включить кнопку выбора **Да, я хочу перезагрузить компьютер сейчас**.

После того как Вы нажмете кнопку **Готово**, процедура обновления завершится.

Если система, установленная на Вашем компьютере, не требует обновления, то вместо окна завершения процесса обновления на экране появится окно, показанное на рис. 18, и никакого изменения компонент системы не произойдет.

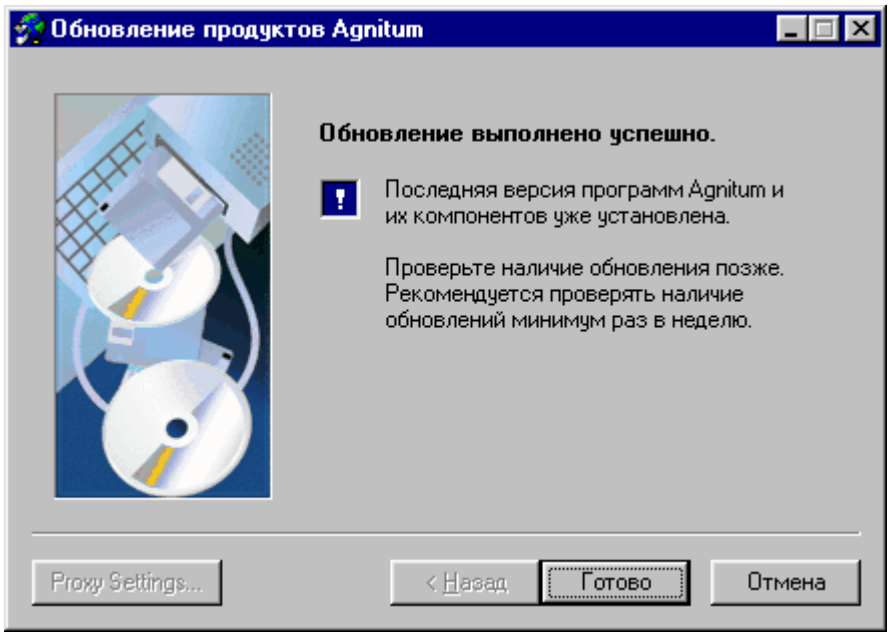

Рисунок 18. Диалоговое окно, появляющееся при отсутствии необходимости обновления системы

2.5. Удаление системы

Для того чтобы удалить систему Outpost Firewall с Вашего компьютера:

1. Вызовите динамическое меню системы **Outpost Firewall**.
2. Выберите в нем пункт **Выход с остановкой сервиса**.
3. Вызовите меню задач системы Windows, нажав на кнопку **Пуск** в панели задач.
4. В открывшемся меню выберите пункт **Программы**.
5. В следующем меню выберите пункт **Agnitum**.
6. В следующем меню выберите пункт **Outpost Firewall 1.0**.
7. В следующем меню выберите пункт **Uninstall Outpost Firewall**.
8. После появления на экране диалогового окна выбора метода удаления системы **Outpost Firewall**, показанного на рис. 19, включите кнопку выбора **Полный**.
9. Нажмите на кнопку **Далее**.

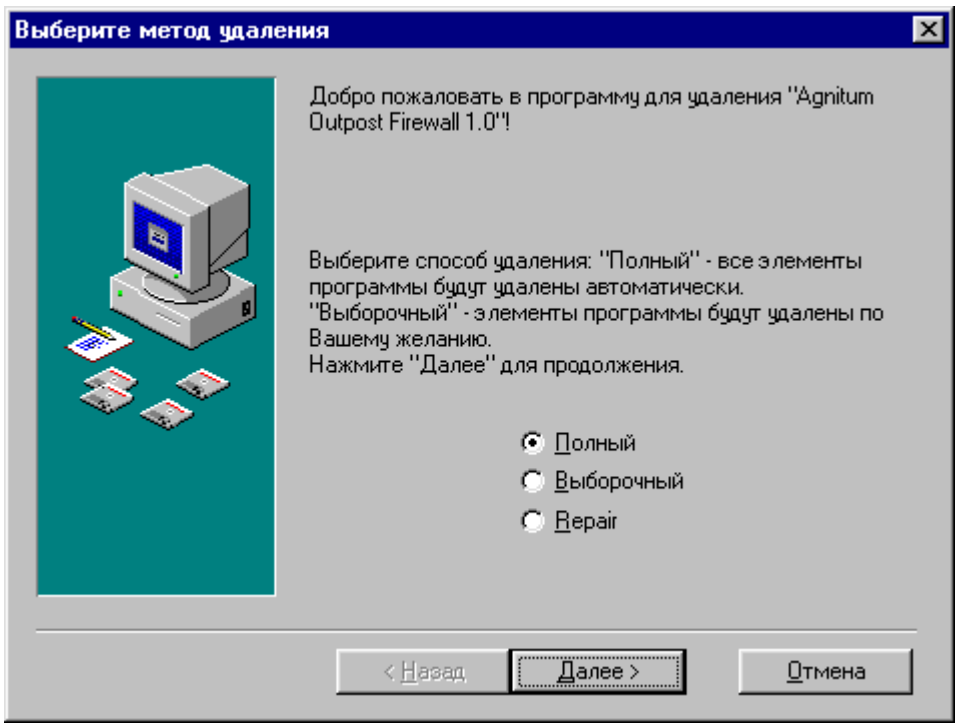

Рисунок 19. Диалоговое окно выбора метода удаления системы Outpost Firewall

Далее на экране появится диалоговое окно с предупреждением о начале процесса удаления, показанное на рис. 20, а после нажатия на кнопку **Готово** в этом диалоговом окне начнется собственно процесс удаления компонент системы. Во время этого процесса на экране будет находиться диалоговое окно, отображающее фазы процесса удаления системы. Состояние этого окна после завершения процесса удаления системы показано на рис. 21.

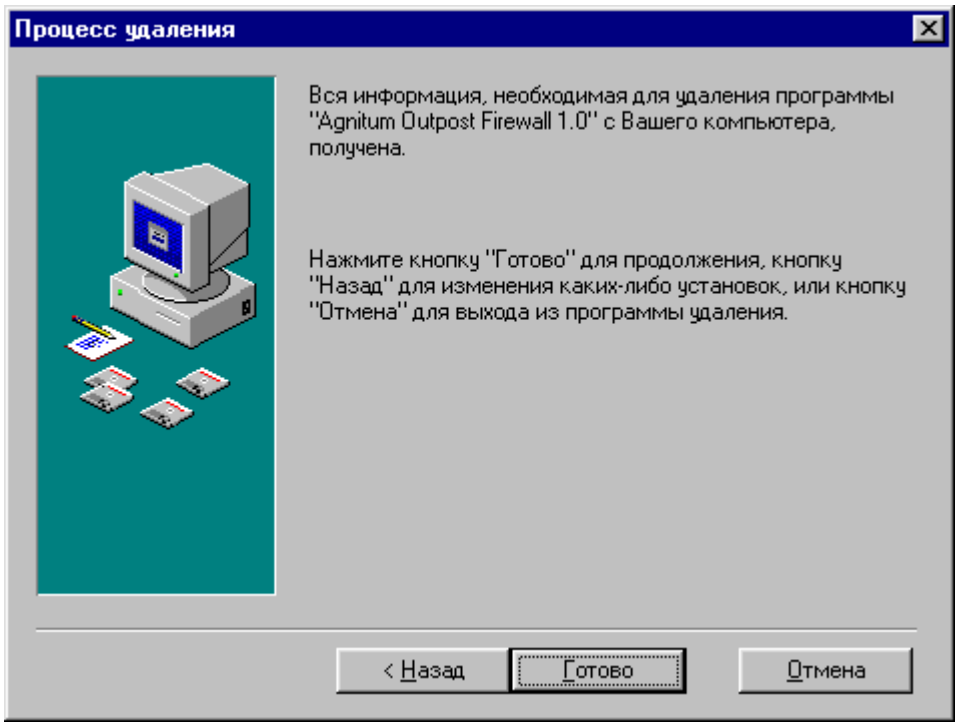

Рисунок 20. Диалоговое окно предупреждения о запуске процесса удаления системы Outpost Firewall

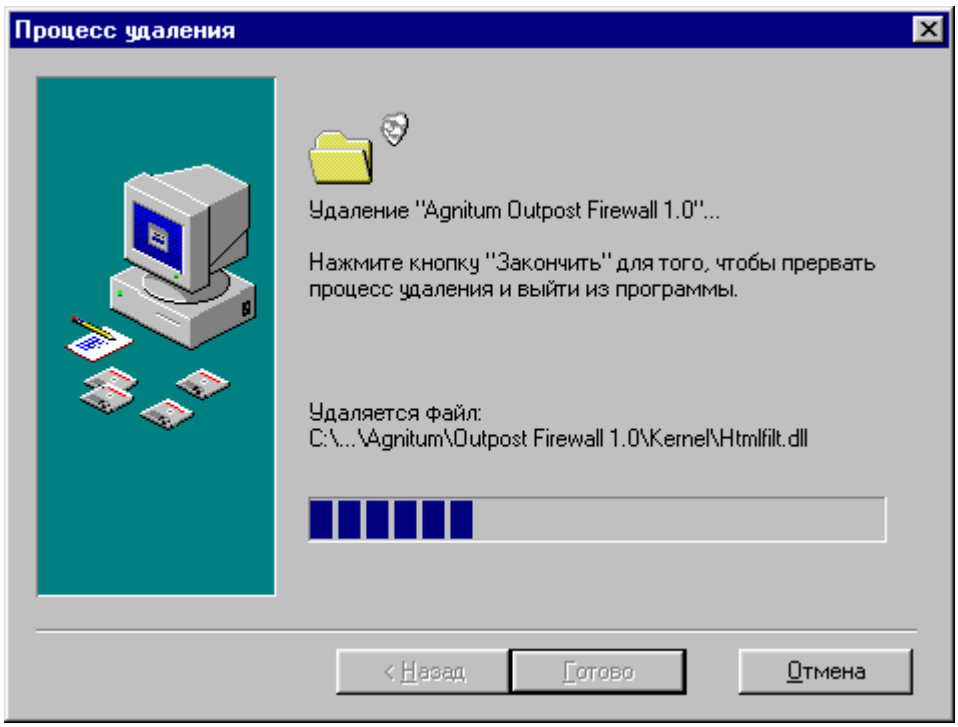

Рисунок 21. Диалоговое окно отображения процесса удаления системы Outpost Firewall

3. Пользовательский интерфейс системы Outpost Firewall

3

Содержание

3.1. Запуск и останов системы. Значок системы Outpost Firewall в панели задач

При установке брандмауэра **Outpost Firewall** задаются следующие настройки:

- система запускается при начальной загрузке системы Windows;
- значок системы размещается в правой части панели задач системы Windows;
- при закрытии главного окна системы **Outpost Firewall** ее значок остается в правой части панели задач системы Windows.

В дальнейшем пользователь может изменить эти настройки.

Для того чтобы вызвать диалоговое окно настроек системы Outpost Firewall, в случае если значок системы не находится в правой части панели задач Windows:

1. В меню **Пуск** Windows выберите пункт **Программы**.
2. В следующем меню выберите пункт **Agnitum**.
3. В следующем меню выберите пункт **Outpost Firewall 1.0**.
4. В следующем меню выберите пункт **Outpost Firewall**. После этого значок системы будет находиться в правой части панели задач Windows.
5. Вызовите динамическое меню системы **Outpost Firewall**.
6. В динамическом меню выберите пункт **Параметры** (вид динамического меню показан на рис. 22). Настройки запуска системы содержатся на закладке **Общие** (более подробно они описываются в п. 6.1).

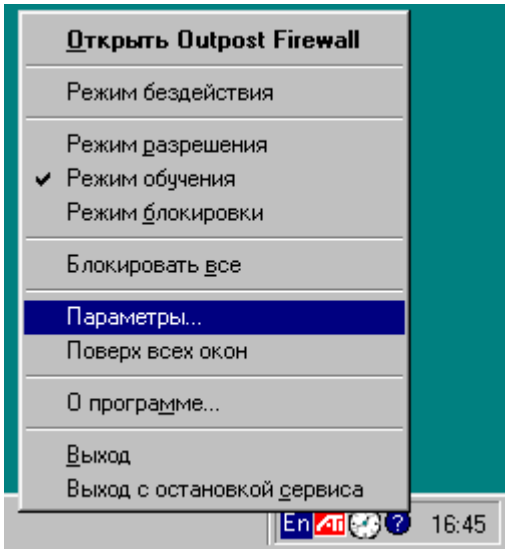

Рисунок 22. Динамическое меню системы Outpost Firewall с выбранным пунктом Параметры...

Если значок системы **Outpost Firewall** уже находится в правой части панели задач Windows, то для вызова диалогового окна настроек выполните шаги 4-5 вышеописанной процедуры.

В процессе работы рекомендуется расположить значок системы **Outpost Firewall** в правой части панели задач Windows.

Если значок системы **Outpost Firewall** располагается в правой части панели задач Windows, то вид этого значка определяется политикой работы системы. При работе в режиме **Блокировать все** значок имеет вид ; при работе в **Режиме блокировки** значок имеет вид ; при работе в **Режиме обучения** значок имеет вид ; при работе в **Режиме разрешения** значок имеет вид ; при работе в **Режиме бездействия** — .

3.2. Главное окно и работа с ним

Для того чтобы вызвать главное окно системы Outpost Firewall:

1. Вызовите динамическое меню системы **Outpost Firewall** (если значок системы находится в правой части панели задач системы Windows**)**.
2. Выберите в динамическом меню пункт **Открыть Outpost Firewall**.

После этого на экране появится главное окно системы **Outpost Firewall**, показанное на рис. 23.

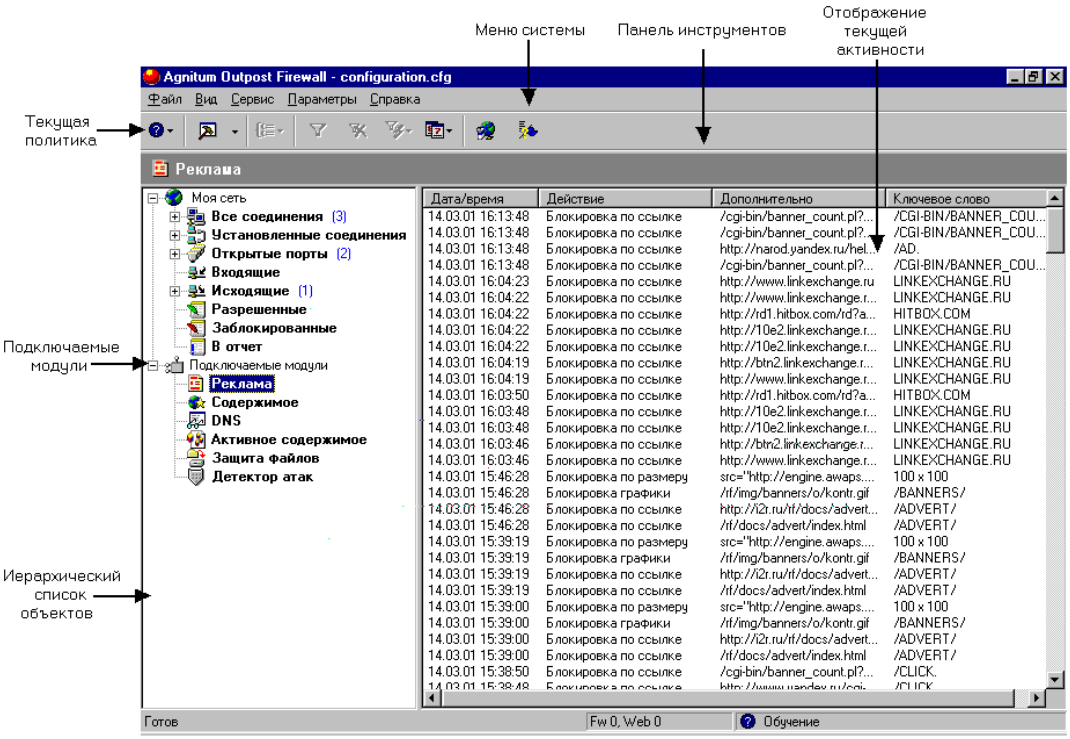

Рисунок 23. Главное окно системы Outpost Firewall

Это окно предназначено для визуального контроля за работой компьютера в сети, а также для изменения настроек системы.

Главное окно системы содержит:

- меню системы;
- панель инструментов;
- информационные панели, отображающие в том или ином виде протокол работы системы;
- строку состояния.

Меню системы, панель инструментов и строка состояния могут не отображаться на экране. Это определяется в зависимости от того, включены или нет переключатели **Панель объектов**, **Панель инструментов**, **Статусная строка** в диалоговом окне **Настройка окна** (рис. 25).

Если в главном окне отображается панель инструментов, то вид ее самой левой кнопки показывает текущую политику работы системы Outpost Firewall, т. е. она выглядит следующим образом:

-  , если система работает в режиме **Блокировать все**;
-  , если система работает в **Режиме блокировки**;
-  , если система работает в **Режиме обучения**;
-  , если система работает в **Режиме разрешения**;
-  , если система работает в **Режиме бездействия**.

Для того чтобы изменить политику работы системы Outpost Firewall:

1. Нажмите на кнопку в панели инструментов, показывающую текущую политику работы системы.
2. В открывшемся меню (рис. 24) выберите пункт с названием той политики, которую Вы хотите задать для системы **Outpost Firewall**.

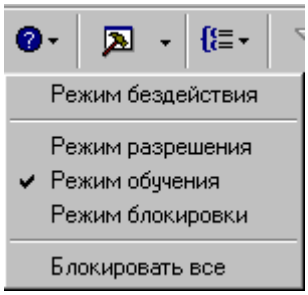

Рисунок 24. Меню выбора политики работы системы

Информационная панель разделена на две части — левую и правую. Левая часть панели содержит иерархический список объектов, протокол работы системы для которых может отображаться в правой части панели. Этот список поддерживает три уровня иерархии. На первом уровне иерархии имеется два объекта:

- **Моя сеть**, содержащий двухуровневый иерархический список всех объектов, определяющих работу с сетью;
- **Подключаемые модули**, содержащий список всех имеющихся в системе подключаемых модулей.

Список **Моя сеть** состоит из следующих элементов (каждый из которых в свою очередь может быть списком), относящихся ко второму уровню иерархии:

- **Все соединения** — список всех объектов, имеющих соединение с сетью;
- **Установленные соединения** — список всех объектов, имеющих установленное соединение с сетью;
- **Открытые порты** — список всех объектов, имеющих открытые порты для сетевого взаимодействия;
- **Входящие** — список всех объектов, инициировавших подключение к удаленным узлам сети;
- **Исходящие** — список всех объектов, которые подключились к Вашему компьютеру;
- **Разрешенные** — список всех работавших, со времени начала ведения протокола, приложений, которым разрешена работа с сетью;
- **Заблокированные** — список всех приложений, попытка работы с сетью которых была блокирована (со времени начала ведения протокола);
- **В отчет** — список всех работавших с сетью, со времени начала ведения протокола, приложений, для которых должен создаваться отчет о работе с сетью (см. гл. 4).

Один и тот же объект может находиться сразу в нескольких списках.

Количество и вид элементов в списке **Моя сеть** определяется пользователем. После установки системы этот список содержит единственный элемент — **Все соединения**.

Для того чтобы изменить список элементов Моя сеть:

1. Выберите в меню главного окна системы **Outpost Firewall** пункт **Вид**.
2. В следующем меню выберите пункт **Расположение…** .
3. В открывшемся диалоговом окне **Настройка окна** (рис. 25) в области **Левая панель** Вы можете включить переключатели, соответствующие тем элементам списка **Моя сеть**, которые необходимо выводить в левой части информационной панели, и выключить переключатели, соответствующие тем элементам списка, которые необходимо исключить из левой части информационной панели.

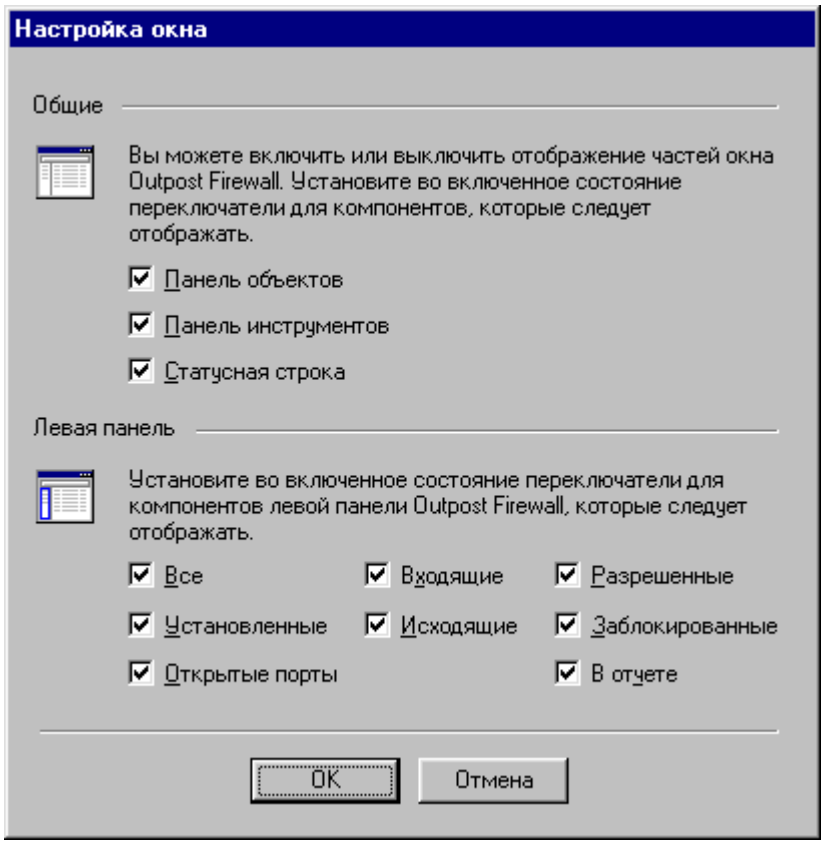

Рисунок 25. Диалоговое окно Настройки окна

Вы можете вызвать диалоговое окно **Настройка окна** из динамического меню элементов первого или второго уровня иерархии списка **Моя сеть** в левой части информационной панели, выбрав в этом меню пункт **Расположение…**.

Иерархический список **Подключаемые модули** после установки системы содержит следующие элементы (каждый из которых соответствует типу информации, выводимой одним из подключаемых модулей):

- **Реклама** — предназначен для вывода протокола о блокировке рекламы;
- **Содержимое** — предназначен для вывода протокола о запрете отображения Web-сайтов или Web-страниц, либо имеющих определенный Интернет-адрес (DNS-адрес), либо содержащих определенные текстовые строки;
- **Активное содержимое** — предназначен для вывода протокола о запрете выполнения программ на языках Java и VB Script, а также Java-апплетов, элементов Active X и т. д.;
- **DNS** — предназначен для кэширования и отображения протокола процесса преобразования DNS-адресов;
- **Защита файлов** — предназначен для проверки файлов, поступающих на Ваш компьютер по электронной почте;
- **Детектор атак** — предназначен для уведомления пользователя о предполагаемой атаке на его компьютер из сети и принятии действий по недопущению нанесения ущерба вашему компьютеру.

Количество и состав элементов списка **Подключаемые модули** могут меняться в зависимости от состава и статуса подключаемых модулей системы **Outpost Firewall**.

3.2.1. Отображение текущей активности для иерархического списка Моя сеть

Элементы **Все соединения**, **Установленные соединения**, **Открытые порты**, **Входящие**, **Исходящие** могут содержать список объектов. Этот список Вы можете развернуть, щелкнув мышью на значке ⊞ слева от соответствующего элемента списка, или свернуть, щелкнув на значке ⊟ слева от этого элемента списка.

Тип объектов, которые входят в списки **Все соединения**, **Установленные соединения**, **Открытые порты**, **Входящие**, **Исходящие**, определяется пользователем. При установке системы этими объектами являются приложения. Например, элемент **Установленные соединения** содержит список всех приложений, установивших соединение с сетью.

Для того чтобы изменить тип объектов, входящих в элементы Все соединения, Установленные соединения, Входящие, Исходящие:

1. Установите курсор на тот из вышеперечисленных списков, в котором Вы хотите изменить тип входящих в него объектов.
2. Выберите в меню главного окна системы **Outpost Firewall** пункт **Вид**.
3. В следующем меню выберите пункт **Группировать по**.
4. В следующем меню выберите пункт, определяющий тип объекта, который должен входить в иерархический список (в этом меню содержатся пункты: **Приложение**, **Локальный адрес**, **Локальный порт**, **Подключение**, **Удаленный адрес** и **Удаленный порт**, определяющие соответствующие типы объектов, а также пункт **Разгруппировать**, при выборе которого список третьего уровня иерархии не отображается).

Слева от элемента меню, определяющего тип выбранного объекта, располагается символ ✔.

Вместо выполнения пунктов 2-3 вышеописанной процедуры Вы можете нажать на кнопку  в панели инструментов.

Вместо выполнения пунктов 2-3 вышеописанной процедуры Вы можете вызвать динамическое меню данного элемента иерархического списка (**Все соединения**, **Установленные соединения**, **Входящие**, **Исходящие**) и выбрать в нем пункт **Группировать по**.

Для того чтобы изменить тип объектов, входящих в элемент **Открытые порты**, выполните описанную выше процедуру.

Как следует из процедуры определения типа объекта, для различных списков (**Все соединения**, **Установленные соединения**, **Открытые порты**, **Входящие**, **Исходящие**) Вы можете выбрать различные типы отображаемых объектов.

В правой части информационной панели (т.е. отображении протокола) указаны значения параметров для объектов, выбранных в ее левой части. Каждая строка в правой части информационной панели связана с одним сетевым взаимодействием. При этом в правой части одно и то же приложение может упоминаться более одного раза в том случае, если его обмен с сетью осуществляется более чем через один порт. Сами отображаемые параметры делятся на две группы. Параметры, относящиеся к первой группе (основные поля), отображаются в табличном виде. Названия основных полей выводятся в верхней строке правой части информационной панели. Параметры второй группы, называемые расширенными полями, могут либо отображаться на экране, либо быть скрыты. Отображением расширенных полей управляет поле **i**, которое содержит символ ⊞ или ⊟. Если в поле **i** находится символ ⊞, то все расширенные поля скрыты. Для того чтобы увидеть значения полей для какой-либо строки, подведите курсор мыши к символу ⊞ и нажмите на левую кнопку мыши. После этого следующее за полем **i** поле (по умолчанию это поле **Приложение**) изменит вид (оно будет выглядеть примерно так, как показано на рис. 26), а в самом поле **i** появится символ ⊟.

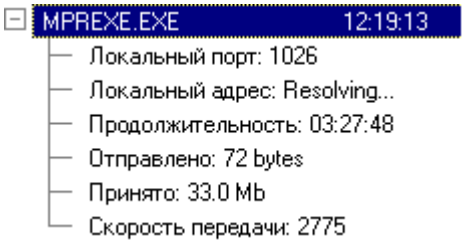

Рисунок 26. Отображение расширенных полей

Для того чтобы скрыть значения расширенных полей, подведите курсор мыши к символу ⊟ и нажмите на левую кнопку мыши.

После установки системы в протоколе отображаются следующие основные поля.

- Для элемента иерархического списка **Все соединения** — поля **i**, **Приложение**, **Установлено в**, **Подключение**, **Протокол**, **Удаленный порт** и **Удаленный адрес**.
- Для элементов иерархических списков **Установленные соединения**, **Открытые порты**, **Входящие**, **Исходящие** — поля **i**, **Приложение**, **Установлено в**, **Протокол**, **Удаленный порт** и **Удаленный адрес**.
- Для элементов иерархического списка **Разрешенные**, **Заблокированные**, **В отчет** — поля **Причина**, **Установлено в**, **Подключение**, **Приложение** и **Состояние**.

Для того чтобы вызвать диалоговое окно для изменения полей, выводимых на экран в протоколе:

1. Установите курсор на тот список, в котором Вы хотите изменить тип отображаемых полей.
2. Выберите в меню главного окна системы **Outpost Firewall** пункт **Вид**.
3. В следующем меню выберите пункт **Столбцы...** . После этого на экране появится окно **Столбцы** (рис. 27), в котором Вы можете изменить состав основных и дополнительных полей, поменять порядок их размещения в главном окне, а также задать дополнительные настройки отображения.

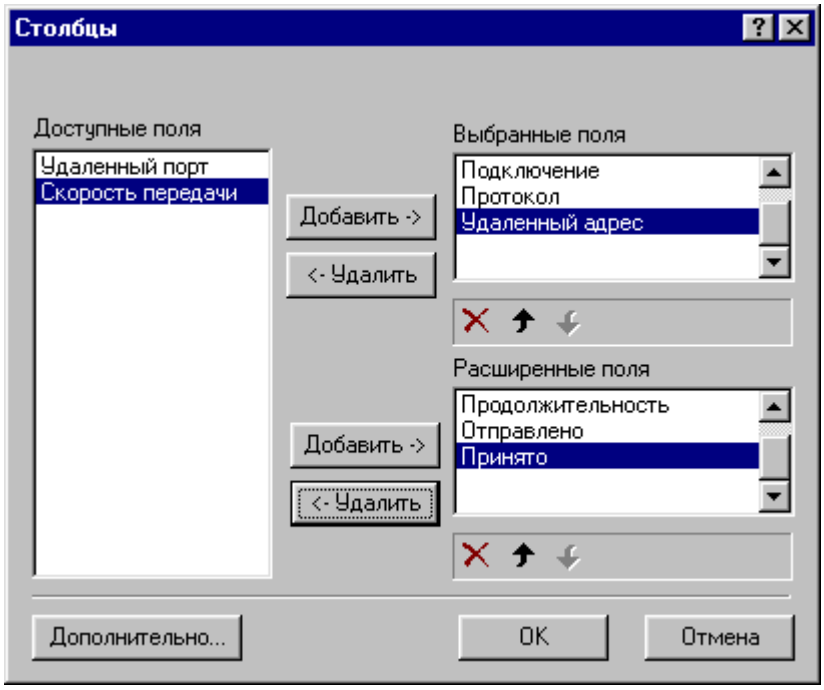

Рисунок 27. Диалоговое окно Столбцы

В этом окне отображаются:

- упорядоченный список **Выбранные поля**;
- упорядоченный список **Расширенные поля**;
- упорядоченный список **Доступные поля** полей, не используемых в данный момент.

Для того чтобы добавить поле в список основных полей:

1. Установите курсор в списке **Доступные поля** на то поле, которое Вы хотите добавить.
2. Нажмите на кнопку **Добавить->**, расположенную слева от списка **Выбранные поля**. После этого добавляемое поле будет удалено из списка **Доступные поля** и включено последним элементом в список **Выбранные поля**.

Для того чтобы удалить поле из списка основных полей:

1. Установите курсор в списке **Выбранные поля** на то поле, которое Вы хотите удалить.

2. Нажмите на кнопку **<-Удалить**, расположенную слева от списка **Выбранные поля**. После этого удаляемое поле будет исключено из списка **Выбранные поля** и включено последним элементом в список **Доступные поля**.

Вместо выполнения шага 2 описанной выше процедуры Вы можете нажать на кнопку  , расположенную под списком **Выбранные поля**.

Для того чтобы добавить поле в список расширенных полей:

1. Установите курсор в списке **Доступные поля** на то поле, которое Вы хотите добавить.
2. Нажмите на кнопку **Добавить ->**, расположенную слева от списка **Расширенные поля**. После этого выделенное поле будет исключено из списка **Доступные поля** и добавлено последним элементом в список **Расширенные поля**.

Для того чтобы удалить поле из списка расширенных полей:

1. Установите курсор в списке **Расширенные поля** на то поле, которое Вы хотите удалить.
2. Нажмите на кнопку **<-Удалить**, расположенную слева от списка **Расширенные поля**. После этого выделенное поле будет исключено из списка **Расширенные поля** и добавлено последним элементом в список **Доступные поля**.

Вместо выполнения шага 2 описанной выше процедуры Вы можете нажать на кнопку  , расположенную под списком **Доступные поля**.

Поле, внесенное в список **Расширенные поля** или в список **Выбранные поля**, будет располагаться там на последнем месте. Вы можете перенести поле на нужную позицию в списке (расположение в списке соответствует и расположению поля в главном окне) в любом из списков **Расширенные поля** или **Выбранные поля** с помощью кнопок  (переместить элемент на одну строку вверх) и  (переместить элемент на одну строку вниз), расположенных под тем из списков, в котором Вы хотите изменить положение элементов.

В диалоговом окне **Столбцы** Вы можете также задать дополнительные характеристики, определяющие, каким образом поля отображаются на экране. Для этого нажмите на кнопку **Дополнительно...**, после чего на экране появится диалоговое окно **Дополнительные параметры**, показанное на рис. 28.

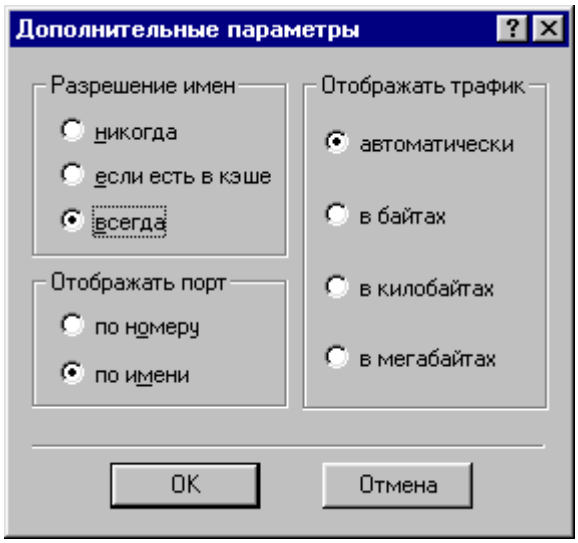

Рисунок 28. Диалоговое окно Дополнительные параметры

В этом диалоговом окне Вы можете задать режим отображения адресов удаленного и локального узлов (поля **Удаленный адрес** и **Локальный адрес** соответственно), для чего включите одну из следующих кнопок выбора в группе кнопок **Разрешение имен**:

- **никогда**, т. е. всегда выводить эти адреса в виде IP-адресов;
- **если есть в кэше**, т. е. производить преобразование этих адресов в символьные имена (DNS-адреса), если информация для преобразования данного адреса хранится в кэше DNS соответствующего модуля **Outpost Firewall**;
- **всегда**, т. е. всегда производить преобразование этих адресов в DNS-адреса и выводить DNS-адреса.

В этом же диалоговом окне Вы можете задать режим отображения значений портов (в полях **Локальный порт** и **Удаленный порт**), включив одну из следующих кнопок выбора в группе **Отображать порт**

- **по номеру**, тогда порты будут отображаться в виде числа;
- **по имени**, тогда порты будут отображаться в виде имени (названия задачи, которой назначен этот порт, если такая информация для данного порта присутствует в системе).

В этом же диалоговом окне Вы можете указать единицы, в которых выводятся величины объемов передаваемой информации (в полях **Отправлено** и **Принято**), включив одну из следующих кнопок выбора в группе **Отображать трафик**. Данные будут указываться:

- в наиболее подходящих, с точки зрения системы, единицах, если включена кнопка выбора **автоматически**;
- в байтах, если включена кнопка выбора **в байтах**;
- в килобайтах, если включена кнопка выбора **в килобайтах**;
- в мегабайтах, если включена кнопка выбора **в мегабайтах**.

После установки параметров в окне **Дополнительные параметры** нажмите на кнопку **OK**, после чего на экране опять появится диалоговое окно **Столбцы**.

После определения состава и расположения полей в списках **Расширенные поля** и **Выбранные поля** диалогового окна **Столбцы**, нажмите на кнопку **OK**.

3.2.2. Управление отображением информации для элементов Разрешенные, Заблокированные и В отчет списка Моя сеть

Элементы **Разрешенные**, **Заблокированные и В отчет** регистрируют все обращения к сети. Если Вы установите курсор на какой-либо из этих элементов в левой части информационной панели, то в области протокола в правой ее части в табличном виде будет представлена информация, соответствующая сетевому обращению (данные о каждом таком обращении выводятся на одной строке). После установки системы в области протокола выводятся:

- для элемента **Разрешенные** — поля **Причина**, **Установлено в**, **Подключение**, **Приложение**, **Протокол**, **Удаленный порт**, **Удаленный адрес**;
- для элемента **Заблокированные** — поля **Причина**, **Установлено в**, **Подключение**, **Приложение**;
- для элемента **В отчет** — поля **Причина**, **Установлено в**, **Подключение**, **Приложение**, **Состояние**.

В поле **Причина** указывается причина, по которой данный обмен с сетью был разрешен или запрещен (ею может быть имя соответствующего правила для приложения, описание служебного обмена, например, для преобразования DNS-адреса в IP-адрес, и т. д.). Если система **Outpost Firewall** работает в **Режиме бездействия**, то для элемента **Разрешенные** никакая причина не указывается. Если же система работает в **Режиме блокировки**, то в качестве причины указывается строка **Режим блокировки**.

Поле **Состояние** для элемента **В отчет** показывает, разрешено или нет данное обращение к сети.

Для того чтобы добавить или удалить поля, выводимые на экран для элемента списков Разрешенные, Заблокированные или В отчет:

1. Установите курсор на тот список, в котором Вы хотите изменить тип отображаемых полей.
2. Выберите в меню главного окна системы **Outpost Firewall** пункт **Вид**.
3. В следующем меню выберите пункт **Столбцы...** . После этого на экране появится окно **Столбцы** (рис. 29).

Вместо выполнения шагов 1-3 этой процедуры Вы можете вызвать динамическое меню, установив курсор мыши на название какого-либо поля таблицы и нажав на правую кнопку мыши. В этом меню выберите пункт **Столбцы...**.

4. Включите переключатели слева от названий полей, если Вы хотите, чтобы данные поля выводились на экран при отображении информации, и выключите их в противном случае.
5. После завершения изменения состава полей, выводимых на экран, нажмите на кнопку **OK**.

Составы полей для разных элементов (**Разрешенные**, **Заблокированные** или **В отчет**) отличаются друг от друга.

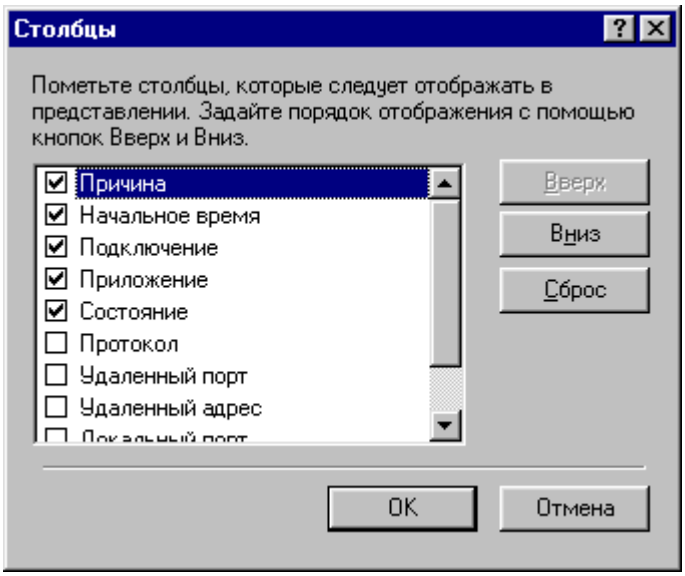

Рисунок 29. Диалоговое окно Столбцы для элементов Разрешенные, Заблокированные и В отчет списка Моя сеть

Вы можете изменить расположение полей на экране с помощью кнопок **Вверх** и **Вниз**. При нажатии на кнопку **Вверх** выбранное поле переместится в списке на одну строчку вверх. При нажатии на кнопку **Вниз** поле, на которое установлен курсор, переместится в списке на одну строчку вниз.

Вы можете восстановить первоначальный состав и расположение полей на экране, нажав на кнопку **Сброс**.

3.2.3. Управление отображением информации для элементов иерархических списков Подключаемые модули и Моя сеть

Элементы **Реклама**, **Содержимое** и **Активное содержимое** предназначены для вывода информации о запрете отображения тех или иных Web-страниц или их

фрагментов. Если установить курсор в левой части информационной панели на какой-либо из этих элементов, то в правой части в табличном виде будет выводиться информация о запрете отображения Web-страниц или их фрагментов. Сразу после установки системы в правой части для этих элементов (**Реклама**, **Содержимое** и **Активное содержимое**) выводятся поля:

- для элемента **Реклама — Дата/время**, **Действие**, **Дополнительно**, **Ключевое слово**;
- для элемента **Содержимое — Дата/время**, **Действие**, **URL**, **Ключевое слово**;
- для элемента **Активное содержимое — Дата/время**, **Действие**, **URL**, **Описание**.

Элемент **DNS** иерархического списка **Подключаемые модули** предназначен для отображения процесса преобразования DNS-адресов. Если установить курсор в левой части информационной панели на элемент **DNS**, то в правой части в табличном виде для каждой операции преобразования DNS-адреса в IP-адрес будут отображаться поля **Дата/время**, **Имя домена** и **Событие**. Поле **Событие** показывает результат операции и может иметь следующие значения: **Не найдено в кэше**, **Новая запись**, **Запись кэширована**.

Элемент **Защита файла** иерархического списка **Подключаемые модули** предназначен для регистрации поступающих на ваш компьютер по электронной почте присоединенных файлов. Если установить курсор в левой части информационной панели на элемент **Защита файла**, то в правой части в табличном виде для каждого такого файла будут отображаться поля **Дата/время**, **От**, **Имя файла** и **Действие**. В поле **От** содержится адрес отправителя.

Элемент **Детектор атак** иерархического списка **Подключаемые модули** предназначен для отображения процесса сканирования портов Вашего компьютера и удаленных атак (таких, как Nuke и др.). Если установить курсор в левой части информационной панели на элемент **Детектор атак**, то в правой части в табличном виде для каждого такого файла будут отображаться поля **Дата/время**, **Тип атаки**, **IP-адрес** и **информация о сканировании портов**.

Вы можете добавить или изменить поля, выводимые для всех этих элементов списка **Подключаемые модули**, поменять порядок их отображения на экране и восстановить их первоначальное состояние таким же образом, как и для элементов **Разрешенные**, **Заблокированные** или **В отчет** списка **Моя сеть** (см. п. 3.2.2).

4. Просмотр данных о взаимодействии с сетью

4

Главное окно системы **Outpost Firewall** дает Вам возможность визуально контролировать сетевые взаимодействия Вашего компьютера с другими узлами сети. Вы можете адаптировать параметры этого контроля к своим задачам, изменив соответствующие настройки отображения информации в главном окне системы **Outpost Firewall**, описанные в п. 3.2.

В настоящей главе будет дан ряд рекомендаций, которые не носят обязательного характера.

В главном окне системы **Outpost Firewall** рекомендуется регулярно просматривать информацию, соответствующую элементам списков **Разрешенные** и **Заблокированные**, входящих в состав объекта **Моя сеть**. Основное назначение информации для списка **Разрешенные** — формирование истории сетевых обращений. При работе с этим списком желательно убедиться в том, что приложения, которым действительно разрешено работать с сетью, взаимодействуют с ней по корректным протоколам, поддерживают связь с корректными удаленными портами и т. д. В случае если информация о каком-либо приложении вызывает у Вас сомнение, рекомендуется изменить для него правила контроля сетевых взаимодействий (см. п. 6.3).

Основное назначение информации для списка **Заблокированные** — обнаружить ошибочно заблокированные сетевые соединения, а также приложения, обращающиеся к портам или протоколам, к которым им обращаться запрещено. Если в протоколе для элемента **Заблокированные** появились приложения, которые должны осуществлять сетевое взаимодействие, и при этом информация о протоколе, удаленном узле, портах и других параметрах, с Вашей точки зрения, является корректной, это свидетельствует о том, что для данных приложений Вы задали слишком жесткие правила работы. Может также оказаться, что Вы вообще не задали никаких правил для этих приложений и выбрали политику работы **Режим блокировки**. В таком случае, если подобная политика является целесообразной с точки зрения безопасности, необходимо сформировать для данного приложения правила, обеспечивающие его нормальную работу в сети. Если же приложение обращается в сеть по протоколам или портам, которые этому приложению действительно должны быть запрещены, то Вы можете предположить, что данное приложение выполняет нерегламентированные операции (например, собирает и передает разработчикам приложения данные о пользователях и т. д.).

Информация о сетевом взаимодействии попадает в протокол для элемента **В отчет** и отображается в главном окне только в том случае, если Вы это явно указали в правиле для приложения. Поэтому в этот список рекомендуется заносить только те сетевые взаимодействия, которые требуют особого контроля.

Необходимо обращать внимание на появление информации о взаимодействии по служебным протоколам, таким как ICMP. Некоторые способы нарушения защиты Вашего компьютера, предусматривающие использование этого протокола, приведены в главе 5.

Вы можете контролировать DNS-адреса узлов сети, с которыми взаимодействует Ваш компьютер, просматривая информацию, отображаемую в главном окне подключаемым модулем **DNS**. Подозрение в первую очередь должны вызывать адреса, обращение к которым Вы не инициализировали.

Информация, выводимая в главном окне системы **Outpost Firewall** модулями, поддерживающими фильтрацию информации в Web-страницах, носит, главным образом, информативный характер. Если Вы отключили активные элементы Web-страниц и это привело к существенному ухудшению интерфейса, Вы можете определить, какие это страницы и какими средствами они пользуются. После этого Вы можете принять решение по каждой конкретной странице. Средства, позволяющие разрешать и запрещать использование активных элементов для каждой конкретной Web-страницы, описаны в п. 6.5.3.3.

Вы можете вести дополнительной контроль сетевой информации, если опасение вызывает какой-то определенный ее элемент. Например, если подозрительным кажется соединение с конкретными узлами в сети, Вы можете сгруппировать информацию по удаленным узлам. Если же наиболее «опасным» представляется соединение с конкретным портом, группировка ведется по портам.

В ходе анализа поступающей информации, находящейся в протоколе системы **Outpost Firewall** для элементов **Разрешенные**, **Заблокированные** и **В отчет** списка **Моя сеть** в левой части главного окна, может оказаться удобным отфильтровать информацию в этом окне. Главное назначение фильтрации информации заключается в том, чтобы на экране оставалась только информация, относящаяся к приложениям, вызывающим Ваше подозрение, либо только информация за определенный промежуток времени.

Для того чтобы отфильтровать информацию в протоколе системы Outpost Firewall для элементов Разрешенные, Заблокированные или В отчет списка Моя сеть необходимо:

1. Установить курсор в списке в левой части диалогового окна на тот из элементов **Разрешенные**, **Заблокированные** или **В отчет**, для которого необходимо отфильтровать информацию.
2. Выбрать пункт меню **Вид**.

3. В следующем меню выбрать пункт **Фильтр…**, после чего на экране появится диалоговое окно задания фильтра, показанное на рис. 30.
4. В этом диалоговом окне пользователь может задать:
   - время и дату начала отображения событий в правой части главного окна, включив кнопку выбора **дата/время** в области **Начать** и задав значение даты и времени (если включена кнопка выбора **с первого события**, то отображаются все события с начала данной сессии работы компьютера);
   - время и дату завершения отображения событий в правой части главного окна, включив переключатель **дата/время** в области **Закончить** и задав значение даты и времени (если включена кнопка выбора **на последнем событии**, то отображаются все события до последнего из произошедших);
   - тип объектов, для которых должны отображаться произошедшие в сети события, выбрав в раскрывающемся списке **Показать историю, где** один из следующих пунктов: **Показать все события**, **Приложение**, **Причина блокировки**, **Протокол**, **Подключение**, **Локальный порт**, **Удаленный порт**, **Удаленный адрес**.
5. Для выбранного типа объекта (кроме **Показать все события**) из раскрывающегося списка **равно** выбрать условие фильтрации (в этом списке в зависимости от выбранного пункта в списке **Показать историю, где** содержатся все обнаруженные в протоколе номера или имена объектов данного типа).
6. Нажать на кнопку **OK**.

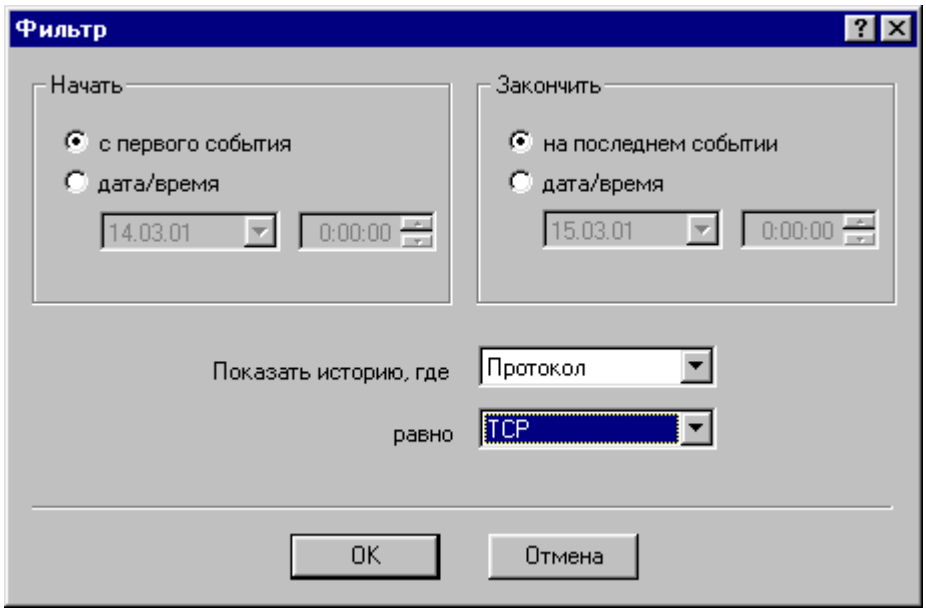

Рисунок 30. Диалоговое окно Фильтр

Вместо выполнения шагов 2 и 3 можно нажать на кнопку  в панели инструментов в главном окне системы **Outpost Firewall**.

Вы можете отфильтровать информацию в протоколе так, чтобы отображались только строки, имеющие такое же значение одного из полей, как и у одной из уже имеющихся в протоколе строк (т.е. взять значение одного из полей этой строки за образец для сравнения).

Для того чтобы отфильтровать информацию в протоколе по значению поля в одной из уже имеющихся в протоколе строк необходимо:

1. Установить курсор на ту строку, значение одного из полей которого необходимо взять за образец.
2. Нажать на кнопку  в панели инструментов в главном окне системы **Outpost Firewall**.
3. В открывшемся меню выбрать имя того поля, значение которого должно быть взято за образец для фильтрации информации.

Для того чтобы отфильтровать информацию, выводимую в протокол, по времени, можно нажать на кнопку  в панели инструментов в главном окне системы **Outpost Firewall**. В открывшемся меню можно выбрать одну из возможностей — выводить информацию, полученную во время текущей сессии работы (эта возможность используется по умолчанию), выводить информацию за текущий день или выводить всю информацию, содержащуюся в протоколе.

Просмотр всей информации, содержащейся в протоколе, может привести к некоторому замедлению времени работы и увеличению объемов требуемой памяти, поэтому использовать этот режим рекомендуется в случае, когда Вам действительно необходимо просмотреть протокол за все время работы системы.

Для того чтобы отменить фильтр на тип отображаемых в протоколе объектов (если он был задан), необходимо нажать на кнопку  , однако это действие не отменяет выбранное время отображения информации в протоколе — текущая сессия, текущий день или все события, содержащиеся в протоколе.

5. Организация защиты компьютера

5

В настоящей главе будут рассмотрены возможности защиты с помощью брандмауэра **Outpost Firewall** Вашего персонального компьютера от наиболее распространенных опасностей, возникающих при работе в сети. Как было сказано в п. 1.1, основными опасностями при работе с сетью являются:

- проникновение на Ваш компьютер посторонних программ;
- попытка получения доступа к информации на Вашем компьютере или информации о работе Вашего компьютера;
- поступление на Ваш компьютер ненужной информации (например, баннеров).

Для защиты от проникновения на Ваш компьютер посторонних программ система позволяет Вам:

- Запретить создание сетевых взаимодействий для всех программ, кроме тех, которым Вы явно даете разрешение. В этом случае система **Outpost Firewall** должна работать в **Режиме обучения** или **Режиме блокировки** с соответствующим образом настроенными правилами сетевого взаимодействия (см. п. 6.2). Кроме того, Вы можете контролировать сетевые соединения с помощью информации, отображаемой в главном окне (см. п. 3.2).
- Запретить использование в Web-страницах таких ресурсов, как ActiveX, Java-апплеты, программы на языках VB и Java Script. Если для некоторых страниц использование таких средств позволяет улучшить интерфейс Web-страниц, то Вы можете воспользоваться возможностью системы, позволяющей запретить использования этих программных средств по умолчанию, но разрешить их использование в известных и проверенных Вами Web-страницах, список которых Вы составляете сами. Эти возможности описаны в п. 6.5.3.

Для предотвращения попыток получения доступа к информации на Вашем компьютере или информации о работе Вашего компьютера Вы можете:

- запретить создание на Вашем компьютере Cookie, использовав для этого возможности системы **Outpost Firewall**, описанные в п. 6.5.3. В частности, Вы можете, как и в случае с ActiveX, Java-апплетами, программами на VB и Java Script, ограничивать или разрешать создание Cookie для всех Web-страниц или только для Web-страниц из заданного Вами списка;
- для защиты от «троянских коней» Вы можете либо:
    - оставить систему работать в **Режиме обучения** и тогда при попытке обращения со стороны «троянца» к сети система проинформирует Вас об этом и поможет заблокировать выход в сеть этого приложения;
    - запретить создание сетевых взаимодействий для всех программ, кроме тех, разрешение для которых Вы даете явно, и работать в **Режиме блокировки**;

При обнаружении подозрительного соединения Вы можете, благодаря информации, выдаваемой системой **Outpost Firewall**, определить DNS-адрес или IP-адрес узла, с которым находящаяся на Вашем компьютере подозрительная программа пытается установить соединение, после чего принять соответствующие меры.

- перейти в «невидимый» для других компьютеров сети режим работы (см. п. 6.4).

Для предотвращения поступления на Ваш компьютер ненужной информации Вы можете:

- запретить отображение *баннеров* на экране. Поскольку имена большинства баннерных служб известны, то Вы можете исключить отображение тех Web-страниц, в которых есть HTML-строки, указывающие на имена баннерных служб (см. п. 6.5.3.1);

Сразу после установки система содержит большой список рекламных HTML-строк. Чтобы добавить в этот список какую-либо HTML-строку из Web-страницы, находящейся в данный момент времени на экране, Вы можете воспользоваться специальной компонентой системы **Outpost Firewall**, называемым **Корзина для рекламы**. Вы также можете отменить запрет на отображение тех или иных частей Web-страницы либо вовсе отказаться от использования **Корзины для рекламы**. Порядок работы с HTML-строками и **Корзиной для рекламы** описан в п. 6.5.3.1.

- Запретить отображение *баннеров* на экране за счет того, что подавляющее большинство баннеров имеют графическое изображение одного из стандартных размеров. С помощью настроек системы **Outpost Firewall** Вы можете запретить вывод на экран графических изображений определенного размера (см. п. 6.5.3).

В настоящее время в российских сетях используются следующие основные размеры баннеров: 468*60, 120*80, 100*100, 88*31 пикселей. Встречаются также и баннеры других размеров (125*125, 234*60), которые весьма распространены в мировых сетях, а кроме того, постепенно становятся популярны такие форматы, как 470*60, 470*70, 400*40, 120*240, 60*60. Сразу после установки система **Outpost Firewall** настроена таким образом, чтобы не отображались графические изображения размером 468*60, 120*80, 100*100 и 88*31 пикселей. Вы можете разрешить вывод на экран всех графических изображений, а также изменить или дополнить список размеров тех изображений, которые не должны отображаться.

- Запретить отображение на экране тех или иных Web-сайтов и Web-страниц. Этот запрет реализуется с учетом списков запрещенных словосочетаний и имен доменов, которые содержатся в системе **Outpost Firewall**. Данные списки формируются при настройке системы и описаны в п. 6.5.3. Оба списка составляются и управляются независимо друг от друга. Таким образом, Вы можете запретить отображение на экране Web-страниц, имеющих определенные DNS-адреса или содержащих определенные словосочетания (например, запретить вывод на экран всех Web-страниц, в которых имеется слово **порнография**). Сразу после установки системы оба эти списка пусты и Вам следует сформировать их самостоятельно.

Если после этого защитить настройки системы **Outpost Firewall** паролем (см. п. 6.5.5), то Вы воспрепятствуете изменению этих данных. Таким способом Вы можете, например, заблокировать на Вашем домашнем компьютере доступ к подобной информации для Ваших детей и т. д.

При использовании системы Вы можете создать зону сетевых адресов, для которых контроль сетевых взаимодействий выполняться не будет. Эта зона представляет собой список узлов или подсетей, задаваемых своими IP-адресами или DNS-адресами, для которых система не блокирует сетевые соединения (как при передаче информации с этих узлов на Ваш компьютер, так и при передаче информации с Вашего компьютера на эти узлы сети). В «доверенную» зону могут быть включены узлы Вашей локальной корпоративной сети, домашний компьютер и т. д. Более подробно правила формирования списка доверенных адресов изложены в п. 6.2.

Важной особенностью системы является возможность настройки системных протоколов, поскольку многие попытки нарушения работоспособности локальных компьютеров связаны с использованием злоумышленниками этих протоколов.

Для предотвращения попыток нарушения работоспособности Вашего компьютера с использованием злоумышленниками служебного протокола ICMP (см. Приложение В) система **Outpost Firewall** позволяет разрешить или запретить использование ICMP-сообщений того или иного типа (см. п. 6.1).

Рекомендуется использовать настройки протокола ICMP, заданные в системе **Outpost Firewall** сразу после ее установки. В случае если Вы меняете настройки, необходимо четко себе представлять, почему Вы это делаете, а также быть уверенными в том, что это не приведет к ухудшению работоспособности системы в целом. Система позволяет восстановить те настройки протокола ICMP, которые были заданы после установки.

Протокол **NetBios** может применяться в системе Windows в качестве протокола для доступа к удаленным файлам и принтерам. Система **Outpost Firewall** позволяет либо запретить использование этого протокола, либо разрешить его использование при сетевом соединении с определенными узлами, задаваемых своими IP-адресами или DNS-адресами (см. п. 6.4).

Целесообразно разрешить использование протокола NetBios только при сетевом соединении с узлами Вашей локальной сети.

6. Средства обеспечения безопасности и их настройка

6

Содержание

Как уже было отмечено выше, настройки системы позволяют Вам сконфигурировать ее таким образом, чтобы она в максимальной степени удовлетворяла Вашим индивидуальным запросам и в наибольшей степени позволяла Вам добиться безопасности и сохранности информации на Вашем компьютере.

Для того чтобы вызвать диалоговое окно настроек системы Outpost Firewall, в случае если значок системы находится в правой части панели задач системы Windows:

1. Вызовите динамическое меню системы **Outpost Firewall**.
2. В этом динамическом меню выберите пункт **Параметры...** .
3. После этого на экране появится диалоговое окно настроек системы, показанное на рис. 31.

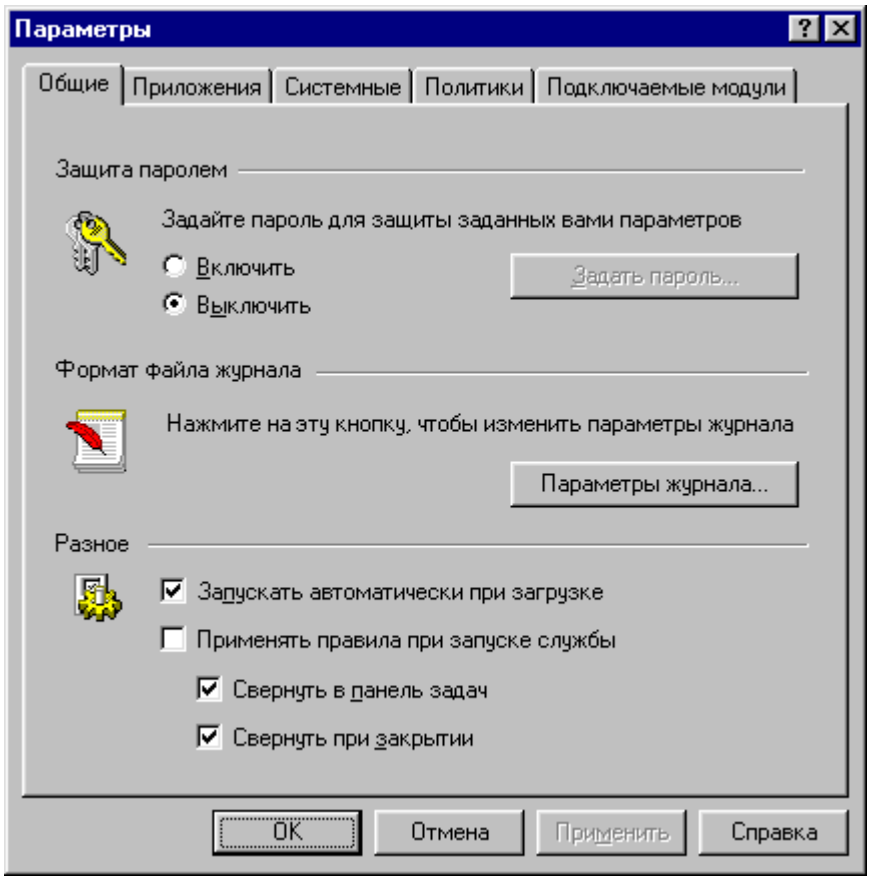

Рисунок 31. Диалоговое окно параметров системы

Это диалоговое окно содержит закладки: **Общие**, **Приложения**, **Системные**, **Политики** и **Подключаемые модули**.

Вы можете также вызвать диалоговое окно настроек из главного окна системы **Outpost Firewall**.

Для того чтобы вызвать диалоговое окно настроек из главного окна системы Outpost Firewall:

1. В меню главного окна системы выберите пункт **Параметры**.

2. В следующем меню выберите пункт, соответствующий названию той закладки, которую Вы хотите сделать активной в диалоговом окне параметров.

После этого на экране появится диалоговое окно настроек системы, в котором активной будет та закладка, которую Вы указали.

Вы можете вызвать диалоговое окно настроек, нажав на кнопку  в панели инструментов главного окна системы **Outpost Firewall**. Если же Вы нажмете на расположенную правее кнопку  , то на экране появится меню, показанное на рис. 32. С помощью этого меню Вы можете вызвать диалоговое окно настроек системы с активной закладкой **Общие**, выбрав пункт меню **Общие**, либо вызвать окно настроек одного из имеющихся в системе подключаемых модулей, выбрав в меню пункт с его названием.

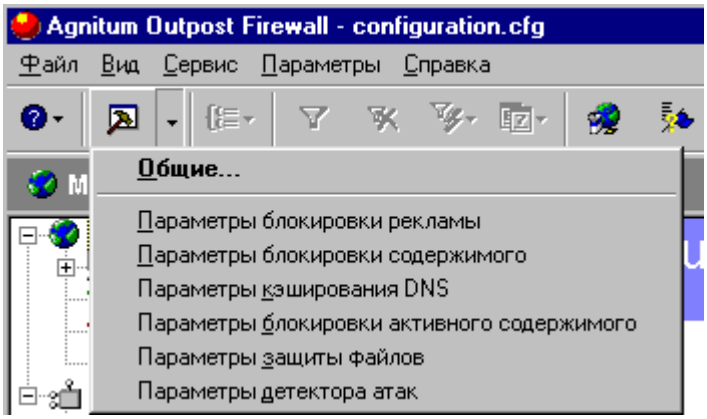

Рисунок 32. Меню вызова настроек системы из панели инструментов главного окна

6.1. Общие настройки. Задание режимов работы системы

Общие настройки позволяют Вам с помощью системы **Outpost Firewall** установить пароль для защиты созданных Вами параметров системы, задать параметры файла протокола и определить, каким образом и когда запускается (или может быть запущена) система **Outpost Firewall**.

Наличие пароля защищает Вас от того, что в Ваше отсутствие кто-то изменит настройки и снимет часть ограничений, которые Вы задали для работы в сети. Такая ситуация характерна, например, для домашнего компьютера, если Вы не хотите разрешать детям играть в on-line игры, получать доступ к порнографическим сайтам и т. д.

Вид диалогового окна настроек с активной закладкой **Общие** показан на рис. 31.

Для того чтобы задать или изменить пароль для защиты параметров:

1. Включите кнопку выбора **Включить** в области **Защита паролем** диалогового окна (сразу после установки системы включена кнопка выбора **Выключить**), если Вы хотите задать пароль или изменить уже существующий пароль.
2. Нажмите на кнопку **Задать пароль...** (если включена кнопка выбора **Выключить**, то кнопка **Задать пароль...** находится в неактивном состоянии).

3. Если пароль уже был задан и Вы хотите его изменить, то в открывшемся диалоговом окне **Изменение пароля** (рис. 33) в поле **Старый пароль** введите старое значение пароля.
4. В этом же диалоговом окне в поле **Новый пароль** введите новое значение пароля (переключение между полями в этом окне осуществляется с помощью клавиши **Tab**).
5. Введите новое значение пароля еще раз в поле **Подтверждение**.
6. Нажмите на кнопку **OK**.

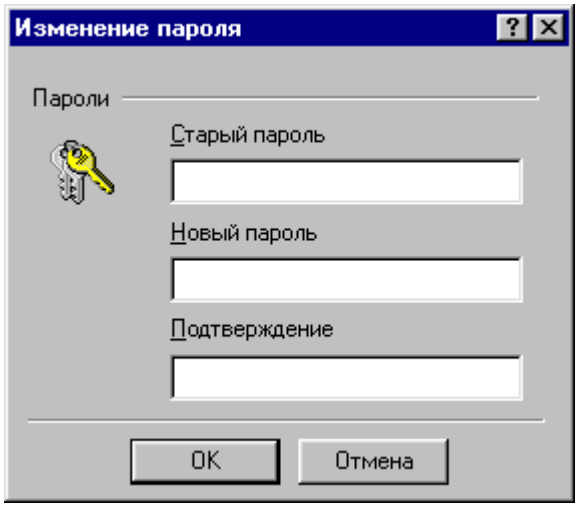

Рисунок 33. Диалоговое окно ввода и изменения пароля

После определения пароля система **Outpost Firewall** будет выводить диалоговое окно для ввода пароля при каждой попытке вызова диалогового окна параметров системы.

Для того чтобы изменить параметры файла протокола:

1. Нажмите на кнопку **Параметры журнала**.
2. В открывшемся диалоговом окне задания параметров файла протокола **параметры файла журнала** (рис. 34) измените, если это необходимо, максимальный размер файла протокола в поле **Максимальный размер** (сразу после установки системы эта величина равна 512 Кб).
3. Если это необходимо, измените условие , при котором осуществляется перезапись старой информации в файле протокола:
   - при включении кнопки выбора **по необходимости** перезапись будет выполняться в случае превышения размера файла;
   - при включении кнопки выбора **сохранить за последние** система будет хранить информацию за последние несколько дней, независимо от размера файла протокола (количество дней задается в поле справа от этой кнопки выбора). Сразу после установки системы включена кнопка выбора **сохранить за последние** и число дней хранения информации равно 7.
4. Нажмите на кнопку **OK**.

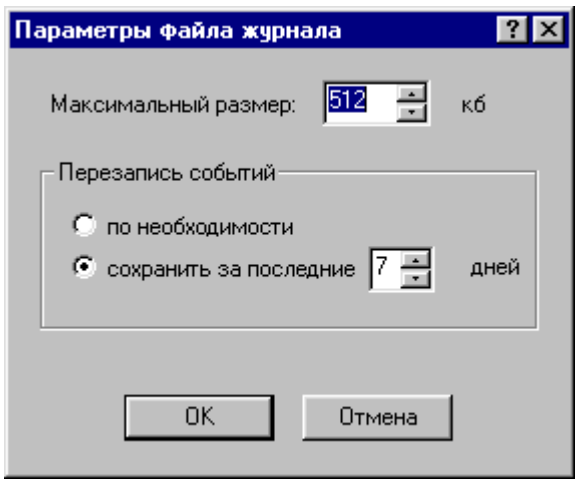

Рисунок 34. Диалоговое окно задания параметров файла протокола

Остальные параметры системы **Outpost Firewall**, которые задаются в этой закладке, находятся в области **Разное** диалогового окна. Эти параметры определяют следующее:

- система **Outpost Firewall** будет запускаться при загрузке компьютера, если включен переключатель **Запускать автоматически при загрузке**, и не запускаться, если этот переключатель выключен.
- при запуске сетевых сервисов и драйверов системы **Outpost Firewall** сетевые взаимодействия будут проверяться в соответствии с заданными для приложений правилами (см. п. 6.3), если включен переключатель **Применять правила при запуске службы**, и не будут, если этот переключатель выключен.

Если Вы установите переключатель **Применять правила при запуске службы** во включенное состояние, то выходы приложений в сеть все равно могут быть заблокированы даже после завершения работы (если это определено имеющимися для этих приложений правилами). Установка данного переключателя во включенное состояние позволяет Вам задать «скрытый» режим системы **Outpost Firewall**, т. е. выполнение основных функций работы при отсутствии пользовательского интерфейса. Кроме того, этот режим может быть полезен при использовании системы **Outpost Firewall** на компьютере с отсутствием свободных ресурсов памяти и процессорного времени.

- После запуска системы в правой части панели задач Windows будет размещен значок системы **Outpost Firewall**, если включен переключатель **Свернуть в панель задач**. Если переключатель выключен, значок в панель задач помещен не будет, а при загрузке каждый раз будет открываться основное окно системы **Outpost Firewall**.
- После закрытия главного окна в правой части панели задач Windows останется значок системы **Outpost Firewall**, если включен переключатель **Свернуть при закрытии**. В противном случае значок системы **Outpost Firewall** после закрытия главного окна будет удален из правой части панели задач системы Windows.

6.2. Политики защиты. Подавление сети и отключение брандмауэра

Политика защиты определяет, для кого и какие сетевые соединения разрешены или запрещены. Возможные политики работы системы описаны в п. 2.2 (табл. 3):

- **Блокировать все** — запрет любых сетевых взаимодействий;
- **Режим блокировки** — запрет всех сетевых взаимодействий, кроме явно разрешенных;
- **Режим обучения** — система помогает Вам принять решение о возможности или запрете выхода в сеть для приложения, выдавая диалоговое окно предупреждения о первом сетевом взаимодействии для данного приложения. В этом же диалоговом окне Вы сразу же можете и настроить правила доступа данного приложения в сеть (эта политика задается сразу после установки системы **Outpost Firewall**);
- **Режим бездействия** — разрешение любых сетевых взаимодействий;
- **Режим разрешения** — разрешение всех сетевых взаимодействий, кроме явно запрещенных;

Для того чтобы изменить политику защиты системы Outpost Firewall:

1. Вызовите диалоговое окно **Параметры** системы **Outpost Firewall** и перейдите на закладку **Политики** (см. главу 6). После этого диалоговое окно примет вид, показанный на рис. 35.
2. В области диалогового окна **Выберите политику брандмауэра** выберите политику системы, щелкнув мышью на одну из кнопок:  Разрешать,  Обучение,  Блокировать,  Запрещать,  Отключить, каждая из которых определяет соответствующую политику. При нажатии любой из этих кнопок под ней появляется краткое описание выбранной политики.
3. Нажмите на кнопку **ОК**.

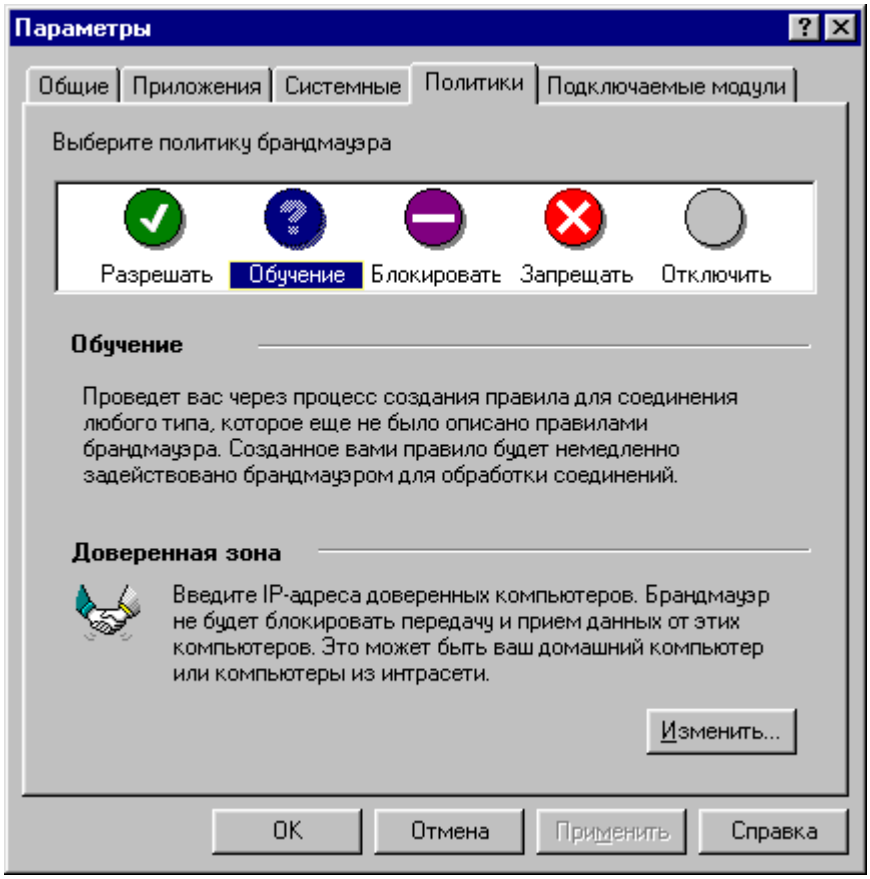

Рисунок 35. Диалоговое окно Параметры с активной закладкой Политики

Вы можете задать политику работы системы непосредственно в контекстном меню, выбрав в нем пункт с названием той политики, которой система **Outpost Firewall** должна придерживаться в работе. Текущая политика помечена в контекстном меню символом ✔.

Вы можете также изменить политику работы системы **Outpost Firewall** с помощью панели инструментов главного окна системы, как это описано в п. 3.2.

В диалоговом окне **Options** с активной закладкой **Политики** Вы можете изменить состав списка доверенных адресов (см. главу 5), нажав на кнопку **Изменить…** в области **Доверенная** диалогового окна. После этого на экране появится диалоговое окно управления списком адресов доверенной зоны, показанное на рис. 29.

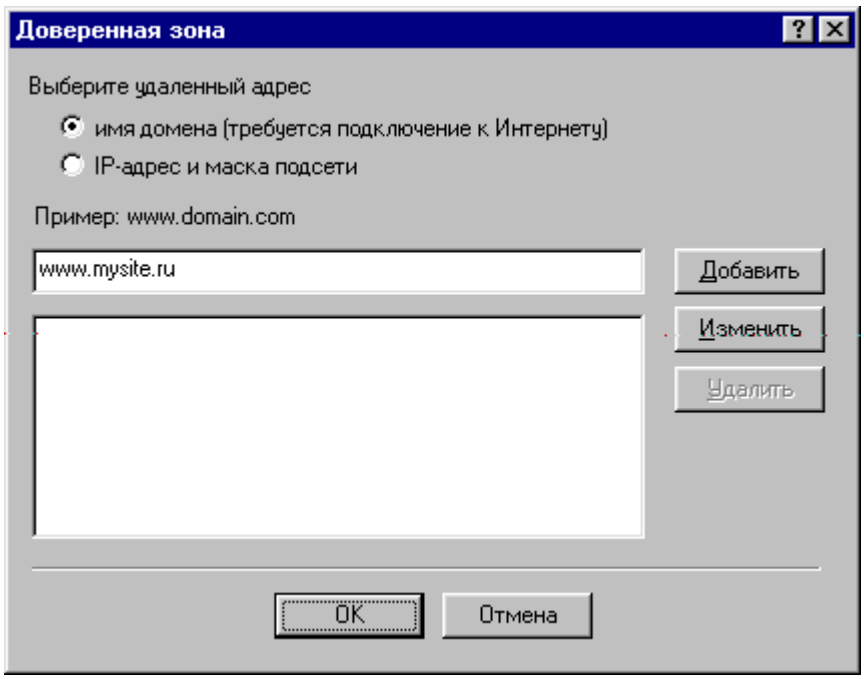

Рисунок 36. Диалоговое окно Доверенная зона

Для того чтобы внести одно или несколько имен в список адресов доверенной зоны:

1. Включите одну из следующих кнопок:

   - Кнопку выбора **имя домена (Требуется подключение к Интернету)**, если Вы хотите использовать DNS-адреса.

Вы можете использовать DNS-адреса, только если в этот момент у Вашего компьютера существует подключение к Интернету, поскольку будет производиться преобразование этого адреса в IP адрес.

   - Кнопку выбора **IP-адрес и маска подсети**, если Вы хотите использовать IP-адреса и маски подсети (по умолчанию маска подсети выставляется равной 255.255.255.0, т. е. в качестве номера сети используются 3 байта, а последний байт определяет номер узла в сети). При включении кнопки выбора **IP-адрес и маска подсети** диалоговое окно **Доверенная зона** примет вид, показанный на рис. 37.

2. Установите курсор в поле ввода имен и введите соответствующий DNS-адрес или IP-адрес (в последнем случае Вы можете не только ввести этот адрес, но и откорректировать значение маски подсети, заданное по умолчанию).
3. Нажмите на кнопку **Добавить** диалогового окна, после чего введенный Вами адрес будет размещен в нижней части окна, где и находится список имен узлов.
4. Повторите шаги 1-3 для каждого из узлов, которые Вы хотите внести в список.
5. Нажмите на кнопку **OK**.

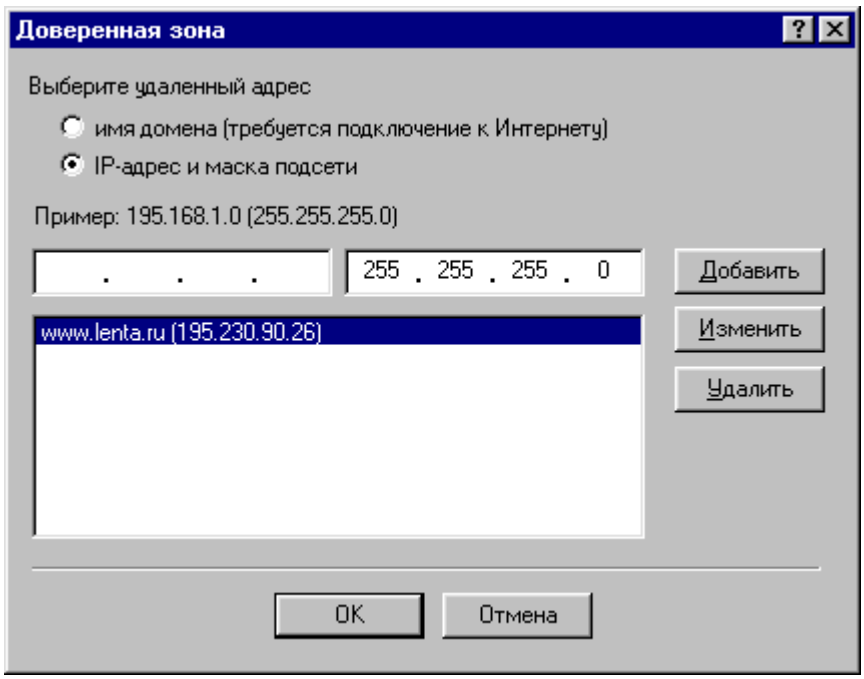

Рисунок 37. Диалоговое окно Доверенная зона с включенной кнопкой выбора IP-адрес и маска подсети

Для того чтобы изменить адрес в списке адресов доверенной зоны:

1. Установите курсор на тот адрес в списке, который Вы хотите изменить, после чего этот же адрес отобразится в поле ввода адресов диалогового окна.
2. Измените адрес в поле ввода адресов диалогового окна.
3. Нажмите на кнопку **Изменить**.
4. Нажмите на кнопку **ОК**.

Для того чтобы удалить адрес из списка адресов доверенной зоны:

1. Установите курсор на тот адрес в списке, который Вы хотите удалить, после чего этот же адрес отобразится в поле ввода адресов диалогового окна.
2. Нажмите на кнопку **Удалить**.
3. Нажмите на кнопку **ОК**.

6.3. Контроль приложений. Правила

6.3.1. Распределение приложений по группам

Как уже было сказано ранее (см. гл. 1), с точки зрения системы **Outpost Firewall**, все приложения делятся на три группы. К первой группе относятся приложения, которым разрешены все сетевые соединения. Ко второй группе принадлежат приложения, для которых явно, в виде специальных правил, указаны те протоколы, порты и направления, с которыми сетевые соединения разрешены или запрещены. В состав третьей группы входят те приложения, которым запрещены все сетевые соединения.

Закладка **Приложения** диалогового окна **Параметры** позволяет управлять распределением приложений по группам, а также формировать правила для

приложений. После перехода на эту закладку диалоговое окно **Параметры** примет вид, показанный на рис. 38.

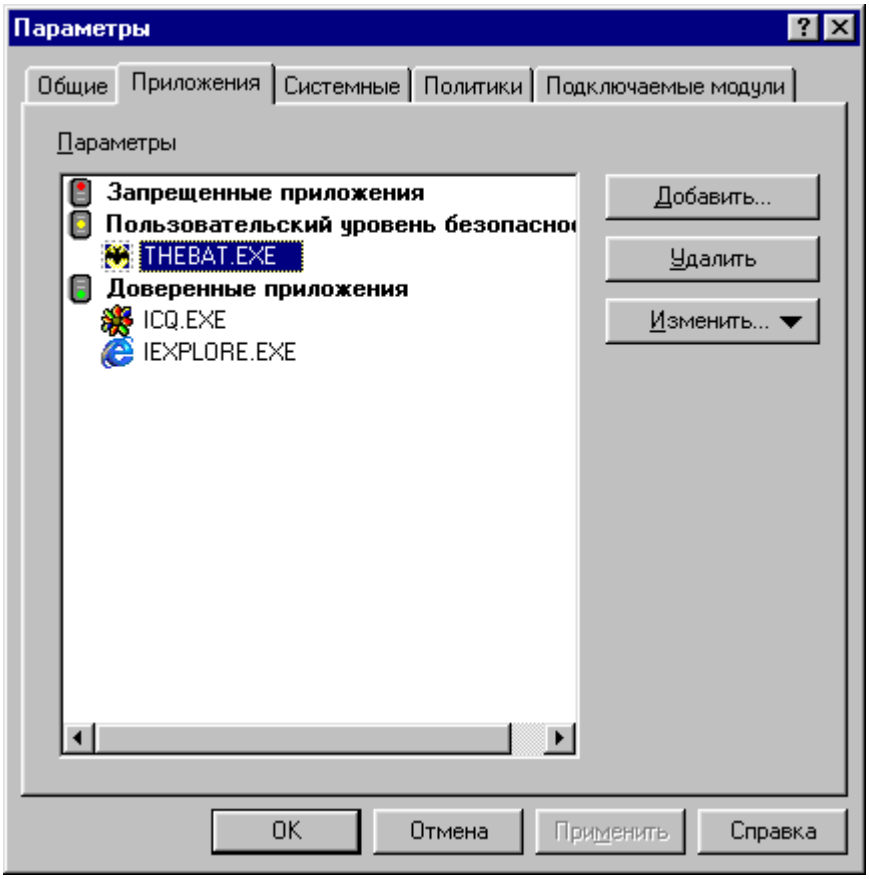

Рисунок 38. Диалоговое окно Параметры с активной закладкой Приложения

В области **Параметры** диалогового окна находится иерархический список приложений, распределенных по трем группам:

- **Запрещенные приложения** — приложения, которым запрещена работа в сети;
- **Пользовательский уровень** — приложения, которым работа в сети разрешена в соответствии с правилами, заданными для этих приложений;
- **Доверенные приложения** — приложения, которым разрешена работа в сети.

Каждая из этих групп содержит список принадлежащих ей приложений.

Для того чтобы внести приложение в одну из этих групп:

1. Установите курсор на название той группы, в которую Вы хотите добавить приложение (можно также установить курсор на любое из приложений в этой группе).
2. Нажмите на кнопку **Добавить**, после чего откроется системное окно выбора имени файла.
3. В системном окне выбора имени файла укажите имя исполняемого файла данного приложения, после чего нажмите на кнопку **Открыть**.

Вы можете внести приложение в одну из этих групп, отбуксировав значок этого приложения из рабочего стола системы Windows или меню **Пуск** системы Windows.

Если приложение, которое Вы внесли в один из трех списков, уже находилось в другом списке, то из последнего оно будет удалено.

Для того чтобы перенести приложение из одной группы в другую:

1. Установите курсор на значок и имя того приложения, которое Вы хотите перенести.
2. Нажмите на кнопку **Изменить**.
3. В открывшемся меню (рис. 39) выберите один из следующих пунктов:
   - **Разрешить сетевую активность этого приложения**, если Вы хотите перенести данное приложение в группу **Доверенные приложения**.
   - **Запретить запуск этого приложения**, если Вы хотите перенести данное приложение в группу **Запрещенные приложения**.
   - **Создать правило…**, если Вы хотите перенести данное приложение в группу **Пользовательский уровень** и задать собственное правило для данного приложения. В этом случае на экране появится диалоговое окно формирования правил для приложения (рис. 41).
   - **Создать правила на основе стандартного**, если Вы хотите перенести данное приложение в группу **Пользовательский уровень** и использовать одно из предопределенных в системе **Outpost Firewall** правил (см. п. 6.3.2). После этого на экране появится меню, показанное на рис. 40. Если выбран один из пунктов меню, соответствующий имени типа программы, для которого задаются предопределенные в системе правила,— соответствующие правила будут внесены в список правил для данного приложения, а при выборе пункта меню **Другие…** на экране появится диалоговое окно формирования правил для приложения (рис. 41).

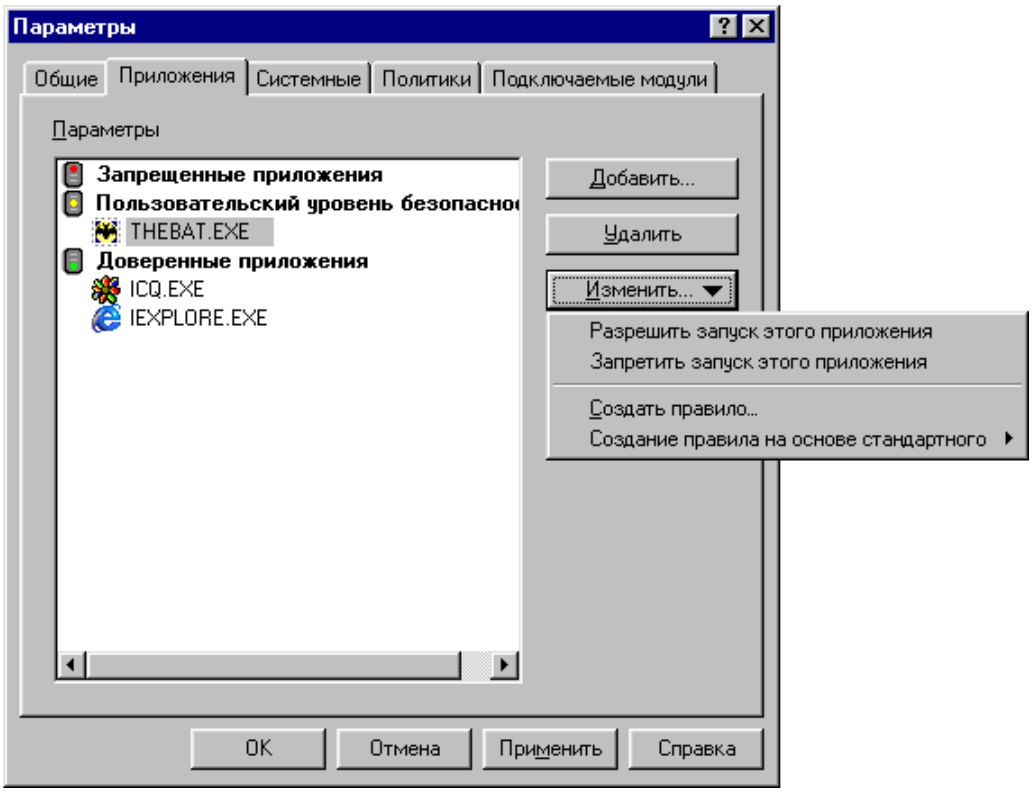

Рисунок 39. Меню для редактирования групп приложений

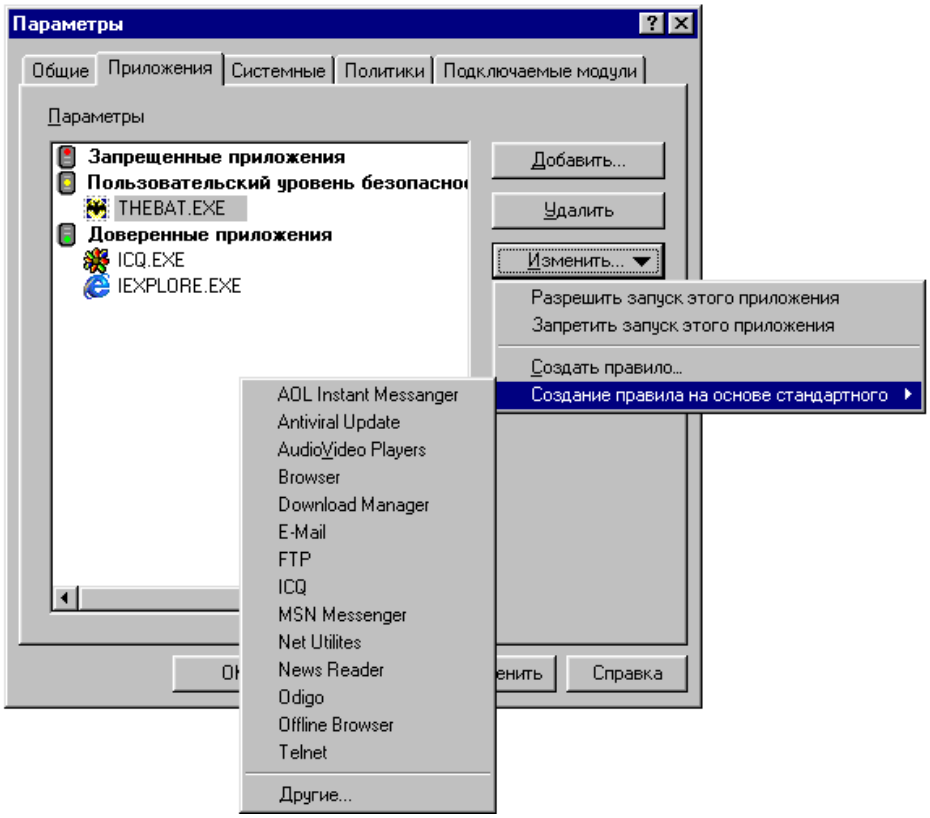

Рисунок 40. Меню выбора предопределенного правила для приложения

Если приложение находится в группе **Доверенные приложения**, то пункта **Разрешить запуск этого приложения** в меню не будет. Если приложение находится в группе **Запрещенные приложения**, то в меню не будет пункта **Запретить запуск этого приложения**.

Если приложение находится в группе **Пользовательский уровень** и выбран пункт **Создать правила...** или **Создать правила на основе стандартного**, то приложение в другую группу не переносится, а для него формируется новое правило.

Вы можете также перенести приложение из одной группы в другую, установив курсор на значок и имя этого приложения и отбуксировав выделенную строку в соответствующую группу.

Если Вы отбуксировали приложение в группу **Пользовательский уровень**, то сначала появится окно формирования правил, показанное на рис. 41. Для всех остальных групп имя приложения вместе с его значком окажется в списке приложений соответствующей группы.

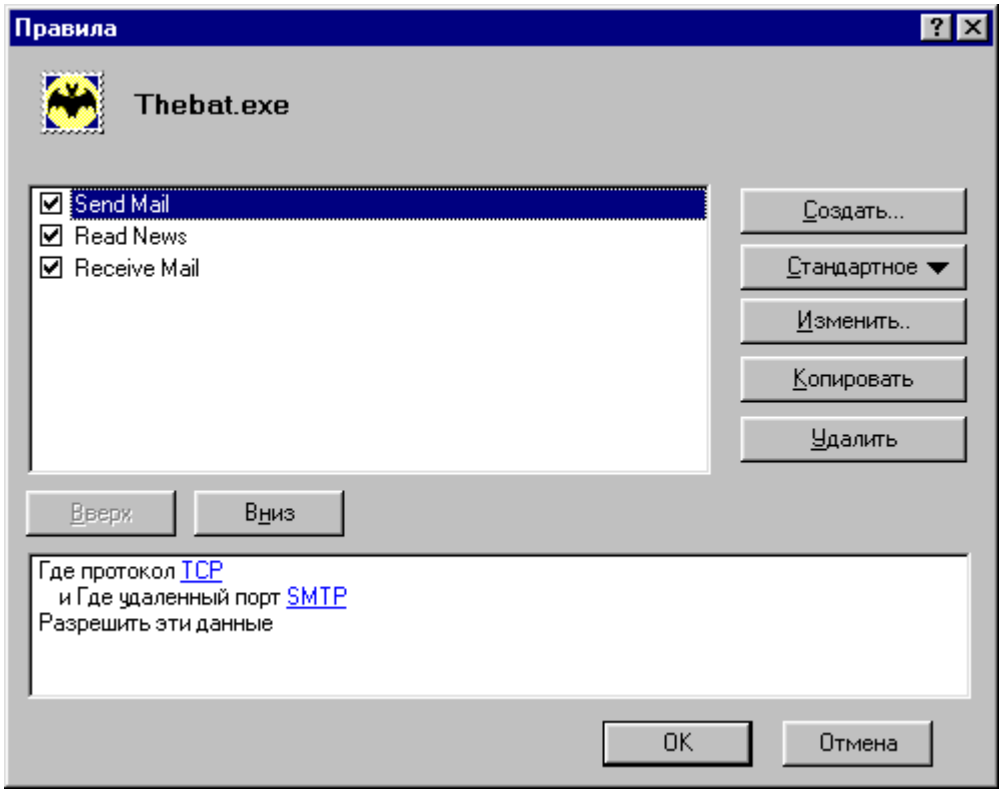

Рисунок 41. Диалоговое окно формирования правил для приложений

В верхней части этого диалогового окна располагается список всех правил для данного приложения, а в нижней части окна появляется описание того правила, на котором в настоящий момент установлен курсор.

Новое правило для какого-либо приложения Вы можете создать одним из двух способов:

- сформировать правило самостоятельно;
- воспользоваться одним или несколькими из имеющихся в системе **Outpost Firewall** правил для приложений.

6.3.2. Использование предопределенных правил в системе Outpost Firewall

Для помощи пользователю при создании правил работы в сети для приложений система **Outpost Firewall** включает в себя большое количество предопределенных правил обращения к сети. Эти правила разбиты по типам приложений. Например, в системе содержатся правила для работы с браузером, FTP-сервисом, электронной почтой, сетевой службой новостей, системой удаленной загрузки программ и т. д.

Список сетевых операций, для которых имеются предопределенные правила, постоянно расширяется, поэтому после установки на Ваш компьютер системы **Outpost Firewall** этот список (и соответственно, количество предопределенных правил) может расширяться в ходе дальнейшей работы.

Если Вы формируете одно или несколько правил для приложения, предназначенного для любой из вышеперечисленных сетевых операций, то рекомендуется пользоваться предопределенными правилами, имеющимися в системе **Outpost Firewall**. В таком случае Вам не придется разбираться, как те или иные программы используют порты и протоколы для выполнения сетевых операций.

Вы можете создать для приложения любое количество правил, но при этом необходимо следить за тем, чтобы они не противоречили друг другу.

Система **Outpost Firewall** при попытке осуществить сетевое взаимодействие для приложения, находящегося в списке 

, будет проверять правила последовательно, сверху вниз, пока не найдет первое правило, для которого выполняются заданные условия. После этого действия системы **Outpost Firewall** по разрешению или запрещению данного сетевого взаимодействия будут определяться данным правилом и текущей политикой работы системы **Outpost Firewall**. Если же не выполнены условия ни одного из правил данного приложения, то действия системы определяются только текущей политикой работы.

Вы можете изменить порядок правил в диалоговом окне формирования правил для приложений (рис. 42) с помощью кнопок **Вверх** и **Вниз**.

Вы можете временно отменить действие любого из правил для данного приложения, выключив переключатель, расположенный слева от имени данного правила в списке.

Для того чтобы добавить в список правил для данного приложения одно из предопределенных в системе правил:

1. Нажмите на кнопку **Стандартное** в диалоговом окне.
2. В появившемся меню выберите тип приложения, правила для которого Вы хотите добавить.
3. После выполнения этой процедуры новое правило (или несколько правил) будет добавлено в список правил последним (последними).

6.3.3. Формирование правил пользователем

Для того чтобы сформировать для данного приложения новое правило, необходимо в диалоговом окне формирования правил для приложений (см. рис. 41) нажать на кнопку **Создать...**, после чего на экране появится диалоговое окно формирования содержимого правила, показанное на рис. 43.

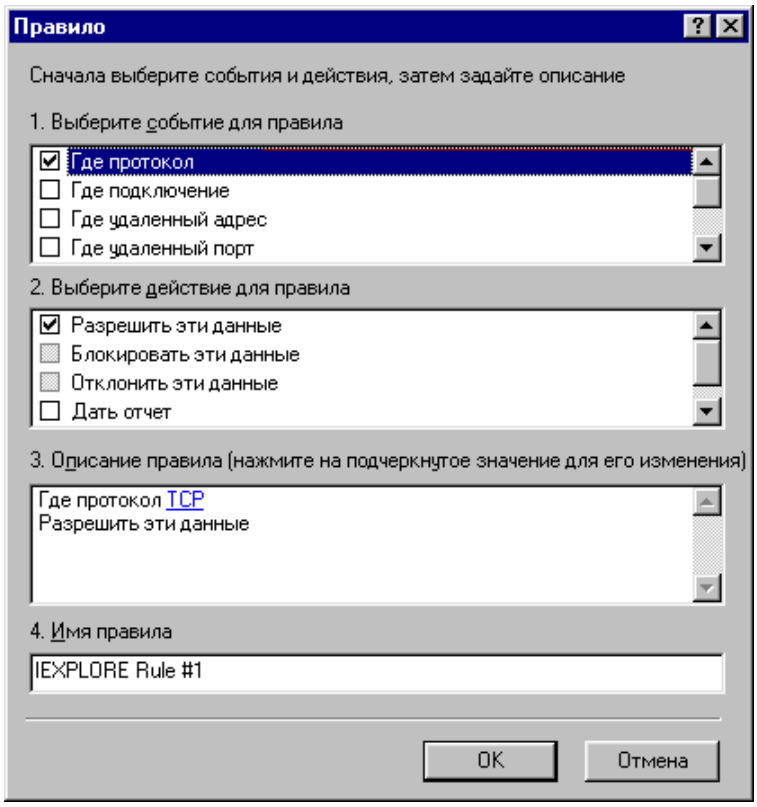

Рисунок 43. Диалоговое окно формирования содержимого правила

В этом диалоговом окне Вы можете:

- в области диалогового окна **Выберите событие для правила** определить условия на сетевое взаимодействие — протокол (протоколы) обмена, направление обмена, номер (номера) локального и удаленного портов;
- в области диалогового окна **Выберите действие для правила** указать действие, которое должна осуществлять система **Outpost Firewall** при выполнении заданных условий (запретить сетевое взаимодействие, разрешить сетевое взаимодействие, занести его в отчет);
- в области диалогового окна **Описание правила** уточнить параметры условий, задаваемых в области **Выберите событие для правила** диалогового окна;
- в области диалогового окна **Имя правила** указать имя формируемого правила (при входе в данное диалоговое окно система **Outpost Firewall** сама генерирует имя правила, но пользователь может это имя изменить).

После появления этого диалогового окна на экране переключатели **Где удаленный порт** и **Где локальный порт** не активны, т. е. доступ к ним закрыт до выбора протокола соединения.

Для того чтобы сформировать условия на протокол и его параметры:

1. Включите переключатель слева от строки **Где протокол**. После этого в области **Описание правила** появится строка Где протокол Не определено.
2. Укажите имя используемого протокола, щелкнув мышью на слове Не определено в строке Где протокол Не определено в области **Описание правила**. После этого на экране появится диалоговое окно выбора протокола, показанное на рис. 44.

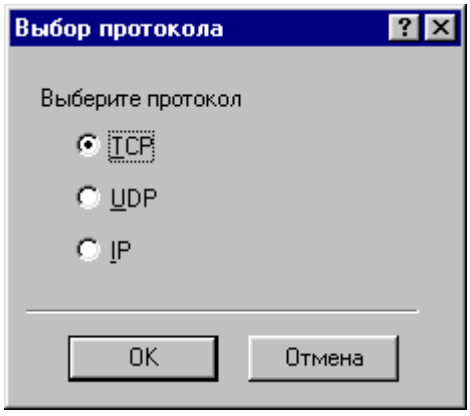

Рисунок 44. Диалоговое окно выбора протокола

3. В этом диалоговом окне:
   - включите кнопку выбора **TCP**, если Вы хотите задать условие на использование протокола TCP;
   - включите кнопку выбора **UDP**, если Вы хотите задать условие на использование протокола UDP;
   - включите кнопку выбора **IP**, если Вы хотите задать условие на использование одного или нескольких протоколов IP.

4. Нажмите на кнопку **ОК**, после чего на экране опять появится диалоговое окно формирования правила, в котором вместо слова Не определено в области **Описание правила** будет указано имя конкретного протокола.

5. Если Вы выбрали протокол IP, то строка в области формирования правила после выбора имени протокола будет иметь вид Где протокол IP и IP-протокол Не определено. Для уточнения имени IP-протокола щелкните мышью на слове Не определено в этой строке. После этого на экране появится диалоговое окно выбора IP-протокола, показанное на рис. 45. В этом диалоговом окне включите переключатели слева от тех IP-протоколов, которые должны использоваться в формируемом Вами правиле, и затем нажмите на кнопку **ОК**. После этого на экране опять появится диалоговое окно формирования правила, в котором вместо слова Не определено в области **Описание правила** будут указаны номера выбранных Вами IP-протоколов.

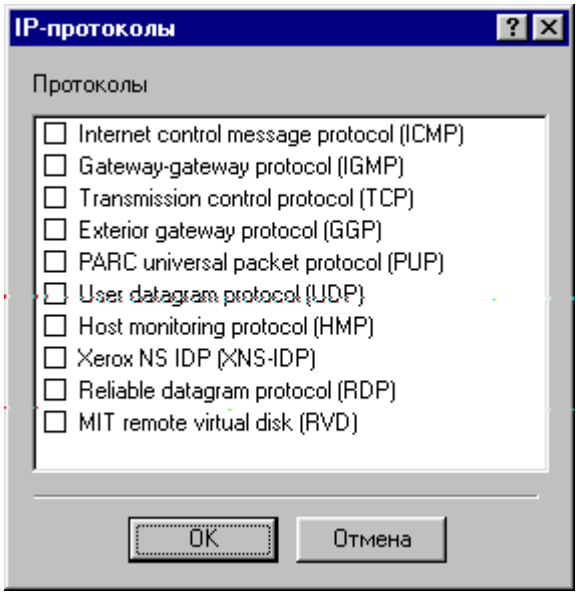

Рисунок 45. Диалоговое окно выбора IP-протоколов

Если Вы выбрали протоколы TCP или UDP, то после завершения описанной выше процедуры в области **Выберите событие для правила** станут активны (т. е. их можно будет включить) переключатели **Где удаленный порт** и **Где локальный порт**, а если выбран протокол IP, то эти переключатели останутся в неактивном состоянии.

Для того чтобы сформировать условия на направление сетевого подключения:

1. Включите переключатель слева от строки **Где подключение**. После этого в области **Описание правила** появится строка Где подключение Не определено.

2. Задайте направление подключения, щелкнув мышью на слове Не определено в строке Где подключение Не определено в области **Описание правила**. После этого на экране появится диалоговое окно выбора типа подключения, показанное на рис. 46.

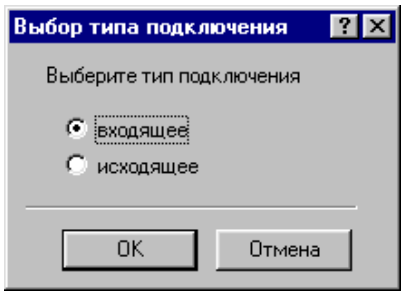

Рисунок 46. Диалоговое окно выбора типа подключения

3. В этом диалоговом окне:
   - включите кнопку выбора **входящее**, если в правиле выбора должна задаваться проверка на входящие подключения;
   - включите кнопку выбора **исходящее**, если в правиле выбора должна задаваться проверка на исходящие подключения.
4. Нажмите на кнопку **ОК**, после чего на экране опять появится диалоговое окно формирования правила, в котором вместо слова Не определено в строке Где подключение Не определено в области **Описание правила** будет указано направление соединения.

Для того чтобы сформировать условия на удаленные порты (только для протоколов TCP и UDP, поэтому формирование условий на порты возможно только после выбора протокола):

1. Включите переключатель слева от строки **Где удаленный порт**. После этого в области **Описание правила** появится строка Где удаленный порт Не определено .
2. Укажите имена (номера) портов, которые должны использоваться в формируемом правиле, щелкнув мышью на слове Не определено в строке Где удаленный порт Не определено в области **Описание правила**. После этого на экране появится диалоговое окно задания номеров локальных портов, показанное на рис. 47.

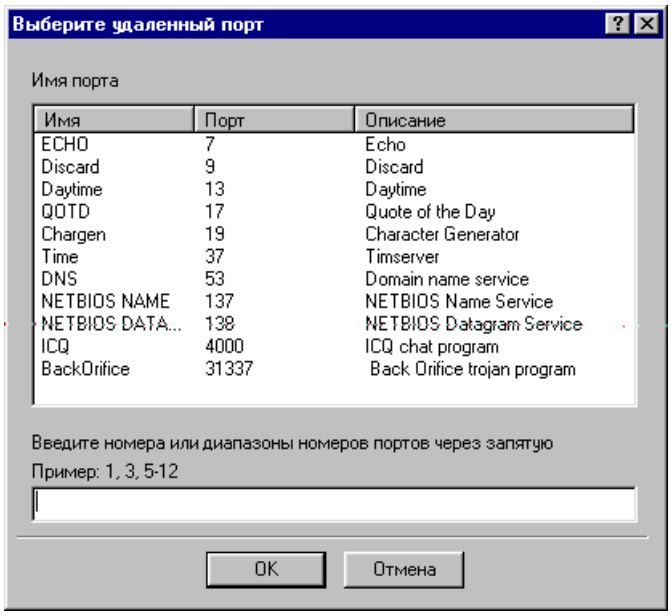

Рисунок 47. Диалоговое окно формирования списка удаленных портов

3. В этом диалоговом окне в поле в нижней части окна введите номера используемых локальных портов, отделяя их друг от друга символом «,». Если номер локального порта может относиться к интервалу значений, то укажите в этом поле наименьшее и наибольшее значения, отделив их друг от друга символом «-». Вместо того чтобы вводить номер порта, Вы можете указать его имя. Для этого в списке, расположенном в области **Имя порта** данного окна, дважды щелкните мышью на строке, соответствующую тому порту, который Вы хотите добавить в поле в нижней области диалогового окна.
4. После ввода списка локальных портов, используемых в формируемом правиле, нажмите на кнопку **ОК**. После этого на экране опять появится диалоговое окно формирования правила, в котором вместо слова Не определено в области **Описание правила** будут указаны имена (номера) используемых в правиле локальных портов.

Условия для локальных портов после установки переключателя, расположенного слева от строки **Где локальный порт**, во включенное состояние задаются аналогично условиям, задаваемым для удаленных портов.

Условие на порты считается выполненным, если сетевое взаимодействие осуществляется через один из портов, указанных в списке.

Условие, заданное в правиле и состоящее из условий для различных объектов (протоколов, направлений обмена, портов), считается выполненным, если выполнены условия для всех этих объектов.

Если в области **Выберите событие для правила** выключить один из переключателей: **Где протокол**, **Где подключение**, **Где локальный порт**, **Где локальный адрес**, **Где удаленный адрес** или **Где удаленный порт**, то в области **Описание правила** соответствующий этому переключателю текст будет удален.

Для того чтобы выбрать действие, которое должна выполнить система Outpost Firewall при выполнении заданных в правиле условий:

1. Включите один из следующих переключателей:
   - **Разрешить эти данные**, чтобы разрешить сетевое взаимодействие при выполнении заданных в правиле условий.
   - **Блокировать эти данные**, чтобы запретить сетевое взаимодействие при выполнении заданных в правиле условий. При этом ответ на запрос возвращаться не будет.
   - **Отклонить эти данные**, чтобы запретить сетевое взаимодействие при выполнении заданных в правиле условий. При этом в ответ на запрос будет

возвращаться «ответное сообщение— **Получатель…**» или **Порт недоступен** (см. Приложение В).

2. Включите переключатель **Дать отчет**, если Вы хотите, чтобы информация о данном соединении отображалась в главном окне системы **Outpost Firemall** в списке **В отчете**.

После включения переключателя **В отчете**, при выполнении соответствующего соединения, пользователю будет выдаваться сообщение о соединении.

Для того чтобы изменить действие, указанное в правиле, необходимо сначала выключить тот из переключателей **Разрешить эти данные**, **Блокировать эти данные** или **Отклонить эти данные**, который в настоящее время включен, после чего включить тот переключатель, который Вы хотите.

Вы можете изменить имя формируемого правила, просто изменив текст, содержащийся в поле **Имя правила**.

Рекомендуется давать формируемым правилам простые и понятные имена. Это облегчит работы с отображением информации в главном окне.

После завершения формирования состава правила нажмите на кнопку **OK**. На экране опять появится диалоговое окно формирования правил, показанное на рис. 41.
В верхней области этого окна появится имя сформированного правила, причем расположенный слева от него переключатель будет включен.

Для того чтобы изменить содержимое правила:

1. В диалоговом окне формирования правил для данного приложения выберите то правило, которое Вы хотите изменить.
2. Нажмите на кнопку **Изменить**, после чего на экране появится диалоговое окно формирования состава правила (см. рис. 43).
3. Измените составные части правила таким же образом, как Вы действовали при формировании нового правила.
4. По окончании изменения составных частей правила нажмите на кнопку **OK**, после чего на экране опять появится диалоговое окно формирования правил для данного приложения.

Для того чтобы удалить правило:

1. В диалоговом окне формирования правил для данного приложения установите курсор на то правило, которое Вы хотите удалить.

2. Нажмите на кнопку **Удалить**.

Для того чтобы создать копию правила для данного приложения:

1. В диалоговом окне формирования правил для данного приложения установите курсор на то правило, для которого Вы хотите создать копию.
2. Нажмите на кнопку **Копировать**, после чего в списке правил для данного приложения появится новая строка с именем, начинающимся со слов **Копировать**, вслед за которой указаны имя исходного правила, символ «**#**» и порядковый номер копии (**1**, **2** и т. д.).

Вы можете изменять расположение правила в списке правил для данного приложения с помощью кнопок **Вверх** и **Вниз**.

6.4. Настройки системных протоколов

Для настроек служебных протоколов предназначена закладка **Системные** диалогового окна **Параметры**. После переключения на эту закладку диалоговое окно **Параметры** будет иметь вид, показанный на рис. 48.

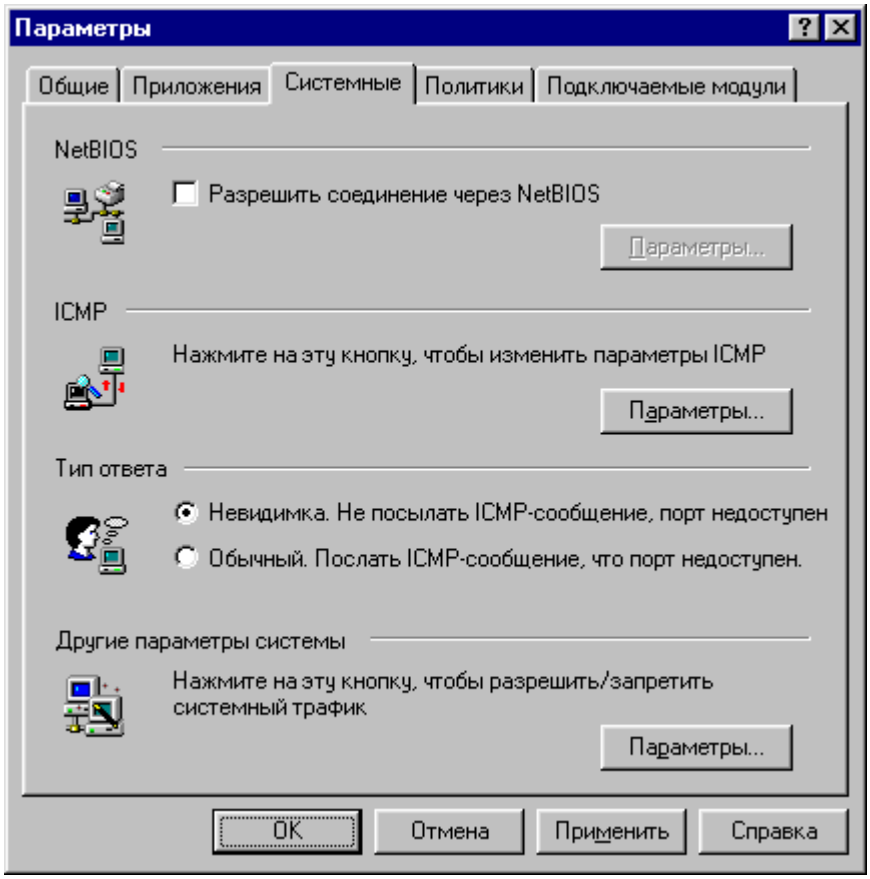

Рисунок 48. Диалоговое окно Параметры с активной закладкой Системные

При работе с этой закладкой Вы можете:

- запретить или разрешить (всем или для некоторого списка адресов) работу по протоколу NetBios;

- определить типы и направление ICMP-сообщений, которые разрешены при работе с данным узлом сети;
- задать режим работы «невидимка»;
- установить остальные системные параметры.

Режим «невидимка» заключается в следующем. Сканирование Вашего компьютера со стороны злоумышленника заключается в посылке запроса на установку соединения. В обычном режиме Ваш компьютер либо посылает подтверждение соединения (если данный порт на Вашем компьютере открыт), либо уведомление, что порт закрыт. В режиме «невидимка» Ваш компьютер не будет высылать уведомления о том, что порт закрыт, что может поставить компьютер-злоумышленник в сложное положение — ему не известно, открыт или нет порт (может быть, пакет утерян, либо узел отсутствует и т. д.).

Для того чтобы разрешить работу для некоторых узлов сети по протоколу NetBios:

1. Включите переключатель **Разрешить соединение через NetBios**.
2. В открывшемся диалоговом окне формирования списка адресов для работы по протоколу NetBios (рис. 49) создайте список адресов, которым разрешена работа по данному протоколу. Формирование этого списка адресов выполняется аналогично формированию списка адресов доверенной зоны (см. п. 6.2).

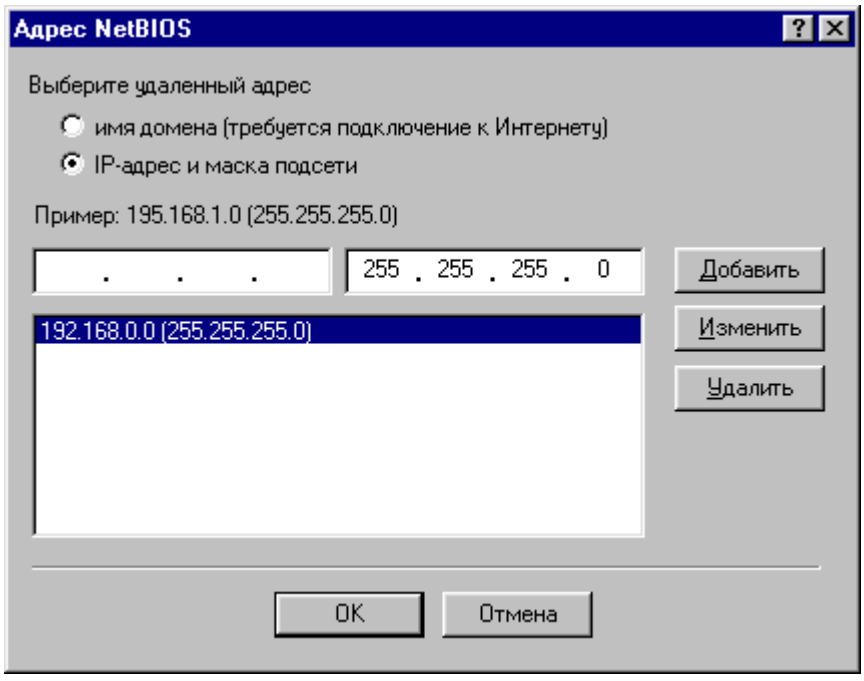

Рисунок 49. Диалоговое окно формирования списка адресов для работы по протоколу NetBios

Если Вы хотите изменить список адресов, для которых разрешена работа по протоколу NetBios, то нажмите на кнопку **Параметры...** в области **NetBios** закладки **Системные** диалогового окна **Параметры**, после чего на экране появится диалоговое окно формирования списка адресов для работы по протоколу NetBios (см. рис. 49).

Для того чтобы определить типы и направление ICMP-сообщений, которые разрешены при работе с данным узлом сети:

1. Нажмите на кнопку **Параметры...** в области **ICMP** закладки **Системные** диалогового окна **Параметры**.
2. В открывшемся диалоговом окне ICMP (рис. 50) содержится список всех возможных типов ICMP-сообщений (см. Приложение В). Справа от описания типа расположены два переключателя, включение одного из которых (**В**) разрешает поступление сообщения данного типа в Ваш компьютер, а другого (**Из**) — передачу сообщения данного типа с Вашего компьютера. Установите переключатели для всех типов ICMP в то состояние, которое считаете необходимым.
3. Нажмите на кнопку **OK**, после чего на экране опять появится диалоговое окно **Параметры**.

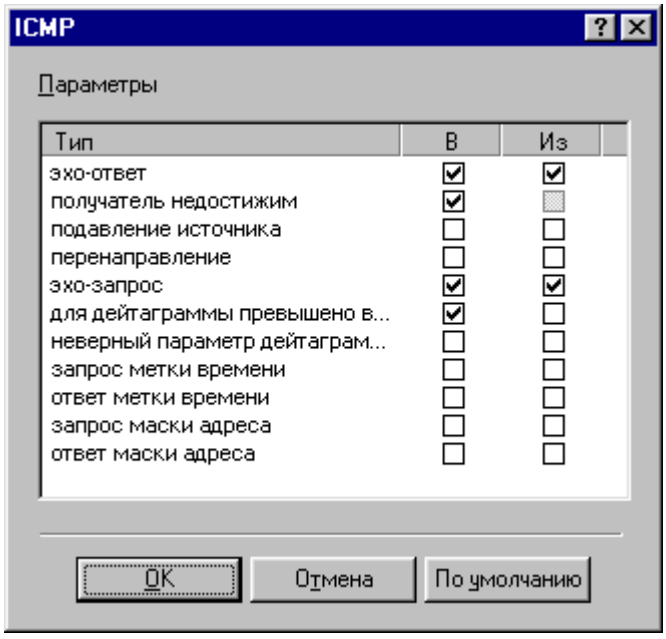

Рисунок 50. Диалоговое окно типов ICMP-сообщений

На рис. 50 значения переключателей соответствуют тем, которые задаются после установки системы **Outpost Firewall**.

При работе с закладкой **Системные** диалогового окна Вы можете указать, нужно или нет посылать уведомление источнику запроса на сетевое взаимодействие о недоступности порта (сетевого узла). Для этого:

- включите кнопку выбора **Невидимка**, если Вы не хотите задать соответствующий режим работы Вашего компьютера (см. выше);
- включите кнопку выбора **Обычный**, если Вы хотите, чтобы Ваш компьютер работал в обычном режиме.

Рекомендуется включить кнопку выбора **Неведимка**, поскольку в этом случае Ваш компьютер будет «невидим» для других компьютеров сети, и возможный злоумышленник, сканирующий Ваши порты, не сможет определить Вашего присутствия в сети.

Для того чтобы установить остальные системные настройки:

1. Нажмите на кнопку **Параметры...** в области **Другие параметры системы** закладки **Системные** диалогового окна **Параметры**, после чего на экране появится диалоговое окно формирования системных настроек, показанное на рис. 51.
2. В этом диалоговом окне включите все переключатели, соответствующие тем возможностям, которые разрешены для работы данного узла сети.
3. Нажмите на кнопку **OK**, после чего на экране опять появится диалоговое окно **Параметры**.

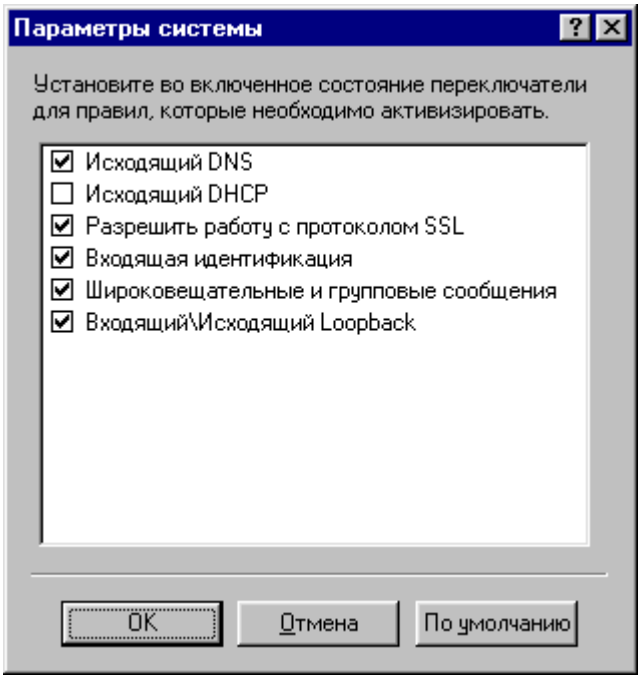

Рисунок 51. Диалоговое окно системных настроек

В этом диалоговом окне отображаются переключатели, позволяющие:

- разрешать преобразование DNS-адресов в IP-адреса с помощью службы DNS, если переключатель **Исходящий DNS** установлен во включенное состояние, или запрещать такое преобразование, если переключатель **Исходящий DNS** установлен в выключенное состояние;

- разрешать динамическое назначение IP-адреса с помощью протокола DHCP, если переключатель **Исходящий DHCP** установлен во включенное состояние, или запрещать такое назначение адресов, если переключатель **Исходящий DHCP** установлен в выключенное состояние;

Если в выключенное состояние установлены оба переключателя **Исходящий DNS** и **Исходящий DHCP**, то в системе могут использоваться только IP-адреса.

- разрешать работу по протоколу *SSL* (через порт HTTPS, имеющий номер 443), если переключатель **Разрешить работу с протоколом SSL** установлен во включенное состояние, или запрещать такие обращение в сеть, если переключатель **Разрешить работу с протоколом SSL** установлен в выключенное состояние;

Через этот порт, в частности, осуществляется передача информации для оплаты покупок в Интернете с помощью кредитных карт. Поэтому, если Вы хотите запретить покупки в Интернете (например, для детей) то Вы можете запретить работу через порт HTTPS, после чего защитить настройки системы **Outpost Firewall** с помощью пароля (см. п. 6.5.5).

- разрешать обращение при обращении от сети к Вашему компьютеру к порту AUTH, имеющему номер 113 при установке переключателя **Входящая идентификация** во включенное состояние, или запрет такого обращения при установке переключателя **Входящая идентификация** в выключенное состояние. К этому порту пытаются подключиться многие почтовые серверы и серверы новостей. Этот порт может быть использован удаленной системой для идентификации Вашего компьютера;
- разрешить использование широковещательных и групповых IP-адресов, если переключатель **Широковещательные и групповые сообщения** установлен во включенное состояние, и запретить использование таких IP-адресов, если этот переключатель установлен в выключенное состояние;
- разрешить использование входящих и исходящих Loopback IP-адресов, если переключатель **Входящий/Исходящий Loopback** установлен во включенное состояние, и запретить использование таких IP-адресов, если этот переключатель установлен в выключенное состояние.

6.5. Подключаемые модули и работа с ними

6.5.1. Модульная архитектура системы Outpost Firewall. Подключение модулей

Система **Outpost Firewall** построена по модульному принципу: часть возможностей системы реализована в виде отдельных библиотек, каждая из которых представляет собой отдельный модуль, способный динамически подключаться к системе. Каждый из этих модулей имеет свои независимые настройки. При установке

системы **Outpost Firewall** будут инсталлированы все поставляемые вместе с системой подключаемые модули. Эти модули интегрированы в систему **Outpost Firewall** так, что информация об их работе отображается в главном окне системы, где они являются элементами списка **Подключаемые модули** (см. п. 3.2.3). В ходе дальнейшей работы пользователь может подключать вновь разработанные модули и удалять модули, уже подключенные к системе.

Для управления составом включенных в систему **Outpost Firewall** подключаемых модулей предназначена закладка **Подключаемые модули** диалогового окна **Параметры**. После перехода на эту закладку диалоговое окно **Параметры** будет иметь вид, показанный на рис. 52.

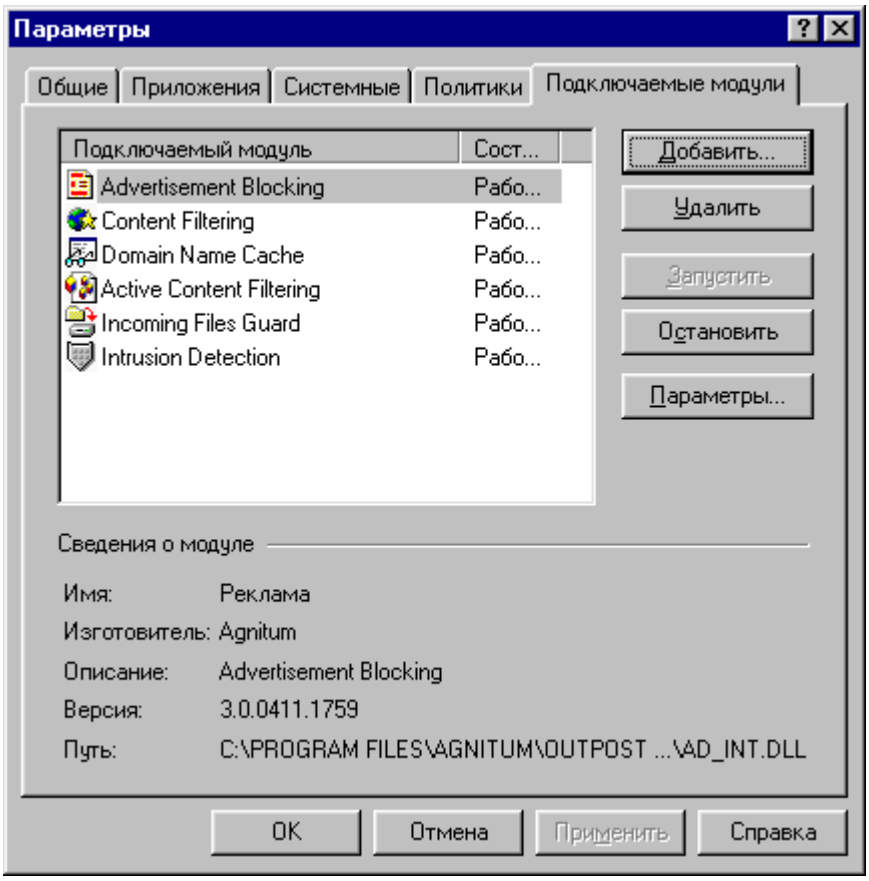

Рисунок 52. Диалоговое окно Параметры с активной закладкой Подключаемые модули

В этой закладке содержится список подключаемых модулей, входящих в систему. В каждой строке этого списка отображаются значок модуля, принятый в системе **Outpost Firewall**, имя файла и статус модуля (работает он в настоящий момент времени или нет).

Для того чтобы добавить в систему Outpost Firewall подключаемый модуль:

1. Нажмите на кнопку **Добавить...** на закладке **Подключаемые модули** диалогового окна **Параметры**.
2. В открывшемся после этого системном окне выбора файла выберите (или введите) имя файла подключаемого модуля.

3. Нажмите на кнопку **Открыть** в этом окне, после чего на экране вновь появится диалоговое окно **Параметры**.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **OK**.
6. После включения модуля в систему **Outpost Firewall** информация о нем попадет в список подключаемых модулей.

Для того чтобы удалить из системы Outpost Firewall подключаемый модуль:

1. Установите курсор на строку списка на закладке **Подключаемые модули** диалогового окна **Параметры**, соответствующую тому подключаемому модулю, который Вы хотите удалить из системы **Outpost Firewall**.
2. Нажмите на кнопку **Удалить**, после чего информация об удаленном модуле будет удалена из списка подключенных к системе модулей.
3. Нажмите на кнопку **OK**.

Для того чтобы временно приостановить работу одного из модулей:

1. Установите курсор на строку списка на закладке **Подключаемые модули** диалогового окна **Параметры**, соответствующую тому подключаемому модулю, работу которого Вы хотите временно приостановить.
2. Нажмите на кнопку **Остановить**, после чего в поле **Состояние** строки списка, соответствующей данному модулю, на закладке **Подключаемые модули** диалогового окна **Параметры** появится слово **Остановлено**.

Для того чтобы вновь запустить временно приостановленный модуль:

1. Установите курсор на строку списка на закладке **Подключаемые модули** диалогового окна **Параметры**, соответствующую тому модулю, который Вы хотите запустить.
2. Нажмите на кнопку **Запустить**, после чего в поле **Состояние** той строки списка, которая соответствует данному модулю, появится слово **Запущено**.

Сразу после установки системы **Outpost Firewall** все включенные в нее модули работают, т. е. имеют статус **Запущено**.

Каждый из включенных в систему модулей имеет свои собственные настройки.

Для того чтобы вызвать настройки одного из модулей, включенных в систему:

1. Установите курсор на строку списка на закладке **Подключаемые модули** диалогового окна **Параметры**, соответствующую тому модулю, настройки которого Вы хотите вызвать.
2. Нажмите на кнопку **Параметры...**, после чего на экране появится диалоговое окно настроек данного модуля.

Вы можете вызвать настройки только того модуля, который имеет статус **Запущено**.

Вы можете получить доступ к настройкам модуля из главного окна системы **Outpost Firewall**, вызвав динамическое меню этого модуля. Для этого щелкните правой клавишей мыши на его название в списке **Подключаемые модули** в главном окне системы **Outpost Firewall**, а в появившемся динамическом меню выберите пункт **Параметры…** .

Вы можете вызвать настройки модуля из панели инструментов главного окна системы **Outpost Firewall**. Для этого нажмите на кнопку , расположенную в панели инструментов справа от кнопки  . В появившемся на экране меню (см. рис. 32) выберите пункт, соответствующий тому модулю, настройки которого Вы хотите вызвать.

Чтобы измененные Вами настройки любого из подключаемых модулей стали использоваться системой **Outpost Firewall**, в диалоговом окне настроек нажмите на кнопку **Применить**, а затем — на кнопку **OK**.

6.5.2. Модуль работы с DNS

Модуль работы с DNS, называющийся **DNS**, реализован в виде библиотеки с именем **DNS_INT.DLL**. Этот модуль предназначен для ускорения работы в сети: он формирует кэш для DNS-адресов, который затем может быть использован при преобразовании DNS-адресов в IP–адреса.

Данный модуль позволяет отображать в главном окне информацию, связанную с работой системы DNS, а также разрешать или запрещать использование кэш-памяти при преобразовании DNS-адресов в IP-адреса. Информация, отображаемая в главном окне при работе с этим модулем, связана с элементом **DNS** списка **Подключаемые модули** и описана в п. 3.2.3.

Вид диалогового окна параметров этого модуля, которое Вы можете вызвать одним из способов, описанных в п. 6.5, показан на рис. 53.

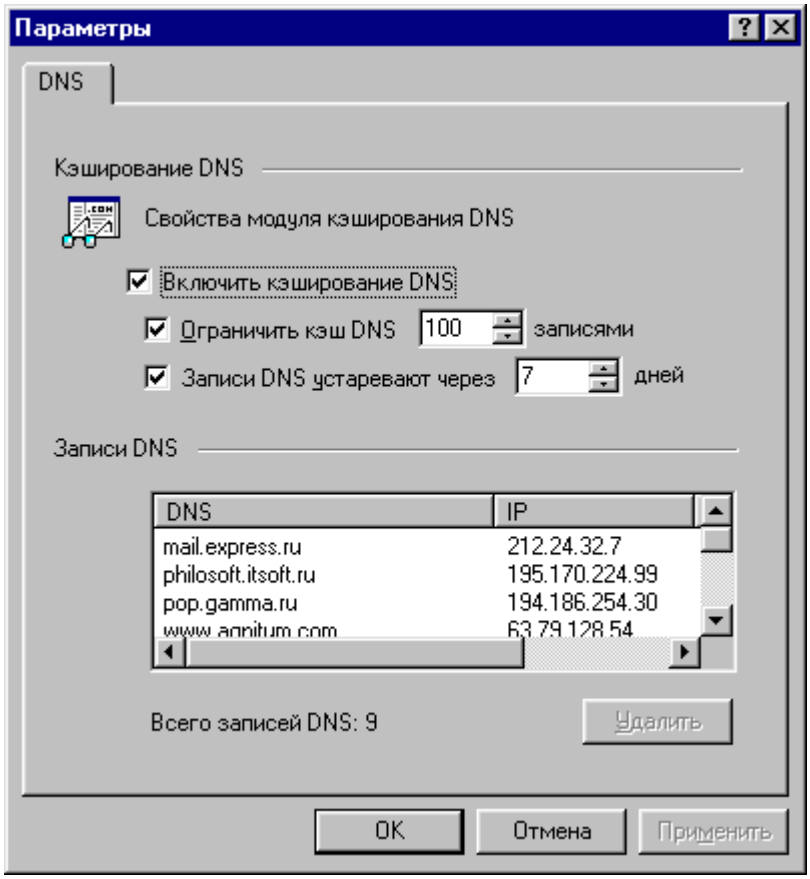

Рисунок 53. Диалоговое окно параметров DNS

В этом диалоговом окне Вы можете запретить использование кэша DNS, выключив переключатель **Включить кэш DNS**. В таком случае информация о последних преобразованиях DNS-адресов в IP-адреса на Вашем компьютере храниться не будет, и, в случае преобразования DNS-адреса, запрос будет передан DNS-серверу. Включив этот переключатель, Вы разрешаете использование кэша DNS.

Если переключатель **Включить кэш DNS** включен, то Вы можете задать ограничения на размер кэша DNS, включив переключатель **Ограничить кэш DNS**. В этом случае максимальное количество записей в кэше DNS задается в поле справа от этого переключателя (сразу после установки системы оно равно 100). Если переключатель **Ограничить кэш DNS** выключен, то ограничений на размер кэша DNS система **Outpost Firewall** не устанавливает.

Если переключатель **Включить кэш DNS** включен, то Вы можете задать время хранения записей в кэше DNS, включив переключатель **Записи DNS устаревают через**. В этом случае время хранения записей в кэше DNS, измеряемое в днях, задается в поле, расположенном справа от этого переключателя (сразу после установки системы оно равно 7). Если переключатель **Записи DNS устаревают через** выключен, то ограничений на время хранения записей в кэше DNS система **Outpost Firewall** не устанавливает.

В области **Записи DNS** диалогового окна настроек DNS кэш DNS отображается в виде списка, содержащего:

- DNS-адрес;
- соответствующий ему IP-адрес;

- дату и время занесения этой информации в кэш DNS.

С помощью этого списка Вы можете удалять информацию из кэша DNS.

Для того чтобы удалить запись из кэша DNS Вашего узла сети:

1. Установите курсор на запись в списке **Записи DNS**, которую Вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

6.5.3. Модули фильтрации содержимого Web-страниц

Для фильтрации содержимого Web-страниц в системе **Outpost Firewall** предназначены три модуля:

- модуль ограничения отображения Web-страниц по содержащимся в них HTML-строкам или размеру графического изображения (имя модуля — **Реклама**, имя файла, содержащего этот модуль — **AD_INT.DLL**);
- модуль запрета отображения Web-страниц (Web-сайтов) по их DNS-адресу либо содержащимся в них текстовым строкам (имя модуля — **Содержимое**, имя файла, содержащего этот модуль — **CNT_INT.DLL**);
- модуль запрета использования активных элементов Web-страниц, а также cookie, всплывающих окон и т. д. (имя модуля — **Активное содержимое**, имя файла, содержащего этот модуль — **WEB_INT.DLL**).

6.5.3.1. Модуль ограничения отображения Web-страниц по содержащимся в них HTML-строкам или размеру графического изображения

Информация об ограничении отображения Web-страниц по содержащимся в них HTML-строках или размеру графического изображения, отображаемая в главном окне системы **Outpost Firewall** при работе с модулем **Реклама**, описана в п. 3.2.3.

Список HTML-строк, при наличии которых определяемые этими строками изображения со ссылками не будут выводиться на экран Web-страницы, также как и список размеров графических изображений, которые не отображаются на экране, задается в окне настроек этого модуля.

На месте этих неотображаемых изображений в Web-странице будут содержаться строки **AD** или **AD-SIZE**.

Вид диалогового окна параметров этого модуля, которое Вы можете вызвать одним из способов, описанных в п. 6.5, показан на рис. 54.

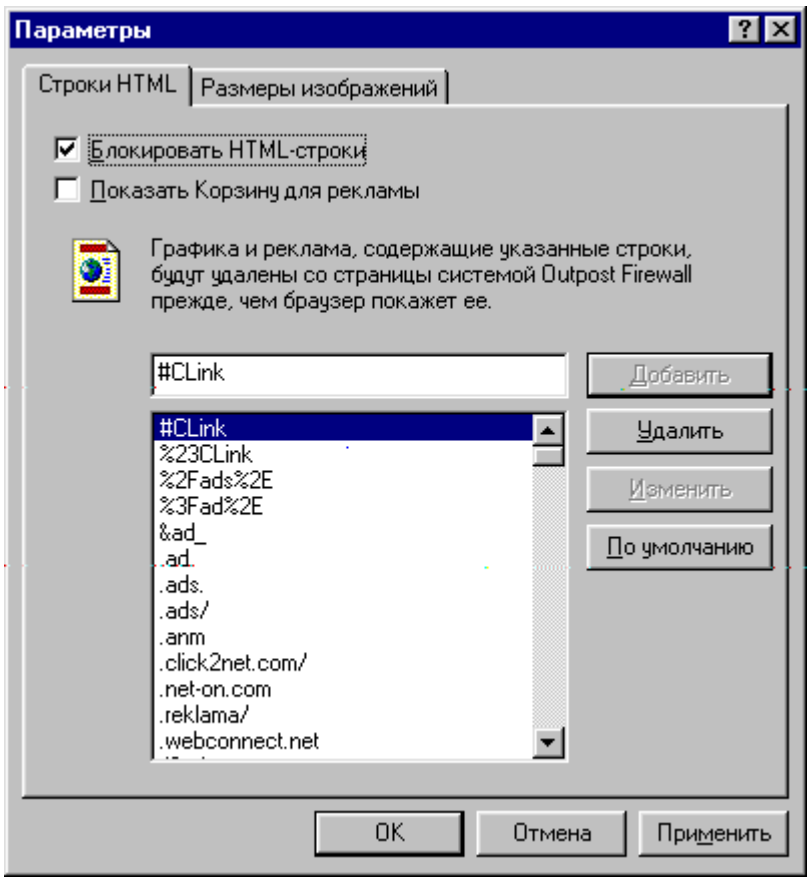

Рисунок 54. Диалоговое окно параметров модуля Реклама с активной закладкой Строки HTML

Диалоговое окно настроек этого модуля содержит две закладки:

- закладка **Строки HTML**, где указывается список HTML-строк;
- закладка **Размеры изображений**, где указывается список размеров неотображаемых графических изображений.

После вызова этого диалогового окна на экран активной будет закладка **Строки HTML**.

При работе с этой закладкой Вы можете включить переключатель **Блокировать HTML-строки**. В этом случае элементы Web-страниц, определяемые HTML-строками из расположенного ниже списка, отображаться не будут. Эта возможность не используется, если переключатель **Блокировать HTML-строки** выключен.

Сразу после установки системы **Outpost Firewall** переключатель **Блокировать HTML-строки** включен, а список HTML-строк, поставляемый с системой, содержит большое количество элементов. Поэтому сразу после начала использования система **Outpost Firewall** оградит Вас от ненужной рекламы без дополнительных настроек.

Для внесения HTML-строк в список, задающий ограничение отображения Web-страниц в системе **Outpost Firewall**, существует два основных способа. Первый из них предусматривает непосредственный ввод HTML-строки в этот список.

Для того чтобы внести HTML-строку (или HTML-строки) в список, задающий ограничение отображения Web-страниц:

1. Установите курсор в поле ввода, расположенное в окне настроек над списком HTML-строк, и введите в это поле текст HTML-строки.
2. Нажмите на кнопку **Добавить**.
3. Повторите шаги 1 и 2 для каждой из строк, которую Вы хотите добавить в список.
4. Второй способ добавления HTML-строк в список, задающий ограничение отображения Web-страниц в системе **Outpost Firewall**, связан с использованием объекта, называемого **Корзина для рекламы**. **Корзина для рекламы** представляет собой диалоговое окно, вид которого приведен на рис. 55.

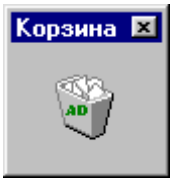

Рисунок 55. Диалоговое окно Корзина для рекламы

Перед тем как использовать **Корзину для рекламы**, необходимо сначала разместить это диалоговое окно на экране.

Для размещения Корзины для рекламы на экране:

1. Вызовите динамическое меню модуля **Реклама**, щелкнув правой клавишей мыши на его названии в списке **Подключаемые модули** в главном окне системы **Outpost Firewall**.
2. В этом динамическом меню выберите пункт **Показать корзину для рекламы**, после чего данное окно будет располагаться на экране поверх остальных диалоговых окон.

Вы можете задать режим размещения **Корзины для рекламы** на рабочем столе системы Windows, включив в диалоговом окне переключатель **Показать корзину для рекламы**.

Для того чтобы добавить HTML-строку (или HTML-строки) в список, задающий ограничение отображения Web-страниц, с помощью Корзины для рекламы:

1. Выделите на изображении Web-страницы, которая сейчас расположена на экране, тот из ее элементов, вывод которого Вы хотите запретить.
2. Отбуксируйте выделенный элемент в диалоговое окно **Корзина для рекламы**. После перемещения выделенного элемента в **Корзину для рекламы** на экране появится диалоговое окно с предупреждением о добавлении выделенной HTML-строки в список, задающий ограничение отображения Web-страниц. Это окно показано на рис. 56.

3. В данном диалоговом окне включите кнопку выбора **Добавить всю строку в список блокируемых строк**, если Вы хотите занести в этот список всю строку целиком.
4. В этом диалоговом окне включите кнопку выбора **Добавить часть строки в список блокируемых строк**, если Вы хотите перед добавлением в список отредактировать содержимое HTML-строки. После включения этой кнопки текст строки будет помещен в поле диалогового окна, расположенное ниже данной кнопки выбора, где Вы сможете изменить ее текст.
5. Нажмите на кнопку **OK**.

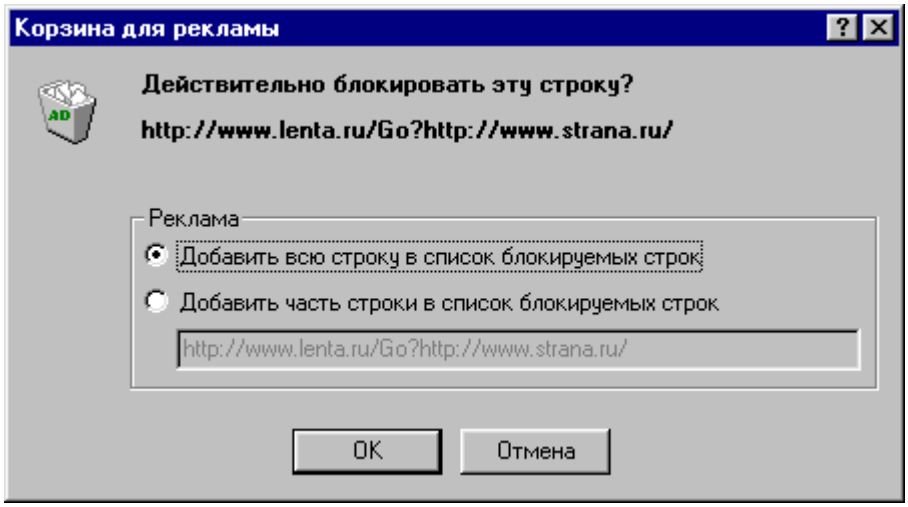

Рисунок 56. Диалоговое окно предупреждения о добавлении выделенной HTML-строки в список, задающий ограничение отображения Web-страниц

Если Вы не хотите добавлять показанную в диалоговом окне HTML-строку в список, то нажмите на кнопку **Отмена**.

Для добавления HTML-строки в список, задающий ограничение отображения Web-страниц, рекомендуется пользоваться **Корзиной для рекламы**.

Для того чтобы удалить элемент из списка HTML-строк:

1. Установите курсор на тот элемент списка, который Вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

Для того чтобы изменить текст одной из строк в списке HTML-строк:

1. Установите курсор на тот элемент списка, который Вы хотите изменить. При этом текст данной строки будет размещен в поле ввода, которое расположено над списком HTML-строк в диалоговом окне настроек модуля.
2. Измените текст HTML-строки в этом поле ввода. После внесения любых изменений в поле ввода в диалоговом окне станет активной кнопка **Изменить**.
3. Нажмите на кнопку **Изменить**.

Вы можете добавить новую строку в список HTML-строк, используя текст уже имеющейся в этом списке строки. Для этого выполните описанную выше процедуру, только на шаге 3 вместо кнопки **Изменить** нажмите на кнопку **Добавить**.

Вы можете вернуть список HTML-строк к состоянию, в котором он находился сразу после установки системы **Outpost Firewall**. Для этого нажмите на кнопку **По умолчанию**.

Для того чтобы изменить содержимое списка размеров графических изображений, которые не должны отображаться на экран при выводе Web-страницы, в диалоговом окне настроек модуля **Реклама** переключитесь на закладку **Размеры изображений**. После этого диалоговое окно примет вид, показанный на рис. 57.

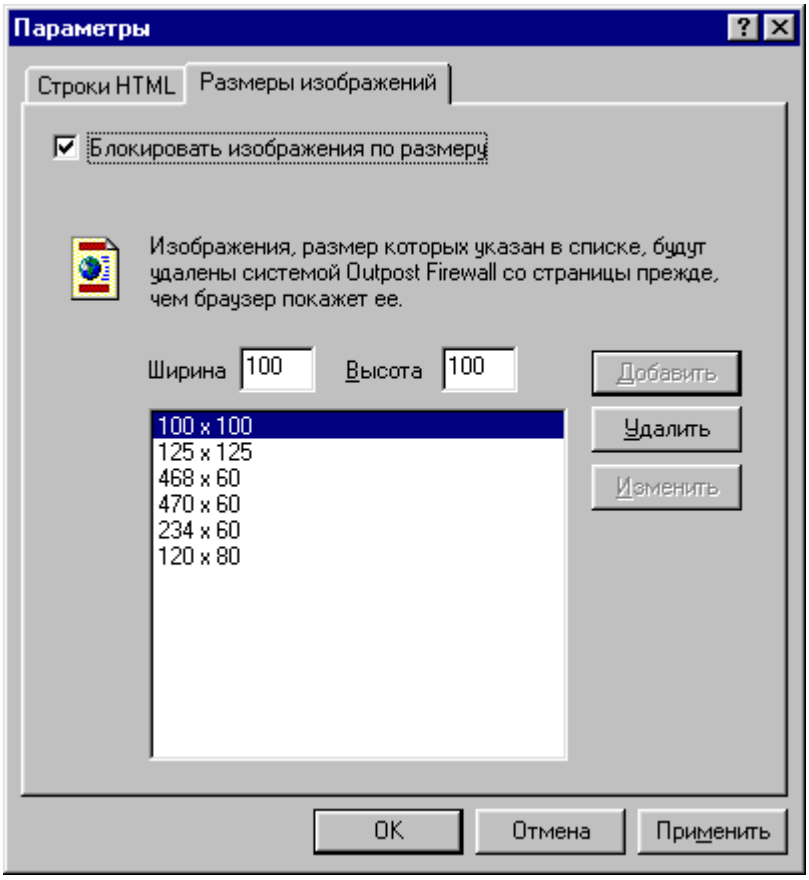

Рисунок 57. Диалоговое окно параметров модуля Реклама с активной закладкой Размеры изображений

Для того чтобы добавить элемент в список размеров графических изображений, которые не выводятся при отображении Web-страницы:

1. Введите значение ширины изображения в поле **Ширина** и высоты изображения в поле **Высота** (эти величины задаются в пикселях).
2. Нажмите на кнопку **Добавить**.

Для того чтобы удалить элемент из списка размеров графических изображений, которые не выводятся при отображении Web-страницы:

1. Установите курсор на тот элемент списка графических изображений, который Вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

Для того чтобы изменить элемент в списке размеров графических изображений, которые не выводятся при отображении Web-страницы:

1. Установите курсор на тот элемент списка графических изображений, который Вы хотите изменить. При этом размеры этого изображения по ширине и высоте будут помещены в поля **Ширина** и **Высота** соответственно.
2. Измените значения этих полей. После внесения любых изменений в этих полях в диалоговом окне станет активной кнопка **Изменить**.
3. Нажмите на кнопку **Изменить**.

6.5.3.2. Модуль запрета отображения Web-страниц по их DNS-адресу либо по заданным строкам

Этот модуль предназначен для того, чтобы оградить Вас от поступления на компьютер ненужной информации по той или иной тематике. Стандартный пример — Вы хотите запретить поступление порнографической информации. Для этого введите в список запрещенных все соответствующие слова и словосочетания: **порно**, **интим-услуги** и т. д. Кроме того, Вы имеете возможность заблокировать выходы на известные Вам Web-страницы аналогичного содержания.

Информация о запрете отображения Web-страниц, имеющих определенный DNS-адрес или содержащих заданные строки, отображается в главном окне системы **Outpost Firewall** при работе с модулем **Содержимое**. Ее описание приводится в п. 3.2.3.

Список DNS-адресов страниц, которые не должны отображаться браузером, а также список строк, наличие которых в Web-странице (Web-сайте) запрещает отображение этой страницы (этих страниц), задается в окне параметров этого модуля.

Вид диалогового окна параметров модуля, который можно вызвать одним из способов, описанных в п. 6.5, показан на рис. 58.

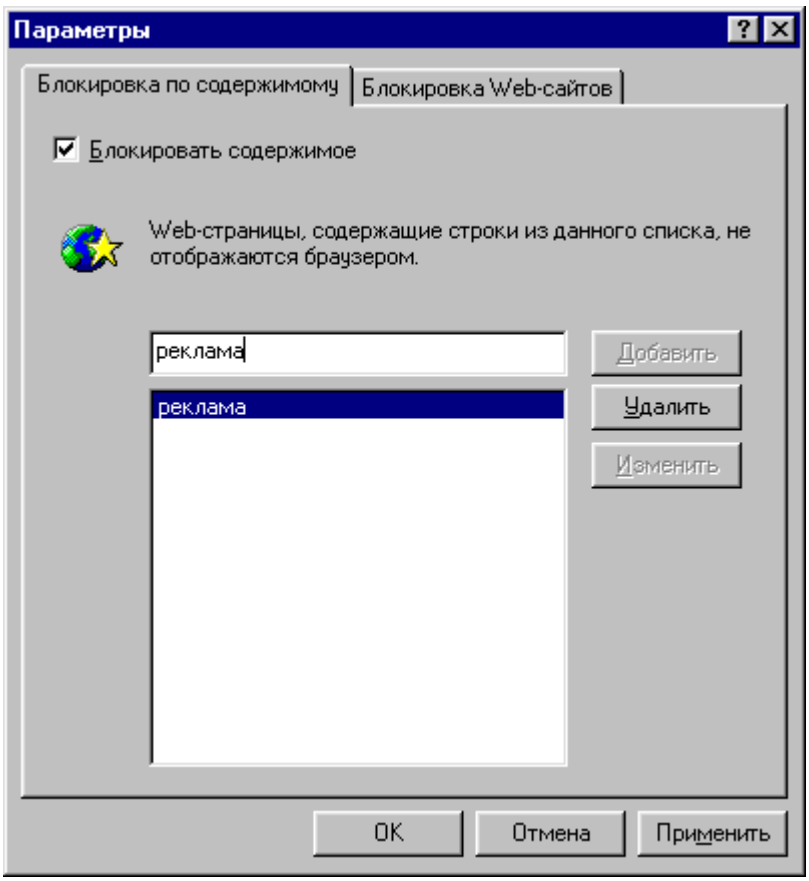

Рисунок 58. Диалоговое окно параметров модуля Содержимое с активной закладкой Блокировка по содержимому

Диалоговое окно настроек этого модуля содержит две закладки:

- закладка **Блокировка по содержимому**, которая позволяет задавать список строк, наличие которых в Web-странице запрещает отображение этой страницы;
- закладка **Блокировка Web-сайтов**, с помощью которой указывается список сайтов (страниц), к которым доступ должен быть заблокирован.

После вызова этого диалогового окна активной будет закладка **Блокировка по содержимому**.

При работе с этой закладкой пользователь может включить переключатель **Блокировать содержимое**. В этом случае на экран не будут выводиться Web-страницы, содержащие определенные текстовые строки. Если переключатель **Блокировать содержимое** выключен, то эта возможность не используется.

Для того чтобы добавить элемент в список текстовых строк, наличие которых в Web-странице запрещает ее отображение:

1. Установите курсор в поле ввода в диалоговом окне, расположенном над списком строк, наличие которых в Web-странице запрещает ее отображение.
2. Введите в это поле необходимую текстовую строку.
3. Нажмите на кнопку **Добавить**.

Для того чтобы удалить элемент из списка текстовых строк, наличие которых в Web-странице запрещает ее отображение:

1. Установите курсор на тот элемент списка текстовых строк, который Вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

Для того чтобы изменить элемент в списке текстовых строк, наличие которых в Web-странице запрещает ее отображение:

1. Установить курсор на тот элемент списка текстовых строк, который Вы хотите изменить. После этого выделенная текстовая строка появится в поле ввода, которое располагается над списком строк.
2. Измените содержимое этого поля. После внесения любых изменений в поле ввода в диалоговом окне станет активной кнопка **Изменить**.
3. Нажмите на кнопку **Изменить**.

Вы можете добавить новую строку в список, используя текст уже имеющейся в этом списке строки. Для этого выполните описанную выше процедуру, только на шаге 3 вместо кнопки **Изменить** нажмите на кнопку **Добавить**.

4. Для того чтобы изменить содержимое списка DNS-адресов, к которым Вы хотите заблокировать доступ, в диалоговом окне параметров модуля **Содержимое** переключитесь на закладку **Блокировка Web-сайтов**. После этого диалоговое окно параметров данного модуля примет вид, показанный на рис. 59.

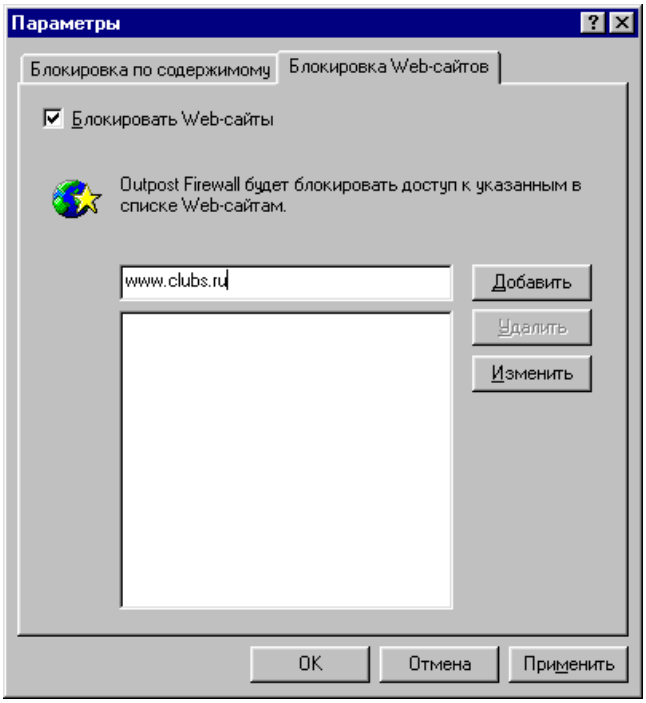

Рисунок 59. Диалоговое окно параметров модуля Содержимое с активной закладкой Блокировка Web-сайтов

5. Работа с этой закладкой полностью аналогична работе с закладкой **Блокировка по содержимому**.

   - Вы можете включить переключатель **Блокировать Web-сайты**, чтобы блокировать доступ к Web-страницам (Web-сайтам), имеющим определенные DNS-адреса, или выключить переключатель **Блокировать Web-сайты**, если не хотите использовать эту возможность;
   - Вы можете добавлять, удалять или модифицировать элементы в списке DNS-адресов точно так же, как и элементы списка текстовых строк, находящегося на закладке **Блокировка по содержимому**.

6.5.3.3. Модуль контроля использования активных элементов Web-страниц

Модуль **Активное содержимое** управляет работой следующих элементов:

- ActiveX;
- Java-апплеты;
- программы на языках Java Script и VB Script;
- cookie;
- всплывающие окна;
- ссылки (referers), т. е. возможность получения URL, с которого перешли на данную Web-страницу.

Информация об ограничении использования этих элементов, отображаемая при работе с этим модулем в главном окне системы **Outpost Firewall**, описана в п. 3.2.3.

Разрешение или запрет работы этих элементов Вы можете задавать независимо для различных Web-страниц через окно параметров модуля **Активное содержимое**.

Вид диалогового окна настроек этого модуля, которое можно вызвать одним из способов, описанных в п. 6.5, показан на рис. 60.

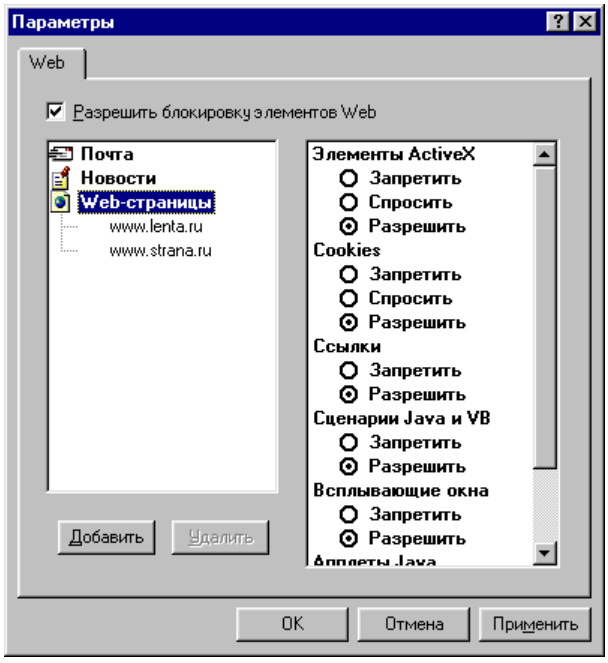

Рисунок 60. Диалоговое окно параметров модуля Активное содержимое

С помощью этого диалогового окна Вы можете управлять работой активных элементов Web-страниц, включив переключатель **Разрешить блокировку элементов Web**, либо отказаться от этой возможности, выключив данный переключатель.

Диалоговое окно настроек модуля **Активное содержимое** состоит из двух частей:

- в левой части находится список объектов, для которых может быть задано управление работой активных элементов;

В настоящее время управление работой активных элементов может быть задано для почтовых программ, службы новостей и Web-страниц.

- в правой части для выделенного элемента списка в левой части диалогового окна указывается, разрешено или нет использовать те или иные активные элементы из списка, приведенного выше.

Для Web-страниц могут быть заданы общие правила работы активных элементов Web-страниц, а для некоторых Web-страниц (определяемых своими адресами) — особые правила. Элемент **Web-страницы** в списке типов объектов в левой части диалогового окна представляет собой иерархический список, корневой элемент которого (**Web-страницы**) определяет общие правила работы активных элементов, а для остальных элементов этого списка могут быть определены особые правила работы.

Сразу после установки системы для всех Web-страниц разрешено использование всех активных элементов, кроме всплывающих окон и ссылок.

Для того чтобы добавить адрес в список Web-страниц в левой части диалогового окна:

1. Установите курсор на любой из элементов списка в левой части диалогового окна.
2. Нажмите на кнопку **Добавить**, после чего на экране появится диалоговое окно для ввода адреса, показанное на рис. 61.
3. В поле этого окна введите адрес Web-страницы, для которой Вы хотите определить возможность использования активных элементов, либо выберите нужный адрес из раскрывающегося списка.
4. Нажмите на кнопку **OK** в этом окне.

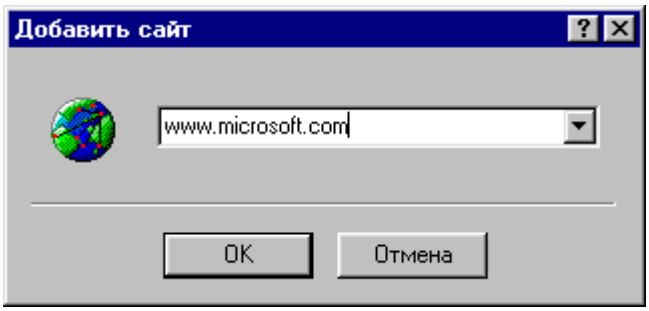

Рисунок 61. Диалоговое окно для ввода DNS-адреса

После того как Вы внесли адрес Web-страницы в список, для данной страницы по умолчанию разрешено использование всех активных элементов.

Для того чтобы удалить элемент из списка DNS-адресов в левой части диалогового окна:

1. В списке адресов в левой части диалогового окна установите курсор на тот адрес, который Вы хотите исключить.
2. Нажмите на кнопку **Удалить**.

Для того чтобы определить режим использования активных элементов Web-страниц для какой-нибудь страницы:

1. В списке адресов в левой части диалогового окна установите курсор на адрес той Web-страницы, для которой Вы хотите определить режим использования активных элементов.
2. Включите кнопки выбора (если хотите изменить их текущее значение):
   - **Запретить** — для всех активных элементов Web-страницы, использование которых Вы хотите запретить;
   - **Разрешить** — для всех активных элементов Web-страницы, использование которых Вы хотите разрешить;
   - **Спросить** — для всех активных элементов Web-страницы, перед использованием которых Вы хотели бы получить уведомление (эта возможность предусмотрена только для ActiveX, Cookie и Java-апплетов).

6.5.4. Модуль защиты файлов

Данный модуль предназначен для организации проверки поступающих на Ваш компьютер по электронной почте присоединенных файлов. Вы можете задать проверку поступающих файлов на наличие вирусов (с помощью какой-либо антивирусной программы, установленной на Вашем компьютере), а также получить соответствующие сообщения. Режимы проверки в данном модуле задаются по типам поступающих на Ваш компьютер файлов.

Вид диалогового окна настроек этого модуля, которое можно вызвать одним из способов, описанных в п. 6.5, показан на рис. 62.

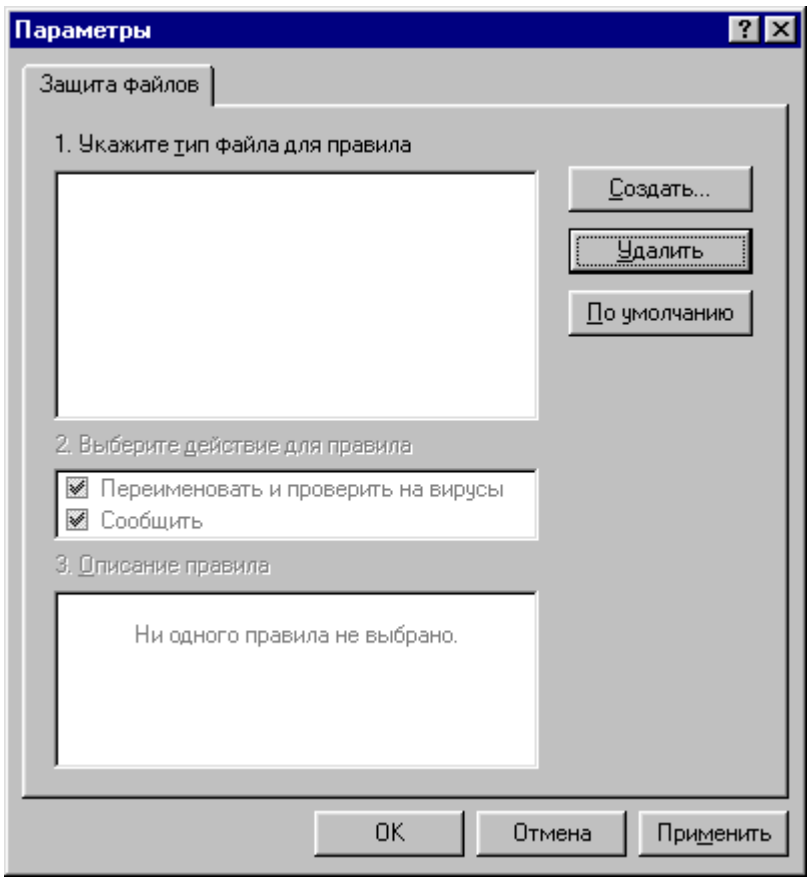

Рисунок 62. Диалоговое окно параметров модуля Защита файлов

Для того чтобы добавить правила проверки поступающих файлов какого-либо типа:

1. Нажмите на кнопку **Создать** в диалоговом окне.
2. В появившемся диалоговом окне **Тип файла** (рис. 63) в поле **Тип файла** введите расширение имен файлов, для которых должны выполняться те проверки, которые Вы задаете. После этого в поле **Описание** появится характеристика выбранного Вами типа файла.

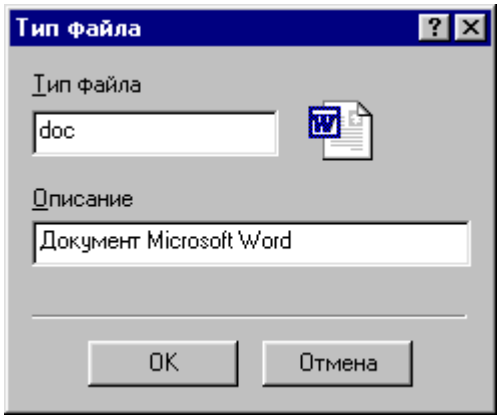

Рисунок 63. Диалоговое окно Тип файла

3. Нажмите на кнопку **OK**, после чего Вы опять вернетесь в диалоговое окно **Параметры**, которое примет вид, показанный на рис. 64.

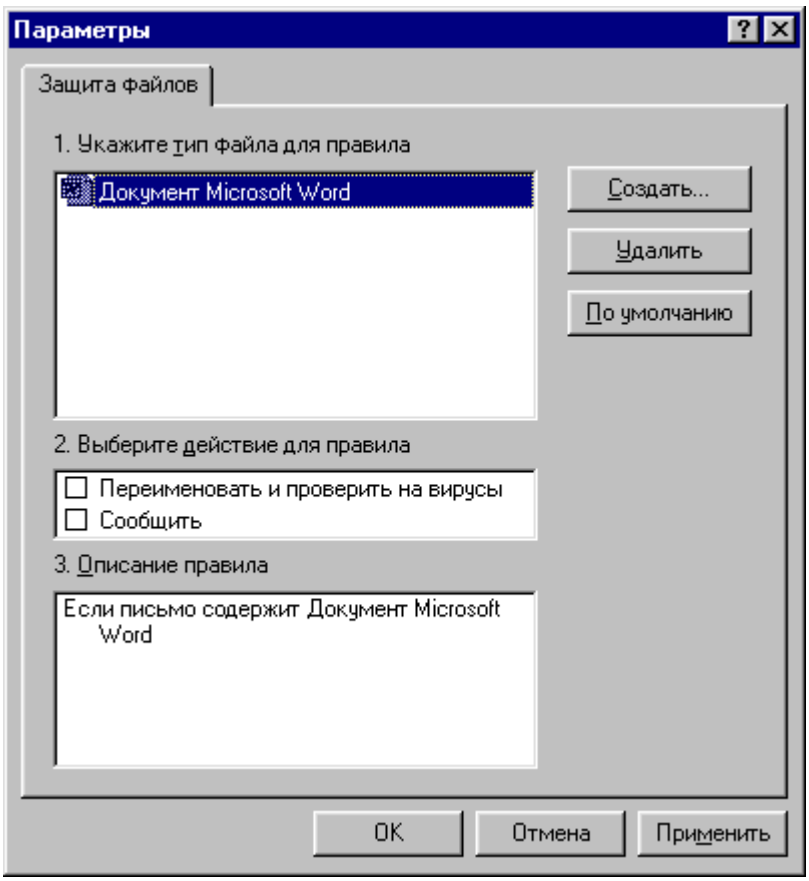

Рисунок 64. Диалоговое окно параметров модуля Защита файлов после выбора типа файла

4. Установите во включенное состояние в области **Выберите действие для правила** те переключатели, которые необходимо.
5. Если Вы установили во включенное состояние переключатель **Переименовать и проверить на вирусы**, то в области **Описание** правила щелкните мышью по появившемуся тексту Антивирусная программа.
6. В появившемся диалоговом окне **Выбор антивирусной программы** задайте имя той антивирусной программы, которая будет проверять данный тип файлов (для вызова системного диалогового окна выбора имени файла нажмите на кнопку **Обзор**).
7. При необходимости, в поле **Параметры командной строки** введите параметры вызова антивирусной программы.
8. Нажмите на кнопку **OK**.
9. Нажмите на кнопку **OK** в диалоговом окне параметров модуля защиты файлов.

Если Вы для данного типа файла установили переключатель **Сообщить** во включенное состояние, то при получении письма с файлом данного типа на экране появится диалоговое окно с предупреждающим сообщением (рис. 65), которое будет отображаться в течение определенного времени, после чего исчезнет с экрана.

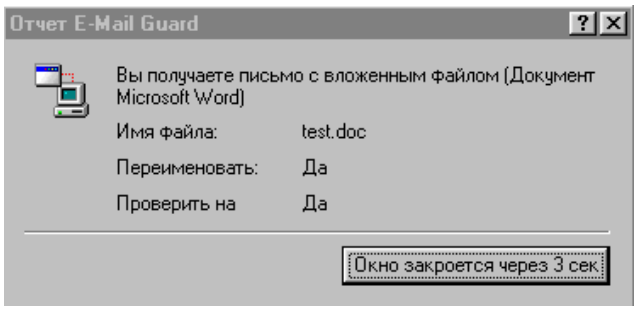

Рисунок 65. Диалоговое окно Отчет E-Mail Guard

Если Вы для данного типа файла установили переключатель **Переименовать и проверить на вирусы** во включенное состояние, то эти операции будут выполняться при открытии данного письма.

Если Вы задали правила проверки для нескольких типов файлов, то в диалоговом окне **Параметры** отображается правило для выбранного в области **Укажите тип файла для правила** типа файла.

6.5.5. Детектор атак

Данный модуль предназначен для уведомления пользователя о предполагаемой атаке на его компьютер из сети и принятии действий по недопущению нанесения ущерба Вашему компьютеру. Модуль **Детектор атак** позволяет задать условия, при которых выдается предупреждение и имеет настройки для задания реакции в случае если заданный уровень безопасности превышен.

Вид диалогового окна настроек этого модуля, которое можно вызвать одним из способов, описанных в п. 6.5, показан на рис. 66.

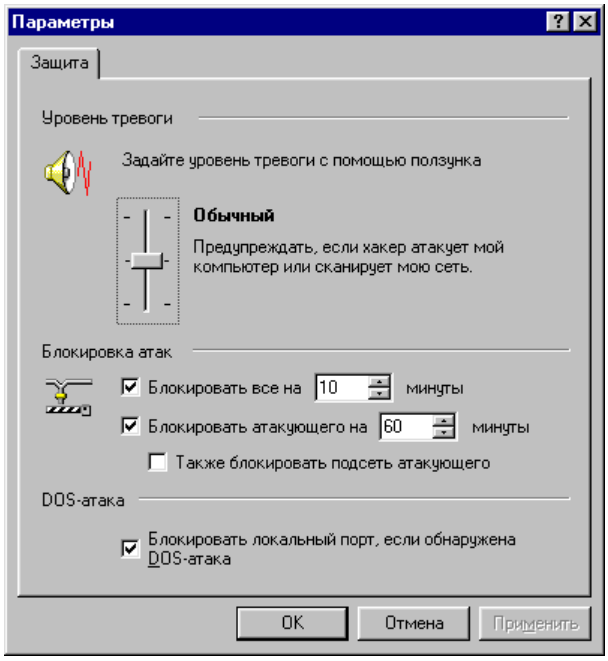

Рисунок 66. Диалоговое окно параметров модуля Защита файлов

В верхней части окна Вы можете задать уровень безопасности с помощью ползунка (чем он выше, тем меньше условий требуется для выдачи предупреждения). Ползунок может находиться в трех положениях:

- верхний (**Параноидальный** уровень тревоги) — предупреждение выдается в случае, если обнаружено даже единичное сканирование порта;
- средний (**Обычный** уровень тревоги) — предупреждение выдается в случае, если осуществляется сканирование нескольких портов или портов с определенными в системе номерами (т. е. в тех ситуациях, которые система распознает как атаку на компьютер);
- нижний (**Безразличный** уровень тревоги) — предупреждение выдается в случае однозначной множественной атаки.

Для того чтобы изменить положение ползунка, подведите к нему курсор мыши, нажмите на левую клавишу и, не отпуская ее, переведите ползунок в то положение, которое необходимо.

В нижней области окна Вы можете задать действия, которые система выполнит при обнаружении атаки на Ваш компьютер:

- блокировку всех сетевых обменов с Вашего компьютера при установке во включенное состояние переключателя **Блокировать все на**. В этом случае в поле справа от этого переключателя Вы можете задать время, на которое будут заблокированы сетевые обмены (по умолчанию — на 10 минут);
- блокировку всех сетевых обменов с того компьютера, с которого осуществляется атака на Ваш компьютер, при установке во включенное состояние переключателя **Блокировать атакующего на**. В этом случае в поле справа от этого переключателя Вы можете задать время, на которое будут заблокированы сетевые обмены атакующего (по умолчанию — на 60 минут);
- блокировку всех сетевых обменов всей подсети, к которой принадлежит компьютер, с которого осуществляется атака на Ваш компьютер, при установке во включенное состояние переключателя **Блокировать атакующего на**;
- блокировку локального порта, если обнаружена DOS-атака (т.е. атака типа «отказ в обслуживании»), при установке во включенное состояние переключателя **Блокировать локальный порт, если обнаружена DOS-атака**.

6.6. Конфигурации системы, их создание, сохранение, загрузка

Система **Outpost Firewall** содержит большое количество настроек, списков, поставляемых вместе с системой, и т. д. Все эти настройки находятся в специальном файле, называемом файлом конфигурации, который определяет окружение, в котором работает система **Outpost Firewall**.

Сформированная Вами конфигурация может быть сохранена в любой момент работы системы и скопирована в другой файл. Настройки системы, как было описано в п. 6.1, могут быть защищены паролем. Имея возможность сохранять несколько вариантов настроек системы, Вы можете, например, настроить Ваш домашний компьютер по-

разному для разных членов семьи и тем самым предотвратить доступ Ваших детей к порнографическим сайтам, неконтролируемым покупкам через Интернет и т. д.

Сразу после установки система использует файл конфигурации **configuration.cfg**, расположенный в каталоге системы **Outpost Firewall**. Вы можете создать несколько файлов конфигурации, и таким образом, работать в разном окружении.

При завершении работы система **Outpost Firewall** запоминает, какой файл конфигурации применялся. При последующем запуске она будет использовать тот же файл конфигурации.

Для работы с файлами конфигурации необходимо войти в главное окно системы **Outpost Firewall**.

Для того чтобы создать новую конфигурацию системы:

1. В меню главного окна выберите пункт **Файл**.
2. В следующем меню выберите пункт **Новая конфигурация**.

После выполнения этой процедуры система **Outpost Firewall** перейдет к новому файлу конфигурации, и, если текущее окружение не было сохранено в файле, оно будет уничтожено.

Новая конфигурация автоматически будет создана в файле с именем **configuration.cfg**, поэтому для работы рекомендуется использовать файлы конфигурации с другими именами.

Для того чтобы сохранить текущую конфигурацию системы в файле:

1. В меню главного окна выберите пункт **Файл**.
2. В следующем меню выберите пункт **Сохранить как…**.
3. В открывшемся системном диалоговом окне выбора имени файла укажите каталог, куда должен быть записан файл конфигурации, и задайте его имя.
4. В этом диалоговом окне нажмите на кнопку **Сохранить**, после чего в заголовке главного окна системы **Outpost Firewall** появится имя файла конфигурации, которое Вы задали.

Для того чтобы открыть файл конфигурации:

1. В меню главного окна выберите пункт **Файл**.
2. В следующем меню выберите пункт **Загрузить конфигурацию**.
3. В открывшемся системном диалоговом окне выбора имени файла укажите каталог, откуда должен быть считан файл конфигурации, и имя этого файла.

4. Нажмите в этом диалоговом окне на кнопку **Открыть**, и, после того как файл будет прочитан, в заголовке главного окна системы **Outpost Firewall** появится его имя.

После выполнения этой процедуры система **Outpost Firewall** перейдет к новому файлу конфигурации, и, если текущее окружение не было сохранено в файле, оно будет уничтожено.

Система **Outpost Firewall** запоминает файлы конфигурации, с которыми она уже работала, и выводит их имена в меню **Файл** главного меню. Поэтому Вы можете открыть файл конфигурации, с которым работали ранее, просто выбрав его имя в меню **Файл**.

Для того чтобы сохранить текущее состояние файла конфигурации:

1. В меню главного окна выберите пункт **Файл**.
2. В следующем меню выберите пункт **Сохранить конфигурацию…**.

7. Устранение неисправностей

7

В данной главе будут рассмотрены действия, которые разработчики системы **Outpost Firewall** рекомендуют Вам предпринять при возникновении тех или иных проблем в ходе Вашей работы в сети. Среди этих проблем будут рассмотрены следующие:

- Вы не можете получить доступ к Web-сайту, который пытались загрузить;
- Web-сайт, который Вы загрузили, отображается не полностью;
- не блокируется обращение к некоторым баннерам;
- некоторые программы после установки системы **Outpost Firewall** перестали работать;
- система **Outpost Firewall** не устанавливается на Ваш компьютер;
- что делать, если в ходе работы системы **Outpost Firewall** возникли ошибки.

Что делать, если Вы не можете получить доступ к Web-странице, которую пытались загрузить?

Это, в первую очередь, может быть связано с ограничениями, заданными в модуле запрета отображения Web-страниц (см. п. 6.5.3.2):

- либо DNS-адрес этой страницы в явном виде указан в списке страниц, доступ к которым должен быть заблокирован (в этом случае вместо отображения Web-страницы на экране окна браузера появится информация, показанная на рис. 67);
- либо данная Web-страница содержит текстовую строку, входящую в список запрещенных строк (в этом случае вместо отображения Web-страницы на экране окна браузера появится информация, показанная на рис. 68).

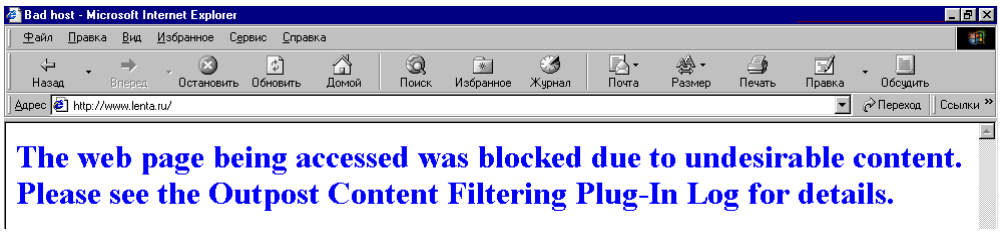

Рисунок 67. Фрагмент окна браузера с информацией о запрете отображения Web-страницы по ее адресу

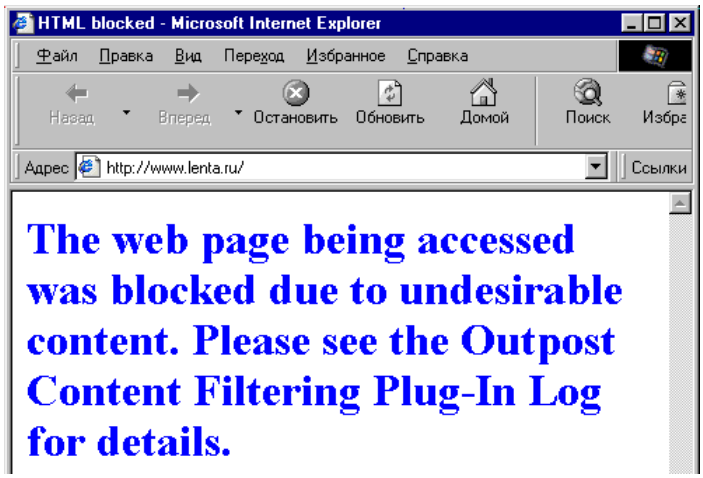

Рисунок 68. Фрагмент окна браузера с информацией о запрете отображения Web-страницы по содержимому

Для того чтобы определить причину блокировки доступа к данной странице Вы можете:

1. Открыть главное окно системы **Outpost Firewall** (или перейти в это окно, если оно уже было открыто).
2. Выбрать элемент **Содержимое** списка **Моя сеть** в левой части главного окна.
3. В правой части окна в области отображения текущей активности найти строку, соответствующую этому обращению. В этой строке:
   - в поле **URL** должен находиться URL той страницы, доступ к которой был заблокирован;
   - в поле **Действие** должна находиться строка **Блокировка узла**, в случае если обращение заблокировано по имени Web-страницы или строка **Блокировка узла по слову**, в случае если обращение заблокировано по содержимому этой страницы.
4. Конкретная причина блокировки страницы указана в поле **Ключевое слово**:
   - в случае блокировки по имени Web-страницы — имя этой Web-страницы;
   - в случае блокировки по содержимому страницы — текстовая строка, которая вызвала блокировку.

В случае если Вы хотите получить доступ к странице, заблокированной по ее имени, то достаточно просто исключить адрес этой страницы из списка страниц, доступ к которым должен быть заблокирован.

В случае если Вы хотите отменить блокировку данной страницы по содержимому:

- либо отменить (возможно, временно) режим блокировки отображения Web-страниц по их содержимому. Для этого Вы можете установить переключатель **Блокировать содержимое** на закладке **Блокировка по содержимому** в диалоговом окне настроек модуля запрета отображения Web-страниц (см. п. 6.5.3.2) в выключенное состояние, после чего нажмите на кнопку **ОК** в этом диалоговом окне;
- либо исключить на закладке **Блокировка по содержимому** в диалоговом окне настроек модуля запрета отображения Web-страниц соответствующую строку из списка строк, блокирующих отображение Web-страниц.

Что делать, если Web-сайт, который Вы загрузили, отображается не полностью?

Некоторые Web-страницы не будут работать, если отключены активные элементы данной страницы, например VB Script или Java Script, Cookie и т. д. (см. п. 6.5.3.3). Если Вы уверены в том, что эта страница абсолютно безопасна, то Вы можете определить, какие именно активные элементы используются в данной странице, и разрешить их.

Для того чтобы определить причину, по которой данная страница не отображается корректно на экране, Вы можете:

1. Открыть главное окно системы **Outpost Firewall** (или перейти в это окно, если оно уже было открыто).

2. Выбрать элемент **Активное содержимое** списка **Подключаемые модули** в левой части главного окна.

3. В правой части окна в области отображения текущей активности найти строку, соответствующую этому обращению. В этой строке определите активный элемент, который не работает:

   - в поле **URL** должен находиться URL той страницы, доступ к которой был заблокирован;
   - в поле **Действие** должна находиться строка с описанием того, какой именно активный элемент был заблокирован, например **Уничтожен Java Script** в случае, если заблокирована работа программы на Java Script и т. д.

4. Вызовите динамическое меню элемента **Активное содержимое** списка **Моя сеть** и выберите в нем пункт **Параметры...**, как показано на рис. 69.

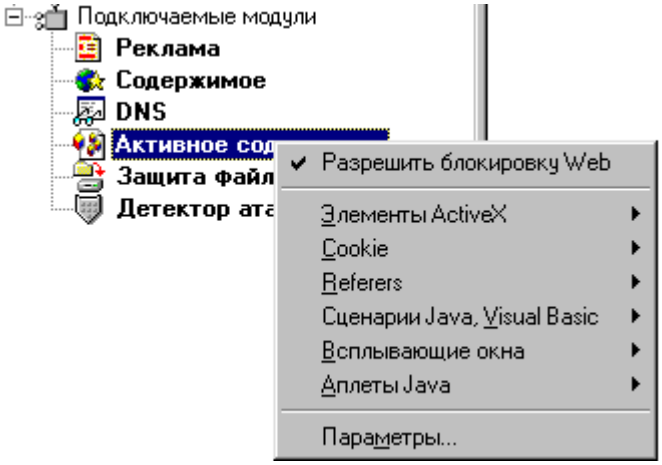

Рисунок 69. Фрагмент главного окна Outpost Firewall с динамическим меню элемента Active Content

5. В диалоговом окне настроек модуля внесите эту страницу в список Web диалогового окна настроек модуля контроля использования активных Web-страниц, выбрав в левой области окна элемент **Web-страницы** и нажав на кнопку **Добавить**, и задав имя Web-страницы, как указано в п. 6.5.3.3.

6. Задайте для этой страницы возможность использования тех активных элементов Web-страницы, которые необходимо.

Страница может отображаться некорректно, если Вы ошибочно указали, что не надо отображать такие конструкции, как например **/images/** или **http://**, которые управляют изображением частей страниц. Для того чтобы убедиться, что этого не произошло, Вы можете выбрать элемент **Реклама** списка **Подключаемые модули** в левой части главного окна и убедиться, что строки подобного вида не были внесены в список запрещенных.

Что делать, если не блокируется обращение к некоторым баннерам?

Основными причинами блокировки баннеров служат:

- обращение к нему с помощью строки, попавшей в список запрещенных HTML-строк модуля ограничения отображения Web-страниц (см. п. 6.5.3.1);
- размер баннера совпадает с одним из запрещенных для модуля ограничения отображения Web-страниц (см. п. 6.5.3.1) размеров.

Для того чтобы заблокировать баннер, Вы должны либо внести HTML-строку обращения к нему (или фрагмент этой строки), либо внести его размеры в список неотображаемых изображений (основные размеры баннеров указаны в гл. 5).

Если Вы установите курсор на этот баннер, то браузер покажет строку обращения к данному баннеру в своей строке состояния.

Эти операции описаны в п. 6.5.3.1.

Что делать, если некоторые программы после установки системы Outpost Firewall перестали работать?

Основной причиной того, что то или иное **приложение** стало некорректно работать с сетью, являются ошибочное формирование правила для этого приложения или работа в одном из запрещающих режимов.

Для того чтобы определить причину блокировки доступа к данной странице Вы можете:

1. Открыть главное окно системы **Outpost Firewall** (или перейти в это окно, если оно уже было открыто).
2. Выбрать элемент **Заблокированные** списка **Моя сеть** в левой части главного окна.
3. Найти в правой части окна в списке заблокированных приложений приложение, которому был ошибочно заблокирован доступ к сети. В поле **Причина** для этого приложения будет указана причина блокировки выхода в сеть.

Приложения

Приложение А. Меню и панели инструментов

Таблица 5. Пункты меню Файл главного окна системы Outpost Firewall

Пункт меню	Описание
Новая конфигурация	Переход к новой конфигурации системы
Загрузить конфигурацию...	Загрузить конфигурацию системы из файла
Сохранить конфигурацию...	Сохранить текущую конфигурацию системы
Сохранить как...	Сохранить текущую конфигурацию в файле
Всегда сверху	Всегда размещать главное окно системы **Outpost Firewall** поверх остальных диалоговых окон
Выход	Закрыть главное окно

Таблица 6. Пункты меню Вид главного окна системы Outpost Firewall

Пункт меню	Кнопка панели инструментов	Описание
Сортировать по		Задать порядок сортировки строк в правой части главного окна
Группировать по		Задать порядок группировки строк в правой части главного окна
Столбцы		Задать количество и порядок полей, выводимых на экран в правой части главного окна
Фильтр...		Задать фильтр для строк, выводимых в правой части главного окна
Расположение...		Задать количество и вид элементов в списке **Моя сеть** в левой части главного окна
Язык		Задать язык интерфейса с системой

Таблица 7. Пункты меню Группировать подпункта меню Вид главного окна системы Outpost Firewall

Пункт меню	Описание
Приложение	Задать порядок группировки по именам приложений
Локальный адрес	Задать порядок группировки по именам локальных узлов

Пункт меню	Описание
Локальный порт	Задать порядок группировки по именам локальных портов
Подключение	Задать порядок группировки по типу подключения
Удаленный адрес	Задать порядок группировки по именам удаленных узлов
Удаленный порт	Задать порядок группировки по именам удаленных портов
Разгруппировать	Не задавать порядка группировки

Таблица 8. Пункты меню Параметры главного окна системы Outpost Firewall

Пункт меню	Описание
Общие…	Вызвать окно настроек системы с активной закладкой **Общие**
Приложения…	Вызвать окно настроек системы с активной закладкой **Приложения**
Системные…	Вызвать окно настроек системы с активной закладкой **Системные**
Политики…	Вызвать окно настроек системы с активной закладкой **Политики**
Подключаемые модули	Вызвать окно настроек системы с активной закладкой **Подключаемые модули**

Таблица 9. Пункты меню Справка главного окна системы Outpost Firewall

Пункт меню	Описание
Вызов справки	Вызов справочного файла по системе **Outpost Firewall**
Контекстная справка	Вызов справки на тот из элементов главного окна системы, на котором Вы щелкните мышью
Read me	Вызов файла краткого описания системы **Outpost Firewall**
Автоматическое обновление	Задать режим автоматической проверки необходимости обновления системы
OutPost Pro в Web	Вызов меню Web-страниц для обеспечения поддержки работы системы **Outpost Firewall**
О программе Outpost Firewall	Вызов диалогового окна с информацией о системе **Outpost Firewall**

Таблица 10. Пункты меню OutPost Firewall в Web пункта меню Справка главного окна системы Outpost Firewall

Пункт меню	Описание
Обзор OutPost Firewall	Вызвать Web-страницу с кратким описания системы
Интерактивная поддержка	Вызвать Web-страницы технической поддержки системы
Домашняя страница OutPost Firewall	Вызвать домашнюю Web-страницу системы **OutPost Firewall**
Домашняя страница Agnitum	Вызвать домашнюю Web-страницу компании **Agnitum**

Таблица 11. Кнопки панели инструментов главного окна системы OutPost Firewall

Кнопка панели инструментов	Описание
	Изменить политику работы системы (вид кнопки зависит от текущей политики, как описано в п. 3.2)
	Вызвать диалоговое окно настроек системы **OutPost Firewall**. Если нажать на кнопку справа от этой кнопки, то можно вызвать диалоговые окна подключаемых модулей системы **OutPost Firewall**
	Задать порядок группировки строк в правой части главного окна
	Задать фильтр для строк, выводимых в правой части главного окна
	Отменить фильтр на тип объектов для строк, выводимых в правой части главного окна
	Задать фильтр по типу отображаемых объектов для строк, выводимых в правой части главного окна
	Задать фильтр для строк, выводимых в правой части главного окна, по времени
	Запуск процедуры автоматического обновления системы **OutPost Firewall**
	Вызов диалогового окна с информацией о системе **OutPost Firewall**

Приложение B. Типы ICMP-сообщений

Таблица 12. Список ICMP-сообщений

Значение поля ТИП ICMP-сообщения	Описание ICMP-сообщения
0	Ответ на эхо
3	Получатель недостижим
4	Подавление источника
5	Переназначение (изменение маршрута)
8	Эхо-запрос
10	Анонсирование своего IP
11	Превышено время для дейтаграммы
12	Ошибка параметра в дейтаграмме
13	Запрос временной метки
14	Ответ временной метки
15	Запрос информации(не действует)
16	Ответ на запрос информации(не действует)
17	Запрос маски адреса
18	Ответ на запрос маски адреса

Далее приводится краткое описание различных ICMP-сообщений.

Эхо-запрос — это один из самых простых способов тестирования работоспособности того или иного узла сети. После получения эхо-сигнала любой узел сети формирует **Ответ на эхо-запрос** и возвращает его отправителю. Получение отправителем ответа на эхо-запрос свидетельствует о работоспособности основных частей транспортной системы.

ICMP-сообщение **Получатель недостижим** формируется шлюзом в том случае, когда он не может доставить IP-дейтаграмму.

ICMP-сообщение **Подавление источника** посылается узлом отправителю дейтаграммы в том случае, если входная очередь переполнена и эта дейтаграмма удаляется из очереди.

ICMP-сообщение **Переназначение** посылается в том случае, когда шлюз обнаруживает, что используется неоптимальный маршрут, и запрашивает изменение маршрута в таблице маршрутизации.

ICMP-сообщение **Анонсирование своего IP** посылает широковещательное сообщение для объявления своего IP-адреса.

ICMP-сообщение **Превышено время для дейтаграммы** посылается в том случае, когда дейтаграмма передается от шлюза к шлюзу свыше предельно допустимого количества раз (обычно это свидетельствует о зацикливании маршрута).

ICMP-сообщение **Ошибка параметра в дейтаграмме** посылается шлюзом в том случае, если при передаче конкретной дейтаграммы возникает проблема, не укладывающаяся в рамки вышеописанных сообщений, и дейтаграмма из-за этой ошибки должна быть удалена.

ICMP-сообщения **Запрос временной метки** и **Ответ временной метки** используются для синхронизации часов в узлах сети.

ICMP-сообщения **Запрос информации** и **Ответ на запрос информации** ранее использовались для определения узлами сети своих межсетевых адресов, в настоящее время считаются устаревшими и применяться не должны.

ICMP-сообщения **Запрос маски адреса** и **Ответ на запрос маски адреса** используются для того, чтобы узнать маску подсети (т.е. какие именно биты адреса определяют адрес сети). Локальный узел посылает шлюзу **Запрос маски адреса** и получает в ответ от него **Ответ на запрос маски адреса**.

Глоссарий

ActiveX — технология создания активных Web-страниц. Эта технология реализуется с помощью элемента управления ActiveX control — специализированной программы, для которой браузер отводит участок прямоугольной формы, где эта программа полностью отвечает за интерфейс с пользователем. Технология ActiveX поддерживает полностью автоматическую установку. Встретив HTML-ссылку на элемент управления, браузер сначала проверяет, нет ли его уже на компьютере пользователя (то есть не применялся ли он раньше). Если элемент управления найден, браузер запускает его и передает ему нужные для работы данные. Если же этой компоненты на компьютере еще нет, браузер обращается к серверу, адрес которого указан в теле HTML-документа, и, перекачав с него файл, устанавливает и регистрирует новый элемент управления в Windows. Эта технология жестко привязана к конкретной операционной среде — Windows 9x/NT.

Broadcast — особый вид IP-адреса, предназначенный для рассылки сообщения всем узлам определенной сети.

- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (*limited broadcast*);
- Если все разряды номера узла в адресе содержат только 1, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (*broadcast*).

Cookie — это небольшой фрагмент информации, передаваемый сервером клиенту и размещаемый на пользовательской машине. Клиент будет хранить эту информацию и, в некоторых случаях, передавать ее серверу. Часть cookie хранится только в течение одной сессии и удаляется после закрытия браузера; другие, установленные на определенный период времени, записываются в файл.

DHCP (Dynamic Host Configuration Protocol) — протокол, предназначенный для динамического назначения IP-адресов. Кроме динамического, DHCP может поддерживать и более простые способы статического назначения адресов, позволяющие присваивать адреса как вручную, так и автоматически. Однако с использованием DHCP связаны определенные сложности. Во-первых, возникает проблема согласования информационной адресной базы в службах DHCP и DNS, а во-вторых, нестабильность IP-адресов усложняет процесс управления сетью.

DOS-атака (Denial of Service — атака типа «отказ в обслуживании) — атака из сети на компьютер, которая использует ошибки в сетевом программном обеспечении или протоколах, из-за которых некоторые сетевые действия приводят к нарушению нормальной работоспособности Вашего компьютера.

DNS (*Domain Name System)* —- это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, определяющих соответствие имен компьютеров и IP-адресов.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен — в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных, в которой содержится информация о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Интернет. Клиентам сервера DNS известен IP-адрес сервера DNS их административного домена, и по протоколу IP они передают запрос с символьным именем, ожидая в ответ соответствующий этому имени IP-адрес.

Если запрашиваемая информация хранится в базе данных DNS-сервера, то сервер сразу посылает ответ клиенту. В противном случае сервер посылает запрос DNS-серверу другого домена, который может либо сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы объединены в иерархическую структуру, в соответствии с иерархией доменов сети Интернет. Клиент опрашивает эти серверы имен, пока не найдет нужное соответствие. База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

DNS-адрес — адрес узла сети в символьном виде, в котором имена разных доменов отделяются друг от друга символом «.». Этот адрес соответствует адресу сети в базе данных DNS.

FTP — сервис Интернета, предназначенный для приема и передачи файлов по сети.

GGP (Gateway to Gateway Protocol) — протокол, с помощью которого шлюзы взаимодействуют друг с другом, выполняя задачи управления.

HTML (HyperText Markup Language) — язык, позволяющий дополнять текст различными атрибутами. HTML дает возможность совмещать графику с текстом, изменять внешний вид текста и создавать гипертекстовые документы, которые способны поддерживать взаимодействие с пользователем.

ICMP — Межсетевой Протокол Управляющих Сообщений, позволяющий Интернет-узлам сообщать об ошибках или предоставлять информацию о нестандартных условиях работы. Сообщения ICMP передаются по Интернету в поле данных IP-дейтаграмм. Конечной целью сообщений ICMP является не прикладная программа или пользователь на машине-адресате, а программное обеспечение IP на этой машине. Любая машина может послать сообщение ICMP на любую другую машину.

IGMP (Internet Group Management Protocol) — протокол управления группами Интернета, который используется узлами и маршрутизаторами для поддержки групповой рассылки сообщений. Он информирует системы физической сети о том, какие узлы в настоящее время объединены в группы и к каким группам узлы принадлежат.

IP — протокол сетевого уровня из набора протоколов Интернета.

IP datagram (дейтаграмма) — фундаментальная единица информации, передаваемая через Интернет.

IP–адрес — адрес, состоящий из 4 байт, который принято выводить в виде четырех десятичных чисел, разделенных символом «.», например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором при конфигурации

компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно либо назначен по рекомендации специального подразделения Интернета (Network Information Center, NIC), если сеть должна работать как составная часть Интернет.

Java applet (апплет) — встроенная в Web-страницу программа на языке Java. Хотя эта программа и интегрирована в страницу, она хранится в отдельном файле.

Loopback — особый IP-адрес (127.0.0.1), зарезервированный для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети.

Multicast — особый групповой IP-адрес, начинающийся с последовательности 1110. Если в пакете в качестве адреса назначения указан адрес multicast, то такой пакет получат все узлы, которым присвоен данный адрес. Узлы сами себя идентифицируют, т. е. определяют, к какой из групп они относятся. Один и тот же узел может входить в состав нескольких групп. Такие сообщения называются групповыми. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

NetBios (Network Basic Input/Output System) — базовая сетевая система ввода/вывода, протокол, разработанный компанией IBM. Протокол NetBios поддерживается в сетях IBM (IBM PC LAN), Novell NetWare, Microsoft Windows for Workgroups и в других сетях.

Referer — URL, с которого пользователь перешел на данную Web-страницу.

SSL — специальный протокол, разработанный для обеспечения безопасного доступа к Web-серверам. Этот протокол является доминирующим для шифрования обмена между клиентом и сервером.

TCP — Transmission Control Protocol (Протокол управления передачей). Основной транспортный протокол в стеке протоколов TCP/IP, обеспечивающий надежную, ориентированную на соединение доставку информации. TCP-соединение всегда осуществляется между двумя точками.

Telnet (telecommunications network protocol) — программа, позволяющая использовать средства Интернета для связи с базами данных, каталогами библиотек и прочими информационными ресурсами мира.

UDP (User Datagramm Protocol) — протокол, предоставляющий приложениям простые низкоуровневые средства передачи и приема сетевых пакетов. Протокол UDP не контролирует передачу данных и не определяет взаимосвязь между отдельными получаемыми или отправляемыми сообщениями. Поскольку UDP не гарантирует надежной передачи данных, то использующие этот протокол приложения обычно сами формируют нумерацию пакетов и, в случае необходимости, организуют повторную передачу данных. Все приложения, которым требуются широковещательные и групповые функции IP-соединений, должны работать только с протоколом UDP.

URL (Universal Resource Locator) — универсальный адрес ресурсов, используемый для идентификации ресурса, находящегося на каком-либо узле. Этот адрес имеет вид:

[**protocol**]://**host**/[:**port**][**path**], где **protocol** — имя протокола (http, ftp и т. д., по умолчанию используется http); **host** — IP-адрес или DNS-адрес; **port** — необязательный параметр, задающий номер порта для работы с сервером (для протокола http по

умолчанию используется порт 80); **path** — полный путь к файлу, включая и его имя (если этот параметр не указан, то сервер пересылает свою главную страницу).

Web (Веб) — это абстрактное пространство Интернета, в котором пользователь может получить доступ к многочисленным архивам документов, связанных перекрестными ссылками (гипертекстам).

Баннер — как правило, прямоугольное графическое изображение рекламного характера в формате GIF или JPG (хотя встречаются и баннеры, созданные средствами Java), расположенное на Web-странице и имеющее гиперссылку на сервер рекламодателя.

Маршрутизатор (router) — компьютер, соединяющий две сети и передающий пакеты из одной в другую (то же, что и шлюз).

Троянский конь — программа, каким-либо образом попавшая на Ваш компьютер, которая устанавливает по сети связь с удаленным узлом злоумышленника, а далее действует по указаниям, поступающим с этого узла, или передает на него заранее определенную информацию (например, имеющиеся на компьютере пользователя пароли или другие конфиденциальные данные).

Шлюз (gateway) — компьютер, соединяющий две сети и передающий пакеты из одной сети в другую (то же, что и *маршрутизатор*).