Лабораторная работа №1

Установка и настройка протокола TCP/IP

Цель работы: изучить принципы работы протоколов TCP/IP и научиться их настраивать для работы в сети Интернет.

Теоретическая справка

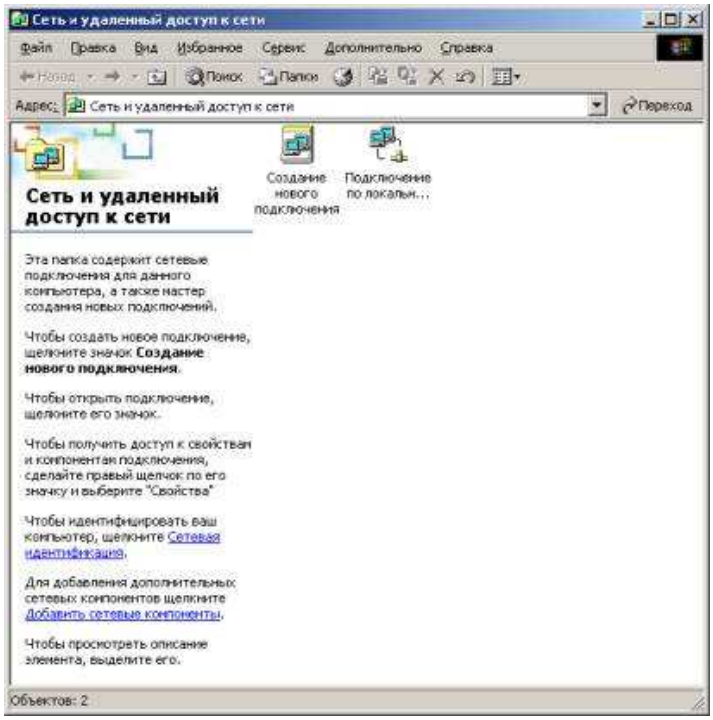
Хотя Windows поддерживает большое количество сетевых протоколов, TCP/IP используется чаще всего по целому ряду причин:

- обеспечивает межсетевое взаимодействие компьютеров с разной аппаратной архитектурой и операционными системами;
- является основным протоколом, используемым в сети Интернет;
- необходим для функционирования Active Directory.

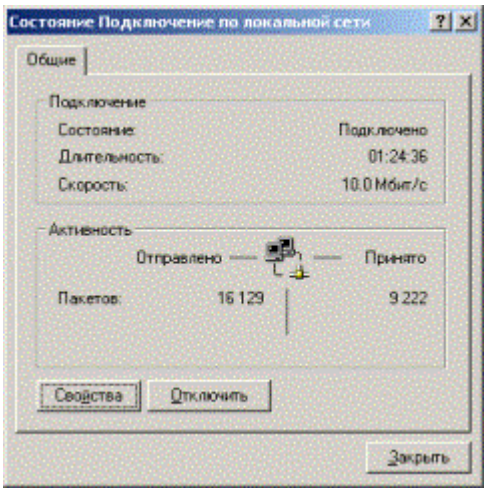
TCP/IP - это аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet). В терминологии вычислительных сетей протокол - это заранее согласованный стандарт, который позволяет двум компьютерам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому вы часто слышите, как его называют набором, или комплектом протоколов, среди которых TCP и IP - два основных.

В Windows параметры протокола TCP/IP являются частью параметров настройки сетевого адаптера, поэтому все изменения, связанные с этим протоколом, осуществляются через ***Панель управления***.

Для настройки сетевых адаптеров и протоколов дважды щелкните значок ***Сеть и удаленный доступ к сети*** в ***Панели управления***. Вы также можете выбрать пункт ***Свойства*** в контекстном меню папки М***ое сетевое окружение***, расположенной на ***Рабочем столе***.



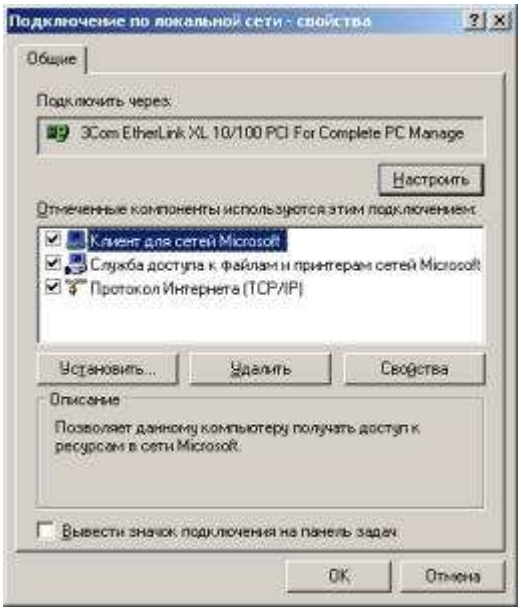
В появившемся окне представлены различные соединения вашего компьютера с внешним миром. После успешной установки сетевого адаптера (во время установки или позже) в окне должен присутствовать как минимум один значок с именем ***Подключение по локальной сети***.



Двойной щелчок значка выводит окно с информацией о состоянии соединения. Можно узнать длительность соединения, его скорость, количество отправленных и принятых пакетов данных.

Кнопка ***Отключить*** позволяет выключить сетевой адаптер, прекратив тем самым обмен данными через него. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения. Отключенные соединения отображаются в виде "серых" значков.

Кнопка ***Свойства*** вызывает окно настройки свойств соединения, в том числе и параметров используемых протоколов. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения.



В этом окне можно получить информацию о сетевом адаптере, через который осуществляется соединение. Щелкнув кнопку ***Настроить***, вы откроете окно свойств сетевого адаптера и сможете их изменить.

Установив флажок ***Вывести значок подключения на панель задач***, вы включите отображение значка, представляющего соединение, на панели задач Windows. Это позволит наблюдать за активностью соединения и быстро осуществлять его настройку, не используя ***Панель управления***.

В центральной части окна в списке представлены все клиенты, службы и протоколы, связанные с соединением. Для нормального функционирования домена или рабочей группы Windows необходимо наличие следующих компонентов.

Компонент	Описание
Клиент для сетей Microsoft	Обеспечивает компьютеру доступ к ресурсам сети Microsoft
Служба доступа к файлам и принтерам сетей Microsoft	Позволяет предоставлять папки и принтеры компьютера в совместный доступ в сетях Microsoft
Протокол Интернета (TCP/IP)	Обеспечивает связь компьютеров в локальных и глобальных сетях

Настройка основных параметров TCP/IP

Стек протоколов TCP/IP, входящий в состав Windows, поддерживает два режима настройки: с использованием статического или динамического IP-адреса. Каждый из этих режимов имеет свои преимущества и недостатки и должен использоваться в зависимости от конфигурации вашей локальной сети:

Преимущества:

Статический IP-адрес	**Динамический IP-адрес**
Не требуются дополнительные серверы и дополнительная подготовка администратора сети. Соответствие имени компьютера и IP-адреса практически	Все параметры настройки TCP/IP определяются один раз на сервере и автоматически используются рабочими станциями. Нет необходимости вести учет

никогда не изменяется.	используемых IP-адресов. Изменение одного или нескольких глобальных параметров IP-сети требует изменения параметров настройки только на сервере. Общее количество компьютеров может превышать количество выделенных IP-адресов, так как адрес выделяется на время работы компьютера в сети. Удобство настройки TCP/IP на компьютерах временных пользователей.

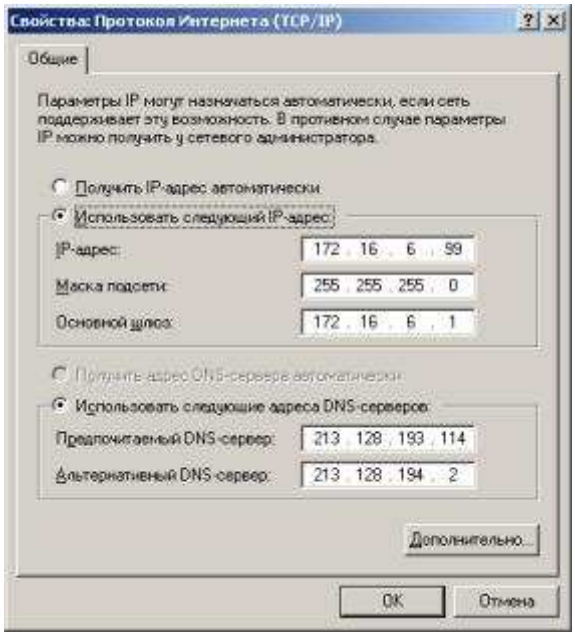
Недостатки:

Статический IP-адрес	Динамический IP-адрес
Параметры необходимо изменять вручную на каждом компьютере в сети. Администратор должен вести учет используемых IP-адресов во избежание конфликтов. Изменение одного или нескольких глобальных параметров IP-сети (например адреса DNS-сервера) требует перенастройки TCP/IP на каждом компьютере.	Необходимо наличие сервера, осуществляющего выделение IP-адресов и передачу параметров настройки протокола TCP/IP. DHCP-сервер, входящий в состав Windows Server, обеспечивающий механизм динамического распределения адресов, требует наличия Active Directory и своей авторизации в домене, что существенно усложняет администрирование сети. Постоянное закрепление за компьютером одного и того же адреса не гарантируется. Существуют определенные трудности при использовании DHCP в сложных маршрутизируемых сетях. Работоспособность рабочих станций с динамическими IP-адресами может быть нарушена при выходе из строя или недоступности DHCP-сервера.

В общем случае статическая адресация удобна в небольших (10-20 компьютеров) одноранговых сетях, состав которых редко изменяется. Если количество компьютеров в сети превышает 20, а компьютеры входят в домен Windows, гораздо проще и удобнее использовать динамическое выделение адресов.

Использование статического IP-адреса

По умолчанию Windows настраивает стек TCP/IP на использование динамически выделяемого IP-адреса. Чтобы использовать статический адрес, это необходимо указать в свойствах протокола TCP/IP. После этого вы должны задать следующие параметры.



IP-адрес - 32-разрядный адрес, представленный в формате W.X.Y.Z. Адрес должен быть уникальным не только в пределах локальной, но и в пределах всего Интернета. Обычно используется один из IP-адресов, выделенный провайдером.

Маска подсети - 32-разрядное число, представленное в формате W.X.Y.Z, которое используется для разделение крупных сетей на несколько более мелких.

Основной шлюз - IP-адрес маршрутизатора, используемого для выхода в глобальные сети и взаимодействия с другими сетями.

Предпочтительный и альтернативный DNS-серверы - IP-адреса основного и резервного DNS-серверов, которые будут использоваться стеком TCP/IP для разрешения символьных имен компьютеров в их IP-адреса.

Настроив параметры протокола, щелкните кнопку ***OK***. Для применения новых параметров TCP/IP щелкните кнопку ***OK*** в окне свойств соединения.

Использование динамически выделяемого IP-адреса

Для использование динамически выделяемого IP-адреса необходимо в настройках протокола TCP/IP указать автоматическое получение IP-адреса. Также рекомендуется указать автоматическое получение адресов DNS-серверов, хотя можно указать эту информацию вручную.

Для динамического выделения IP-адреса в локальной сети должен быть установлен и настроен DHCP-сервер.

При недоступности DHCP-сервера используется служба APIPA (автоматическая настройка частных IP-адресов), которая генерирует IP-адрес вида 169.254.Y.Z и маску подсети 255.255.0.0. Если выбранный адрес уже используется, служба генерирует следующий адрес.

Отключение автоматической адресации

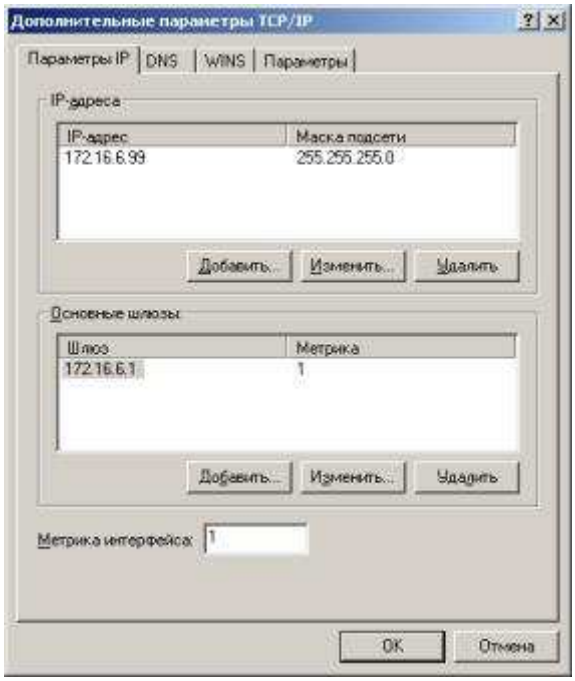
По умолчанию функция автоматической настройки частных IP-адресов включена, но можно ее отключить, добавив в системный реестр соответствующий параметр.

Дерево реестра	HKEY_LOCAL_MACHINE
Раздел реестра	SYSTEM\CurrentControlSet\Services\Tcpip \Parameters\Interfaces\{GUID_адаптера}
Имя параметра	IPAutoConfigurationEnabled
Тип параметра	REG_DWORD
Значение	0 - отключить автоматическую адресацию; 1 - включить автоматическую адресацию

Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

Настройка дополнительных параметров TCP/IP

Стек протоколов TCP/IP в Windows достаточно сложен и позволяет настраивать множество дополнительных параметров. Доступ к ним можно получить, щелкнув кнопку ***Дополнительно*** в окне свойств протокола TCP/IP.



На вкладке ***Параметры IP*** можно связать с сетевым адаптером несколько IP-адресов и задать несколько основных шлюзов.

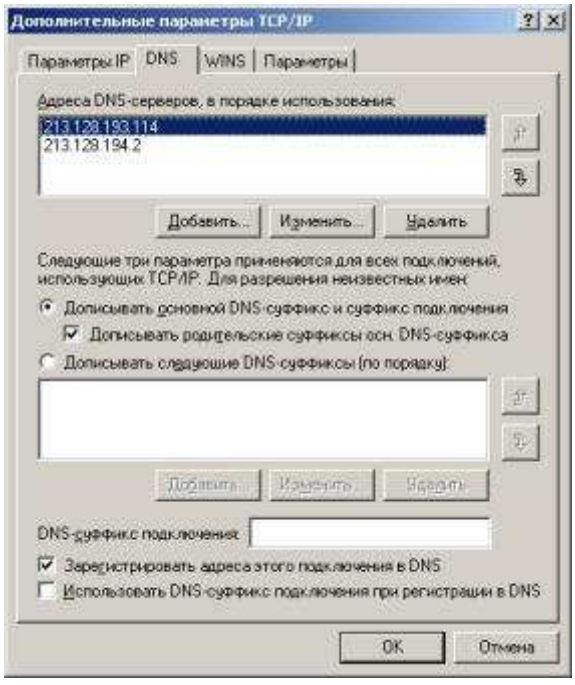
Стек TCP/IP Windows позволяет связать с любым сетевым адаптером несколько IP-

адресов. Для каждого из адресов может быть задана своя маска подсети.

Несколько IP-адресов для одного сетевого адаптера принято использовать в следующих случаях:

- на web и ftp-серверах, обслуживающих большое количество сайтов, каждому из которых должен быть выделен отдельный IP-адрес;
- при подключении компьютера к локальной сети с несколькими наложенными IP-сетями; при постоянном перемещении компьютера из одной сети в другую.

Добавить адрес можно, щелкнув кнопку ***Добавить***. Первый адрес из списка будет считаться основным и отображаться в окне основных свойств протокола TCP/IP. При использовании нескольких IP-адресов, особенно из разных сетей, необходимо указать несколько основных шлюзов, чтобы обеспечить возможность связи с компьютером извне по любому из связанных с ним адресов. Кроме того, для повышения надежности можно использовать несколько маршрутизаторов, соединяющих вашу сеть с другими. В этом случае имеет смысл указать в параметрах адреса нескольких основных шлюзов. Для каждого шлюза кроме его адреса задается метрика - целое число от 1 до 9999. Метрики служат для определения приоритета шлюзов. В любой момент времени используется первый доступный шлюз с минимальной метрикой. Таким образом, альтернативный шлюз с метрикой 2 будет использован только при недоступности основного с метрикой 1.
Кроме того, можно задать метрику и самого интерфейса. Метрики интерфейсов служат для определения интерфейса, используемого для установления нового соединения. При использовании нескольких сетевых адаптеров метрики применяются для определения приоритета этих адаптеров.



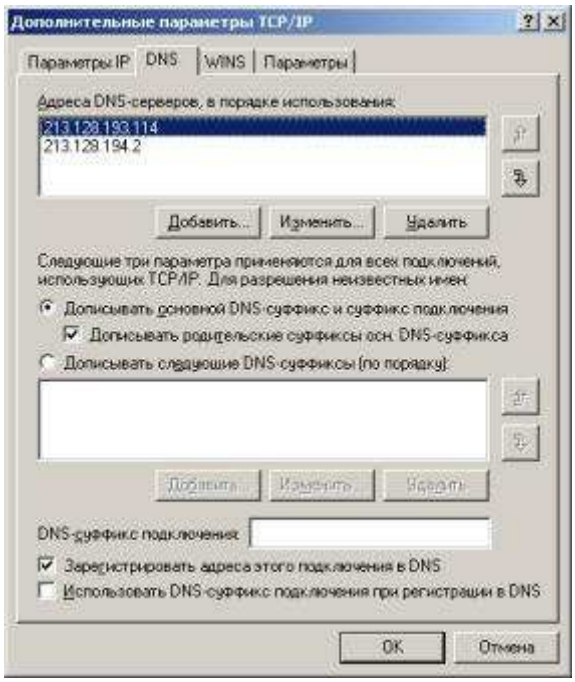
На вкладке ***DNS*** можно настроить все параметры, связанные со службой DNS. По аналогии с IP-адресами можно задать несколько (более двух) адресов DNS-серверов и определить порядок их использования. Метрики для определения порядка здесь не используются, т. к. при недоступности первого сервера будет использован второй, при

недоступности второго - третий и т. д.

В работе DNS используются два параметра, отвечающие за разрешение неполных имен. Первый - основной суффикс DNS - задается на вкладке ***Сетевая идентификация*** свойств системы и обычно является полным DNS-именем домена, в который входит компьютер. При работе в рабочей группе этот суффикс может быть произвольным и задается при настройке Windows. Второй - DNS-суффикс подключения - задается на вкладке DNS свойств каждого подключения.

Если в параметрах настройки DNS указано ***Дописывать основной DNS-суффикс и суффикс подключения***, то при разрешении неполных имен будет использованы соответствующие суффиксы. Например, при использовании основного суффикса **msk.net.fio.ru** и суффикса подключения **lab.msk.net.fio.ru** при вводе команды **ping xyz** будет предпринята попытка разрешения имен **xyz.msk.net.fio.ru** и **xyz.lab.msk.net.fio.ru**. Кроме того, если включен параметр ***Дописывать родительские суффиксы***, то при разрешении будут проверены еще и имена xyz.net.fio.ru, xyz.fio.ru и xyz.ru.

Если в параметрах настройки DNS указано ***Дописывать следующие DNS-суффиксы***, то основной суффикс и суффикс подключения использованы не будут, а будет использован (последовательно) указанный список суффиксов. При разрешении неполных имен этот список будет использован аналогично приведенному примеру. Параметр ***Зарегистрировать адреса этого подключения в DNS*** использует основной DNS-суффикс для определения DNS-сервера, обеспечивающего функционирование соответствующей зоны, и автоматически регистрирует на нем запись A со своим именем и IP-адресом соединения. Если для соединения задано несколько IP-адресов или используется несколько соединений, то в DNS будут зарегистрированы несколько записей A с одним и тем же именем, но разными IP-адресами. Параметр ***Использовать DNS-суффикс подключения при регистрации в DNS*** позволяет осуществить регистрацию соответствующей записи A на DNS-сервере по аналогии с предыдущим параметром.

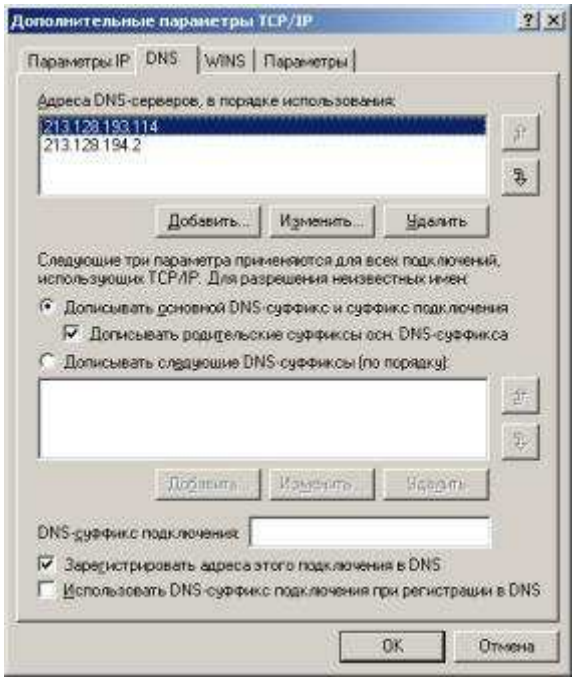


На вкладке ***WINS*** можно настроить параметры, связанные со службой WINS. Эта

служба предназначена для разрешения имен NetBIOS в IP-адреса. При использовании домена и клиентов Windows использование этой службы не требуется - все ее функции выполняются службой DNS.

Для работы этой службы требуется WINS-сервер, адрес (адреса) которого добавляется в соответствующий список.

Помимо использования WINS-сервера Windows поддерживает устаревший способ разрешения имен NetBIOS- файл LMHOSTS. Можно включить использование этого файла и при необходимости импортировать уже существующий файл. Файл LMHOSTS можно редактировать самостоятельно в любом текстовом редакторе. Этот файл расположен в папке **%systemroot%\ system32\drivers\etc**. Кроме того, на этой вкладке осуществляется управление поддержкой NetBIOS поверх TCP/IP. Такая поддержка требуется для обеспечения совместной работы со старыми NetBIOS-клиентами (Windows 9x, NT). При использовании в локальной сети только Windows, NetBIOS поверх TCP/IP может быть отключен. При использовании динамически выделяемого IP-адреса можно задавать этот параметр через DHCP.



На вкладке ***Параметры*** можно настроить ряд необязательных параметров стека TCP/IP. Windows поддерживает настройку IP-безопасности (протокол IPSec) и фильтрации TCP/IP. Для настройки необходимо выбрать параметр из списка и щелкнуть кнопку ***Свойства***.

Безопасность компьютеров в сети

Проблемы безопасности при работе в сети могут быть решены на уровне аппаратных средств *(аппаратная безопасность),* на уровне программного обеспечения *(программная безопасность)* и на уровне проведения определенных организационных мероприятий *(логическая безопасность).*

Вопросы общей безопасности компьютера

Как правило, говоря о безопасности при работе в Internet, выделяют три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании.

Следует отметить, что достичь полной безопасности вряд ли возможно, так как методы атак развиваются вместе с развитием методов защиты. Но максимально снизить вероятность поражения компьютерной системы и находящейся в ней информации вполне возможно.

Первая угроза – угроза **раскрытия или утечки информации**. Угроза раскрытия заключается в том, что информация становится известной посторонним лицам. Причиной возникновения данной угрозы может быть как прямое несанкционированное подключение стороннего лица через Internet к Вашему компьютеру, так и результат работы некоторых программ, созданных с этой целью (и вирусов тоже). Реализация именно этой угрозы наносит наибольший ущерб. Чаще всего, интересуются Вашим логином и паролем на доступ в Internet. Но ещё более опасно воровство конфиденциальной информации. Если Вы недостаточно надежно "закрыли", хранящиеся на компьютере договора или финансовую информацию, то существует вероятность, что знать её будете не только Вы. Другой способ получения информации из Вашего компьютера - использование программ класса keyboard loggers (программа записывает все, что вводится с клавиатуры, а затем, при очередном сеансе связи, передает записанную информацию "заказчику").

Угроза **потери целостности** информации - любое умышленное изменение или удаление данных, но особенно ощутимо затрагивает пользователя в случае полного уничтожения информации. Основной источник этого вида угроз - вирусы. Попасть на Ваш компьютер вирус может с письмом из электронной почты, с программой, которую Вы взяли из сети, в некоторых случаях с файлами, полученными с других серверов (например, с прайс-листом в формате Excel). Но и при несанкционированном подключении к Вашему компьютеру, злоумышленник может "пошутить" и уничтожить некоторые Ваши файлы. Другой вариант - преднамеренное искажение информации, размещенной на Вашем сайте (сервере).

Угроза **отказа в обслуживании** возникает в том случае, когда в результате некоторых действий блокируется доступ к ресурсам компьютера. В принципе блокирование может быть временным или постоянным. Временная блокировка может вызвать только задержку запрашиваемого ресурса, иногда достаточно долгую. Во втором случае, запрашиваемый ресурс вообще становится недоступен.

Виды программ-паразитов

Хотя некоторые пользователи часто называют любую вредную программу вирусом, специалисты по безопасности знают, что это не так. Вот краткое описание трех наиболее распространенных видов "зловредных" программ:

Вирус (virus) представляет собой самовоспроизводящийся код, присоединяющийся к другому файлу точно так же, как настоящие вирусы прикрепляются к живым клеткам. Изначально вирусы поражали программные файлы, имеющие расширения *.com или *.exe, однако на сегодняшний день могут "заражаться" и офисные документы, и даже, сообщения электронной почты.

"Червь" (worm) - это автономная программа, обычно воспроизводящаяся путем копирования себя на другие компьютеры в сети. Наибольшее распространение получила программа happy99.exe, парализовавшая множество компьютеров два года назад и все еще изредка появляющаяся - особенно под Новый год.

"Логическая бомба" (logic bomb) не воспроизводится, но может принести серьезный ущерб. Обычно это простые программы, выполняющие вредные функции, такие, как удаление пользовательских файлов, форматирование дисков на вашем компьютере, порча загрузочной записи, делающая недоступной любую информацию с Вашего

компьютера при выполнении определенного условия (например, по случаю наступления к-л праздника: Новый год, Первое Апреля и т.п.).

Защита личной информации при работе в сети

Полностью защитить свой компьютер от возможных атак из сети практически невозможно. Но можно принять определенные меры предосторожности и соблюдать некоторые правила при работе в Internet. Это не ликвидирует полностью, но существенно снизит вероятность успешной атаки или заражения вирусом.

Защита от вирусов.

- Регулярно используйте программы-антивирусы для проверки своего компьютера. (Наиболее известные среди них - AVP Лаборатории Касперского,DrWEB, Norton Antivirus фирмы Symantec);
- Внимательно читайте предупреждения, которые выдает вам система - в большинстве случаев при запуске исполняемого файла вам будет выдано соответствующее сообщение;
- Работая с электронной почтой, не запускайте полученные программы и не открывайте прикрепленные файлы, так называемые "вложения", если Вы не уверены в отправителе. Уважающая себя (и своих потенциальных клиентов) фирма, даже если она присылает Вам рекламу, разместит свои материалы в зоне "сообщение" или даст ссылку на свой сервер;
- Не скачивайте без крайней необходимости на свой компьютер прайс - листы в формате Excel. Таким путем Вы тоже можете получить вирус. Но если это все же необходимо, то всегда используйте программы - антивирусные мониторы, которые постоянно проверяют всю поступающую на Ваш компьютер информацию на предмет возможного наличия вирусов;
- Не открывайте "чужие" документы с помощью редактора WordPad, который поставляется вместе с Windows. Программа не чувствительна к вредоносным макросам (как и ко всем макросам вообще), но содержит ошибки, приводящие к переполнению буфера и вытекающей отсюда возможности передачи управления на код злоумышленника. Не ограничивайтесь собственной защитой Word-a от макросов, поскольку данная защита не всегда работает и может быть легко отключена злоумышленником.

Пароли.

При выборе компьютерного пароля многие из нас слишком предсказуемы.

Специалисты по системам защиты уже давно указывают на то, что большинство брешей в компьютерных системах хакеры проделывают только потому, что пользователи берут слишком простые пароли. Далее по популярности использования идут специальные хакерские программы, которые легко можно скачать из Internet. Эти программы могут взломать пароль, автоматически перебирая целые словари.

Какой из всего этого следует вывод? Нельзя в качестве пароля брать "осмысленные" слова. В пароле по возможности должны одновременно присутствовать прописные и строчные буквы, цифры и знаки препинания.

Пароль должен быть не менее восьми символов и быть составлен из прописных, строчных, специальных и цифровых символов одновременно.

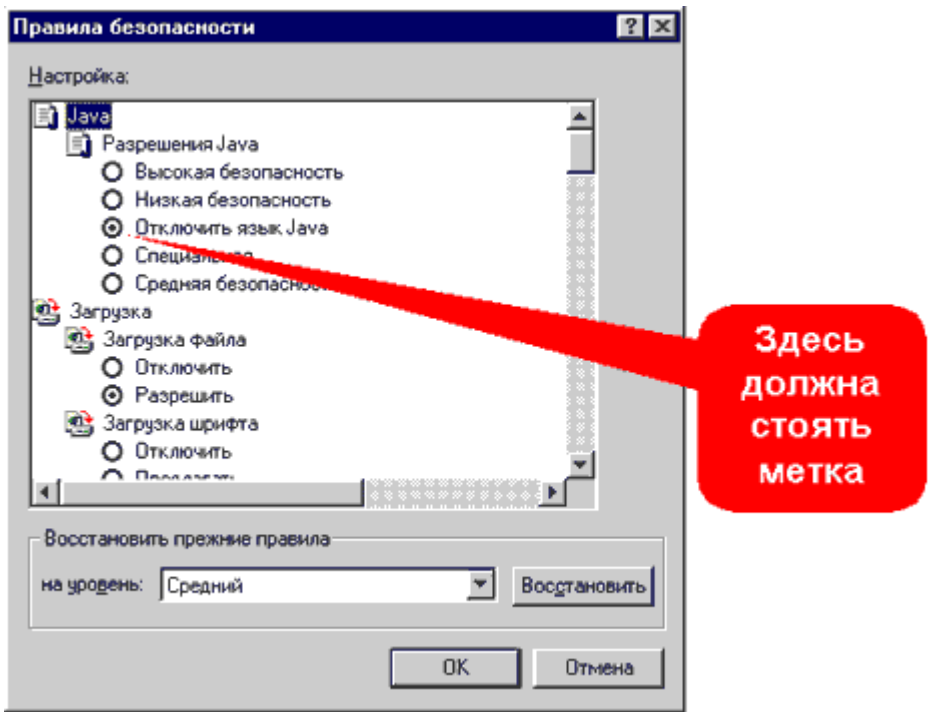
Пример правильного задания пароля: **3Urtf_J5p**
В этом примере используются цифры **"3", "5",** заглавные буквы **"U", "J",** строчные символы **"r", "t", "f", "p"** и специальный символ подчеркивания "_".

На каждое отдельно взятое устройство, системный счет или другой ресурс необходимо установить неодинаковые и несхожие пароли, не являющиеся синонимами, а также простыми словосочетаниями или словами. Кстати, при использовании PGP (программы криптографической защиты) даже при перехвате вашей почты воры не смогут ее прочитать, не имея Вашего ключа, который при получении Вашего пароля на Ваш компьютер можно легко узнать.

Защита от взлома.

- Не стремитесь использовать новые версии программного обеспечения: в первое время в них всегда обнаруживается много ошибок. Это не значит, что продукты одно-двух годичной давности защищены лучше, но злоумышленники склонны сосредотачивать свои усилия именно на новинках, а анализировать старые версии - занятие неблагородное и бесперспективное: у кого они сейчас установлены?
- Постарайтесь не использовать, без крайней необходимости, неизвестные программные файлы из Internet. Если вы ищете какую-то программу - делайте это на серверах известных компаний;
- Не забывайте, что технологии java, JavaScript и Active-x (языки программирования на которых создаются динамические объекты Internet-страниц) остаются небезопасными;

  Основная опасность состоит в том, что написанные с использованием данных языков объекты, могут при желании их создателя получить полный доступ к ресурсам вашего компьютера. При этом, Вы не сможете проконтролировать, что же они делают, какую информацию и где меняют, что записывают на ваш компьютер или что списывают с него.
  Именно поэтому, лучше отключить данные приложения в настройках браузера ***(Пуск / Настройки / Панель управления / Свойства обозревателя / Безопасность):***



- *На сегодняшний день все современные операционные системы позволяют включить свой компьютер в Internet, в качестве WWW-сервера. Если компьютер с разделенным диском и не закрытым паролем доступом к нему окажется в сети, то при желании к Вашему диску получит доступ любой "сетевой житель".*
- Если на вашем компьютере установлен протокол TCP/IP, ликвидируйте "Службу доступа к файлам и принтерам" (Пуск/Настройки/Панель управления/Сеть). Если же Вы выходите в Internet через локальную сеть своего предприятия и исключение данной опции невозможно, то убедитесь, что Ваш сетевой администратор предпринял необходимые меры защиты сети от несанкционированного доступа извне;
- Узнать о возможных несанкционированных подключениях к Вашему компьютеру поможет программа Netstat. В результате работы она выдаёт информацию обо всех активных подключениях к компьютеру с указанием ip-адреса удалённого компьютера и порта, по которым происходит взаимодействие;
- Во время работы с конфиденциальной информацией лучше всего отключиться от сети.

Основы адресации в Internet

Зачастую в решении многих проблем, связанных с безопасностью, может помочь знание правил адресации в сети. Это помогает выявить источник происхождения угрозы (адрес с которого производится попытка нарушения безопасности). Остановимся на этом моменте подробнее.

Основа адресации в Internet - протокол tcp/ip, который позволяет различным компьютерам в сети обмениваться информацией.

Все адреса в Internet начинаются либо с *http://* либо с *ftp://*. Этот параметр

определяет метод передачи информации - протокол передачи данных:

- Hyper Text Transfer Protocol (HTTP) - протокол передачи гипертекста;
- File Transfer Protocol (FTP) - протокол передачи файлов.

При подключении к Internet, каждый компьютер получает уникальный 32-х битный номер, который и называют ip-адресом. Он представлен в виде 4-х чисел в диапазоне от 1 до 255 и имеет вид типа 194.125.113.85. Ip-адрес может быть динамическим - т.е. меняться при каждом подключении.

Очень важно понимать, что знание ip-адреса подключенного к сети компьютера, дает возможность доступа к нему из сети с любого другого компьютера. Таким образом, не только Вы можете получить информацию с сетевого сервера, но и любой компьютер, подключенный к Internet, может получить доступ к информации на Вашем диске. Конечно, если Вы не предпримете некоторых мер, направленных на ограничение этого доступа.

В общем случае, адрес имеет вид www.что-то.где-то. Аббревиатура в конце адреса это сокращенное название страны:

- RU - Россия;
- US - Соединенные Штаты;

и т.д.

Но иногда адрес может иметь и другой вид - *www.что-то.чье-то.* В этом случае "чье-то" определяет принадлежность сервера:

- COM - коммерческие организации;
- MIL - военные организации;
- GOV - правительственные;
- ORG - некоммерческие учреждения;
- NET - административные компьютеры Интернет.

Web: кажущаяся анонимность

Достаточно часто, начинающие пользователи понятие анонимности в Internet связывают с анонимностью личности человека, в сети работающего. То есть, зарегистрировал почтовый ящик на вымышленное имя или зашел в чат поговорить под произвольным псевдонимом, и все - анонимность достигнута. На самом деле это не совсем так. Как бы Вы себя ни называли ip-адрес сообщит - здесь был или есть один и тот же человек, а вернее один и тот же компьютер.

"Гуляя" по WWW-страницам, многие не задумываются о том, что при каждом посещении "умница" сервер фиксирует некоторую информацию о Вас в своих log-файлах. Это может быть и ip-адрес, и другие, необходимые web-мастеру сведения.

Основной источник подобных сведений - программы, которые Вы используете при работе в Internet. Практически все программы, при помощи которых Вы получаете

из Internet какую-либо информацию, предварительно сообщают свои, а следовательно, и Ваши данные, т.е. некоторые сведения, которые определяют какую именно информацию, куда и как необходимо отправить - это тот минимум, без которого невозможен процесс обмена информацией. Но максимум передаваемых при запросе сведений никак не ограничен.

Например, браузер - сообщает серверу, с какого ip-адреса вы вошли в сеть, на какой странице были перед этим, каким браузером пользуетесь.

Ip-адрес сообщают и программы для работы с электронной почтой. Например, OutLook Express предоставляет возможность узнать адрес отправителя.

Наибольшие же проблемы создают разнообразные программы для интерактивного общения. Большинство из них позволяет получить достаточно большое количество информации о пользователе - от самого факта его нахождения в сети и ip-адреса до типа операционной системы. Правда, некоторые (MS Comic Chat либо ICQ) скрывают ip-адрес собеседника. Но если Вы общаетесь "один на один", соединение устанавливается непосредственно между компьютерами. В этом случае, используя, например, стандартную программу Netstat каждый из собеседников может определить сетевой адрес другого.

Итак, что можно узнать о Вас, не задав ни одного вопроса и не устанавливая на Ваш компьютер свои программы (эта возможность, естественно, даст еще больший эффект)?

Непосредственная информация о пользователе:

- Местонахождение (страна, фирма, провайдер Internet и пр.);
- Тип Вашего компьютера;
- Разрешение экрана;
- Местное время (по часам Вашего компьютера);
- Операционную систему, установленную на компьютере;
- Тип и версию программы, из которой Вы обратились к серверу;
- Наличие цифрового удостоверения (сертификата) и из него - регистрационные данные;

Информация о пользователе, связанная с посещаемым ресурсом.

В основном, данная информация используется при проведении маркетинговых исследований популярности разделов самого ресурса:

- Работаете ли Вы с того же самого (физического) компьютера, что и в прошлый раз;
- Какие именно страницы или файлы Вы получили (или регулярно забираете) с сервера;
- По каким ссылкам "ходите" на данном сервере;
- Какую страницу смотрели до того, как попали на данный сервер;
- Какие вопросы задаете их поисковой системе;
- На какие бюллетени (списки почтовой рассылки) подписаны;

Много этой информации или мало? Кто-то решит, что нет ничего особенного в передаче "какой-то" рабочей или маркетинговой информации о собственном

компьютере или о своих предпочтениях при перемещениях по сети. Это если Вы - школьник, студент или пенсионер. А если сотрудник или владелец фирмы? Конечно, зная реальный адрес местонахождения компьютера, с которого осуществляется вход в сеть еще нельзя сказать, кто конкретно за ним сидит. Но, пронаблюдав за пользователем некоторое время, можно составить очень точный его портрет (вернее, "портрет" его интересов), для уточнения которого останется лишь сопоставить ему реальное имя пользователя...

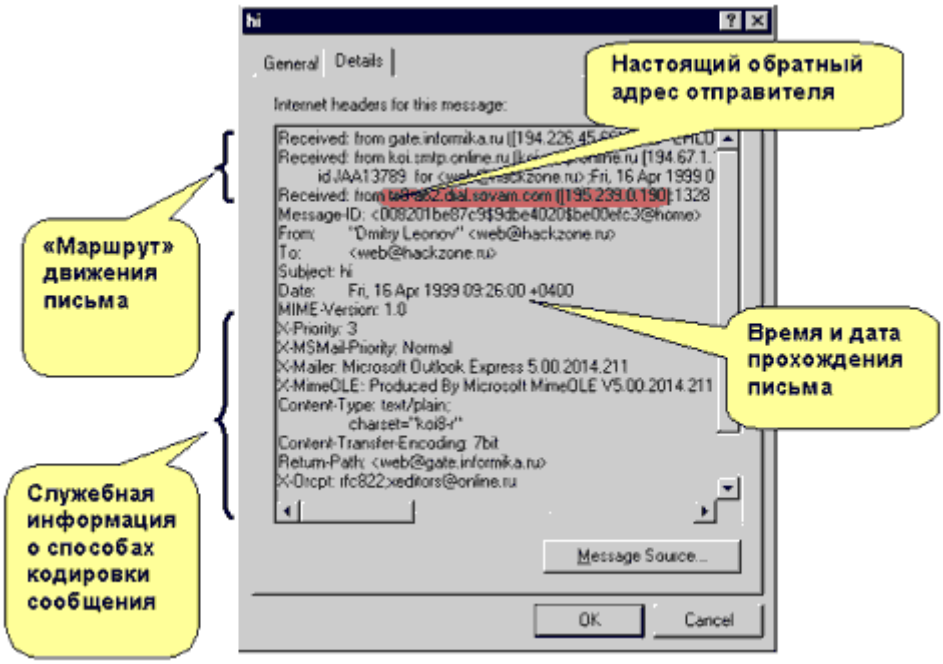
Использование электронной почты

К сожалению, технология обеспечения обмена информацией по электронной почте также предоставляет массу возможностей получить информацию о Вас так, что, будучи неподготовленным пользователем, Вы можете об этом даже и не знать. Поэтому мы рассматриваем данный вопрос здесь несколько подробнее.

Механизм работы с электронной почтой достаточно понятен - у Вас есть электронный почтовый ящик, Вы получаете или отправляете сообщения с помощью специальных программ "мейлеров". Наиболее известная из таких программ - OutLook Express, которая встроена в Windows и потому достаточно часто используются. При организации почтового ящика возможны два варианта: почтовый ящик предоставляет Вам провайдер либо Вы создаете его на одном из бесплатных почтовых сервисов. Работать с почтой так же можно по-разному. Наиболее небезопасно работать на страничках почтовых служб в браузере. Более предпочтительный вариант - использовать программы мейлеры.

При организации своего почтового ящика, Вам будет необходимо указать пароль. Остановимся несколько подробнее на вопросе - как должен выглядеть пароль, чтобы его было труднее "сломать"? Основная рекомендация выглядит следующим образом: делайте пароль длиннее 8-ми символов и используйте цифры и символы разного регистра. Обратите внимание, что пароль не должен совпадать с логином. Кроме того, не рекомендуется использовать цифровые или короткие пароли, а так же не стоит в качестве пароля выбирать имена или распространенные слова.

Метод перехвата пароля основан на том, что пользователь, обращаясь к серверу (для прочтения почты, подключения к личной папке и т. д.), должен передать ему свой пароль, который, естественно, идет по самому обычному кабелю в виде самых обычных электрических импульсов. По этой причине, основное внимание при установлении "закрытой" связи уделяется не столько ограничению возможности перехватить сигнал (хотя и это, конечно, тоже важно учитывать, хотя бы на участке от Вашего компьютера (офиса) до точки ввода кабеля в общую магистраль передачи информации), сколько ограничению возможности понять, что именно Вы передаете (или принимаете), т.е. механизму шифрования информации. Более подробное изучение данного вопроса относится к компетенции специалистов в области сетевых коммуникаций, для рядового пользователя отметим лишь, что почтовые пароли относительно безопасно передавать, установив опцию **Secure Password Authentification (SPA)** *(безопасное подтверждение пароля)*. Теперь давайте посмотрим, какую информацию об отправителе сообщения можно получить с помощью программы Outlook Express. Так, ip-адрес отправителя письма можно считать из его заголовка (в Outlook Express для этого достаточно выбрать пункт меню File->Properties при просмотре сообщения):



Кстати, очень полезно заглянуть туда, чтобы убедиться в том, что ваш корреспондент - действительно тот, за кого себя выдает. Там же можно проследить весь маршрут движения письма от отправителя к адресату, включая время отправления, время прохождения промежуточных почтовых серверов и время поступления сообщения на сервер Вашего провайдера.

Присоединение к рабочей группе или создание рабочей группы

При настройке сети системой Windows автоматически создается рабочая группа, которой присваивается имя. Можно как присоединиться к уже существующей рабочей группе в сети, так и создать новую.

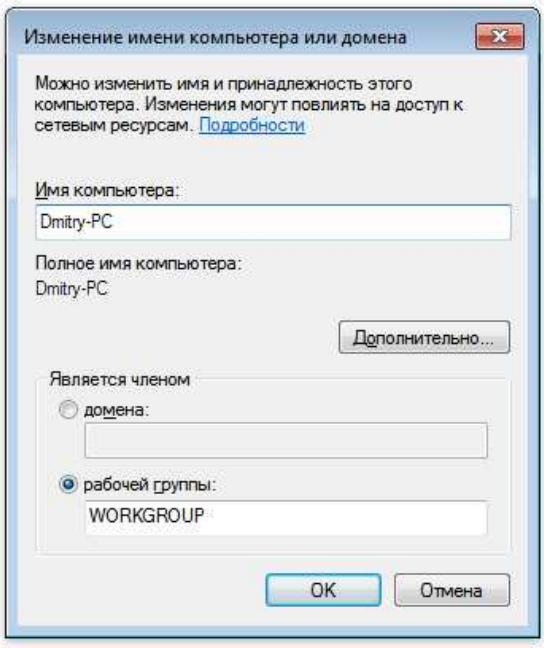
Примечание.

Рабочие группы служат основой для общего доступа к файлам и принтерам, но не осуществляют фактическую настройку общего доступа. Напротив, в этой версии Windows можно создать и присоединиться к домашней группе, которая автоматически включает общий доступ к файлам и принтерам домашних сетей. При наличии домашней сети рекомендуется создать домашнюю группу или присоединиться к ней. Чтобы получить дополнительные сведения, произведите поиск по слову «домашняя группа» в центре справки и поддержки.

1. Откройте компонент «Система». Для этого нажмите кнопку **Пуск**, щелкните правой кнопкой мыши **Компьютер** и выберите пункт **Свойства**.
2. В группе **Имя компьютера, имя домена и параметры рабочей группы** нажмите кнопку **Изменить параметры**. Если отображается запрос на ввод пароля администратора или его подтверждения, укажите пароль или предоставьте подтверждение.
3. В диалоговом окне **Свойства системы** перейдите на вкладку **Имя компьютера** и затем нажмите кнопку **Изменить**.
4. В диалоговом окне **Изменение имени компьютера или домена** щелкните в

разделе **Член групп** пункт **Рабочая группа** и выполните одно из следующих действий.

- Чтобы присоединиться к существующей рабочей группе, введите имя рабочей группы, к которой будет присоединен компьютер, а затем нажмите **ОК**.
- Чтобы создать новую рабочую группу, введите имя новой рабочей группы, а затем нажмите **ОК**.



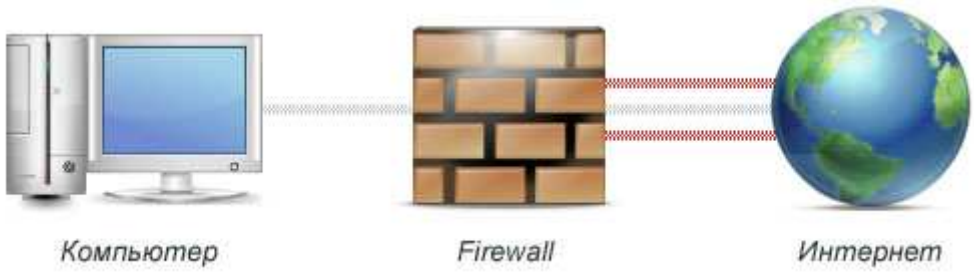
Если перед присоединением к рабочей группе компьютер входил в домен, то он будет удален из него, а учетная запись компьютера в домене будет отключена.

Firewall.

Firewall в переводе с английского означает горящая стена *(fire - огонь, wall - стена)*, также часто можно встретить название фаервол (это обозначение firewall только русскими буквами) или Brandmauer это в переводе с немецкого значит тоже самое *(brand - гореть, mauer - стена)*, наиболее часто употребляется как брандмауэр. В народе очень часто firewall называют просто стена или стенка.

Итак, давайте попробуем разобраться, что же такое firewall и зачем он нужен. Представьте себе, что ваш компьютер это ваша квартира. В квартире есть окна и двери. Я уверен, что все окна и двери вы держите на замке и не думаю, что вы были бы довольны, если бы каждый прохожий мог бы зайти к вам через открытую дверь или влезть через открытое окно. По аналогии, вы должны быть заинтересованы в том, чтобы никто чужой не смог просто так войти в ваш компьютер и взять что ему захочется или удалить какие-нибудь важные для вас данные.

На окнах и дверях вашего дома есть замки, вы запираете их и чувствуете себя в безопасности. Если вам нужно выйти или впустить к себе знакомого, вы открываете двери и впускаете или выпускаете нужных вам людей. Установив фаервол, вы можете настроить его таким образом, чтобы он пропускал в интернет или запускал из интернета только те программы, которые вы ему разрешите. Все остальное будет блокировано как на вход так и на выход.



Фактически вы ставите фильтр между вашим компьютером и интернет, который пропускает только нужное и важное для вас, все остальное фильтруется.

Согласно статистике, компьютер, на котором не установлен firewall и который находится в сети, остается не зараженным максимум 2 минуты. По истечении этого времени вы обязательно получите свою порцию вредоносных программ. Не стоит бояться процедуры установки и настройки, хотя этот тип программ и нельзя назвать простым, большинство из них настраиваются автоматически. Вам нужно будет лишь нажимать на кнопку разрешить или запретить доступ определенной программе.

Настройка сетевого экрана

Если вы хотите использовать на своем компьютере сетевой экран Microsoft Firewall, его надо включить. Сетевой экран Microsoft Firewall включается следующим образом. В главном меню Windows выбрать Settings ==> Control Panel (см. Рис. 1), затем в открывшемся окне <Control Panel> найти и открыть окно сетевого экрана двойным щелчком по значку Windows Firewall (см. Рис. 2).

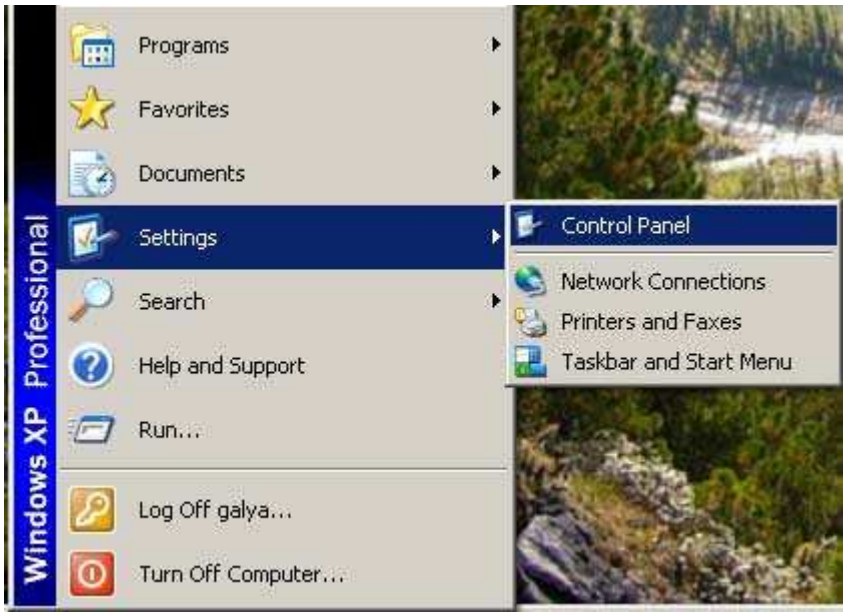


Рис. 1

Рис. 2

Во вкладке **General** окна <Windows Firewall> включить опцию **On (recommended)** и, таким образом, включить работу сетевого экрана Microsoft Firewall (см. Рис. 3). Далее выполняется настройка сетевого экрана. Чтобы настройки соответствовали требованиям Регламента, надо разрешить следующее сетевые взаимодействия:

- Разрешить *ping*-тестирование вашего компьютера;
- Разрешить доступ к вашему компьютеру по протоколу HTTP для программ пакета BotikTools.

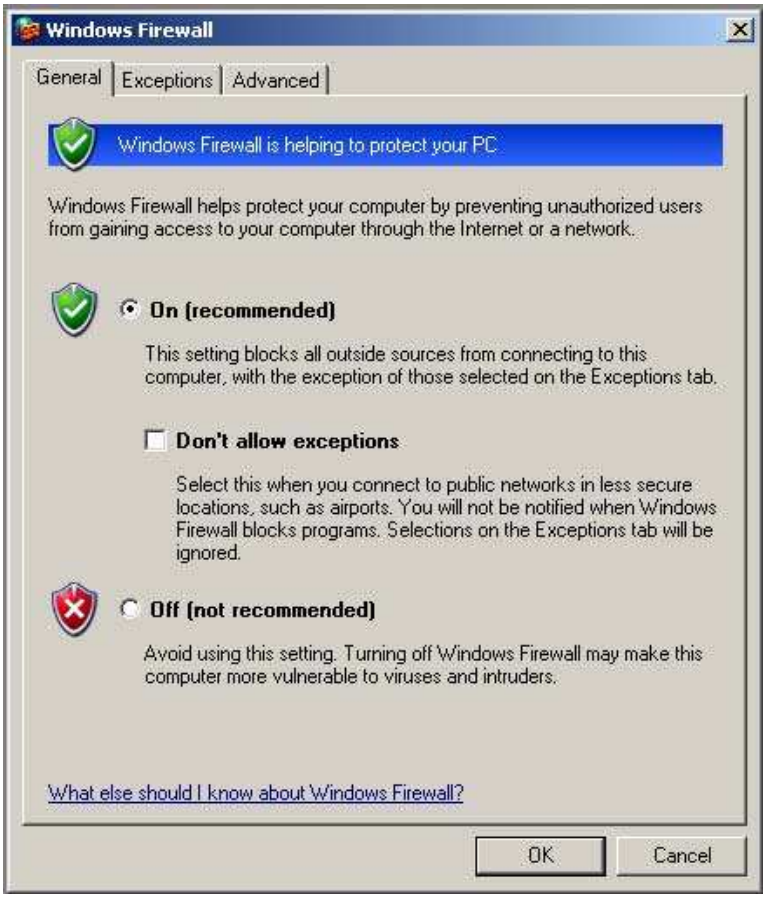


Рис. 3

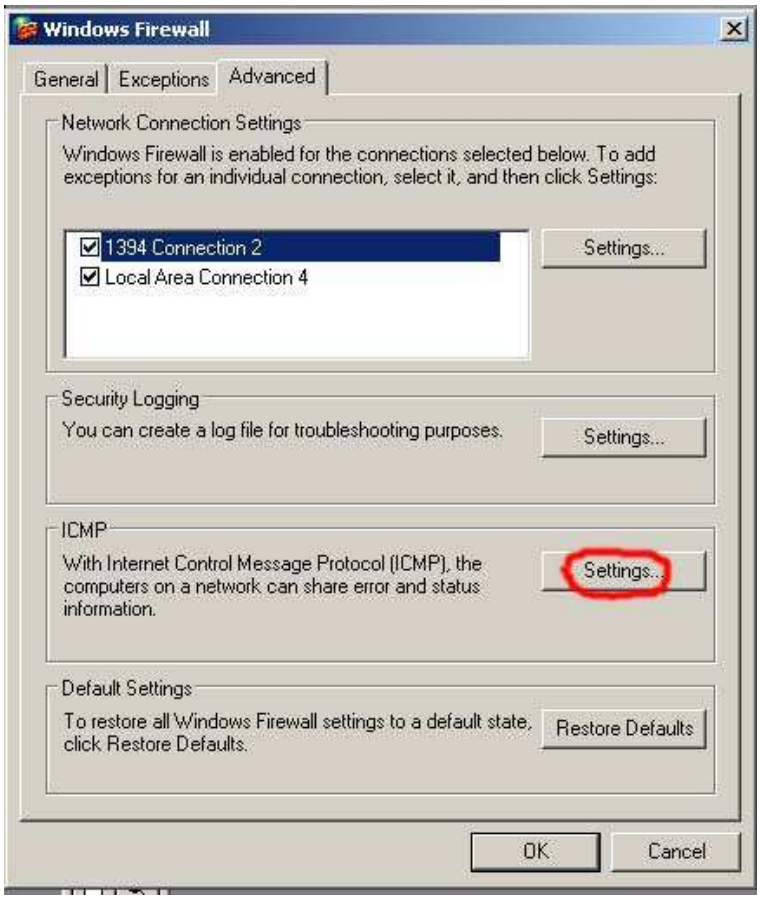


Рис. 4

Во вкладке Advanced окна <Windows Firewall> (см. Рис. 4) щелкнуть Settings в разделе ICMP (отмечено красным на Рис. 4). В открывшемся окене <ICMP Settings> установить флаг Allow incoming echo request (см. Рис. 5) и щелкнуть OK. Теперь ваш компьютер доступен для *ping*-тестирования.

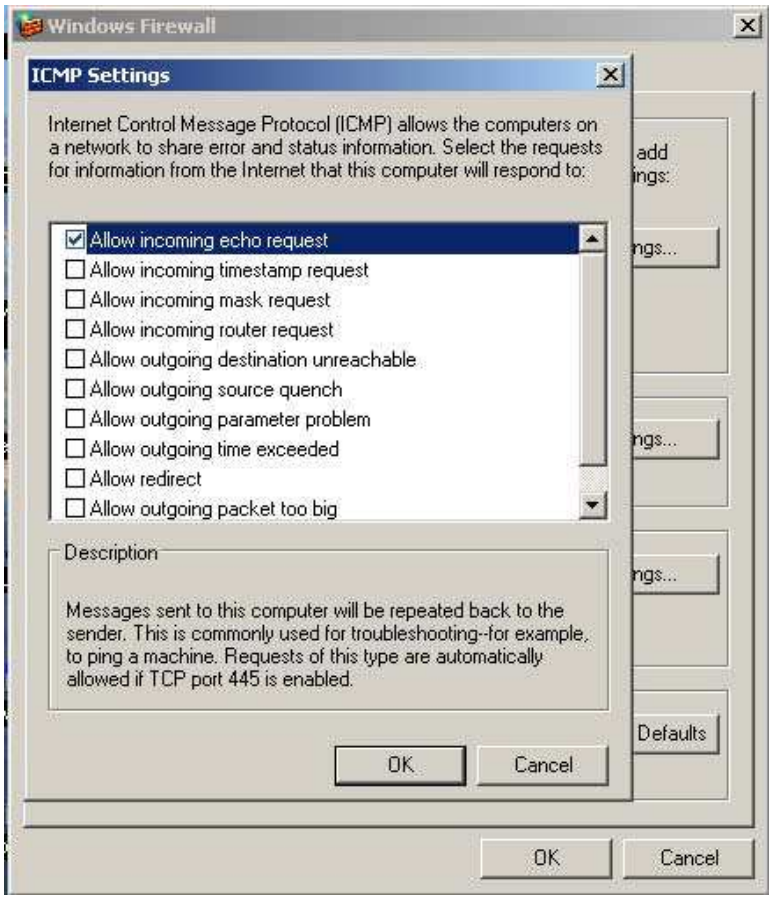

Windows Firewall
ICMP Settings
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:
Allow incoming echo request
Allow incoming timestamp request
Allow incoming mask request
Allow incoming router request
Allow outgoing destination unreachable
Allow outgoing source quench
Allow outgoing parameter problem
Allow outgoing time exceeded
Allow redirect
Allow outgoing packet too big
Description
Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting--for example, to ping a machine. Requests of this type are automatically allowed if TCP port 445 is enabled.
OK
Cancel
Defaults
OK
Cancel

Рис. 5

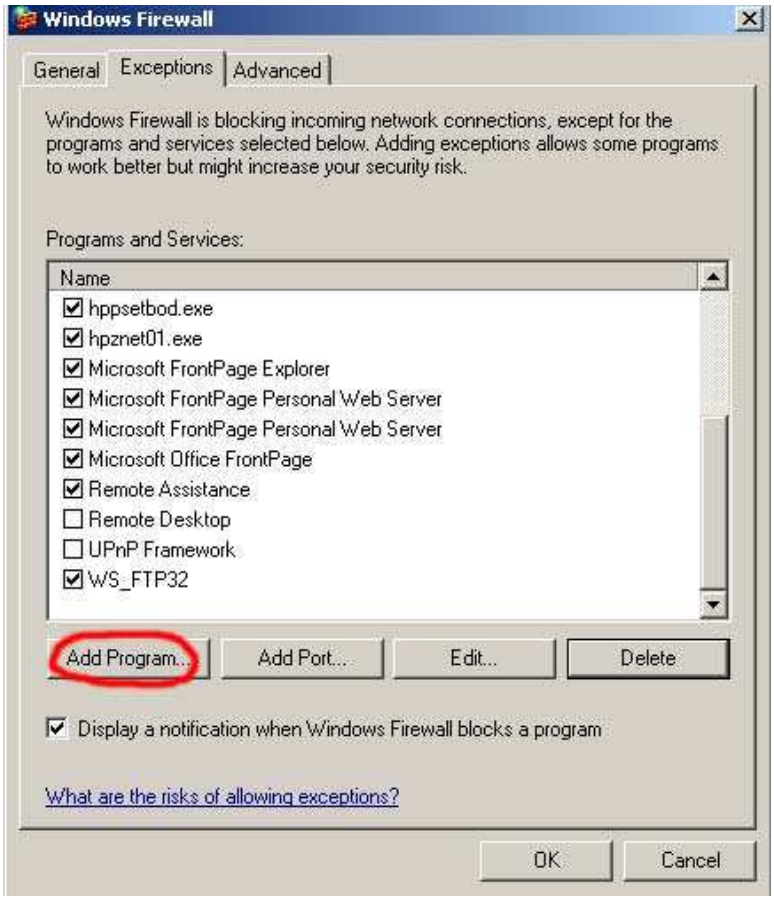

Windows Firewall
General
Exceptions
Advanced
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.
Programs and Services:
Name
hppsetbod.exe
hpznet01.exe
Microsoft FrontPage Explorer
Microsoft FrontPage Personal Web Server
Microsoft FrontPage Personal Web Server
Microsoft Office FrontPage
Remote Assistance
Remote Desktop
UPnP Framework
WS_FTP32
Add Program...
Add Port...
Edit...
Delete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK
Cancel

Рис. 6

Настройка разрешения доступа по протоколу HTTP для программ пакета BotikTools

Сетевой экран блокирует входящие сетевые соединения с программами, которые установлены на вашем компьютере. Тем самым обеспечивается защита от несанкционированного доступа. Для корректной работы некоторых программ (в том числе программ пакета BotikTools) необходимо сделать исключение и разрешить возможность таких соединений. Эти программы перечислены во вкладке **Exceptions** (Исключения).

В окне <Windows Firewall> выберите вкладку **Exceptions** (см. Рис. 6). Здесь перечислены программы и сервисы, которым разрешены входящие соединения по протоколу HTTP. В число этих программ надо включить программу *wish.exe*, которая обеспечивает сетевые соединения для программ пакета BotikTools. Для этого щелкните **Add Program...** (на Рис. 6 отмечено красным). В открывшемся окне <Add a Program> (см. Рис. 7) щелкните**Browse**, чтобы указать путь к программе *wish.exe*. Если вы установили программы пакета BotikTools в папку Program Files, то путь к программе *wish.exe* будет таким, какой показан на Рис. 7.

Рис. 7

Рис. 8

На Рис. 8 показано стандартное окно <Browse> папки C:\Program Files\BotikTools\bin, в которой хранится программа *wish.exe*. Отметив программу *wish.exe*, щелкните Open в окне <Browse> и, таким образом, введите путь к программе *wish.exe* в поле Path окна <Add a Program>. В окне <Add a Prograam> щелкните OK, чтобы добавить программу *wish.exe* в список Exceptions. Теперь сетевой экран разрешит доступ по протоколу HTTP программам пакета BotikTools.

Настройка сетевого экрана Outpost Firewall

Персональный сетевой экран Outpost Firewall позволят создавать более подробные настройки для ограничения сетевого доступа на уровне приложений. В Outpost Firewall пользователь может создавать списки приложений, имеющих сетевой доступ и указывать действующие протоколы, порты и направления сетевого трафика для каждого из приложений, то есть создавать для приложений правила, разрешающие или запрещающие приложениям те или иные сетевые взаимодействия.

Что настроить?

Чтобы разрешать использование программы *ping.exe* для проверки связи с компьютером Абонента, а также обеспечить корректную работу программ, входящих в состав пакета BotikTools, сетевой эран Outpost Firewall должен быть настроен так, чтобы:

1. разрешать входящие и исходящие TCP-пакеты для приложения *wish.exe* (*C:\Program Files\Botik Tools\bin\wish.exe*) через порты 9, 25, 53, 80, 443, 12040;

2. разрешать входящие и исходящие UDP-пакеты для приложения *wish.exe* через порт 53;
3. разрешить ICMP Эхо-запрос и ICMP Эхо-ответ для приложения *tping.exe*, входящего в состав BotikTools (*C:\Program Files\Botik Tools\bin\tping.exe*);
4. разрешить ICMP Эхо-запрос и ICMP Эхо-ответ для встроенных в Windows приложений *ping.exe* и *tracert.exe* (*C:\Wondows\system32\ping.exe и C:\Wondows\system32\tracert.exe*).

Как настроить?

Далее опишем для примера, как создать правило для приложения *wish.exe*, разрешающее передачу исходящих TCP-пакетов через порты 9, 25, 53, 80, 443, 12040. Остальные правила для приложения *wish.exe*, описанные в разделе "**Что_настроить?**", могут быть созданы аналогично.

1. Сначала надо добавить приложение *wish.exe* в список пользовательских приложений, для которых будут создаваться правила. Для этого в меню **Параметры** программы Outpost Firewall надо выбрать **Приложения** (см. Рис. 9), чтобы открыть в окне <Параметры> вкладку **Приложения** (см. Рис. 10). Выбрав **Пользовательский уровень** во вкладке **Приложения**, щелкнуть **Добавить**.

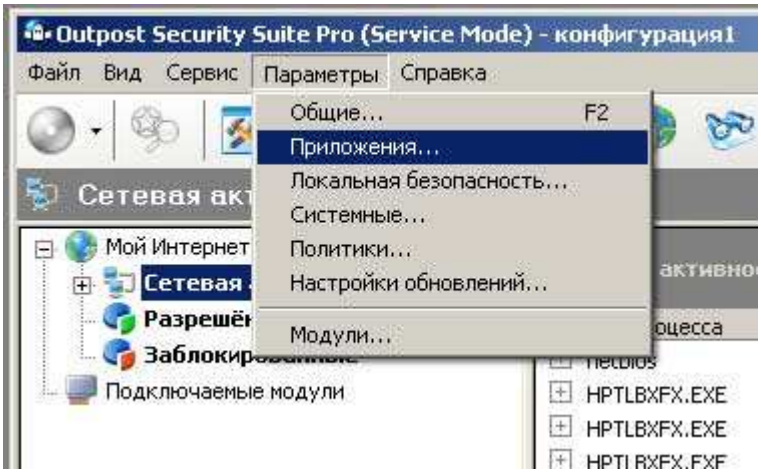


Рис. 9

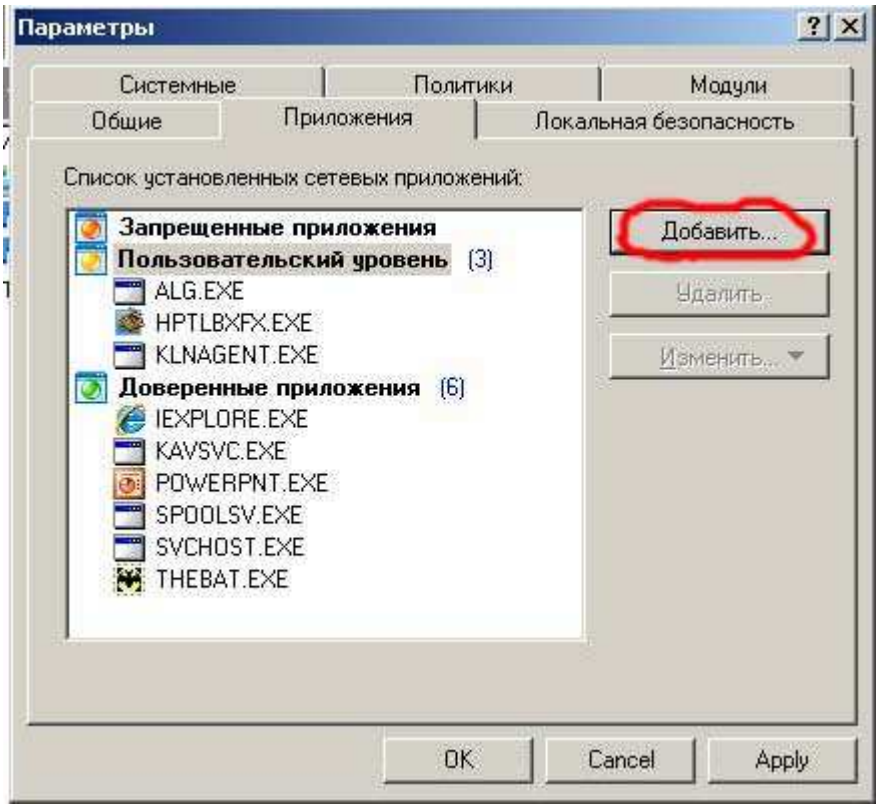


Рис. 10

2. Откроется стандартное окно <Open> (см. Рис. 11), в котором надо открыть папку *C:\Program Files\Botik Tools\bin*, выбрать в ней файл приложения *wish.exe* и щелкнуть ОК. В результате откроется окно <Правила Wish Application>, в котором пока еще нет ни одного правила для приложения *wish.exe* (см. Рис. 12). В этом окне есть инструменты, которые позволяют создавать правила, редактировать их, копировать или удалять. Начнем создавать первое правило для приложения *wish.exe*, щелкнув Создать.

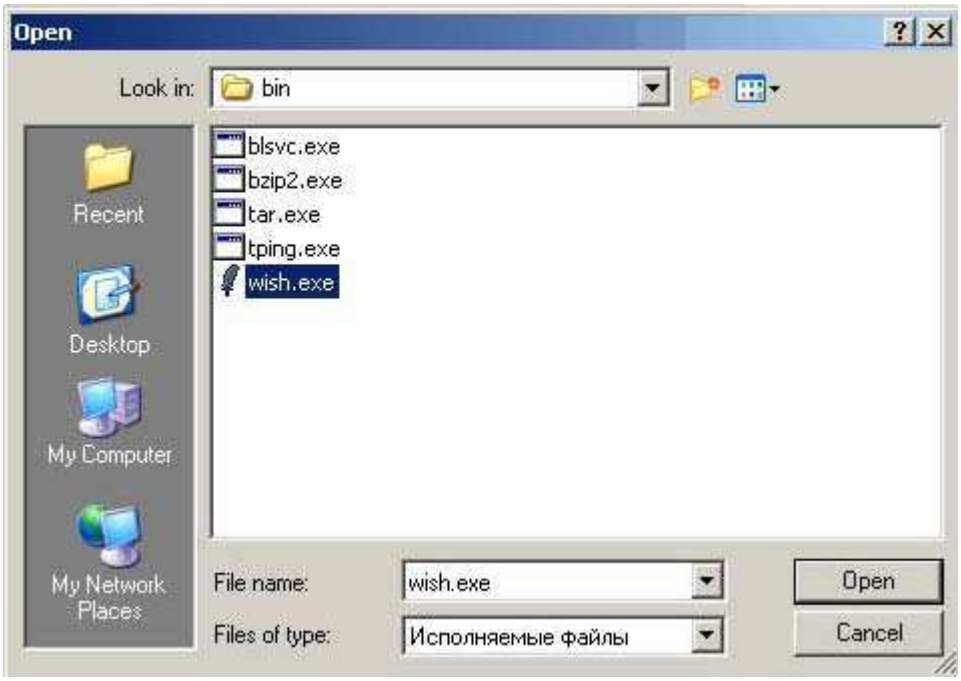
3. 

Рис. 11

Рис. 12

3. Откроется окно <Правило>, в котором можно выбирать событие, действие и описание правила (см. Рис. 13) в трех полях ввода этого окна: "1. Выберите событие для правила", "2. Выберите действие для правила" и "3. Описание правила".
   Создадим правило для разрешения исходящих пакетов по протоколу TCP через порты 9, 25, 53, 80, 443, 12040.
   Сначала выберем событие. В поле ввода "1. Выберите событие для правила" (см. Рис. 14) установим флаг Где протокол. В поле "3. Описание правила" появится строка "Где протокол Не определено". Щелчком по ссылке Не определено откроем окно <Выбор протокола>, в котором выберем параметр TCP и щелкнем OK. Таким образом, дальше будем описывать такое событие, как передача пакетов по протоколу TCP для программы *wish.exe*.

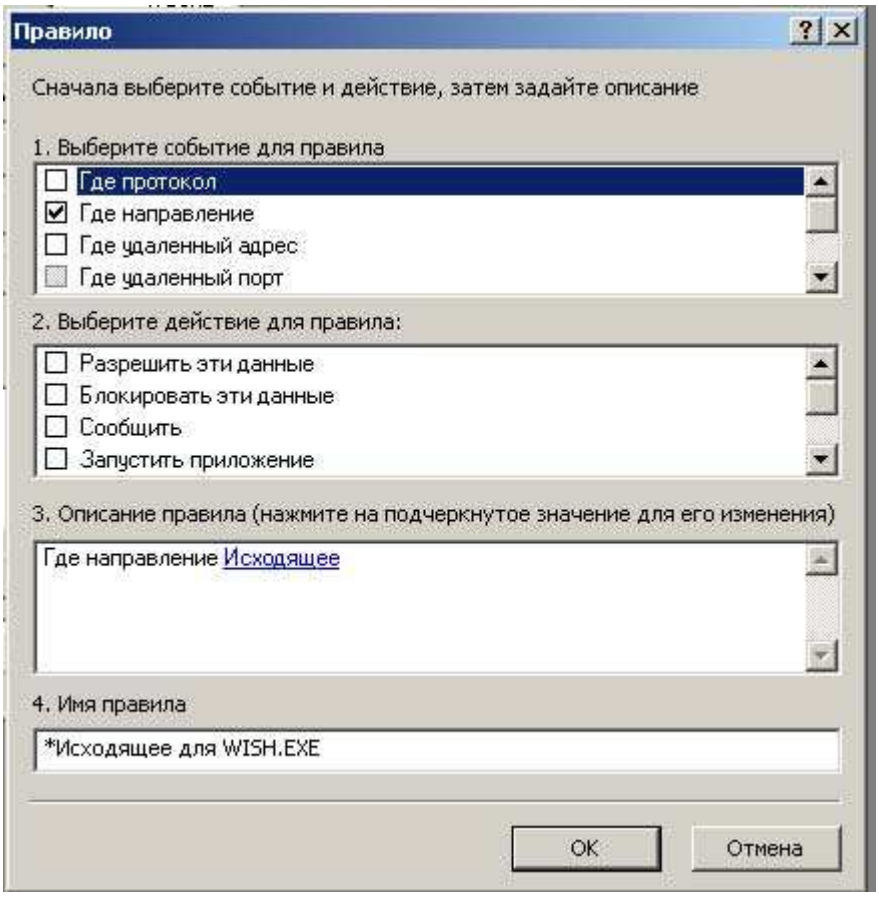

Правило
Сначала выберите событие и действие, затем задайте описание
1. Выберите событие для правила
Где протокол
Где направление
Где удаленный адрес
Где удаленный порт
2. Выберите действие для правила:
Разрешить эти данные
Блокировать эти данные
Сообщить
Запустить приложение
3. Описание правила (нажмите на подчеркнутое значение для его изменения)
Где направление Исходящее
4. Имя правила
*Исходящее для WISH.EXE
OK
Отмена

Рис. 13

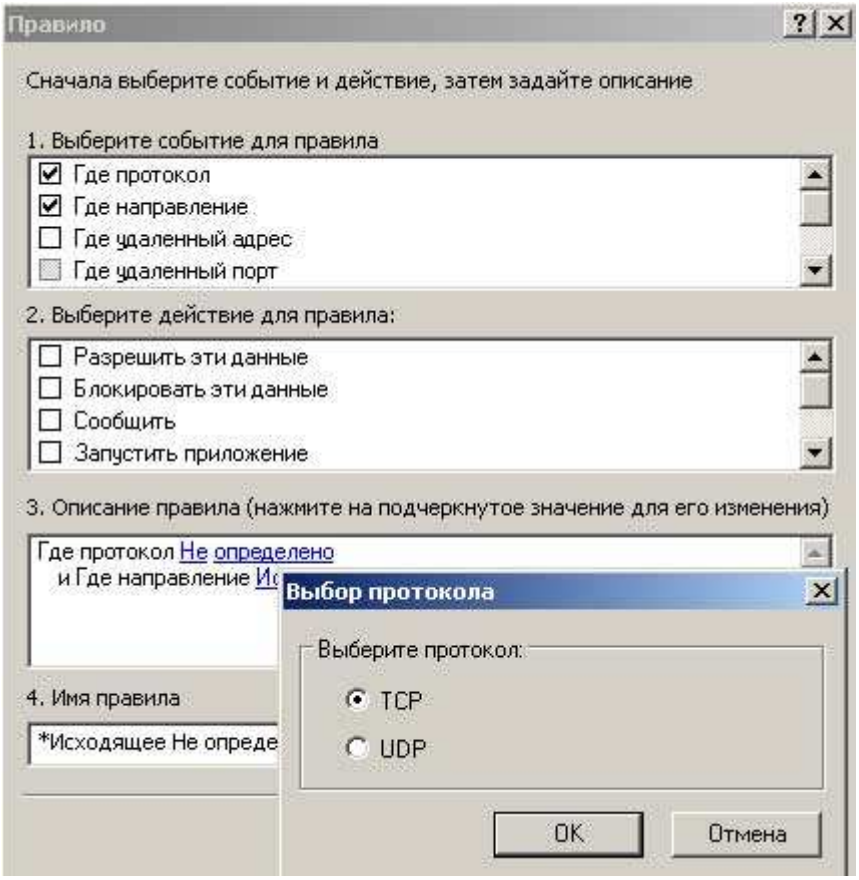

Правило
Сначала выберите событие и действие, затем задайте описание
1. Выберите событие для правила
Где протокол
Где направление
Где удаленный адрес
Где удаленный порт
2. Выберите действие для правила:
Разрешить эти данные
Блокировать эти данные
Сообщить
Запустить приложение
3. Описание правила (нажмите на подчеркнутое значение для его изменения)
Где протокол Не определено
и Где направление Ис
4. Имя правила
*Исходящее Не опреде
Выбор протокола
Выберите протокол:
TCP
UDP
OK
Отмена

Рис. 14

Выполним описание этого события. Поскольку при создании нового правила по умолчанию установлено направление Исходящее (см. Рис. 13 раздел **Описание правила**), оставим это описание без изменения.

Однако, если бы нужно было выбрать направление Входящее, то следовало бы щелчком по ссылке Исходящее открыть окно <Выбор типа соединения> и установить соответствующий параметр **Входящее** (см. Рис. 15).

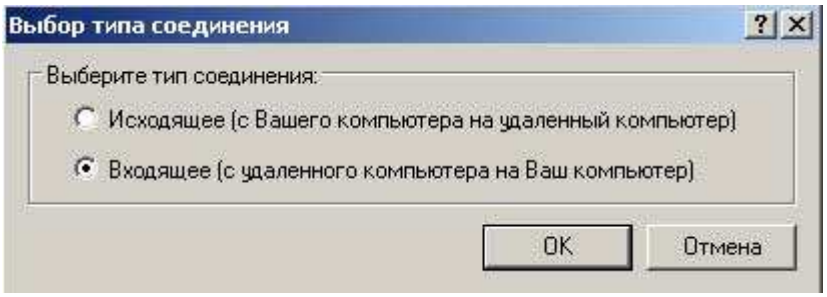


Рис. 15

Далее необходимо выбрать порты, через которые будем разрешать передачу исходящих TCP-пакетов. Для этого в поле ввода "1. Выберите событие для правила" устанавливаем флаг **Где удаленный порт**. В поле "3. Описание правила" появится строка "Где удаленный порт Не определено". Щелчком по ссылке Не определено откроем окно <Выберите удаленный порт> (см. Рис. 16). Нам нужно установить следующие номера портов: 9, 25, 53, 80, 443, 12040. Можно выбрать номера из списка или ввести их в поле ввода так, как показано на Рис. 16.

Наконец, завершает создание правила выбор действия для этого правила -- в поле "2. Выберите действие для правила" устанавливаем флаг **Разрешить эти данные** (см. Рис. 17) и щелчком по кнопке **ОК** завершаем создание первого правила.

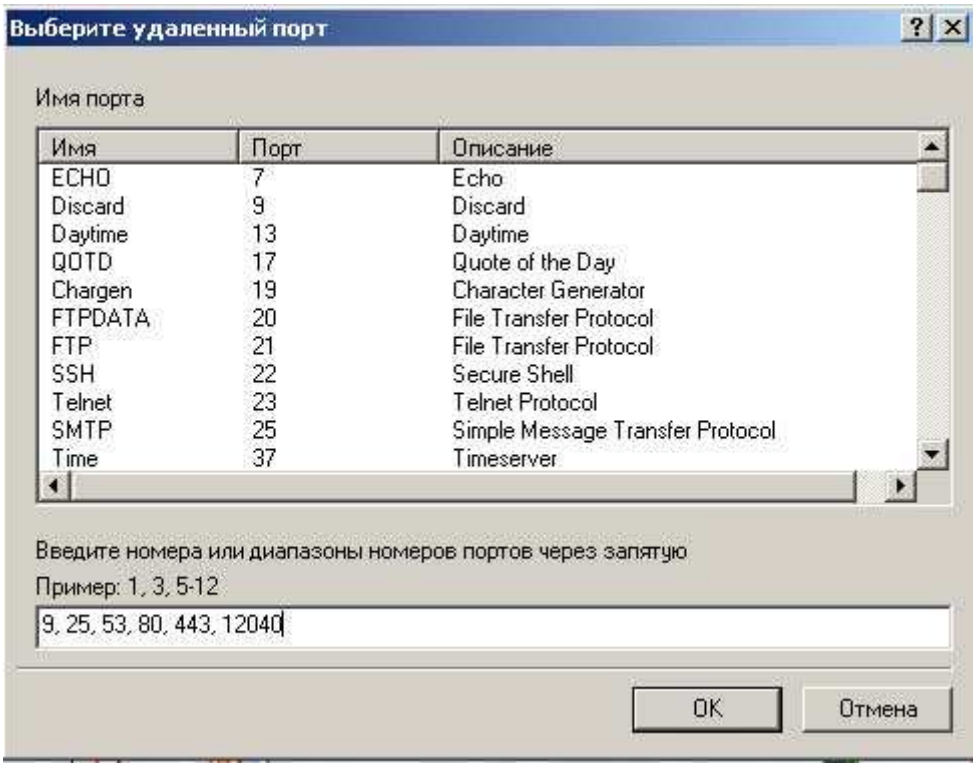


Рис. 16

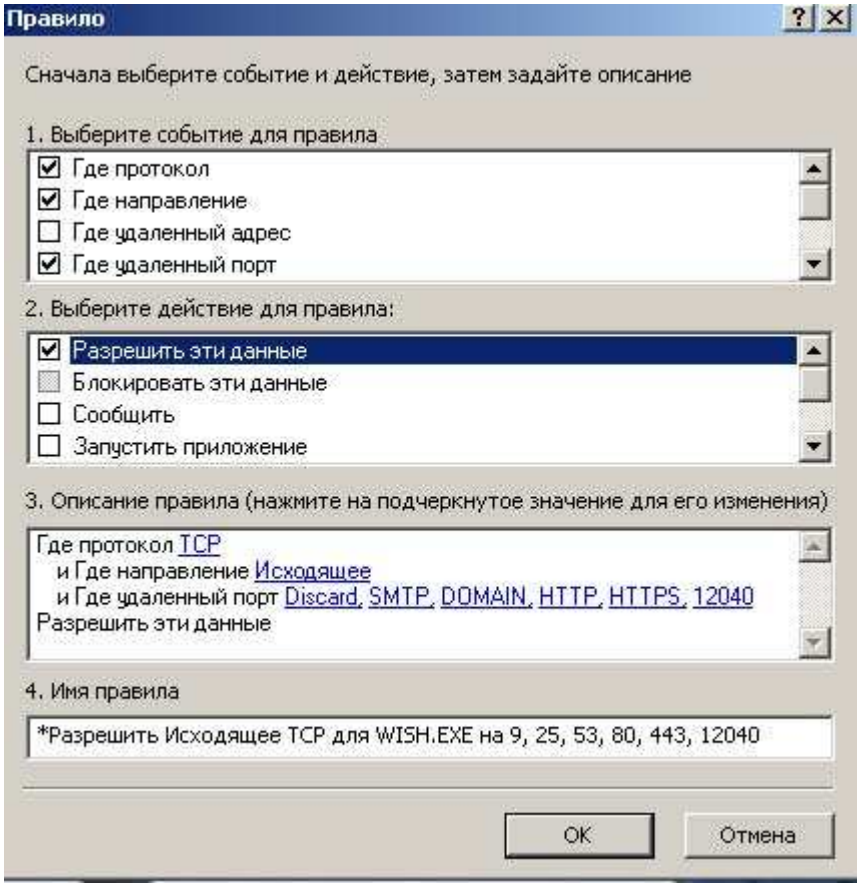


Рис. 17

Остальные три правила для приложения *wish.exe*, перечисленные в пунктах 1 и 2 раздела "**Что настроить?**", создаются аналогично. Еще раз напомним здесь эти правила:

- правило, разрешающее прием входящих пакетов по протоколу TCP через порты 9, 25, 53, 80, 443, 12040;
- правило, разрешающее передачу исходящих UDP-пакетов через порт 53;
- правило, разрешающее прием входящих UDP-пакетов через порт 53.

В результате список правил, созданных для приложения *wish.exe*, будет выглядеть так, как показано на Рис. 18

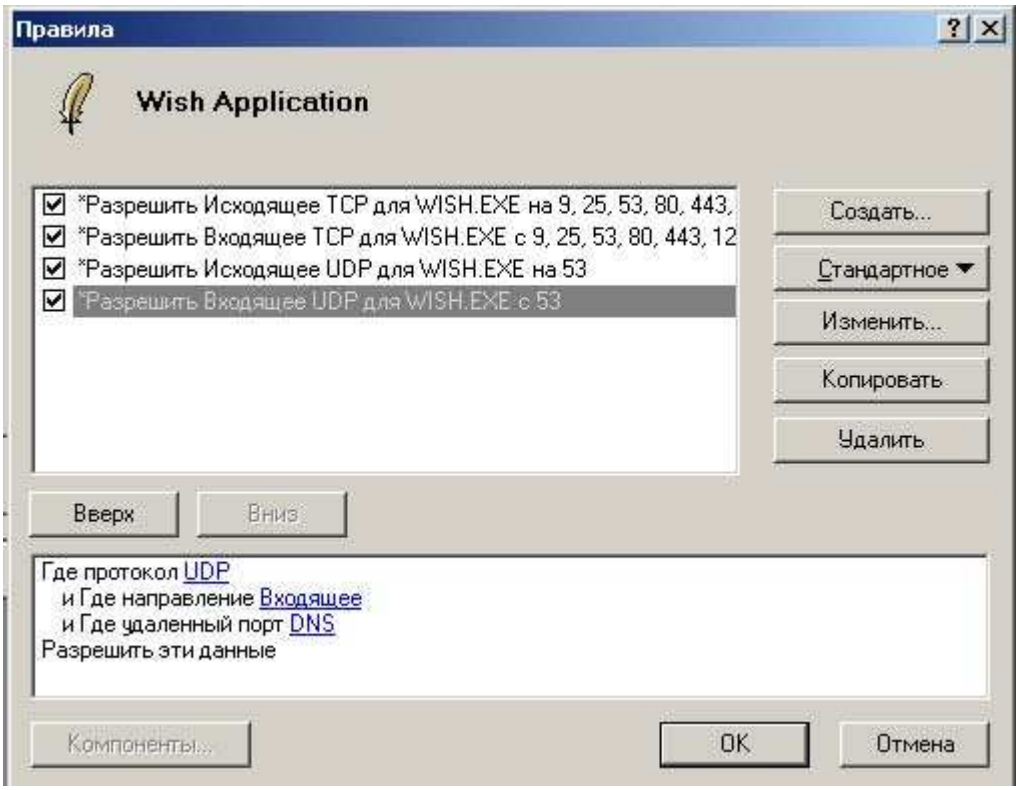


Рис. 18

Далее необходимо установить параметры протокола ICMP, что позволит проводить *ping*-тестирование вашего компьютера. А именно, как это перечислено в п.п. 3 и 4 раздела "**Что настроить**", надо сделать следующее:

3. разрешить ICMP Эхо-запрос и ICMP Эхо-ответ для приложения *tping.exe*, входящего в состав Botik Tools (*C:\Program Files\Botik Tools\bin\tping.exe*);
4. разрешить ICMP Эхо-запрос и ICMP Эхо-ответ для встроенных в Windows приложений *ping.exe* и *tracert.exe* (*C:\Wondows\system32\ping.exe* и *C:\Wondows\system32\tracert.exe*).

В меню **Параметры** программы Outpost Firewall выбрать **Системные** (см. Рис. 19), чтобы открыть в окне <Параметры> вкладку **Системные** (см. Рис. 20). Во вкладке **Системные** для установки параметров ICMP-протокола щелкнуть **Параметры** (кнопка отмечена на Рис. 20 красным).

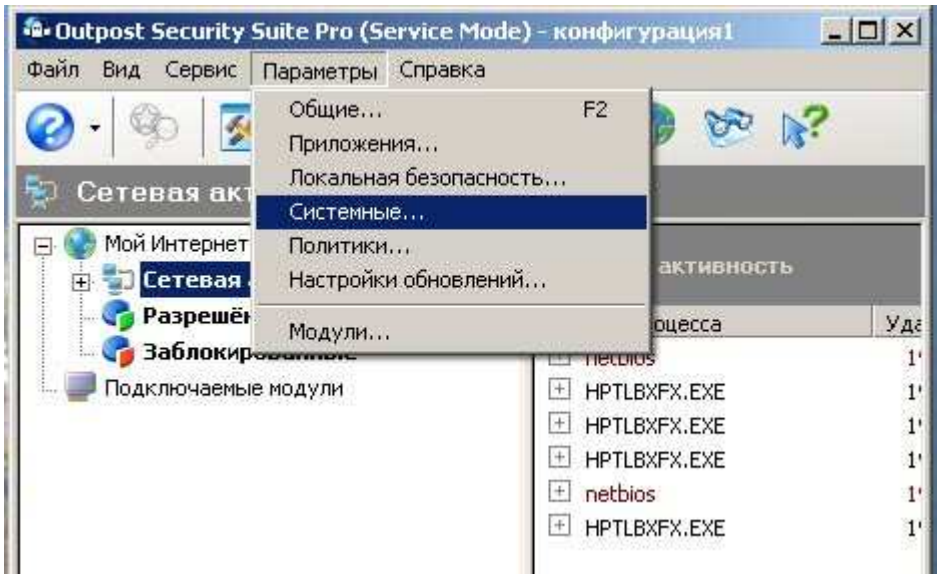


Рис. 19

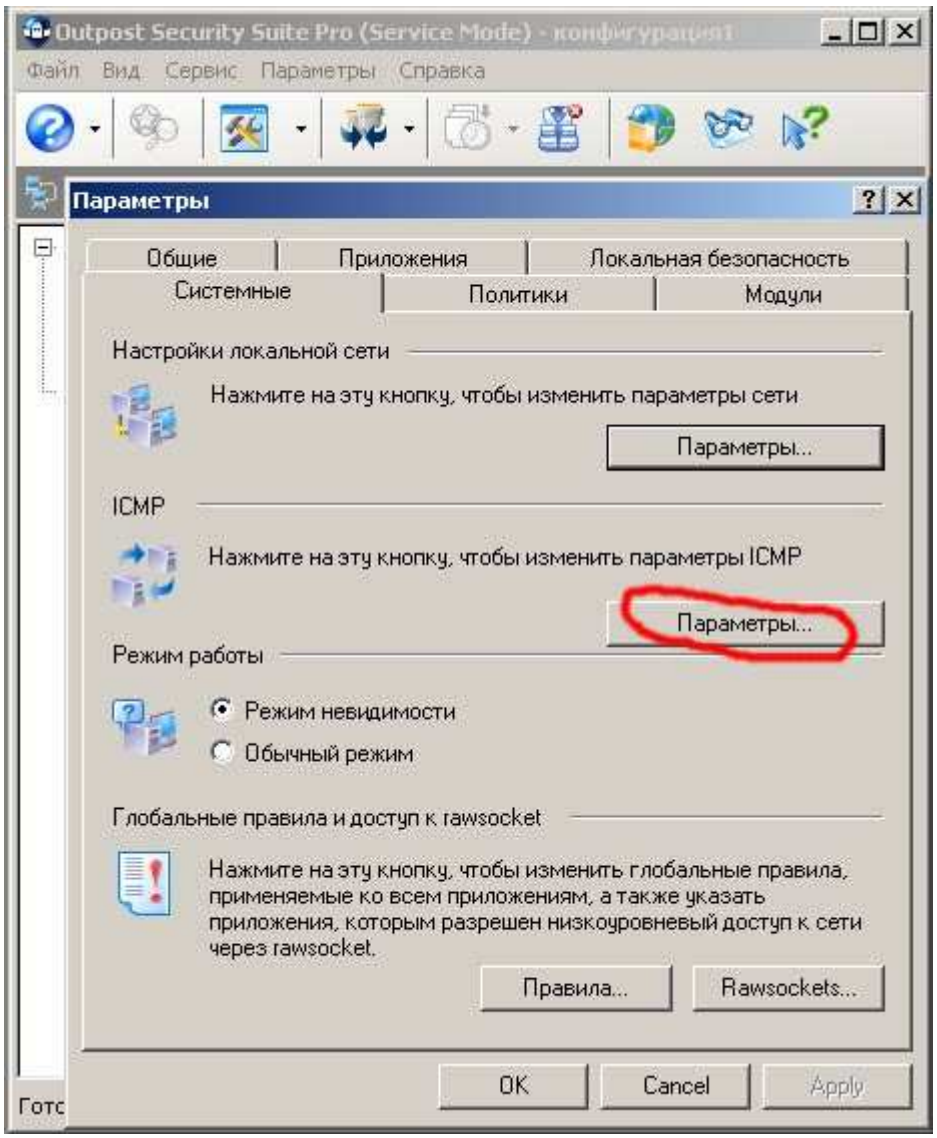


Рис. 20

Откроется окно <Параметры ICMP> (см. Рис. 21), в котором нужно для ICMP-сообщений типа Эхо-ответ и Эхо-запрос установить такие флажки В и Из, которые

показаны на Рис. 21 и щелкнуть OK.

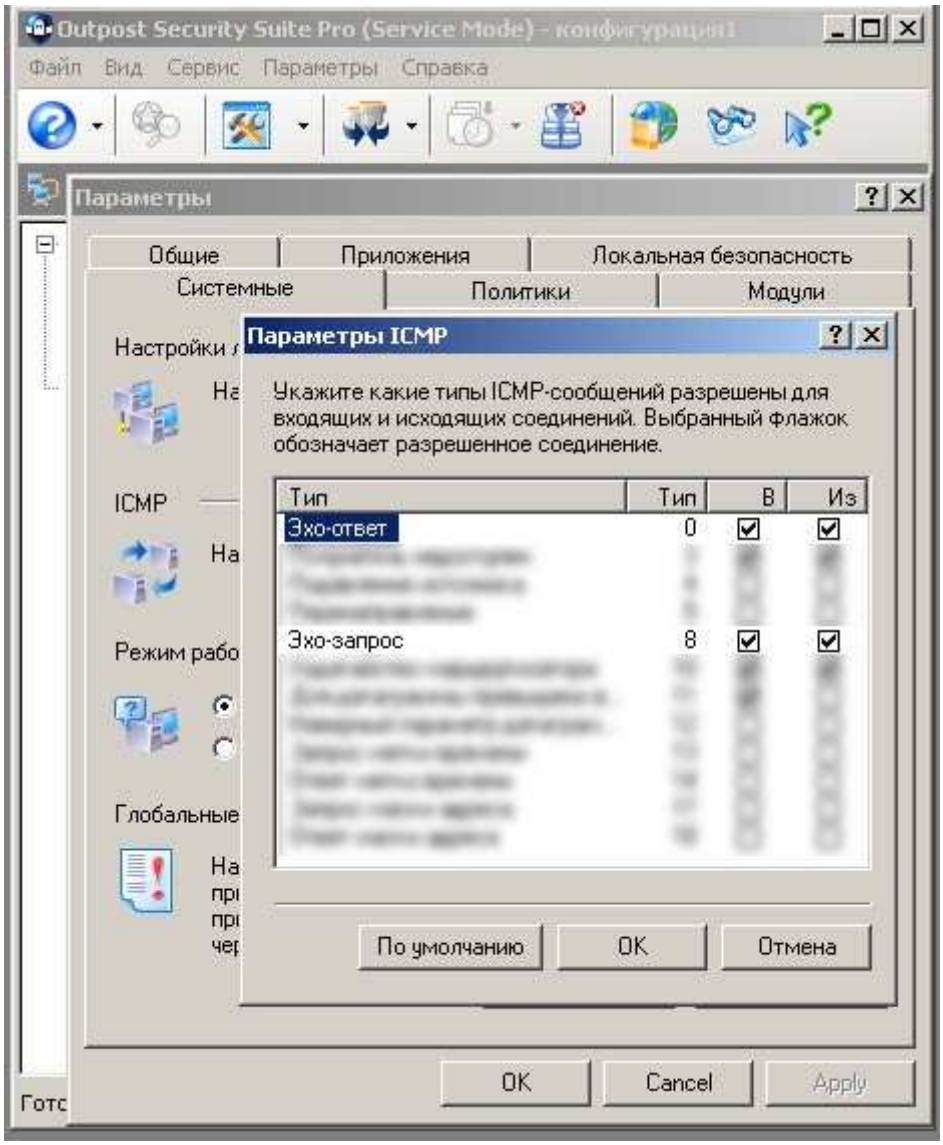


Рис. 21

На этом настройку сетевого экрана Outpost Firewall можно считать завершенной.

Порядок выполнения работы

1. Изучить состав и назначение протоколов стека TCP/IP.
2. В системе Windows выполнить настройку стека протоколов TCP/IP для организации работы в сети Интернет. Для этого получить необходимые данные у преподавателя.
3. Создать группу в сети. Добавить в эту группу несколько компьютеров.
4. Поэкспериментировать с настройками Firewall. (пропускание/блокирование ping, HTTP и др.)

Контрольные вопросы.

1. Сколько протоколов образуют стек TCP/IP?
2. Какие уровни протоколов содержит стек TCP/IP?
3. что такое IP – адресация?
4. На каком уровне применяется IP – адресация?
5. Является ли IP – адресация абсолютной или относительной?
6. Поясните понятия статический и динамический IP – адрес.
7. Что такое шлюз?
8. Что такое маршрутизатор?
9. Для чего применяется маска подсети?
10. Какие службы, устройства, клиенты необходимы для работы в сетях?
11. Какие три основных вида угроз безопасности при работе в сети Internet?
12. Рассказать о каждой угрозе при работе в сети Internet.
13. Виды программ-паразитов (и в чем их различие)?
14. Адресация в сети Internet.
15. Основные сетевые протоколы (TCP, IP, UDP, POP, SMTP, DNS, WINS, ICMP, HTTP, FTP,). Рассказать о любом по выбору преподавателя.
16. Какие средства сетевой защиты существуют?
17.