OUTPOST

Outpost

Personal Firewall

Приступая к работе

Содержание

1. Введение

1

Содержание

1.1. Персональный брандмауэр Outpost Firewall. Обзор возможностей

Подключение Вашего компьютера к глобальной сети Интернет, наряду с резким расширением Ваших возможностей, влечет также определенные риски и неудобства. Главная причина возникновения проблем связана с тем, что, получая доступ к ресурсам многих тысяч и миллионов компьютеров в Интернете, Вы одновременно, в той или иной степени, открываете доступ к ресурсам Вашего компьютера со стороны других компьютеров сети.

На Вашем компьютере:

- могут начать исполняться (например, при отображении активных Web-страниц, содержащих ActiveX или Java-апплеты) поступившие извне программы, которые, вообще говоря, 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;
- может размещаться информация (Cookie или referrers), по которой другие компьютеры сети смогут определять, к какой информации Вы обращались и, напротив, кто обращался к Вашему компьютеру;
- могут размещаться «троянские кони», т. е. программы, которые передают приватную информацию (например, пароли доступа в Интернет или номера кредитных карточек) с Вашего компьютера на компьютер-злоумышленник. Распространенным вариантом вторжения является установка на компьютере различных серверов для удаленного управления. Если подобная программа оказалась в Вашей системе, то ее хозяин сможет работать на Вашем компьютере почти как на своем собственном (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 рекламы. Хотя сами по себе эти объекты 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).

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 сеть компьютеров

от несанкционированного доступа из сети. Персональный брандмауэр устанавливается на локальном компьютере и предназначен для защиты персональной информации.

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

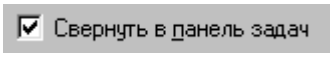
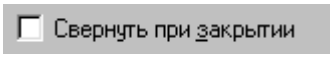
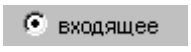
- возможностью использования сразу же после установки без необходимости предварительной настройки;
- возможностью легко и быстро создавать безопасную конфигурацию при работе в сети, используя приглашающие сообщения системы и настройки по умолчанию;
- простым пользовательским интерфейсом, в котором даже сложные настройки формируются 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 перехода в «невидимый» режим работы, когда остальные компьютеры сети не в состоянии обнаружить Ваш компьютер;
- модульной организацией системы, позволяющей встраивать в систему новые защитные модули (даже сторонних разработчиков);
- совместимостью со всеми версиями системы Windows и низкими системными требованиями.

Для успешного применения брандмауэра **Outpost Firewall** Вы не обязаны уметь пользоваться всеми возможностями системы. Система способна эффективно работать с настройками, установленными по умолчанию.

1.2. Терминология и условные обозначения

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

Таблица 1. Термины, применяющиеся при описании диалоговых окон

Элемент интерфейса	Термин
	Переключатель во включенном состоянии
	Переключатель в выключенном состоянии
	Кнопка выбора во включенном состоянии
	Кнопка выбора в выключенном состоянии

	Закладка
	Поле ввода
	Кнопка

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

Таблица 2. Условные обозначения

Обозначение	**Смысл**
Троянский конь	Определяемый термин или термин, впервые встретившийся в тексте
Режим обучения	Название какого-либо элемента системы: меню, пунктов меню, диалоговых окон, элементов диалоговых окон и т. п.
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

1.3. О чем этот документ?

В настоящем документе описывается, как немедленно после установки **Outpost Firewall** на Ваш компьютер Вы можете приступить к работе в глобальной сети Интернет под защитой программы-брандмауэра.

Установка системы **Outpost Firewall** подробно описана в Руководстве пользователя. В настоящем документе описывается работа с системой в условиях, заданных установками по умолчанию, а также некоторые возможные изменения этих установок и рекомендации по их применению.

Кратко описываются основные опасности и неудобства, с которыми сталкивается пользователь при работе в Интернете, а также способы, которыми **Outpost Firewall** помогает их предотвратить.

2. Первичная настройка системы

2

Содержание

2.1. Первый запуск системы после установки. Выбор языка интерфейса

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

- система запускается при начальной загрузке 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.

Сразу после установки Outpost Firewall на Ваш компьютер система готова к работе. Независимо от того, какой язык Вы выбрали для интерфейса программы установки, система Outpost Firewall, установленная на Ваш компьютер, использует интерфейс на английском языке. Вы можете установить русскоязычный интерфейс.

Для этого:

1. Дважды щелкните по значку в панели задач. Откроется главное окно системы (рис. 1).

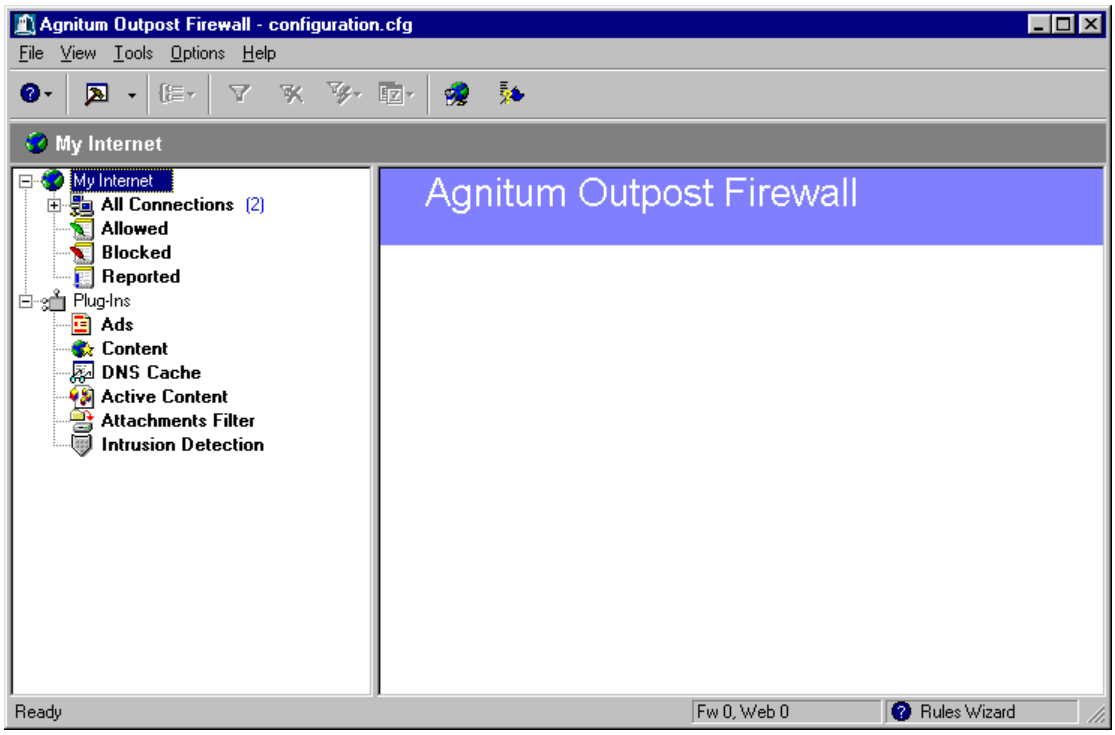


Рисунок 1. Главное окно системы (язык интерфейса установлен по умолчанию)

2. Выберите в строке меню этого окна пункт **View**.
3. Выберите в открывшемся подменю пункт **Language**.
4. Выберите в открывшемся списке наименование языка интерфейса системы (в дальнейшем предполагается, что Вы выберете пункт **Russian**).

Если вы выберете язык интерфейса системы, не совпадающий с ранее установленным, система выдаст предупреждение: фактическое изменение интерфейса произойдет только после ближайшей перезагрузки компьютера (рис. 2).

Рисунок 2. Сообщение об изменении языка интерфейса системы

2.2. Настройка политики работы с сетью (режима работы)

Одной из наиболее важных характеристик системы **Outpost Firewall** является *политика работы с сетью* (режим работы). Политики системы описываются в табл. 3.

Таблица 3. Политики системы Outpost Firewall

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

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 этом режиме облегчит Вам при необходимости задания 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: будет выдано предупреждение о сетевом взаимодействии (рис. 3).

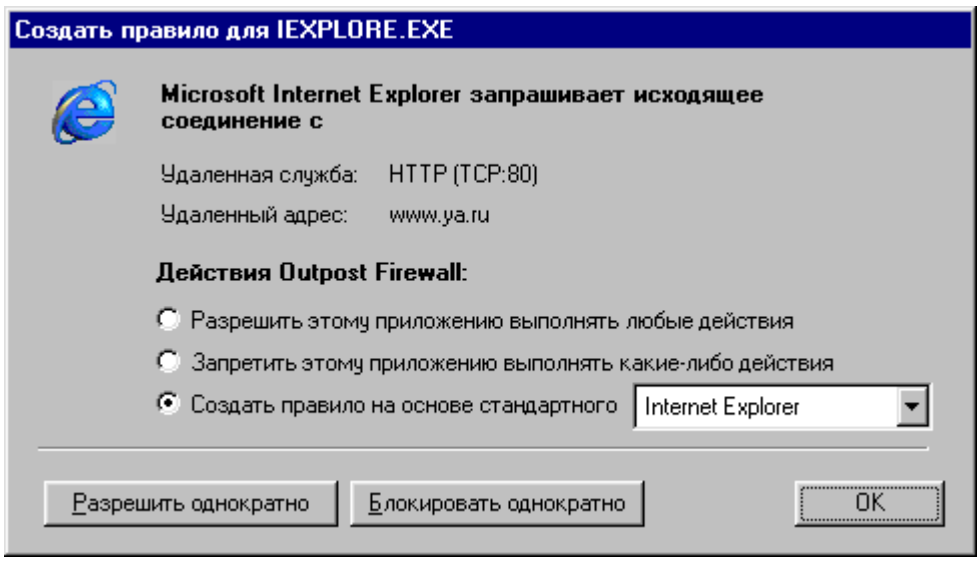


Рисунок 3. Окно предупреждения о сетевом взаимодействии

В этом диалоговом окне Вы получаете информацию о том, какое приложение (в данном примере — **Netscape Navigator**), в каком направлении (в данном примере — **исходящее**), через какой именно порт (в данном примере — **21**, зарезервированный за **FTP**), по какому именно протоколу (**TCP**) и по какому сетевому адресу (в данном примере — **philosoft.itsoft.ru**) устанавливает связь. 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 рекомендовано**	**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 **Приложение** диалогового окна **Параметры** (подробнее об этом списке см. в Руководстве пользователя).

Выбранное действие	**Для каких приложений рекомендовано**	**Что произойдет**
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 **Приложение** диалогового окна **Параметры** (подробнее об этом списке см. в Руководстве пользователя)
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	Для приложений, которые могут выходить в сеть по определенным протоколам, через определенные порты и т. д.	Сформируйте правило (правила), определяющее возможности выхода данного приложения в сеть (эта процедура подробно описана в Руководстве пользователя). Это приложение попадет в список **Пользовательский уровень безопасности**, расположенный на закладке **Приложение** диалогового окна **Параметры** (подробнее об этом списке см. в Руководстве пользователя)
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 предупреждение 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 предупреждение о сетевом соединении. Никакого правила для данного приложения не создается

По умолчанию в этом диалоговом окне установлена во включенное состояние кнопка выбора **Создать правило на основе**, а в качестве типа правила — тип, определенный системой **Outpost Firewall**.

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 режимом блокирования.

Для того чтобы изменить режим работы системы:

1. Щелкните правой клавишей мыши по значку  в панели задач.
2. В открывшемся динамическом меню (рис. 4) выберите новый режим работы (список режимов см. в табл. 3).

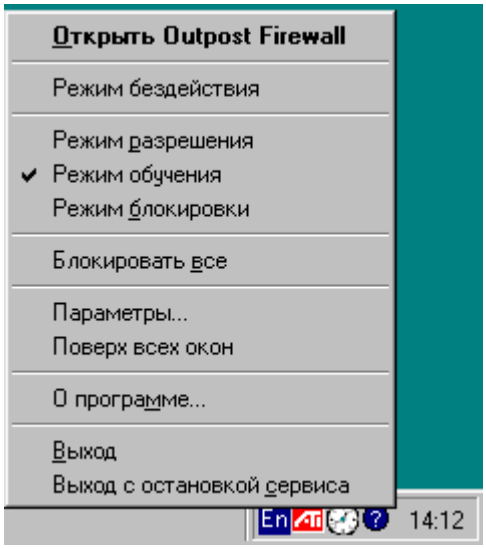


Рисунок 4. Динамическое меню значка системы в панели задач

2.3. Завершение работы системы и ее перезапуск

Как указано выше, по умолчанию система **Outpost Firewall** автоматически запускается при загрузке компьютера. При необходимости (например, когда Ваш

компьютер полностью отключен от сети) Вы можете завершить ее работу и освободить занятые ею ресурсы.

Для этого:

1. Щелкните правой клавишей мыши по значку  в панели задач.
2. В открывшемся динамическом меню (см. рис. 4) выберите пункт **Выход с остановкой сервиса**.

Для того чтобы запустить систему, не перезагружая компьютер, выберите в главном меню Windows пункт **Программы**, в открывшемся меню — пункт **Agnitum**, в очередном открывшемся меню пункт **Outpost Firewall 1.0**, затем пункт **Outpost Firewall**.

2.4. Автоматическое обновление

Система **Outpost Firewall** осуществляет обновление своих компонент через Интернет. Для этого система периодически (по умолчанию один раз в сутки) обращается к соответствующему Интернет-серверу и проверяет, появились ли на этом сервере компоненты системы, последняя версия которых отличается от установленной на Вашем компьютере. При обнаружении таких версий производится переустановка этих компонент. В частности, такое обращение произойдет при первом подключении компьютера, на который была установлена система, к Интернету. Вы также можете запустить этот процедуру вручную, независимо от того, когда последний раз производилось обновление.

Для того чтобы запустить вручную процедуру автоматического обновления системы Outpost Firewall:

1. Вызовите Главное меню системы Windows, нажав на кнопку **Пуск** в панели задач.
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**.

После этого будет запущен мастер настройки обновления системы:

1. На экране появится диалоговое окно выбора типа обновления системы (рис. 5). В этом диалоговом окне Вы можете установить во включенное состояние 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.

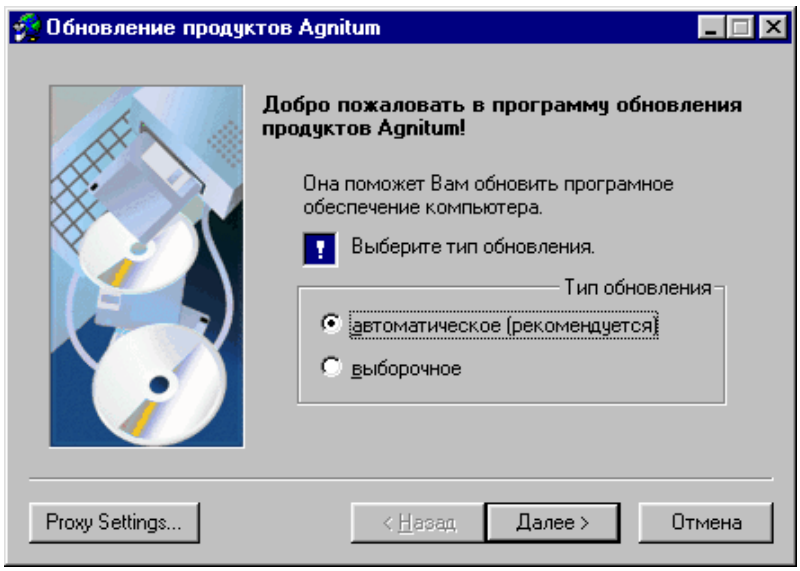


Рисунок 5. Диалоговое окно выбора типа обновления системы

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 установить во включенное состояние кнопку выбора **автоматическое**. Тип обновления **выборочное** рекомендуется использовать только при возникновении каких-либо проблем.

2. После выбора типа обновления нажмите на кнопку **Далее**. Если Вы установили во включенное состояние кнопку выбора **выборочное**, то на экране появится диалоговое окно выбора обновляемых компонент (рис. 6).

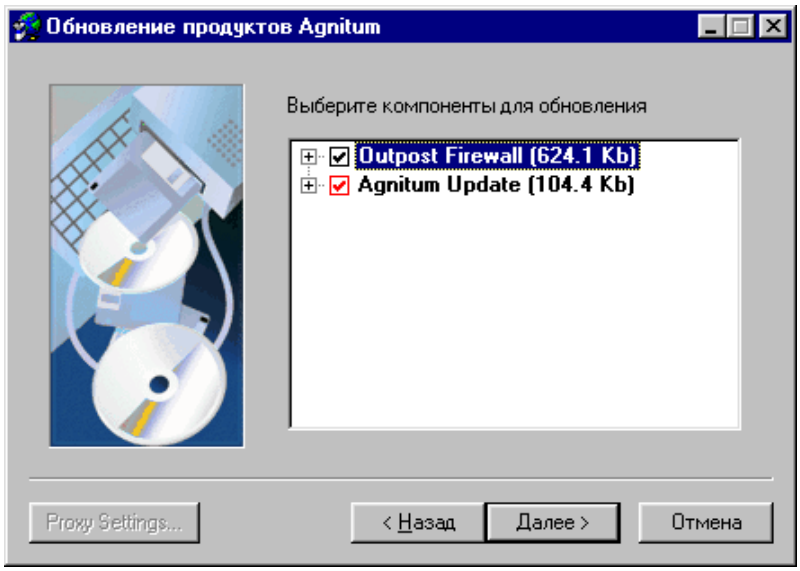


Рисунок 6. Диалоговое окно выбора обновляемых компонент системы

3. 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 кнопкой мыши на символ ☑, расположенный слева от этой компоненты.

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

4. После выбора всех компонент, которые следует обновлять, 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, в которых показывается ход процесса. Большую часть времени на экране будет находиться диалоговое окно обновления компонент системы **Outpost Firewall** (рис. 7).

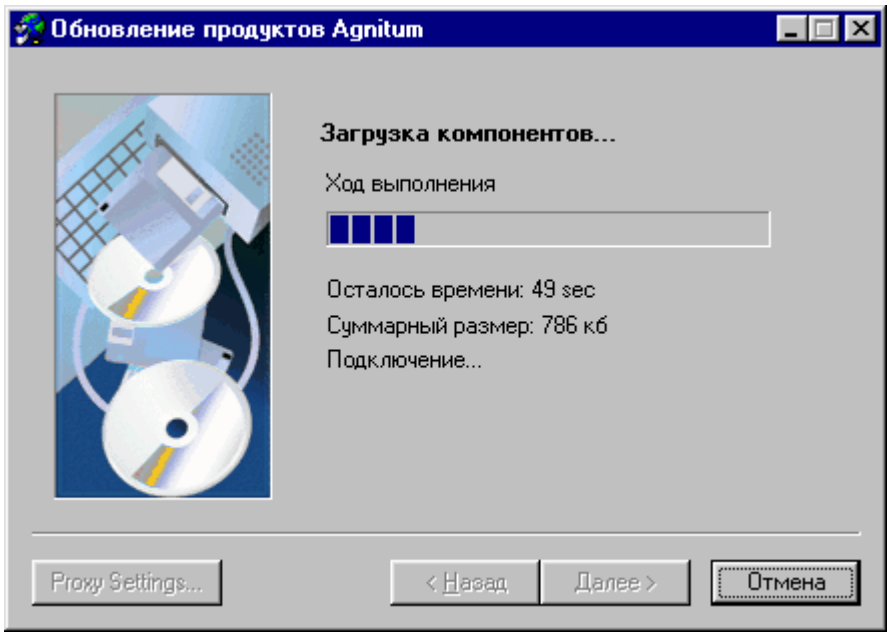


Рисунок 7. Диалоговое окно обновления компонент системы

5. После завершения процедуры обновления компонент на экране появится информационное окно: обновления системы будут завершены только после перезагрузки (рис. 8).

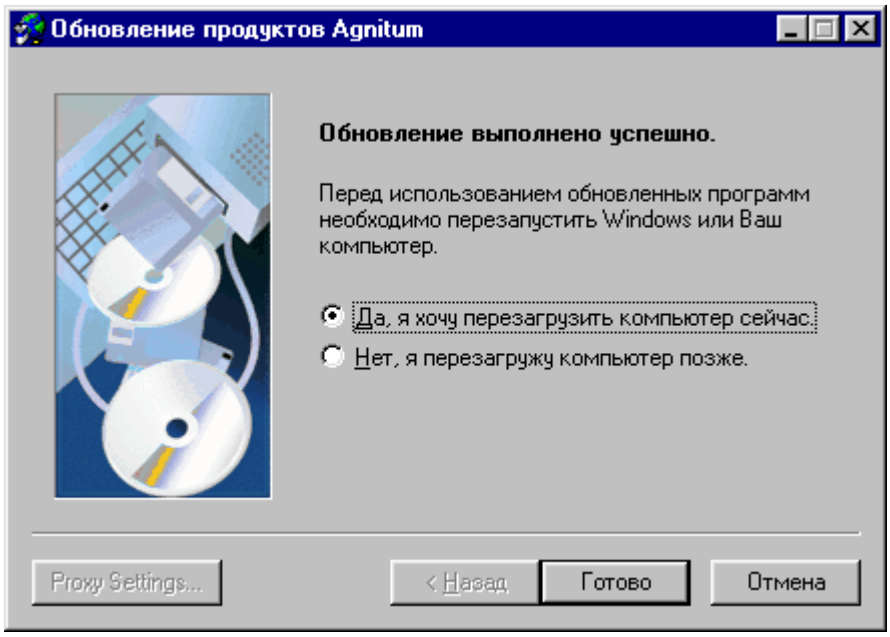


Рисунок 8. Диалоговое окно завершения процесса обновления. Выбор порядка перезагрузки

Если система, установленная на Вашем компьютере, не требует обновления, то окно завершения процесса обновления выглядит иначе (рис. 9). Никаких изменений компонент системы не произойдет.

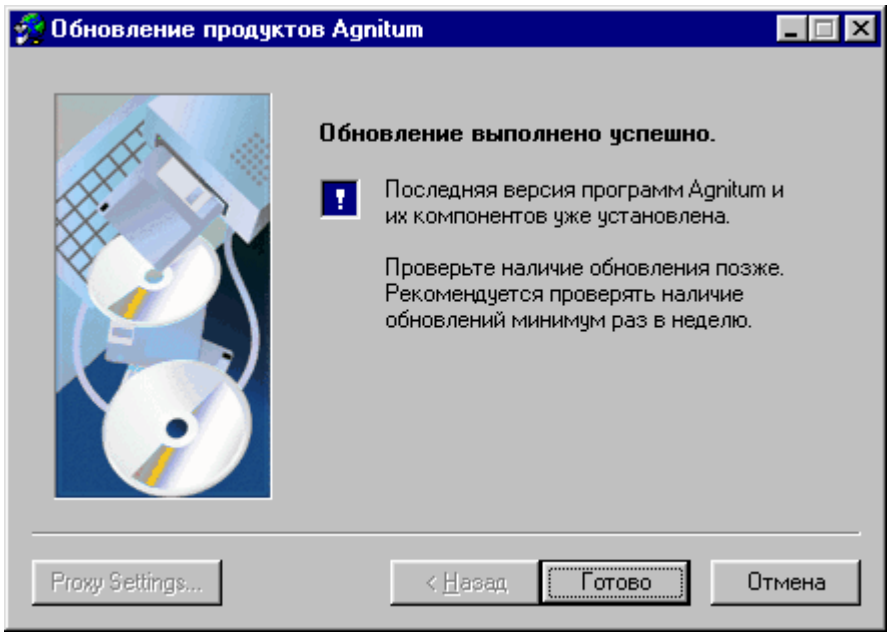


Рисунок 9. Диалоговое окно завершения процесса обновления. Необходимость обновления системы отсутствует

3. Организация защиты компьютера

3

Содержание

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 уже говорилось в п. 1.1, основными опасностями при работе в сети являются:

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

3.1. Защита от проникновения посторонних программ

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 правилами сетевого взаимодействия, настроенными соответствующим образом. Пока Вы не имеете достаточного опыта использования персонального брандмауэра, используйте правила, созданные системой по умолчанию. Самостоятельная настройка правил подробно описана в Руководстве пользователя.
- 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 поступить следующим образом. Вы запрещаете использование данных программных средств по умолчанию, однако разрешаете в известных и проверенных Вами Web-страницах, список которых составляете самостоятельно.

Для того чтобы запретить или ограничить использование потенциально опасных элементов Web-страниц:

1. Дважды щелкните по значку в панели задач. Откроется главное окно системы (рис. 10).

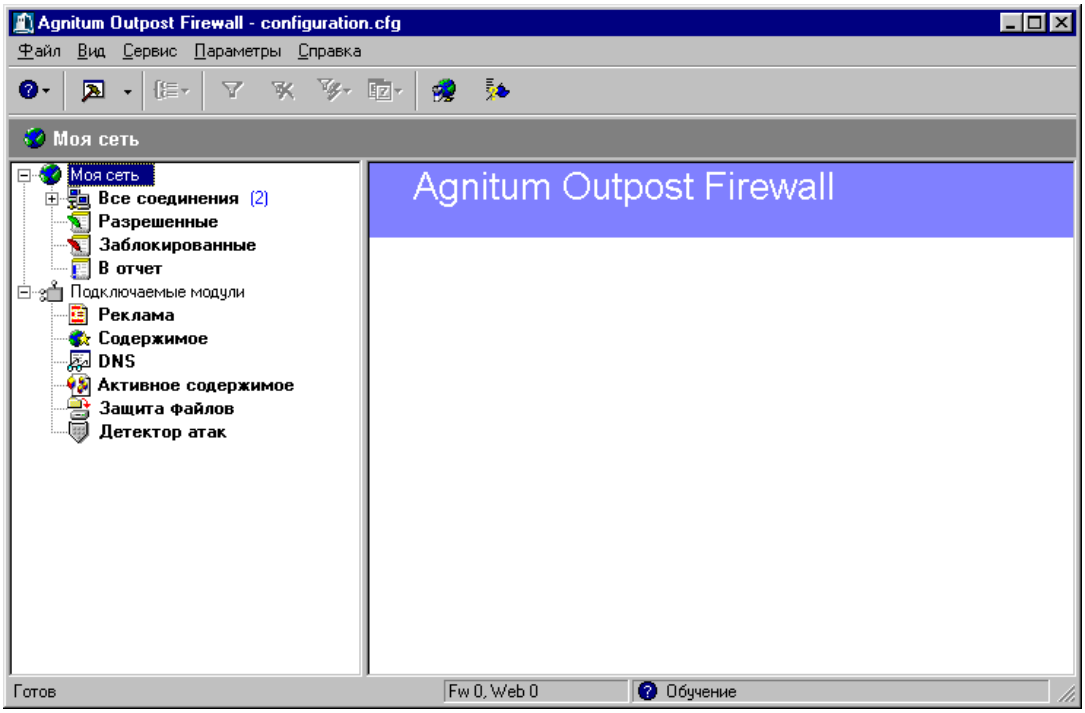


Рисунок 10. Главное окно системы

2. Щелкните правой клавишей мыши по пункту **Активное содержимое** иерархического списка, расположенного в левой части окна. Откроется динамическое меню (рис. 11).

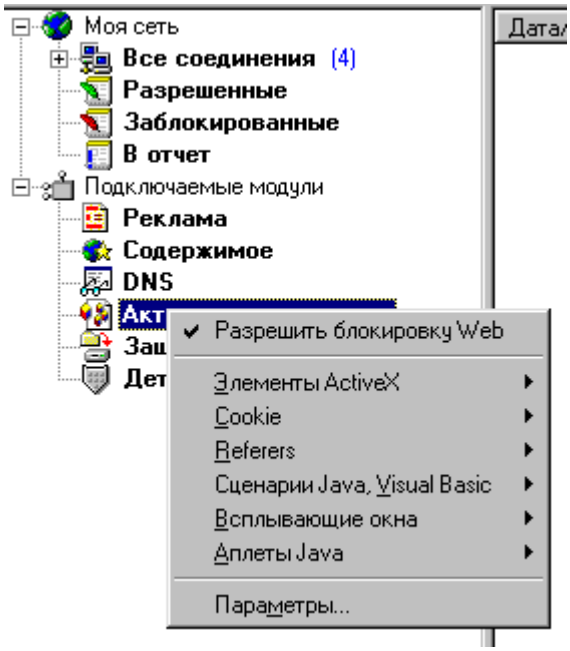


Рисунок 11. Меню операций с активным содержимым

3. Для того чтобы отменить ограничения на активное содержимое Web-страниц, установите в выключенное состояние переключатель у пункта **Разрешить блокировку Web** динамического меню. По умолчанию переключатель установлен во включенное состояние, т. е. блокировка разрешена, однако для каждого отдельного активного элемента по умолчанию установлено разрешение его использования.

4. Для того чтобы ограничить исполнение Java-апплетов, сценариев или элементов ActiveX, выберите соответствующий пункт динамического меню и затем в открывшемся подменю (на рис. 12 приведен пример для ActiveX) выберите пункт **Запретить**. В некоторых подменю имеется также пункт **Спросить**. Установив переключатель против этого пункта, можно запретить исполнение активного содержимого без предварительного запроса пользователя).

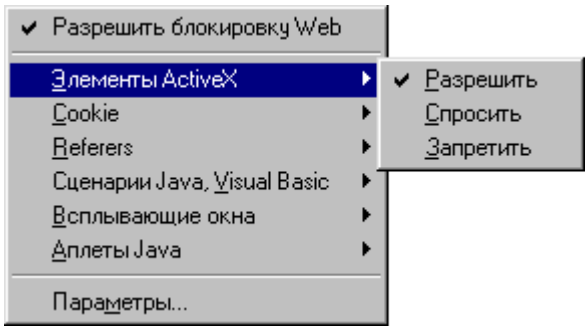


Рисунок 12. Ограничение использования элементов ActiveX

Для того чтобы запретить или ограничить использование потенциально опасных элементов Web-страниц для отдельных доверенных страниц:

1. Выберите в вышеописанном динамическом меню пункт **Параметры**. Откроется окно **Параметры** на закладке **Web** (рис. 13).

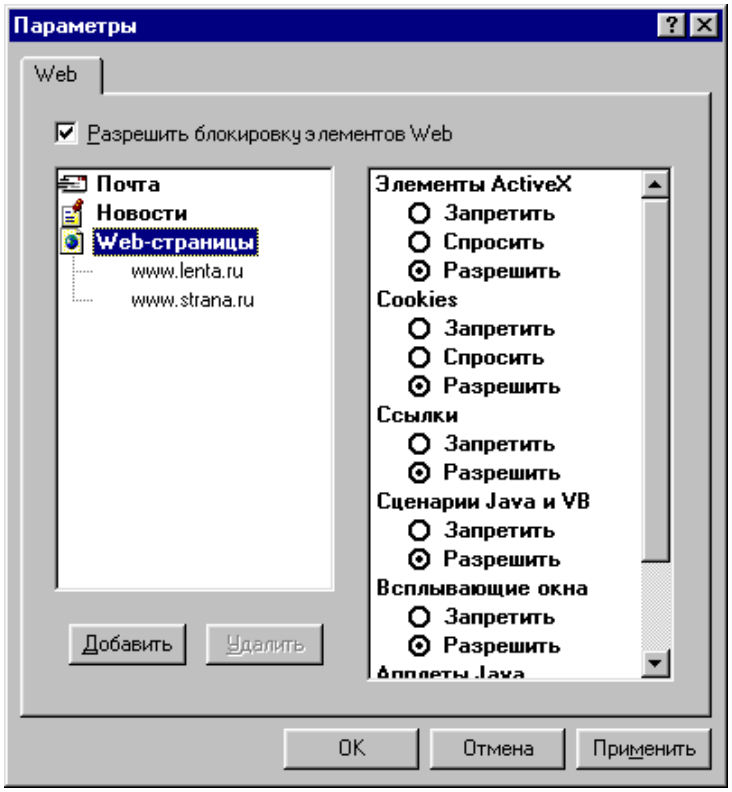


Рисунок 13. Настройка ограничений элементов Web-страниц

2. Иерархический список в левой части окна содержит в качестве узлов второго порядка, подчиненных узлу **Web-страницы**, перечень адресов страниц, для которых ограничения настраиваются индивидуально (сразу после установки системы этот список пуст). Для того чтобы добавить новый адрес в этот список, нажмите на кнопку **Добавить** и в открывшемся окне (рис. 14) введите новый адрес.

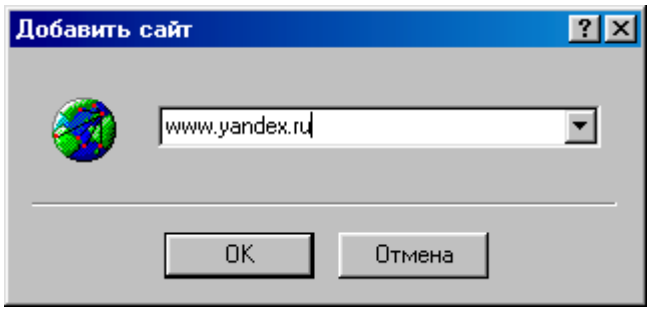


Рисунок 14. Ввод адреса новой страницы

3. В правой части окна **Параметры** (см. выше рис. 13) находится набор кнопок выбора, соответствующих различным элементам активного содержимого Web-страниц. Положение этих кнопок зависит от того, какой элемент иерархического списка выбран (на указанном рисунке выбран элемент **Web-страницы**, положение кнопок соответствует ограничениям, которые Вы указали для Web-

страниц в общем случае; в частности, запрещено использование ActiveX). Для всех вновь добавляемых к списку отдельных страниц первоначально устанавливается разрешение использования всех элементов. Вы можете, однако, установить для любой отдельной страницы свой набор ограничений. Для этого выберите ее адрес в иерархическом списке и воспользуйтесь кнопками выбора в правой части окна.

4. Вы можете удалить страницу из списка доверенных. Для этого выберите ее адрес в иерархическом списке и нажмите на кнопку **Удалить**.

3.2. Ограничение доступа к информации о Вашем компьютере

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

- Запретить создание на Вашем компьютере Cookie. 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. Это действие осуществляется средствами, описанными в предыдущем разделе.
- Для защиты от «троянских коней» Вы можете, по своему выбору:
  - оставить систему работать в режиме обучения (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 в явном виде (работа будет вестись в режиме блокировки);

При обнаружении подозрительного соединения Вы можете, благодаря информации, выдаваемой системой **Outpost firewall**, определить DNS-адрес или IP-адрес узла, с которым размещенная на Вашем компьютере подозрительная программа пытается установить соединение, после чего принять соответствующие меры. Соответствующие средства подробнее описаны в Руководстве пользователя.

- перейти в «невидимый» для других компьютеров сети режим работы. Для этого выберите в меню главного окна системы пункт **Параметры**, а в открывшемся подменю пункт **Системные**. На закладке **Системные** окна **Параметры** (рис. 15) установите во включенное состояние кнопку выбора **Невидимка** в поле **Тип ответа**.

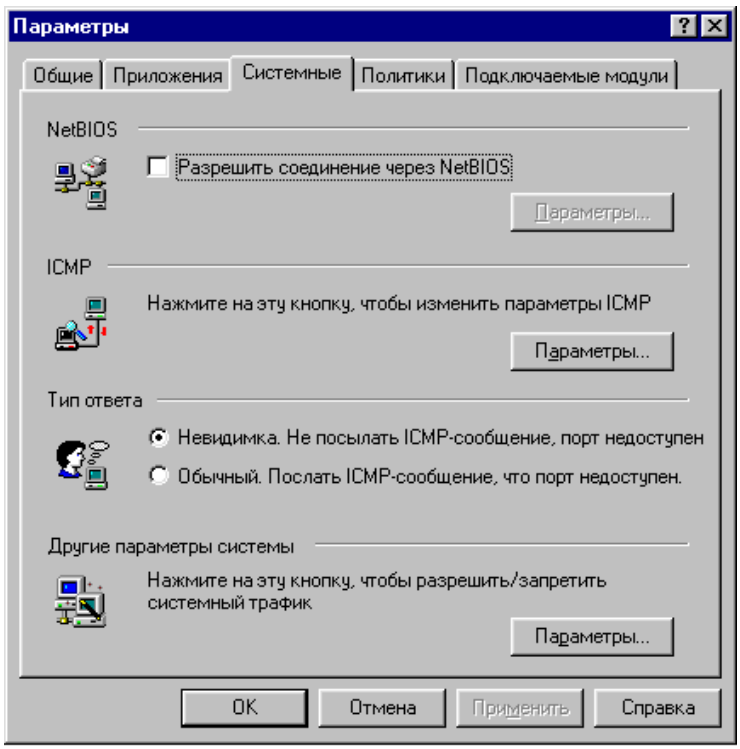


Рисунок 15. Установка «невидимого» режима

3.3. Защита от опасных элементов в сообщениях электронной почты и групп новостей

Большинство потенциально опасных элементов, встречающихся в Web-страницах, могут также входить в состав сообщений электронной почты и групп новостей. В отличие от обычных Web-страниц, в которых эти элементы (ActiveX, сценарии и апплеты) встречаются довольно часто, появление их в сообщениях с большой вероятностью свидетельствует о заражении сообщения вирусом или «троянцем» либо иной разновидности злонамеренной атаки на Ваш компьютер. Рекомендуется запретить элементы активного содержимого в сообщениях.

Для этого:

1. Откройте, как описано выше в разделе 3.1, окно **Параметры** (закладка **Web**).
2. Выберите в иерархическом списке пункт **Почта** или **Новости**.
3. Воспользуйтесь кнопками выбора в правой части окна, чтобы запретить те виды активного содержимого, использование которых в письмах или новостях нежелательно.

3.4. Защита от поступления на компьютер ненужной информации

Для предотвращения поступления на Ваш компьютер ненужной информации Вы можете:

- Запретить отображение рекламных *баннеров* на экране по адресам рекламных служб. Поскольку адреса большинства баннерных служб известны, то Вы

можете исключить отображение тех Web-страниц, в которых есть HTML строки, указывающие на эти службы.

Сразу после установки система содержит большой список рекламных HTML-строк. Вы можете, как описано ниже, добавить в этот список какую-либо HTML-строку из Web-страницы, находящейся в данный момент времени на экране, а также можете отменить запрет на отображение тех или иных частей Web-страницы либо вовсе отказаться от использования этой формы защиты.

- 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. ниже).

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 пикселей. 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 подробно описаны в Руководстве пользователя. 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, то Вы воспрепятствуете изменению этих данных. Таким способом Вы можете, например, заблокировать на Вашем домашнем компьютере доступ к подобной информации для детей.

Для того чтобы ограничить поступление на Ваш компьютер рекламы:

1. Щелкните правой клавишей мыши по пункту **Реклама** иерархического списка, расположенного в левой части главного окна системы.

2. В открывшемся динамическом меню выберите пункт **Параметры**. Откроется окно **Параметры** на закладке **Строки HTML** (рис. 16).

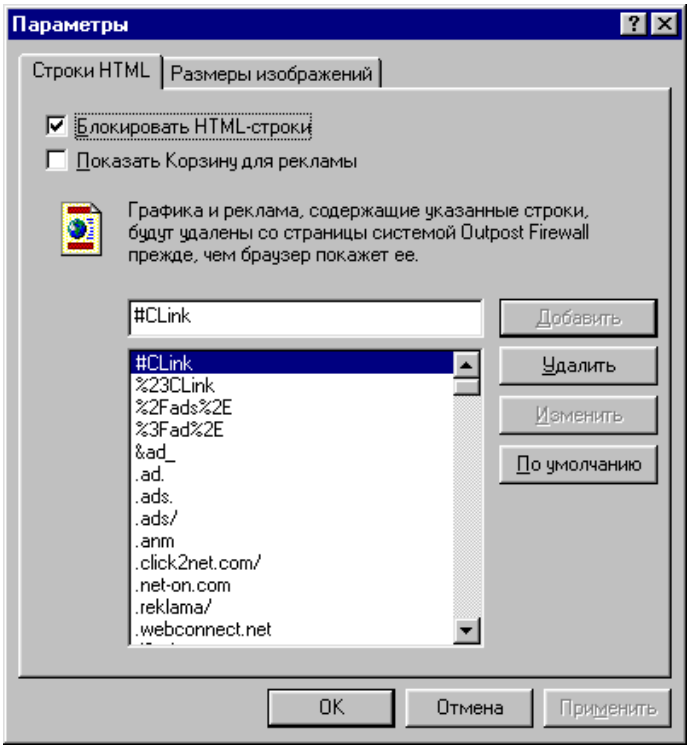


Рисунок 16. Запрет рекламы по адресам баннерных служб

3. В списке, занимающем большую часть окна, отображаются строки, являющиеся адресами или фрагментами адресов рекламных служб. Для того чтобы добавить новый адрес в этот список, введите его в поле ввода над списком и нажмите на кнопку **Добавить**. Для того чтобы отредактировать адрес, выберите его в списке (при этом соответствующая строка отображается в поле ввода), отредактируйте строку в поле ввода и нажмите на кнопку **Изменить**. Для того чтобы удалить какой-либо адрес из списка, выберите его и нажмите на кнопку **Удалить**.

4. Для того чтобы восстановить список запрещенных к использованию рекламных служб по состоянию на момент установки системы, нажмите на кнопку **По умолчанию**.

5. Для того чтобы отказаться от этой формы защиты, установите в выключенное состояние переключатель **Блокировать HTML-строки**.

Для того чтобы запретить вывод на экран графических баннеров определенного размера:

1. Перейдите в вышеописанном окне на закладку **Размеры изображений** (рис. 17).

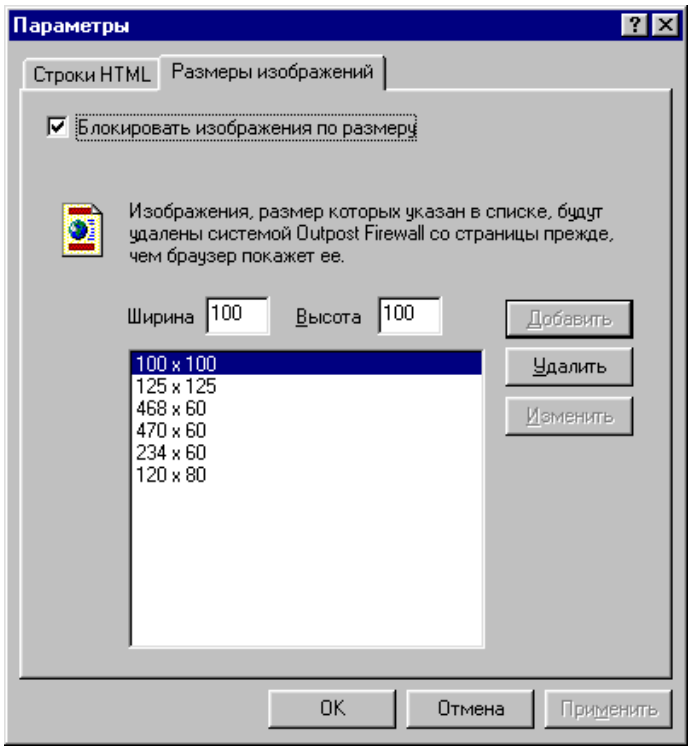


Рисунок 17. Блокировка рекламы по размеру графического баннера

2. Выберите любой элемент из списка размеров изображений в центральной части окна. Ширина и высота этого изображения выводятся в полях ввода над списком.
3. Если Вы хотите удалить какой-либо элемент и тем самым разрешить показ баннеров такого размера, нажмите на кнопку **Удалить**. Если Вы хотите отредактировать размеры изображения, задаваемые каким-либо элементом списка, отредактируйте значения в полях ввода **Ширина** и **Высота** и нажмите на кнопку **Изменить**; если же Вы хотите добавить полученную пару размеров к списку, не удаляя выбранного элемента списка, нажмите на кнопку **Добавить**.
4. Если Вы хотите отказаться от использования этой формы защиты, установите в выключенное состояние переключатель **Блокировать изображения по размеру**.

Следует иметь в виду, что защита по размеру графических баннеров запрещает отображение любого изображения со ссылкой указанного размера, в том числе и не являющегося рекламным. Данный вид защиты не может использоваться для исключения текстовых баннеров.

Для того чтобы запретить отображение Web-сайтов с определенным содержимым:

1. Щелкните правой клавишей мыши по пункту **Содержимое** в иерархическом списке в главном окне системы. Окно **Параметры** откроется на закладке **Блокировка по содержимому** (рис. 18).

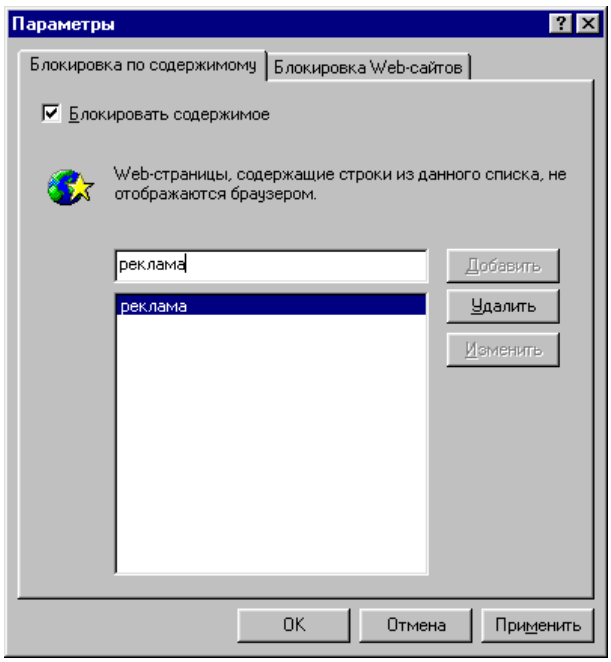


Рисунок 18. Блокировка страниц с заданным содержимым

2. Сформируйте список запрещенных строк, вводя их в поле ввода над списком. Для добавления введенной строки нажмите на кнопку **Добавить**, для замены выбранной в списке строки нажмите на кнопку **Изменить**. Для того чтобы удалить какую-либо строку из этого списка, выберите ее в списке и нажмите на кнопку **Удалить**.

3. Если Вы хотите отключить эту форму контроля, но сохранить список для дальнейшего использования, установите в выключенное состояние переключатель **Блокировать содержимое**.

Для того чтобы запретить отображение Web-сайтов с определенными доменными именами:

1. Перейдите на закладку **Блокировка Web-сайтов** (рис. 19).

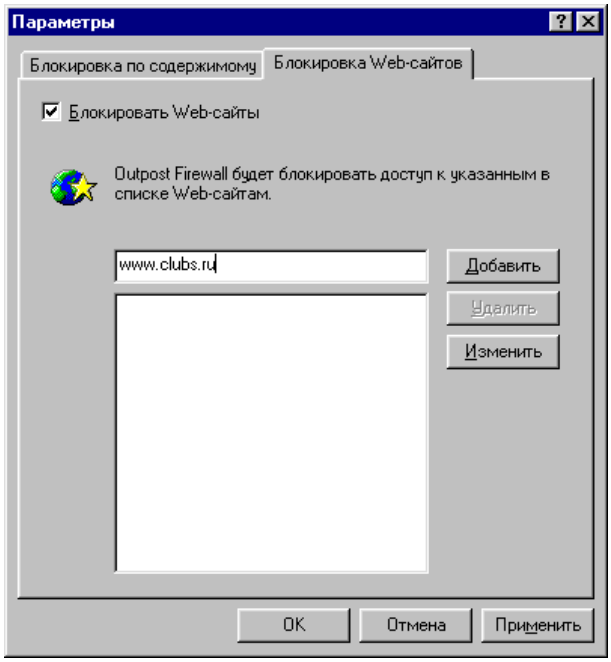


Рисунок 19. Блокировка сайтов по именам

2. Способами, описанными для предыдущей закладки, сформируйте или отредактируйте список имен сайтов, которые не должны отображаться на Вашем компьютере.

Для того чтобы защитить паролем изменения, внесенные Вами в конфигурацию системы:

1. Выберите в меню главного окна пункт **Параметры**, а в открывшемся подменю пункт **Общие**. Откроется окно **Параметры** на закладке **Общие** (рис. 20).

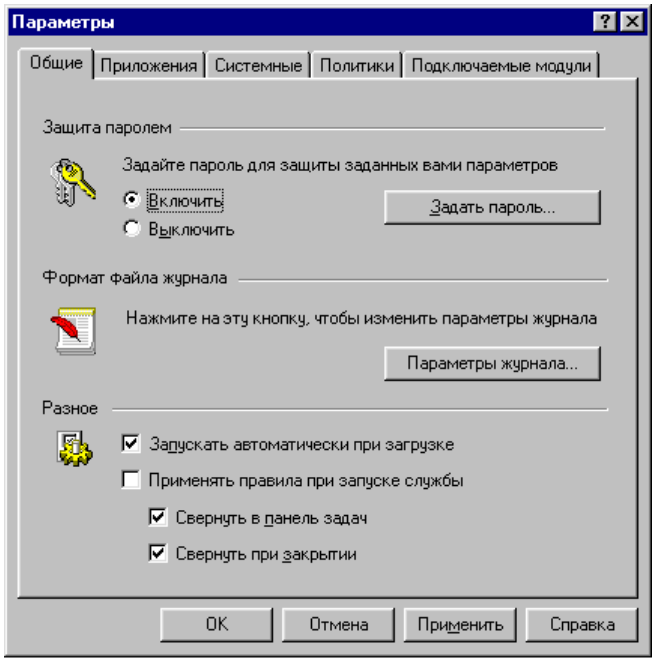


Рисунок 20. Основные параметры системы

2. Установите во включенное состояние кнопку выбора **Включить** в поле **Защита паролем**. Откроется окно изменения пароля (рис. 21)

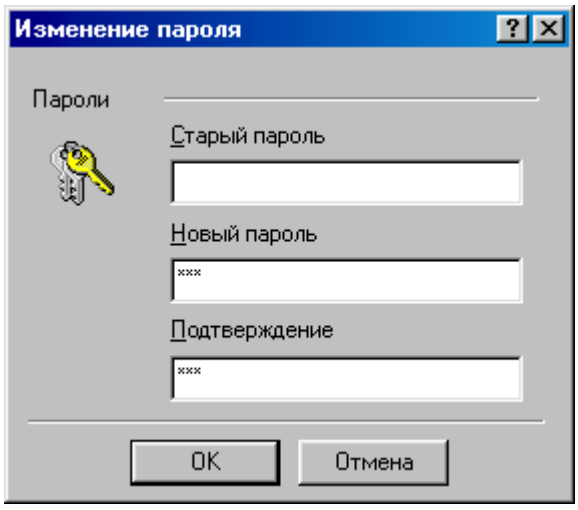


Рисунок 21. Ввод пароля защиты конфигурации

3. Введите пароль в поле ввода **Новый пароль**, повторите его ввод в поле **Подтверждение** и нажмите на кнопку **OK**.

3.5. Выделение доверенной зоны

При использовании системы Вы можете создать зону сетевых адресов, для которых контроль сетевых взаимодействий выполняться не будет. Эта зона представляет собой список задаваемых своими IP-адресами либо DNS-адресами узлов или подсетей, 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.

Для того чтобы задать подсеть, соединения для которой не блокируются независимо от установок других параметров системы (доверенную зону):

1. Выберите в меню главного окна пункт **Параметры**, в открывшемся подменю выберите пункт **Политики**.
2. На закладке **Политики** открывшегося окна (рис. 22) нажмите на кнопку **Изменить**.

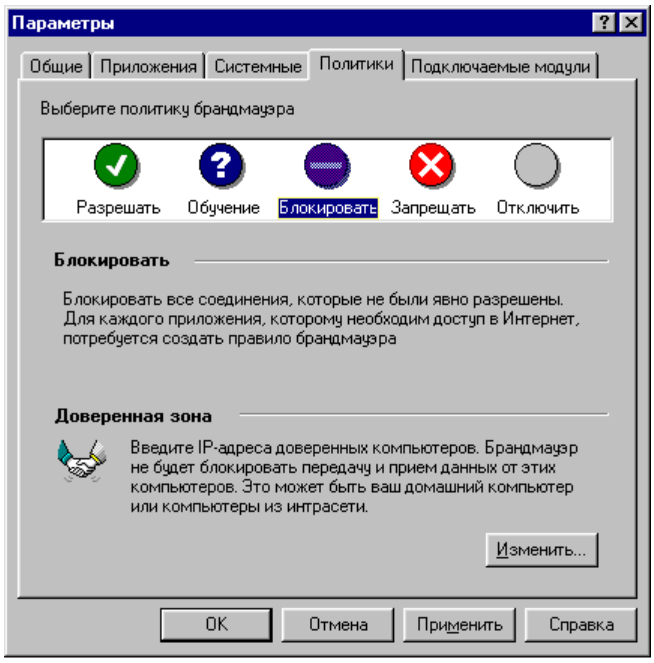


Рисунок 22. На этой закладке задается доверенная зона

3. Откроется окно настройки параметров доверенной зоны. Нажмите на одну из кнопок выбора **имя домена** или **IP-адрес и маска посети**, в зависимости от желаемого способа задания подсети. Вид окна будет несколько отличается в зависимости от выбранного способа (рис. 23 и 24).

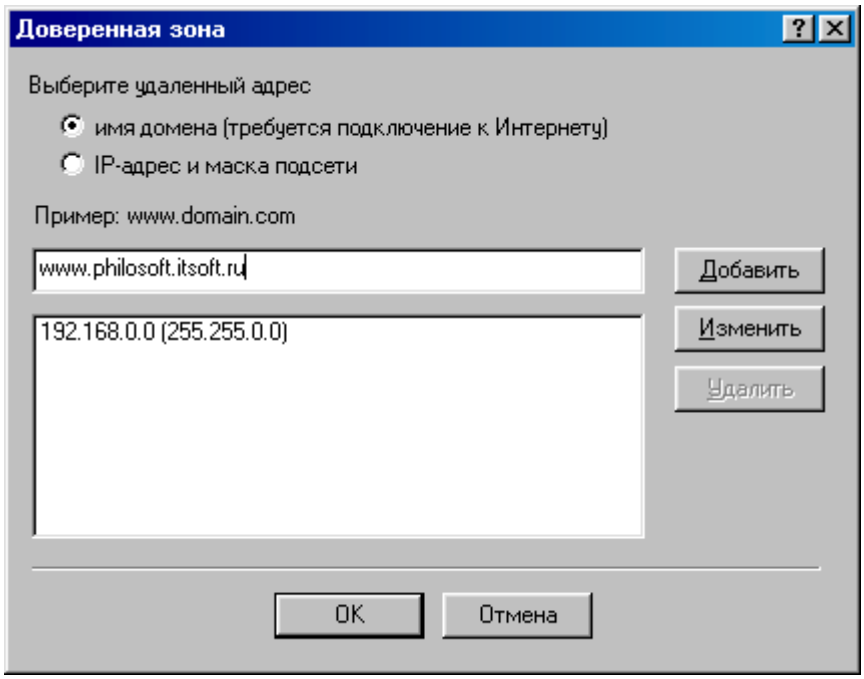


Рисунок 23. Задание доверенной зоны по доменному имени

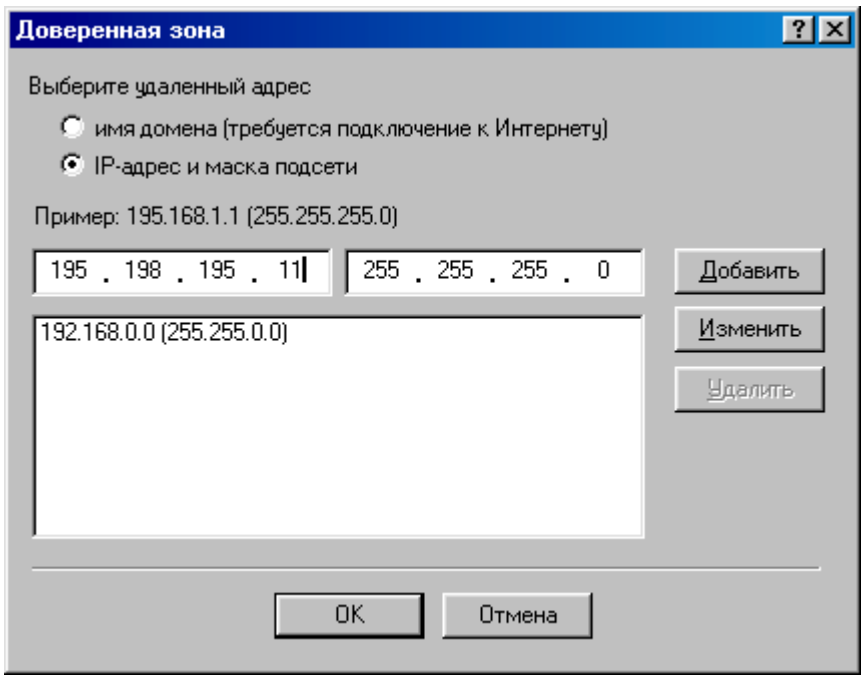


Рисунок 24. Задание доверенной зоны по IP-адресам

4. Задайте указанным на предыдущем шаге способом (по доменному имени либо по IP-адресу и маске подсети) подсеть, добавляемую к доверенной зоне, и нажмите на кнопку **Добавить**. Вы также можете удалить или отредактировать любой элемент списка подсетей. Для этого следует выбрать его в списке (кнопка выбора, соответствующая способу задания подсети, установится автоматически) и воспользоваться кнопками **Удалить** или **Изменить**.

При задании подсети по доменному имени необходимо иметь соединение с Интернетом.

3.6. Настройка системных протоколов и другие системные настройки

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

Для предотвращения попыток нарушения работоспособности Вашего компьютера с использованием злоумышленниками служебного протокола ICMP система **Outpost Firewall** позволяет разрешить или запретить использование ICMP-сообщений того или иного типа. Подробнее об этом рассказано в Руководстве пользователя. Начинающему пользователю системы рекомендуется сохранить настройки по умолчанию.

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 всегда или при сетевом соединении с определенными узлами, задаваемыми своими IP-адресами или DNS-адресами.

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

По умолчанию доступ с использованием этого протокола не запрещен, однако список адресов, с которыми разрешено соединение, пуст. При необходимости разрешить соединение с использованием этого протокола выберите в меню главного окна системы пункт **Параметры**, в открывшемся подменю — пункт **Системные**. Откроется закладка **Система** окна **Параметры** (см. выше рис. 15).

В поле **NetBIOS** этой закладки Вы можете запретить соединение с использованием этого протокола. Для этого установите в выключенное состояние переключатель **Разрешить соединение через NetBIOS**. Вы можете также настроить список допустимых адресов, для чего следует нажать на кнопку **Параметры**. Откроется окно настройки допустимых адресов (рис. 25).

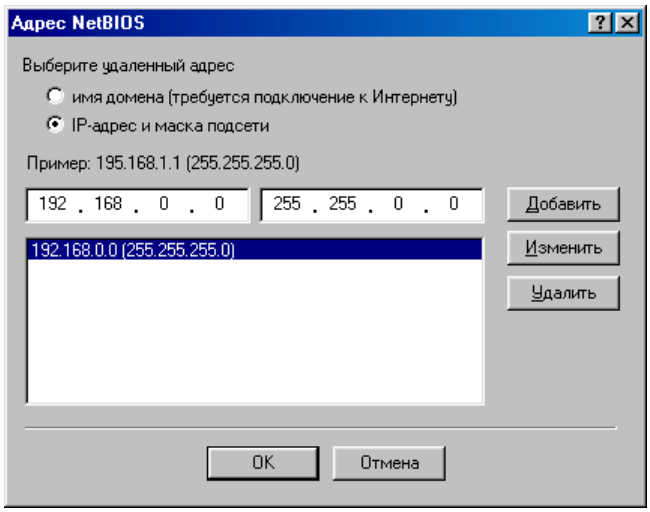


Рисунок 25. Настройка адресов, для которых допустим доступ с использованием NetBIOS

Настройка адресов в этом окне полностью аналогична описанной выше в 3.5.