И.Я. Минаев

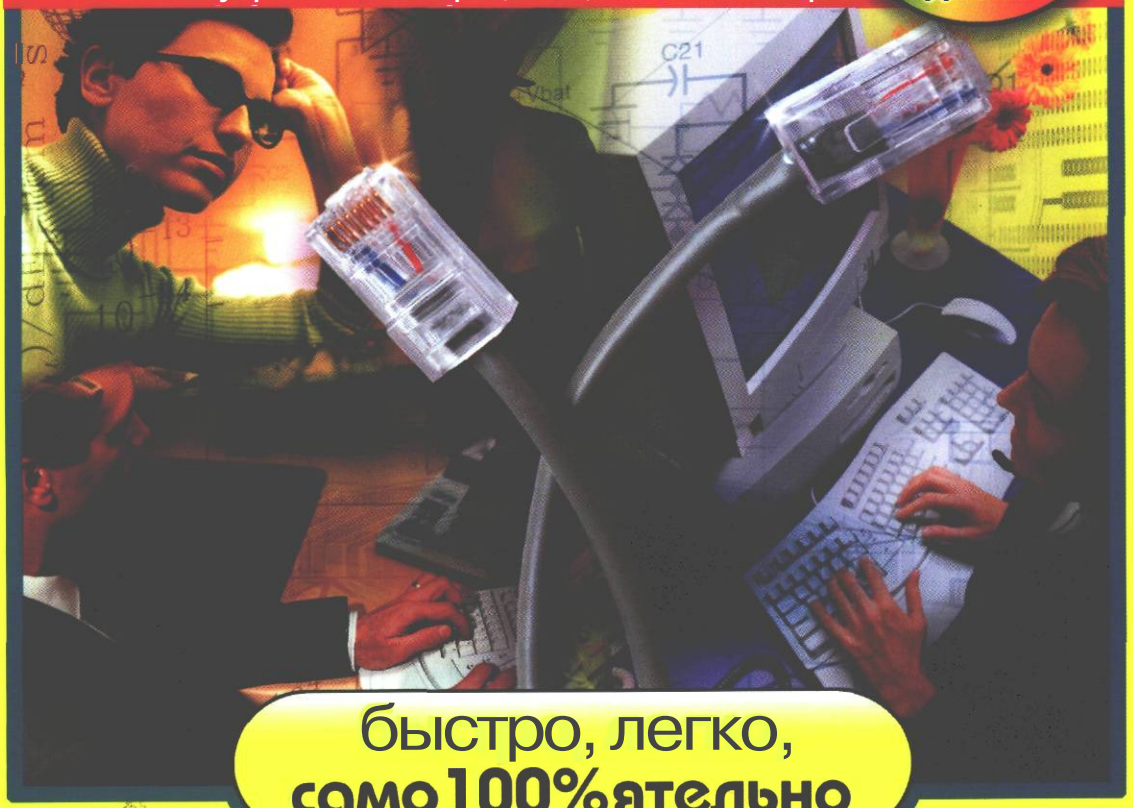
100% самоучитель

# ЛОКАЛЬНАЯ СЕТЬ СВОИМИ РУКАМИ

## Создание локальной сети дома и в офисе

- Локальная сеть без сетевой карты!!!
- Подключение локальной сети к **Интернету**
- Максимальная защита сети
- Электронная почта внутри и снаружи локальной сети
- Жизнь внутри сети: игры, чат, видеотелефон

Все программы из книги + ещё 25 программ на компакт-диске



быстро, легко, само100%ятельно

И.Я. Минаев

# 100% САМОУЧИТЕЛЬ

# ЛОКАЛЬНАЯ СЕТЬ СВОИМИ РУКАМИ

«ТЕХНОЛОДЖИ - 3000»
Москва

УДК 004.732(075.4)
ББК 32.973.202я78-1
М61

**Минаев, И.Я.**

М61 Локальная сеть своими руками. 100% самоучитель : [учеб. пособие] / И. Я. Минаев. — М. : ТЕХНОЛОДЖИ - 3000, 2004. — 368 с. CD-ROM : ил.— (Серия «100%»). — **ISBN 5-94472-023-9.**

Агентство CIP РГБ

Настоящая книга позволит Вам быстро и самостоятельно создать локальную сеть дома или в офисе. Вы узнаете, как обойтись без сетевых карт; легко выполнить диагностику сети; подключить свою сеть к Интернету; защитить сеть от хакеров и вирусов; запустить электронную почту, чат, видеоконференции и сетевые игры внутри сети.

Все необходимые программы записаны на компакт-диск, который прилагается к книге.



**ISBN 5-94472-023-9**

# Содержание

(подробное содержание находится в конце книги)

ГЛАВА 1.

# Все, что нужно знать и иметь для создания локальной сети: топологии, кабели, протоколы, адреса, сетевые карты и сетевое оборудование

Компьютерной сетью можно считать соединение двух и более компьютеров с помощью кабеля или телефонной линии и модема, при котором становится возможен обмен данными между ними. Компьютеры, расположенные в одном помещении или здании и связанные между собой, называют **локальной компьютерной сетью** (LAN - Local Area Network). Количество компьютеров, подключенных к такой сети, ограничивается возможностями применяемой кабельной системы и сетевого оборудования. Несколько локальных компьютерных сетей при объединении образуют кампусную сеть (CAN - Campus Area Network), например, локальные сети расположенных по соседству зданий или корпусов одного предприятия или учебного заведения. MAN (Metropolitan Area Network) - сеть уже городского масштаба, к которой могут быть подключены несколько кампусных или локальных сетей предприятий и организаций. WAN (Wide Area Network) - широкомасштабная сеть, охватывающая, например, несколько городов, область или край. GAN (Global Area Network) - глобальная компьютерная сеть - это объединение нескольких широкомасштабных компьютерных сетей, например, в масштабе страны. И, наконец, сетью всех сетей является Интернет, в состав которого входят Всемирная Компьютерная Паутина (World Wide Web), система электронной почты и другие системы хранения и передачи информации.

## Оборудование, необходимое для построения различных компьютерных сетей

Для реализации сетевых возможностей необходимо соединить два или более компьютеров в локальную сеть. Какой бы способ соединения вы не выбрали, вам не обойтись без дополнительного оборудования. В случае если вы будете использовать для связи прямое кабельное соединение, потребуются многожильный кабель и разъемы для подключения его к COM- или LPT-портам компьютеров. Обычно используются разъемы типа DB-9 или DB-25. Более подробно о том, как объединить два компьютера в сеть с помощью прямого кабельного соединения, мы расскажем в одной из следующих глав нашей книги.

Если у вас имеется телефонная линия, то, чтобы подсоединиться к другому компьютеру или к Интернету, вам нужен модем, который необходимо подключить к свободному COM- или USB-порту или установить в слот на материнской плате, после чего настроить модем на соединение с Интернетом или другим компьютером. Подробно об этом будет рассказано далее.

И, наконец, если вы хотите создать локальную компьютерную сеть в своем подъезде, доме или офисе, то вам потребуются сетевые карты, кабель необходимой длины, а также могут потребоваться хабы, свитчеры и репитеры, в зависимости от протяженности и

разветвленности вашей сети. Более подробно со всеми этими устройствами и особенностями их подключения мы познакомимся далее.

Локальная сеть представляет собой коммуникационную систему, обеспечивающую высокоскоростной обмен данными между несколькими компьютерами в пределах ограниченной территории. В отличие от нее, глобальная сеть (Wide Area Network, сокращенно - WAN) может простираться на сотни и тысячи километров. Обе разновидности компьютерных сетей имеют много общего в программном обеспечении, но отличаются используемыми телекоммуникационными каналами и оборудованием связи.

В данной главе мы рассмотрим вопросы установки и настройки локальных сетей на основе наиболее распространенных технологий и оборудования. Некоторые вопросы, касающиеся способов организации и функционирования компьютерных сетей, кратко затронутые здесь, в дальнейшем будут обсуждаться более подробно.

# Принципы построения локальных сетей

При построении локальных компьютерных сетей необходимо учитывать множество различных факторов, например, количество объединяемых в сеть компьютеров, удаленность их друг от друга, обеспечение конфиденциальности передаваемых по сети данных и т.д. Поэтому для выбора наиболее подходящей в каждом конкретном случае структуры сети необходимо знать, какие бывают сети, и познакомиться с основными понятиями, используемыми при описании компьютерных сетей. К таким понятиям относятся:

- сетевые компоненты;
- способы организации сети, определяющие возможность доступа компьютера к данным, передаваемым по сети и хранящимся на других сетевых компьютерах;
- роли компьютеров в сети;
- топология компьютерной сети;
- технология компьютерной сети;
- тип кабельной системы, используемой для соединения компьютеров;
- соединение сетей и маршрутизация.

## Сетевые компоненты

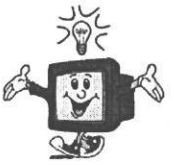
Основными компонентами локальной сети являются **узлы** (Node), связанные между собой соединительным кабелем, который иначе называется **сегментом** (Segment) (Рис. 1.1).


*Рис. 1.1. Основные компоненты локальной сети*

В сетевых узлах чаще всего находятся компьютеры, однако может располагаться и другое оборудование, например:

- сетевой принтер;
- концентратор;
- повторитель;
- мост;
- маршрутизатор.

*Этот список может быть продолжен. Но даже здесь встречается много новых терминов. Подробно разъяснять их значения сейчас не имеет смысла, так как они будут рассматриваться в соответствующих разделах книги.*



## Способы организации компьютерной сети

Компьютерные сети, в зависимости от роли каждого конкретного подключенного к сети компьютера, делятся на два вида:

- **одноранговые;**
- **иерархические.**

В одноранговой сети все компьютеры имеют равные права, и каждый пользователь делает доступными или недоступными для общего использования ресурсы своего компьютера: файлы, принтеры и т.п. В такой сети компьютеры находят друг друга по имени или по уникальному адресу и этого оказывается достаточно для нормальной работы сети.

В иерархической сети права доступа отдельного компьютера к сетевым ресурсам и адресация, т.е. присвоение каждому конкретному компьютеру, входящему в сеть, уникального адреса, регулируется выделенным сервером. Сервер, с помощью специальных программных средств, следит за тем, чтобы адреса в сети не повторялись, и чтобы информация, посланная с одного компьютера, попала адресату и была недоступна другим пользователям сети. Управление правами доступа и распределение сетевых адресов называется администрированием и выполняется специалистами - сетевыми администраторами.

## Роли компьютеров в сети

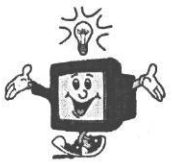
Компьютер, подключенный к локальной сети, может называться по-разному, в зависимости от основных выполняемых им функций:

- **рабочая станция** (Workstation);
- **сервер** (Server).

Рабочая станция представляет собой обычный компьютер, предназначенный для работы конечного пользователя. Рабочая станция использует только доступные для нее ресурсы локальной сети.

Сервер выполняет определенные действия по запросам рабочих станций, предоставляя им свои ресурсы, например, дисковое пространство, вычислительную мощность процессора, принтер, модем и другое оборудование.

*На самом деле, если рассмотреть вопрос еще глубже, все взаимодействия в сети происходят на уровне программ. Это выглядит примерно так: программа-сервер получает по сети запрос от программы-клиента с рабочей станции, обрабатывает его и посылает ответ.*



## Разновидности серверов

Чаще всего название сервера включает и наименование его основной функции:

- файловый сервер;
- сервер печати;
- почтовый сервер;
- сервер новостей;
- Web-сервер;
- сервер баз данных;
- факс-сервер и т. д.

Серверы также могут классифицироваться по признаку, указывающему на характер его использования:

- выделенный сервер;
- невыделенный сервер.

Выделенный сервер в локальной сети предназначен исключительно для предоставления своих ресурсов в общее пользование, а не для непосредственной работы на нем, поэтому может полноценно функционировать без монитора и клавиатуры. Обычно он обладает повышенной мощностью и надежностью аппаратуры, а также используемого программного обеспечения. В качестве операционной системы выделенного сервера чаще всего используются:

- Microsoft Windows 2000 Server;
- Microsoft Windows 2003 Server;
- Linux, FreeBSD, Sun Solaris и другие разновидности Unix;
- Novell NetWare;

Невыделенный сервер совмещает функции сервера и рабочей станции. Иными словами, это рабочая станция, некоторые ресурсы которой выделены для совместного доступа к ним по сети. На рабочей станции (невыделенном сервере) операционной системой может быть, например:

- Microsoft Windows 98/ME;
- Microsoft Windows XP Professional;
- Microsoft Windows 2000 Workstation;
- Linux.

В одноранговых локальных сетях компьютеры объединены в **рабочие группы** (Workgroups), где они функционируют в качестве рабочих станций или невыделенных серверов, предоставляя часть своих ресурсов для использования своей рабочей группе. Одноранговые сети проще в администрировании, но не обеспечивают высокой степени защиты информации.

Локальные сети с выделенным сервером, напротив, имеют повышенную надежность и защищенность информации, которая хранится на сервере.

## Топологии локальных сетей

Компьютеры и другие компоненты локальной сети могут соединяться между собой различными способами. Используемая схема физического расположения сетевых компонентов называется **топологией** (Topology). Топология сети определяется геометрической фигурой, образованной линиями связи между компьютерами, или физическим расположением по отношению друг к другу компьютеров, связанных между собой. Топология сети может служить одной из характеристик для сравнения и классификации различных компьютерных сетей.

Существуют три основные топологии построения локальной сети:

- **звезда (Star).**
- **кольцо** (Ring);
- **шина** (Bus).

### Звезда

В сети с топологией «звезда» все компьютеры соединены с центральным компьютером, или **хабом** (hub - центр) (Рис. 1.2). Все данные поступают на центральный узел, который передает их получателю непосредственно. В этой топологии отсутствуют прямые связи между компьютерами сети. Передача всей информации происходит только через хаб (центральный компьютер). В качестве хаба может использоваться специальное устройство - концентратор, представляющий собой многопортовый репитер (repeater - повторитель). Основная функция репитера - получив данные на одном из портов, немедленно перенаправить их на другие порты.

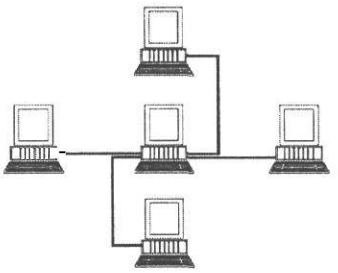


*Рис. 1.2. Топология «звезда»*

Организация сети с топологией «звезда» проста и эффективна. При обрыве одного из кабелей, соединяющего отдельный компьютер сети с хабом, связь между остальными компьютерами, включенными по данной схеме, останется работоспособной. Если же из строя будет выведен сам центральный компьютер, то передача данных между компьютерами такой сети будет невозможна.

Достоинства звездообразной топологии:

- нарушение соединения в одном месте, кроме центрального узла, не прерывает работы локальной сети;
- при подключении большого количества компьютеров не происходит снижения производительности;
- безопасность информации обеспечивается на высоком уровне, так как компьютеры не получают чужих данных.

Недостатки звездообразной топологии:

- большой расход соединительного кабеля;
- поломка центрального узла приводит к неработоспособности всей сети;
- наращивание сети сопряжено с большими финансовыми затратами.

## Кольцо

В топологии типа «кольцо» отсутствуют концевые точки соединения, т.е. сеть получается замкнутой в неразрывное кольцо (Рис. 1.3).

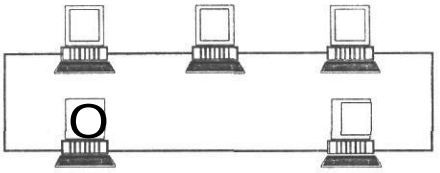


*Рис. 1.3. Топология «кольцо»*

В сети, построенной по кольцевой топологии, данные передаются в одном направлении от одного компьютера «кольца» к другому. Компьютер не передает информацию, пока не получит специальный маркер.

Достоинства кольцевой топологии:

- при подключении большого количества компьютеров происходит лишь незначительное снижение производительности.

Недостатки кольцевой топологии:

- нарушение соединения в одном месте приводит к прекращению работы всей локальной сети;
- безопасность информации обеспечивается не на очень высоком уровне: данные, посланные одним компьютером сети другому, могут быть легко перехвачены любым из компьютеров сети, которому они не предназначены, что может нарушить конфиденциальность передаваемой информации.

## Шина

Топология «шина» использует для передачи данных один общий канал связи (чаще всего выполненный на основе коаксиального кабеля), к которому подключаются все компьютеры локальной сети (Рис. 1.4).

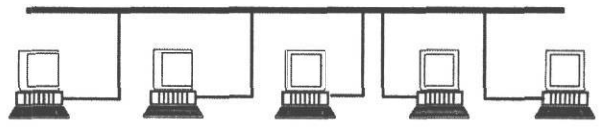


*Рис. 1.4. Топология «шина»*

Работа в сети с топологией «шина» осуществляется следующим образом. Когда один из компьютеров локальной сети с шинной топологией отправляет данные, они передаются по кабелю в обоих направлениях и принимаются всеми без исключения компьютерами, но использует их только тот из них, кому они были предназначены. Данные в сети с топологией «шина» могут следовать в любом направлении одновременно. На противоположных концах шины устанавливаются специальные заглушки - терминаторы.

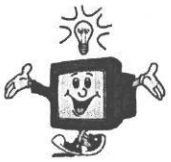
Достоинства шинной топологии:

- легкость наращивания сети;
- не очень высокая стоимость оборудования.

Недостатки шинной топологии:

- нарушение соединения в одном месте приводит к неработоспособности всей локальной сети;
- при подключении большого количества компьютеров к одной шине происходит резкое снижение производительности;
- безопасность информации обеспечивается не на высоком уровне.

*Кроме перечисленных простых разновидностей сетевых топологий, существуют и более сложные, но все они строятся на базе этих трех основных топологий.*



## Сетевые технологии

Понятия технологии и топологии локальных сетей нередко путают между собой. Если топология компьютерной сети описывает геометрическую конфигурацию кабельных соединений между компьютерами, то под сетевой технологией следует понимать совокупность стандартов, описывающих процесс передачи информации, или особенности в аппаратной реализации **сетевых адаптеров** и заложенных в них принципов передачи информации. Сетевые адаптеры (Рис. 1.5) представляют собой электронные устройства, предназначенные для передачи данных от одного компьютера к другому по компьютерной сети. Они выполнены в виде печатной платы, которая устанавливается в свободный слот шины ISA или PCI материнской платы компьютера и имеет один или несколько разъемов, которые выводятся на заднюю панель компьютера для подключения к ним сетевого кабеля. Многие современные материнские платы имеют встренные сетевые карты.

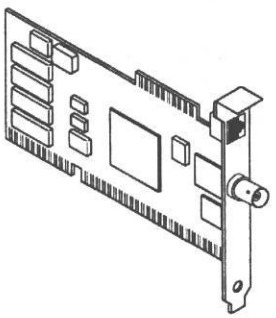


*Рис. 1.5. Сетевой адаптер*

Наиболее известными и часто реализуемыми сетевыми технологиями являются:

- **Ethernet;**
- **ARCNET;**
- **IBM Token Ring.**

Технология Ethernet была разработана фирмой Xerox в 1973 г. и предназначена для построения сетей с топологией «звезда» или «шина». Когда в качестве канала связи используется коаксиальный кабель, то сеть Ethernet конфигурируется как «шина». Если же применяется витая пара, то строится сеть с топологией «звезда». На сегодняшний день эта технология является наиболее распространенной благодаря низкой стоимости, расширяемости и поддержке практически всеми производителями сетевого оборудования. Поэтому в следующих главах мы будем рассматривать построение сетей преимущественно на базе именно технологии Ethernet.

Технология ARCNET (Attached Resource Computer NETwork) разработана компанией Datapoint Corporation в 1977 году и, так же, как Ethernet, может использоваться при построении сетей с топологией «звезда» или «шина». На основе ARCNET было построено множество сетей Novell NetWare 2.x; многие из них используются и сегодня. Тем не менее, данная технология считается устаревшей и в настоящее время уже не применяется.

Технология Token Ring, разработанная фирмой IBM в 1986 году, предназначена для построения сетей со смешанной топологией («звезда» и «шина»). Компьютеры, объединенные в сеть по технологии Token Ring, подключаются к специальному устройству,

которое называется станцией многопользовательского доступа (Multy-station Access Union, MAU), по топологии «звезда». MAU используется в качестве центрального хаба, но для соединения с каждым компьютером сети используется два кабеля: по одному данные посылаются, по другому принимаются. Таким образом, получается, что сеть, построенная по технологии Token Ring, представляет собой кольцо, оформленное в виде звезды (Рис. 1.6).

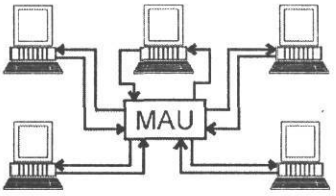



*Рис. 1.6. Компьютерная сеть, построенная по технологии Token Ring*

Сети Token Ring значительно дороже сетей Ethernet. Например, стоимость сетевой карты Token Ring в 3-5 раз превышает стоимость карты для Ethernet. Такое же соотношение характерно и для другого сетевого оборудования. По этой, а также по некоторым другим причинам технология Token Ring не нашла широкого признания. Так, сетевые карты и другие компоненты сети Token Ring производят всего несколько фирм, в то время как для Ethernet можно выбирать продукцию множества производителей.

## Кабели, применяемые в локальных сетях

Для соединения двух и более компьютеров в единую компьютерную сеть чаще всего применяются кабельные системы на основе медных экранированных электрических проводов (Cupper cable). Существуют также и оптоволоконные кабельные системы (Fiber-optic cable), которые по сравнению с электрическими кабелями обладают большей пропускной способностью и малыми потерями, однако более дороги. Поэтому оптоволоконные кабельные соединения применяются там, где нужно с большой скоростью передавать большой поток информации на большое расстояние, например, между районами города или при создании междугородной или международной сети. Альтернативой простому кабельному соединению может служить радиосвязь и связь, основанная на инфракрасном излучении. Однако эти виды связи не получили широкого распространения.

Электрические кабельные системы используют два типа кабелей. Первый тип представляет собой экранированный коаксиальный кабель с волновым сопротивлением 50 Ом (Рис. 1.7), другой - витую пару (Рис. 1.8, Рис. 1.9).

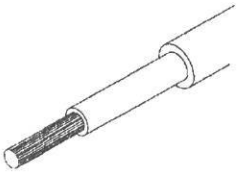


*Рис. 1.7. Коаксиальный кабель*

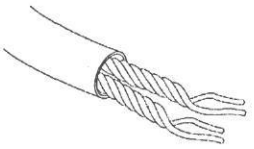


*Рис. 1.8. Неэкранированная витая пара*

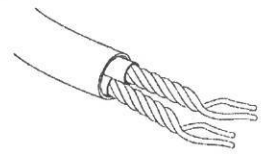


*Рис. 1.9. Экранированная витая пара*

Витая пара представляет собой два изолированных медных провода, скрученных между собой, но такой вид соединения в чистом виде не подходит для связи между двумя компьютерами и используется только для соединений в специальных коммутационных шкафах. Для связи между компьютерами используются кабели, содержащие несколько витых пар (3, 4 ... 1000 и более) в общей изоляционной оболочке. В зависимости от эффективного диапазона рабочих частот витые пары делятся на несколько категорий, в соответствии с таблицей.

| Полосачастот, МГц | Категория | Класс |
|---|---|---|
| до 0.1 | 1 | A |
| до 1 | 2 | B |
| до 16 | 3 | C |
| до 20 | 4 | |
| до 100 | 5 | D |
| до 200 | 6 | E |
| до 600 | 7 | F |

Витая пара может быть экранированной (STP - Shielded Twisted Pair) (Рис. 1.9) и неэкранированной (UTP - Unshielded Twisted Pair) (Рис. 1.8). Экранированная витая пара имеет множество разновидностей в зависимости от типа применяемого экрана. Экранированные витые пары, по сравнению с неэкранированными, имеют большую помехозащищенность, но и более дороги. Чаще всего для кабельной системы Ethernet применяется неэкранированный кабель пятой категории с 4 витыми парами.

## Другие способы соединения компьютеров в сеть

Для связи двух компьютеров можно использовать и более простые способы соединения, такие как прямое кабельное соединение и соединение с помощью модема через телефонную линию. Кроме того, существуют и активно развиваются технологии, использующие существующую телефонную и электрическую проводку, а также беспроводную связь.

### Прямое кабельное соединение

Прямое кабельное соединение использует для передачи данных встроенные в материнскую плату компьютера коммуникационные порты COM (Communication Port) или LPT (Line PrinTer). В современных компьютерах появилась также возможность связи двух и более компьютеров с помощью шины USB (Universal Serial Bus - универсальная последовательная шина). Порты COM обеспечивают асинхронный обмен данными по прото-

колу RS-232C со скоростью до 115 Кбит/сек. LPT-порты современных компьютеров являются скоростными двунаправленными устройствами ввода-вывода и обеспечивают работу с DMA (Direct Memory Access - прямой доступ к памяти). Скорость передачи данных через LPT-порт может достигать до 1,5 Мбит/с. Скорость передачи данных между компьютерами, соединенными с помощью шины USB 1.1, может достигать 12 Мбит/сек и до 480 Мбит/сек для USB 2.О. К достоинствам таких соединений можно отнести их простоту и малые затраты на построение, к недостаткам - небольшую дальность связи, ограниченную обычно несколькими десятками метров и, в случае соединения через COM-порты, низкую скорость передачи данных.

В дальнейшем мы еще раз вернемся к простым способам соединения компьютеров и опишем их более подробно.

## Соединение с помощью модема

Если в вашей квартире или офисе установлен телефон, то для передачи данных с одного компьютера на другой можно использовать модем (сокращение от модулятор-демодулятор). Модемы бывают внутренние (Internal), которые устанавливаются непосредственно в разъем материнской платы компьютера, и внешние (External), которые связаны с компьютером через COM-порт или шину USB. Большинство современных модемов обеспечивают скорость передачи данных до 33,6 Кбит/сек, а приема - до 56 Кбит/сек. К достоинствам такого вида связи можно отнести практически неограниченную дальность (любое место, куда можно дозвониться по телефону), к недостаткам - низкую скорость передачи, которая к тому же сильно зависит от качества телефонной связи.

## Сети на телефонных линиях

Для создания локальных сетей можно использовать имеющуюся в квартире или в офисе телефонную проводку. Для реализации таких сетей используется стандарт HomePNA (Home Phoneline Networking Alliance - Альянс домашних телефонных сетей), разработанный в 1998 году. В 2000 году появилась его новая версия - **HomePNA 2.О.** Данный стандарт определяет сети с пропускной способностью до 32 Мбит/сек при длине сегмента до 300 м. В ближайшее время ожидается появление сетей HomePNA с пропускной способностью до 100 Мбит/сек.

Сети данного типа используют существующие телефонные линии, но работают в особом частотном диапазоне, чтобы не создавать помех для обычных телефонных разговоров. После установки внутреннего или внешнего адаптера компьютер подключается к телефонной розетке с помощью обычного телефонного кабеля. Каждая телефонная розетка в доме становится портом сети, что позволяет обойтись без сетевого концентратора. HomePNA - это удобное решение для домашней сети, избавляющее от необходимости протягивать сетевые кабели по всему дому. Однако, учитывая высокую стоимость оборудования, а также низкое качество отечественных телефонных линий, сети HomePNA в странах СНГ пока не имеют широкого распространения.

## Сети на основе электропроводки

Некоторый интерес представляет технология построения локальной сети на основе существующей электропроводки, которая называется **HomePLC** (Home Power Line Cable - Кабель домашней электросети). В этой технологии используются сетевые карты, подключаемые через специальные разъемы к розеткам электропитания. При передаче

информации компьютер посылает по электросети низкочастотный радиосигнал, не влияющий на электрический ток в линиях электропитания. Этот радиосигнал принимает другой компьютер, также подключенный к сетевой розетке через адаптер HomePLC.

Основным недостатком сети HomePLC является незащищенность передаваемой информации от перехвата посторонним компьютера, подключенным к той же линии электропитания. Эту проблему можно решить созданием системы защиты, блокирующей доступ к локальной сети с помощью брандмауэра. Другой недостаток заключается в наличии в электросети электрических помех, вызванных бытовым электрооборудованием.

### Беспроводные сети

Технологии беспроводных сетей включают в себя широкий диапазон решений, начиная от глобальных сетей передачи голоса и данных, позволяющих пользователю устанавливать беспроводные соединения на значительных расстояниях, и заканчивая технологиями инфракрасной и радиосвязи, используемыми на небольших расстояниях. Технологии беспроводных сетей применяются в портативных и настольных компьютерах, карманных компьютерах, персональных цифровых помощниках (PDA), сотовых телефонах, компьютерах с перьевым вводом и пейджерах. Беспроводные технологии могут использоваться для самых различных целей. Например, мобильные пользователи могут использовать свои сотовые телефоны для доступа к электронной почте. Путешественники с портативными компьютерами могут подключаться к Интернету через базовые станции, установленные в аэропортах, на вокзалах и в других общественных местах. У себя дома можно подключать устройства к настольному компьютеру для синхронизации данных и передачи файлов.

Беспроводные технологии позволяют использовать многообразные устройства для доступа к данным по всему миру, а также снижают или полностью устраняют затраты на прокладку дорогостоящих оптоволоконных или кабельных каналов передачи данных, предоставляя при этом все возможности проводных сетей.

Адаптеры беспроводной сети, которые бывают внутренними и внешними, позволяют подключать компьютеры к сети без помощи кабелей или каких-либо иных физических соединений. Передаваемые данные разбиваются на небольшие пакеты и транслируются между компьютером и приемопередатчиками в виде радиосигналов в специально отведенном диапазоне частот.

## Соединение сетей и маршрутизация

Чтобы разобраться, как именно происходит обмен данными между сетями, рассмотрим пример двух локальных сетей A и B, связанных между собой в одной точке соединения, называемой **узлом** (Node) (Рис. 1.10). В сетевом узле может находиться специальное устройство или компьютер с двумя сетевыми картами, выполняющий одну из следующих функций:

- **повторитель** (Repeater);
- **мост** (Bridge);
- **маршрутизатор** (Router), иногда также называемый **межсетевым шлюзом** (Gateway).

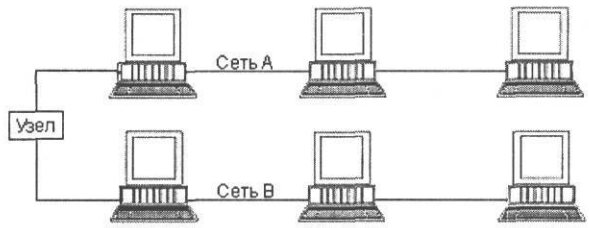



*Рис. 1.10. Схема соединения двух локальных сетей*

Выбор того или иного устройства, расположенного в узловой точке, зависит от степени сетевой интеграции.

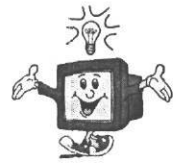
Повторитель используется при необходимости соединения двух относительно далеко расположенных участков (сегментов) одной и той же сети. Повторитель просто усиливает сигнал в линии связи в обе стороны, делая это совершенно незаметно для компьютеров, подключенных к разным сетевым сегментам.

Мост является более интеллектуальным устройством, чем повторитель. Мост соединяет локальные сети, базирующиеся на единой технологии. Он отличается от повторителя тем, что отфильтровывает информацию, пропуская через себя только ту часть, которая адресована компьютерам, расположенным в другом сегменте. Естественно, попутно с этим электрический сигнал подвергается усилению до нужного уровня. Использование мостов снимает ограничения на максимальное количество соединенных ими кабельных сегментов. Мосты находят довольно широкое применение в сетевой операционной системе Novell NetWare, а в Windows используются редко, поэтому нас больше интересуют маршрутизаторы.

Маршрутизатор (межсетевой шлюз) выполняет сходные с мостом функции, но, в отличие от него, имеет в каждой подсети собственный сетевой адрес и может связывать сети, использующие различные технологии, например, Ethernet и Token Ring. Маршрутизатор связывает между собой не кабельные сегменты одной локальной сети, а уже разные сети, которые могут даже отличаться по используемым технологиям, например, на базе коаксиального кабеля и витой пары. Количество локальных сетей, соединенных между собой маршрутизаторами, может быть очень велико. Интернет представляет собой именно такое объединение.

В роли маршрутизатора обычно используется компьютер с двумя сетевыми картами, каждая из которых подключена к своему кабельному сегменту. Этот компьютер должен быть включен постоянно или хотя бы на время работы локальных сетей, иначе связь между ними прервется.

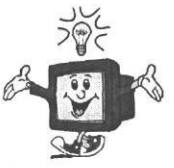
*Имейте в виду, что одна сетевая карта типа Combo не может работать в качестве маршрутизатора. Хотя она имеет несколько разъемов для разных видов кабеля, но в одно и то же время может работать только через один из них.*



Рассмотрим алгоритм работы маршрутизатора.

Предположим, что компьютер №1 (Рис. 1.10) посылает пакет данных, адресованный компьютеру №2. Так как оба эти компьютера находятся в сети А, компьютер №2 распознает свой адрес и принимает пакет. Аналогичным образом происходит непосредственная доставка пакетов данных в сети В между компьютерами №3, №4 и №5. В данном случае маршрутизатор не задействуется.

*Непосредственная доставка пакетов данных в пределах одной сети происходит независимо от ее топологии: общая шина, звезда или кольцо. Не играет роли и используемая сетевая технология.*



А что произойдет, если компьютер №1 из сети А, захочет отправить пакет данных, адресованный компьютеру №5, находящемуся в сети В? Компьютер №1 в процессе отправки определит, что адрес получателя пакета не входит в адресный диапазон сети А, и перешлет его на пункт промежуточной доставки - шлюз А, являющийся функциональным компонентом маршрутизатора (Рис. 1.11).

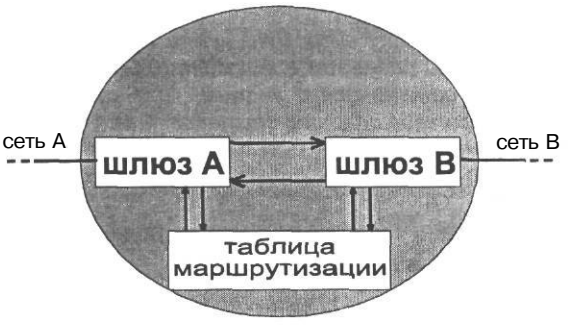
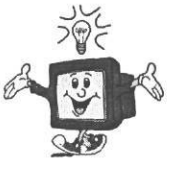



*Рис. 1.11. Функциональная схема маршрутизатора*

Маршрутизатор, получивший пакет данных, просмотрит свою **таблицу маршрутизации** (Routing Table) и определит, что пакет нужно отправить через шлюз В. Когда пакет данных через шлюз В попадет в соответствующую сеть, он благополучно будет принят компьютером №5.

*Имейте в виду, что здесь рассмотрена наиболее простая схема. Во-первых, к маршрутизатору может быть подключено не две, а несколько сетей. Во-вторых, получатель не обязательно должен быть непосредственно связан с сетью, куда передается пакет. Например, в Интернете пакет данных может пройти через десятки маршрутизаторов, прежде чем достигнет своего получателя.*



# Базовые принципы технологии Ethernet

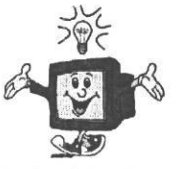
Нас интересует, прежде всего, технология Ethernet. На ее основе лучше всего создавать локальные сети по ряду причин:

- широкая распространенность;
- большой ассортимент оборудования, имеющегося в продаже;
- умеренные цены на большинство продаваемых устройств;
- возможность выбора необходимой скорости передачи данных;
- поддержка различных топологий;
- поддержка нескольких стандартов используемой кабельной системы.

## Скорости передачи данных

Скорость передачи данных, характеризующая тот или иной сетевой стандарт, обычно измеряется в мегабитах в секунду (Мбит/с).

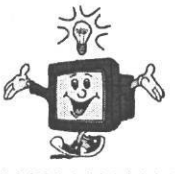
*Чтобы лучше представлять эту скорость, нужно иметь в виду, что количество информации размером 8 мегабит (0,008 Гигабит) равно 1 мегабайту. Для ориентировки укажем, что на обычной дискете умещается 1,44 мегабайта, что составит 1,44*8= 11,52 мегабит (0,01152 Гигабит).*



Различные варианты реализации технологии Ethernet поддерживают следующие уровни максимальной скорости передачи данных:

- 10 мегабит в секунду (Ethernet);
- 100 мегабит в секунду (Fast Ethernet);
- 1 гигабит в секунду (Gigabit Ethernet).

*Реальная скорость передачи данных всегда значительно ниже максимально возможной из-за имеющихся особенностей процесса передачи на физическом уровне.*



## Используемые стандарты Ethernet

Скорости величиной 10 Мбит/с и 100 Мбит/с в настоящее время являются наиболее распространенными. Вариант технологии со скоростью передачи 1 Гбит/с разработан совсем недавно, соответствующее оборудование стоит очень дорого, и найти его труднее.

Поэтому нас интересуют, прежде всего, недорогие в реализации стандарты технологии Ethernet, поддерживающие скорости 10 Мбит/с и 100 Мбит/с:

- 10Base-2;
- 10Base-T;
- 100Base-T.

Рассмотрим их более подробно, так как на их основе чаще всего строятся локальные сети для дома и офиса.

## Стандарт 10Base-2

Основные характеристики стандарта 10Base-2:

- максимальная скорость передачи данных - 10 Мбит/с;
- топология - шина;
- тип кабеля — тонкий коаксиальный;
- максимальная длина кабельного сегмента - 185 метров;
- количество компьютеров, подключенных к общей шине, - до 30.

Достоинства:

- легкость наращивания сети;
- не очень высокая стоимость оборудования;
- хорошая помехоустойчивость.

Недостатки:

- скорость передачи данных не слишком высока;
- нарушение соединения в одном месте приводит к прекращению работы всей локальной сети;
- при подключении большого количества компьютеров происходит резкое снижение производительности;
- безопасность информации обеспечивается не на слишком высоком уровне.

## Стандарт 10Base-T

Основные характеристики стандарта 10Base-T:

- максимальная скорость передачи данных - 10 Мбит/с;
- топология - звезда;
- тип кабеля - витая пара;
- максимальная длина кабельного сегмента - 100 метров;
- максимальное количество компьютеров, находящихся в одной «звезде», - в зависимости от числа портов концентратора.

Достоинства:

- возможность несложного апгрейда до скорости 100 Мбит/с;
- нарушение соединения в одном месте, кроме центрального узла, не прерывает работы локальной сети;
- при подключении большого количества компьютеров не происходит снижения производительности;
- безопасность информации обеспечивается на высоком уровне, так как компьютеры не получают чужих данных.

Недостатки:

- скорость передачи данных не слишком высока;
- большой расход соединительного кабеля;
- поломка центрального узла приводит к неработоспособности всей сети;
- наращивание сети сопряжено с большими финансовыми затратами;
- помехоустойчивость ниже, чем у 10Base-2.

## Стандарт 100Base-T

В сущности, 100Base-T (часто называемый **Fast Ethernet** - быстрый **Ethernet)** - это собирательное название нескольких аналогичных стандартов:

- iOOBase-T4;
- 100Base-TX;
- 100Base-VG.

Тем не менее, все они работают на витой паре и обеспечивают одинаковую максимальную скорость передачи данных.

Основные характеристики стандарта 100Base-T:

- максимальная скорость передачи данных - 100 Мбит/с;
- топология - звезда;
- тип кабеля - витая пара;
- максимальная длина кабельного сегмента - 100 метров;
- максимальное количество компьютеров, находящихся в одной «звезде», - в зависимости от числа портов концентратора.

Достоинства:

- высокая скорость передачи данных;
- нарушение соединения в одном месте, кроме центрального узла, не прерывает работы локальной сети;
- при подключении большого количества компьютеров не происходит снижения производительности;

- безопасность информации обеспечивается на высоком уровне, так как компьютеры не получают чужих данных.

Недостатки:

- большой расход соединительного кабеля;
- поломка центрального узла приводит к неработоспособности всей сети;
- наращивание сети сопряжено с большими финансовыми затратами;
- помехоустойчивость несколько ниже, чем у 10Base-2.

# Оборудование сетей 10Base-T и 100Base-T на витой паре

Наибольший интерес для построения локальных домашних и офисных сетей представляют стандарты 10Base-T и 100Base-T на витой паре. Оборудование для создания таких сетей включает кабели, сетевые карты, разъемы, концентраторы, монтажные инструменты.

## Кабели

Для монтажа локальных сетей стандартов 10Base-T и 100Base-T может использоваться:

- толстый коаксиальный кабель (Thick Ethernet Coaxial Cable);
- витая пара (Twisted Pair).

### Толстый коаксиальный кабель

Толстый коаксиальный кабель аналогичен тонкому, но диаметр у него составляет 1 см. Чаще всего он применяется в больших сетях на базе 10Base-T и 100Base-T для организации связи между несколькими центральными узлами. Максимальная длина кабельного сегмента на толстом коаксиальном кабеле составляет 500 метров, что позволяет использовать его для соединения сетей, находящихся в разных домах.

### Витая пара

Витая пара используется преимущественно в домашних и малых офисных сетях. По своему внешнему виду и структуре напоминает импортный телефонный кабель. Но, если быть более точным, то дело обстоит как раз совсем наоборот - телефонный кабель является одной из многочисленных разновидностей витой пары.

В зависимости от наличия или отсутствия экрана витая пара может быть следующих видов:

- неэкранированная витая пара (Unshielded Twisted Pair - UTP);
- экранированная витая пара (Shielded Twisted Pair - STP);
- фольгированная витая пара (Foiled Twisted Pair - FTP).

Неэкранированная витая пара стоит намного дешевле экранированных вариантов, поэтому используется чаще всего. Конструктивно она представляет собой несколько пар скрученных изолированных проводников, размещенных в общей внешней изоляции (Рис. 1.12).

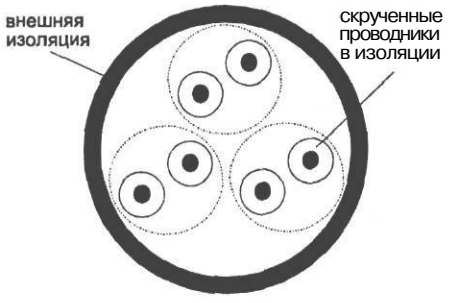



*Рис. 1.12. Неэкранированная витая пара в разрезе*

Экранированная и фольгированная витая пара устроены точно так же, но под слоем внешней изоляции находится защитный экран из плетеной проволоки или слоя алюминиевой фольги.

Промышленностью выпускается пять различных категорий неэкранированной витой пары, предназначенных для голосовой телефонной связи и использования в локальных сетях. Их назначение показано в следующей таблице.

| Категория | Назначение |
|---|---|
| 1 | Передача голосовых сообщений. |
| 2 | Передача голосовых сообщений и данных на скорости до 1 Мбит/с. |
| 3 | Передача голосовых сообщений и данных на скорости до 10 Мбит/с (Ethernet 10Base-T). |
| 4 | Передача данных в сетях Token Ring со скоростью 16 Мбит/с. |
| 5 | Передача данных на скорости до 100 Мбит/с (Ethernet 100Base-T). |

Оптимальным выбором для домашней сети 10Base-T или 100Base-T будет неэкранированная витая пара (UTP) пятой категории, позволяющая осуществлять передачу данных на скорости до 100 Мбит/с, конечно, при наличии соответствующих сетевых карт.

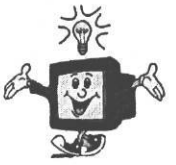
## Сетевые карты

В зависимости от типа разъемов сетевые карты, работающие на витой паре, бывают следующих видов:

- TP;
- Combo.

Сетевые карты TP с разъемом RJ-45 предусматривают подключение только с помощью витой пары. Что же касается карт Combo, то они имеют разъемы для подключения кабелей различных типов.

*Если планируется связать между собой локальные сети из двух или нескольких домов через узловой компьютер, то нужно купить сетевую карту с разъемом AUI, необходимым для связи с помощью толстого коаксиального кабеля.*



Сетевые карты для витой пары могут поддерживать различные скорости передачи данных:

- 10 Мбит/с;
- 100 Мбит/с;
- 10/100 Мбит/с.

В зависимости от варианта подключения к шинам данных компьютера, сетевые карты бывают следующие:

- PCI;
- ISA;
- USB;
- PCMCIA (PC Card).

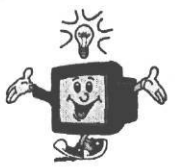
Карты PCI вставляются в разъем шины PCI внутри системного блока компьютера. Они поддерживают режим Plug & Play и сами инициализируются операционной системой в момент загрузки.

Сетевые карты ISA также находятся внутри компьютера, но подключаются к шине ISA. Сейчас эта шина уже устарела и встречается не на всех компьютерах. Данные карты обычно приходится настраивать вручную с помощью перемычек или специальной установочной программы, задавая нужное прерывание, адрес и прочее.

Внешние сетевые карты, выполненные в виде отдельного устройства, подключаются к разъему USB, расположенному на задней стенке системного блока. Как и PCI-карты, они настраиваются автоматически.

Сетевые карты для ноутбуков поддерживают стандарт PCMCIA (PC Card) и вставляются в соответствующий разъем.

*Из личного опыта: при выходе из строя сетевой карты Combo, работавшей на коаксиальном кабеле, ее часто можно использовать для витой пары, так как на коаксиале почти всегда горит микросхема, которая не используется на витой паре.*



Из сказанного следует, что лучше всего приобретать сетевые карты PCI, рассчитанные на скорость передачи данных 100 Мбит/с. Карты ISA покупать не рекомендуется, так как они сложнее в настройке и используют устаревший шинный разъем, который в

современных компьютерах может отсутствовать. Производитель особой роли не играет, но, по соображениям совместимости и надежности, лучше использовать сетевые карты известных фирм, таких как Realtek, Intel, D-Link, 3COM.

## Разъемы

Для соединения витой пары с сетевыми картами нужны пластмассовые вилки с разъемом RJ-45. Внешний вид данной вилки, также называемой «карамелькой», изображен на Рис. 1.13 и Рис. 1.14.

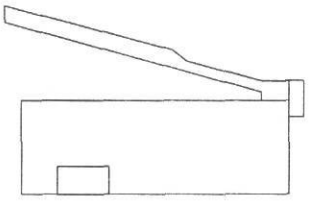


*Рис. 1.13. Вилка с разъемом RJ-45, вид сбоку*

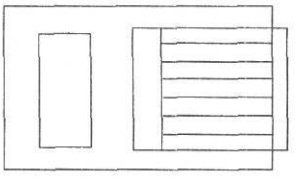


*Рис. 1.14. Вилка с разъемом RJ-45, вид снизу*

## Концентраторы и коммутаторы

При соединении трех и более компьютеров с помощью витой пары необходимо использовать специальное устройство - **концентратор,** или, другими словами, **хаб** (Hub). Концентратор располагается в центре звезды и обеспечивает информационный обмен между компьютерами. Обычный «классический» хаб не делает ничего кроме соединения компьютеров в узле и усиления сигнала, но в настоящее время обычно хабы имеют функции коммутаторов, или свитчей, от английского слова Switch - переключатель. Коммутатор обеспечивает более быструю связь между компьютерами в сети за счет того, что разрешает коллизии в узле при попытке компьютеров одновременно передавать данные, уменьшая при этом паузы ожидания данных. Коммутаторы, или свитчи, похожи на маршрутизаторы, но если маршрутизаторы работают на уровне адресов программных протоколов, о которых речь пойдет ниже, то коммутаторы ориентируются на физические адреса сетевых карт компьютеров и являются менее интелектуальными устройствами по сравнению с маршрутизаторами.

Концентратор представляет собой небольшую пластмассовую коробку с разъемами для вилок RJ-45.

Выпускаемые концентраторы поддерживают определенную скорость и имеют фиксированное количество портов, то есть — разъемов для подключения компьютеров, которое кратно двум. Наибольшее распространение получили хабы с 4, 8 и 16 портами.

Таким образом, основными параметрами приобретаемого концентратора является поддерживаемая скорость и число портов. Оптимальным выбором будет универсальный концентратор 10/100 Мбит/с, число портов которого не меньше количества подключаемых компьютеров. Не последней характеристикой является и цена, так как концентратор - устройство дорогостоящее. Однако если средства позволяют, следует купить хороший хаб фирмы 3COM или Cisco.

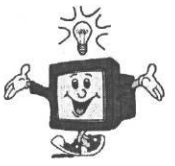
## Монтажные инструменты

Для монтажа соединений на витой паре используются следующие инструменты:

- устройство для обрезки витой пары;
- устройство для обжима вилки с разъемом RJ-45.

Эти инструменты можно не покупать, а взять у кого-нибудь на время, так как монтажные работы производятся редко.

*В случае крайней необходимости вместо монтажных инструментов можно воспользоваться острым ножом и обычной отверткой с прямым шлицем подходящего размера.*



# Физическое подключение сетевых карт к компьютерам

Как уже отмечалось, сетевые карты бывают внешними и внутренними. Соответственно различаются способы их подключения к компьютеру.

## Внешние сетевые карты (USB или PCMCIA)

Проще всего подключить к компьютеру внешнюю карту, для чего нужно сделать следующее:

➤ Выключите компьютер, если он до этого был включен.

➤ На задней стенке компьютера найдите разъем порта USB или PCMCIA, подключите к нему кабель, идущий от внешней сетевой карты.

## Внутренние сетевые карты (PCI или ISA)

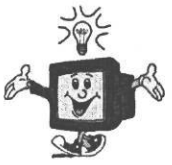
Подключение любой внутренней карты требует разборки компьютера. Если вы делаете это впервые, то лучше обратиться за помощью к специалисту. Однако можно попробовать все сделать и самому.

➤ Выключите компьютер, если он до этого был включен.

> Вытащите вилку питания системного блока компьютера из электрической розетки.

> Снимите крышку системного блока компьютера, открутив с помощью крестообразной отвертки несколько болтов на задней панели.

*Крышка системного блока во многих современных корпусах может открываться и без отвертки. Чаще всего требуется нажать на кнопку, отодвигающую защелку, а затем снять крышку. Подробно об этом можно прочитать в техническом руководстве к компьютеру.*



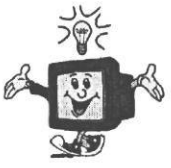
> Выберите подходящий по размеру свободный шинный разъем на материнской плате. Современные сетевые карты обычно вставляются в разъем системной шины PCI, а старые модели - в разъем ISA.

Если это старая карта ISA, настраивающаяся установкой переключателей (Jumpers), которые определяют номер базового адреса порта (Port) и прерывания (IRQ), выполните их установку, воспользовавшись прилагаемым руководством. Обычно используется комбинация: Port 300, IRQ 3.

> Открутите и вытащите заглушку на задней панели системного блока напротив выбранного разъема. Если же она закреплена «намертво» без болтов, то выломайте ее.

➤ Слегка покачивая, вставьте сетевую карту в разъем и убедитесь, что она вошла туда до упора.

*При установке сетевой карты в разъем не прилагайте чрезмерных усилий, чтобы не повредить материнскую плату. Лучше вытащите карту и попробуйте вставить ее снова.*



> Прикрутите сетевую карту болтом к корпусу системного блока в том месте, где раньше была закреплена заглушка.

➤ Наденьте и закрепите болтами крышку системного блока компьютера.

После установки сетевых карт в компьютеры, необходимо смонтировать сеть.

# Монтаж локальной сети на основе витой пары

В зависимости от количества компьютеров, монтаж локальной сети на основе витой пары несколько различается.

## Два компьютера

Для соединения двух компьютеров с помощью витой пары необходимо иметь:

- 2 сетевые карты TP или Combo;
- 2 вилки с разъемом RJ-45;
- кусок витой пары пятой категории.

Порядок выполнения монтажа:

- Проложите витую пару по нужному пути между двумя компьютерами, не допуская повреждений, сильных изгибов и перекручивания. Оставьте с каждой стороны запас пару метров на случай возможных перестановок компьютеров и для удобства монтажа разъемов.
- Обрежьте слои изоляции на нужную длину с обоих концов кабеля. Проще всего сделать это с помощью специального устройства для обрезки витой пары.
- Закрепите вилки RJ-45 на обоих концах кабеля в соответствии со схемой «cross-over» (нуль-хабного кабеля), предназначенной для соединения 4-х или 8-жильной витой пары.

Схема соединения 4-жильной витой пары с вилками RJ-45 для подключения двух компьютеров «cross-over» (нуль-хабного кабеля) показана в следующей таблице:

| **одна вилка RJ-45** | **цвет провода** | **другая вилка RJ-45** |
|---|---|---|
| **1** | **бело-оранжевый** | **3** |
| **2** | **оранжевый** | **6** |
| **3** | **бело-синий** | **1** |
| **6** | **синий** | **2** |

Схема соединения 8-жильной витой пары с вилками RJ-45 для подключения двух компьютеров «cross-over» (нуль-хабного кабеля) показана в следующей таблице:

| одна вилка RJ-45 | цвет провода | другая вилка RJ-45 |
|---|---|---|
| 1 | бело-зеленый | 3 |
| 2 | зеленый | 6 |
| 3 | бело-оранжевый | 1 |
| 4 | синий | 4 |
| 5 | бело-синий | 5 |
| 6 | оранжевый | 2 |
| 7 | бело-коричневый | 7 |
| 8 | коричневый | 8 |

- Установите до щелчка вилки RJ-45 в разъемы на сетевых картах.

В результате должно получиться нужное соединение, которое будет выглядеть примерно так, как показано на схеме (Рис. 1.15).

*Рис. 1.15. Два компьютера, соединенные витой парой*

## Небольшая локальная сеть

При создании небольшой локальной сети, состоящей из трех или более компьютеров (Рис. 1.16), придется несколько изменить технологию монтажа по сравнению с двумя компьютерами, а именно:

- использовать концентратор;
- по-другому подключать провода витой пары к вилке RJ-45.

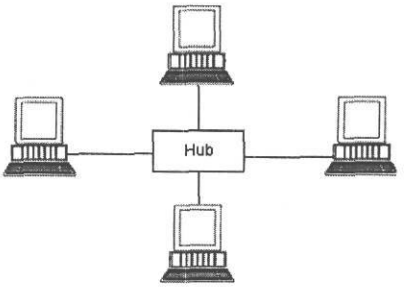



*Рис. 1.16. Локальная сеть на базе витой пары*

Порядок выполнения монтажа:

➤ Проложите витую пару по нужному пути между концентратором и всеми компьютерами, не допуская повреждений, сильных изгибов и перекручивания. Оставьте с каждой стороны запас длиной в пару метров на случай возможных перестановок компьютеров и для удобства монтажа разъемов.

➤ Обрежьте слои изоляции на нужную длину с обоих концов кабеля. Проще всего сделать это с помощью специального устройства для обрезки витой пары.

➤ Закрепите вилки RJ-45 на обоих концах кабеля в соответствии со схемой прямого соединения, предназначенной для 4-х или 8-жильной витой пары.

| **одна вилка RJ-45** | **цвет провода** | **другая вилка RJ-45** |
|---|---|---|
| **1** | **бело-оранжевый** | **1** |
| **2** | **оранжевый** | **2** |
| **3** | **бело-синий** | **3** |
| **6** | **синий** | **6** |

Схема соединения 8-жильной витой пары с вилками RJ-45 для подключения к концентратору показана в следующей таблице:

| одна вилка RJ-45 | цвет провода | другая вилка RJ-45 |
|---|---|---|
| 1 | бело-зеленый | 1 |
| 2 | зеленый | 2 |
| 3 | бело-оранжевый | 3 |
| 4 | синий | 4 |
| 5 | бело-синий | 5 |
| 6 | оранжевый | 6 |
| 7 | бело-коричневый | 7 |
| 8 | коричневый | 8 |

> Установите до щелчка вилки RJ-45 в разъемы на сетевых картах и концентраторе.

## Большая сеть

Для создания большой сети в доме или районе на базе витой пары необходимо связать концентраторы между собой с помощью толстого коаксиального кабеля (Рис. 1.17).

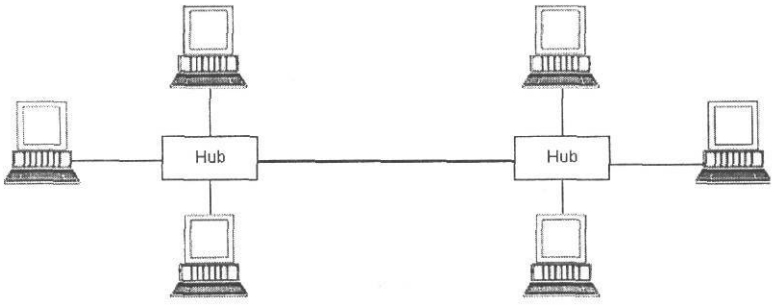



*Рис. 1.17. Большая локальная сеть на базе витой пары*

Таким образом можно соединить несколько концентраторов, но суммарная длина сегмента из толстого коаксиального кабеля не должна превышать 500 метров.

В случае необходимости дальнейшего увеличения сети можно воспользоваться повторителями (Repeater). Один повторитель позволяет увеличить общую длину кабеля в два раза. Повторителей может быть несколько, но здесь также существуют свои ограничения:

- максимальное число повторителей - 4;
- максимальное число кабельных сегментов, напрямую связанных между собой повторителями, - 5, в том числе 3 сегмента с концентраторами и 2 связующих;
- суммарная длина этих сегментов - 2500 метров;
- максимальное количество повторителей, подключенных к одному сегменту, - 100.

## Протоколы передачи данных по компьютерным сетям

Теперь от вопросов организации и принципов построения компьютерных сетей перейдем к рассмотрению основных принципов и протоколов передачи данных по сети. Знание основных сетевых протоколов поможет вам правильно настроить работу любой компьютерной сети.

Подобно незнакомым людям из разных стран, которые, встречаясь, следуют определенным правилам поведения - приветствуют друг друга, договариваются, на каком языке будут вести беседу, и только после этого приступают к общению, компьютеры также используют определенные правила (протоколы) для общения (передачи данных). Сетевые протоколы - это набор правил для передачи данных между компьютерами, объединенными в сеть. Без протоколов передачи данных было бы невозможно обмениваться информацией между компьютерами. Очевидно, что отправитель и получатель должны сначала согласовать между собой точный способ обмена данными, т.е. выбрать подходящие для обеих сторон протоколы, иначе передача данных между ними будет невоз-

можна. Другими словами, каждая программа, работающая в сети, должна следовать определенным правилам для приема и передачи данных. Использование всеми компьютерами сети одного протокола гарантирует, что ваш IBM-совместимый компьютер сможет связаться, например, с компьютером Macintosh фирмы Apple в заокеанском университете. При использовании одного протокола для функционирования всей сети не имеет значения, какие компьютеры подключены к сети и какое программное обеспечение на них установлено.

# Модель OSI

Существует большое количество различных протоколов передачи данных по компьютерным сетям. Выбор того или иного протокола определяется как используемым сетевым оборудованием, так и операционными системами, установленными на подключенных к сети компьютерах. С целью стандартизации сетевых протоколов, облегчения работы с ними и понимания их функций разработана семиуровневая модель OSI (Open System Interconnection - Взаимодействие открытых систем) - общая модель, помогающая систематизировать все аспекты сетевого взаимодействия компьютеров (Рис. 1.18). Каждый уровень этой модели соответствует определенному аспекту работы сети.


*Рис. 1.18. Модель OSI*

Установленные на компьютере сетевые программы не сразу посылают данные на сетевую карту. Данные, подготовленные программой для передачи по сети, проходят несколько этапов обработки. Эти этапы называются уровнями. В модели OSI их семь: прикладной, уровень презентации, или представления данных; уровень сеанса; транспортный; сетевой; уровень связи данных, или канальный; физический.

На самом высоком, прикладном уровне обрабатываются запросы прикладных программ, которым требуется сетевая связь, например, для доступа к Web-страницам. На этом уровне используются такие протоколы, как HTTP (Hypertext Transfer Protocol - Протокол

передачи гипертекста), обеспечивающий просмотр Web-страниц с помощью браузеров, и FTP (File Transfer Protocol - Протокол передачи файлов), используемый для передачи файлов, и другие.

Протоколы уровня презентации, или представления данных осуществляют шифрование и дешифрование, сжатие и восстановление данных, а также перекодирование текста.

На сеансовом уровне устанавливается и поддерживается сеанс связи между приложениями на разных компьютерах. Для этого используется удаленный вызов процедур (Remote Procedure Call - RPC), позволяющий устанавливать сеанс связи двух удаленных сетевых компьютеров путем передачи сообщений. На данном уровне используется протокол NetBIOS (Network Basic Input Output System - Сетевая базовая система ввода-вывода), и его расширенная версия - NetBEUI (NetBIOS Extended User Interface - Расширенный пользовательский интерфейс).

Транспортный уровень отвечает за передачу сообщений между компьютерами без потери данных. При необходимости, выполняется повторная пересылка пакетов и коррекция ошибок. К протоколам этого уровня относится протокол TCP (Transfer Control Protocol - Протокол управления передачей данных).

На сетевом уровне осуществляется пересылка пакетов между компьютерами сети. Следует обратить внимание на один момент, важный для понимания принципов передачи данных по компьютерной сети. Дело в том, что данные передаются в сети не непрерывным потоком, а пакетами (кадрами) определенной длины. В свою очередь, каждый пакет данных состоит из набора полей (нескольких следующих друг за другом разрядов), предназначенных для хранения адреса получателя данных, контрольной суммы, информации для коррекции ошибок и т.п. и самих данных. Протоколы сетевого уровня отвечают также за определение наилучших маршрутов для передачи данных между компьютерами сети. Для этого средствам сетевого уровня при создании сети указывают *логические сетевые адреса* компьютеров, подключенных к сети. В качестве логических сетевых адресов используются IP-адреса, о которых мы поговорим далее. Для работы с IP-адресами используется протокол IP (Internet Protocol - Протокол Интернета). Наилучший маршрут доставки информации в сети определяют специальные устройства, называемые маршрутизаторами, работающие на сетевом уровне.

Протоколы уровня связи данных (канального) обеспечивают надежные каналы связи между средствами сетевого уровня. На этом уровне из потока битовых данных, направляемых для передачи по сети, формируются фреймы (кадры) - небольшие фрагменты, каждый из которых содержит информацию о количестве данных в этом фрейме и адрес назначения. Структура и содержимое фреймов зависит от типа сети. Если сеть использует две технологии, например, Ethernet и Token Ring, то для их связи необходимо использовать устройство, называемое мостом. Место назначения фреймов на уровне связи данных определяется **MAC-адресом** (Media Access Control - Управление доступом к среде передачи) сетевого компьютера. **MAC-адрес** представляет собой шестнадцатеричное число из 12 цифр, например 00 04 AC 26 5E 8E.

Физический уровень беспечивает работу компонентов оборудования. Он описывает способ пересылки сигналов через среду передачи, например, кабель или беспроводную линию связи. Этот уровень оперирует непосредственно с электрическими сигналами, соответствующими двум состояниям бита информации: 0 (выключено) или 1 (включено).

На данном уровне передаваемая информация рассматривается в виде последовательности битов потока двоичных данных. Если сигнал ослабевает, то его можно усилить с помощью устройства, называемого повторителем. На физическом уровне выполняется последняя обработка данных, после чего они передаются в канал связи.

Каждому уровню обработки данных соответствует одноименный протокол передачи данных. На сетевом уровне - сетевой протокол, на транспортном уровне - транспортный протокол и т.д. Таким образом, данные до реальной передачи проходят через так называемый **стек протоколов** - цепочку протоколов от верхних, более абстрактных уровней, до нижнего, физического, уровня, на котором и осуществляется собственно передача данных. При приеме данные проходят через точно такой же стек протоколов, но в обратном порядке. Стек протоколов был разработан для обеспечения совместимости между сетевым оборудованием и операционными системами разных производителей.

Протоколы каждого уровня решают сходные задачи и «не лезут в дела» протоколов другого уровня. Протоколы верхнего уровня используют для своих задач функции протоколов нижнего уровня. Так протокол физического уровня отвечает лишь за правильное преобразование информации в сигнал, используемый в канале связи, а также последующее восстановление информации из этого сигнала. Протоколу транспортного уровня безразлично, каким образом кодируется информация в канале связи. Он отвечает лишь за передачу части данных от одного компьютера к другому, используя функции протокола физического уровня. Если вдруг будет придуман какой-то новый способ передачи данных, то для его внедрения достаточно будет написать протоколы физического уровня. Самый верхний уровень протоколов - уровень приложений. Он определяет правила взаимодействия прикладных программ, работающих на разных машинах.

Данные передаются от протоколов верхнего уровня к протоколу канала связи, причем на каждом уровне соответствующий протокол добавляет к данным свои служебные поля. Вполне возможно также деление информации на более мелкие пакеты. Затем информация передается по каналу связи и декодируется в обратном порядке.

Таким образом, процесс обработки данных для передачи по сети напоминает отправку письма по обычной почте, где на каждом этапе происходит добавление ему новых свойств: письмо упаковывается в конверт, на конверте пишется адрес, далее письма сортируются и т.д. Так же и при передаче данных между компьютерами: на каждом уровне обработки к передаваемым данным добавляется дополнительная информация, необходимая для безошибочной доставки их адресату.

## Основные сетевые протоколы

В общем случае для нормальной работы сети и сетевых программ вполне достаточно, чтобы на сетевых компьютерах, работающих под управлением операционной системы Windows, были установлены и настроены следующие сетевые протоколы: **NetBEUI, IPX/SPX и TCP/IP.**

Протокол **NetBEUI** (NetBIOS[1] Extended User Interface - Расширенный пользовательский интерфейс NetBIOS) — это протокол, дополняющий спецификацию ввода-вывода **NetBIOS,** используемого сетевой операционной системой. Он является базовым сетевым протоко-

[1] NetBIOS - Netware Base Input/Output System - Сетевая базовая система ввода-вывода.

лом для персонального компьютера и был разработан фирмой IBM для LanManager Server (сервера управления локальной сетью). Позднее Microsoft адаптировала этот протокол для своих сетевых продуктов.

Протокол NetBIOS использует для идентификации компьютеров сетевые имена NetBIOS, которые представляют собой произвольную символьную строку длиной не более 16 символов, например, Client-1, Client-2 и так далее. Таким образом, данный протокол позволяет задавать осмысленные имена сетевых компьютеров, соответствующие их сетевым и машинным адресам. Несмотря на некоторые недостатки, протокол NetBIOS поддерживается всеми версиями операционной системы Windows.

Протокол **IPX/SPX** (Internetwork Packet Exchange/Sequenced Packet Exchange - Межсетевой обмен пакетами/Последовательный обмен пакетами) является базовым протоколом для сетей Novell. Но он может использоваться различными службами и программами в сетях Microsoft. Под службами понимаются программы, которые обрабатывают данные в соответствии с определенным сетевым протоколом и обладают определенным набором функций, например, коррекцией ошибок.

Протоколы TCP/IP (Transmission Control Protocol/Internet Protocol — Протокол управления передачей данных/Интернет протокол) являются основными межсетевыми протоколами и управляют передачей данных между сетями разной конфигурации и технологии. Именно это семейство протоколов используется для передачи информации в сети Интернет, а также в некоторых локальных сетях. Семейство протоколов TPC/IP включает все промежуточные протоколы между уровнем приложений и физическим уровнем. Общее их количество составляет несколько десятков. Основными среди них являются:

- транспортные протоколы: TCP - Transmission Control Protocol (Протокол управления передачей данных) и другие - управляют передачей данных между компьютерами;
- протоколы маршрутизации: IP - Internet Protocol (Протокол Интернета) и другие - обеспечивают фактическую передачу данных, обрабатывают адресацию данных, определяет наилучший путь к адресату;
- протоколы поддержки сетевого адреса: DNS - Domain Name System (Доменная система имен) и другие - обеспечивает определение уникального адреса компьютера;
- протоколы прикладных сервисов: FTP - File Transfer Protocol (Протокол передачи файлов), HTTP - HyperText Transfer Protocol (Протокол передачи гипертекста), TELNET и другие - используются для получения доступа к различным услугам: передаче файлов между компьютерами, доступу к WWW, удаленному терминальному доступу к системе и др.;
- шлюзовые протоколы: EGP - Exterior Gateway Protocol (Внешний шлюзовый протокол) и другие - помогают передавать по сети сообщения о маршрутизации и информацию о состоянии сети, а также обрабатывать данные для локальных сетей.
- почтовые протоколы: POP - Post Office Protocol (Протокол приема почты) - используется для приема сообщений электронной почты, SMPT Simple Mail Transfer Protocol (Протокол передачи почты) - используется для передачи почтовых сообщений.

Все основные сетевые протоколы (NetBEUI, **IPX/SPX** и TCPJIP) являются маршрутизируемыми протоколами. Но вручную приходится настраивать лишь маршрутизацию TCPJIP. Остальные протоколы маршрутизируются операционной системой автоматически.

Если вы работаете с операционной системой Windows и подключаетесь к локальной сети или Интернету, то для нормальной работы сетевых программ достаточно, чтобы на вашем компьютере был установлен протокол TCP/IP, однако для некоторых приложений может потребоваться установка других перечисленных выше протоколов.

Для передачи данных по протоколу TCP/IP в операционных системах Windows 2000/XP/2003 используются два основных метода: протокол NetBT (NetBIOS через TCP/IP) и сокеты *Windows* (Windows Sockets), обычно называемые Winsock. Выбор метода определяется типом приложения.

Протокол NetBT, по сути, объединяет два протокола - NetBIOS и TCP/IP и позволяет операционной системе Windows работать с именами NetBIOS, предназначенными для идентификации компьютера в сети, передавать данные, используя транспортный протокол NetBEUI, и управлять сеансом связи.

Сокет Windows представляет собой гнездо или точку входа в систему Windows и используется приложениями для создания между компьютерами сети двунаправленного канала связи. Приложения, использующие сокеты, называются приложениями Winsock. К ним относятся браузеры, в частности, Internet Explorer, почтовые клиенты, например Outlook Express, и другие. Каждому сокету назначается логический сетевой адрес, позволяющий другим компьютерам находить его в сети, и номер порта, указывающий приложение, инициирующее связь с приложением на другом компьютере. В качестве логических адресов используются IP-адреса. О них мы будем говорить далее.

## Сервисы Интернета - WWW, FTP, почта, новости

Все то, к чему получает доступ пользователь, подключившийся к Интернету, принято называть сервисами Интернета. Сервисы осуществляются специальными серверами и могут быть как платными, так и бесплатными. Наиболее популярные среди них: WWW, FTP, электронная почта и новости.

WWW (World Wide Web - Всемирная паутина) - это всемирная информационная система, использующая технологию размещения информации на серверах в виде набора связанных документов. Каждый документ, кроме текста, может содержать графику, звук или видеоизображения. Такая форма представления информации называется мультимедийной. Документ состоит из так называемых Web-страниц, каждая из которых освещает некоторую тему. Просматривая на экране компьютера Web-страницу, можно увидеть основной текст, а также активные изображения или выделенные другими цветами и подчеркнутые фразы. Такие объекты называют гипертекстовыми ссылками и предназначены для связи с другими документами, раскрывающими содержание ссылок. Щелкнув мышью на такой ссылке, можно вызвать на экран Web-страницы из других документов, имеющих отношение к рассматриваемой или родственной теме, даже если документы находятся на серверах в разных концах планеты. Таким способом пользователь черпает необходимую информацию, копирует программы или узнает, куда за ними обратиться. Для этого необходим только доступ в Интернет и программа просмотра Web-страниц - браузер (от английского browser - обозреватель), например Internet Explorer или Opera. Связь браузера с Web-сервером обеспечивается с помощью протокола HTTP.

Сервис FTP (File Transfer Protocol - Протокол передачи файлов) позволяет передавать по сети файлы любого формата. Данный ресурс в последнее время используется, в основном, с целью переписывания файлов с дистрибутивными копиями программ с удаленных серверов на компьютер пользователя. Многие фирмы, имеющие Web-серверы, дополнительно устанавливают FTP-серверы, служащие для распространения программного обеспечения. Например, если вы обратились к Web-серверу корпорации Microsoft, чтобы получить новую версию браузера Internet Explorer, то будете перенаправлены на FTP-серверы, с которых и сможете переписать нужную программу. Заметим сразу, что во многих случаях дистрибутивы программы можно переписать и с Web-сервера. Другая важная функция FTP-серверов - накопление, хранение и распространение файлов. Каждый пользователь, подключившийся к такому хранилищу, может переписать на свой компьютер любые доступные файлы и, кроме того, имеет возможность переслать со своего компьютера на FTP-сервер некоторые файлы, поместив их в специальный каталог, например, для того, чтобы сделать их доступными для своего коллеги. Процесс переписывания файлов на свой компьютер называется загрузкой (downloading). Часто его называют также скачиванием. Пересылка файлов со своего компьютера на другой называется выгрузкой (uploading). Благодаря высокой скорости работы FTP-серверов и отсутствию ограничений на размер файлов, этот сервис является довольно популярным, например, в научной среде.

Для доступа к сервису FTP необходима специальная программа-клиент. Если вы предполагаете лишь периодически переписывать программы с FTP-серверов, то для этого достаточно будет возможностей браузера, например, Internet Explorer. Если же вам необходимо постоянно работать с FTP-серверами, то лучше использовать специальные клиентские программы, например, CuteFTP или WS-FTP32.

Сеть Интернет используется также для пересылки корреспонденции. Этот вид услуг называется электронной почтой (E-mail). По электронной почте можно пересылать тексты, рисунки, фотографии, звукозаписи и другую информацию. Корреспонденция собирается и временно хранится на специальных почтовых серверах. Каждый абонент сети имеет собственный «почтовый ящик», то есть выделенное ему дисковое пространство на почтовом сервере, где хранятся сообщения, приходящие на его имя. Пользователь в любой удобный для него момент времени подключается к почтовому серверу, после чего отправляет и получает корреспонденцию.

Чтобы корреспонденция могла найти своего адресата, каждый компьютер имеет уникальный адрес электронной почты, например, такой: **test@info.ru.** Если на рабочей станции локальной сети работает несколько пользователей, то каждый из них может получить свой собственный адрес E-mail, который будет отличаться от других именем, стоящим перед символом @, например **admin@info.ru.** Подробнее об адресах компьютеров в Интернете мы поговорим ниже. Получив корреспонденцию, пользователь может познакомиться с ней и ответить в любое удобное для него время. Если одинаковые сообщения посылаются разным абонентам, то имеется возможность рассылки по всем адресам, указанным отправителем. Часто списки адресов формируются заранее, например, при организации конференций или подписке на электронный журнал.

Для работы с электронной почтой требуется специальная почтовая программа или почтовый клиент. Наиболее популярные среди них Outlook Express, Eudora, Pegasus.

Еще один вид сервиса Интернета, так называемые телеконференции (Usenet), или новости, позволяет всем абонентам сети участвовать в групповых дискуссиях, в которых обсуждаются различные вопросы. В настоящее время в сети существуют десятки тысяч таких групп, или телеконференций. Их участники обсуждают разнообразные темы — от кулинарных рецептов и НЛО до узкоспециализированных научных.

Организация телеконференций внешне напоминает почтовый обмен сообщениями, но отличается тем, что сообщения посылаются не конкретному пользователю, а в дискуссионную группу - телеконференцию и становятся доступными всем, кто к ним обращается. Распространение сообщений телеконференций в сети выполняют специальные серверы новостей NNTP (Net News Transport Protocol - Транспортный протокол сетевых новостей).

Подключившись к одному из серверов новостей, вы можете получить список содержащихся на нем групп или телеконференций, после чего подписаться на те из них, тематика которых вас заинтересовала. Далее, вы можете загрузить на свой компьютер все сообщения или статьи каждой группы, после чего отключиться от сервера новостей и прочитать статьи. Если вы захотите вступить в дискуссию, то можете написать собственное сообщение в телеконференцию, ответить лично автору любой прочитанной вами статьи или ответить всем участникам данной телеконференции. Чтобы отправить свои сообщения и ответы следует повторно подключиться к серверу новостей.

Работу с серверами новостей обеспечивают специальные программы для чтения телеконференций. Удобные возможности для этого имеются также в почтовой программе Outlook Express.

## Как работают сетевые протоколы для WWW, почты и других сервисов Интернета

Протоколы TPC/IP используют несколько уровней, по которым движется сообщение от одного компьютера к другому. Самый низший уровень - физический - это работа сетевых адаптеров, обеспечивающих преобразование цифровой информации, хранящейся в компьютере, в аналоговые сигналы, которые передаются по кабелям. Следующий уровень - управление передачей пакетов данных. Правильность передачи контролируется. На сетевом уровне организуется прохождение потоков данных через сеть так, чтобы потоки не пересекались. При этом контролируется каждый узел сети. Транспортный уровень обеспечивает упаковку сообщений в пакеты для передачи и сбор пакетов во время приема. Каждый пакет нумеруется и содержит некоторую специальную информацию для контроля передачи данных. В каждом пакете указан также адрес отправителя и получателя. Если во время передачи возникли сбои, то передача сообщений повторяется. Сообщения в сети передаются не непосредственно от одного пользователя к другому, как при телефонном разговоре, а от одного узла сети к другому. Поэтому полученное сообщение может иметь большой заголовок в виде перечня промежуточных адресов, через которые оно прошло. Этот список тем длиннее, чем дальше находится получатель от отправителя.

На каждом узле сети Интернет работают различные программы, обеспечивающие тот или иной сервис. Так, на одной машине могут работать и WWW и FTP-серверы. В данном случае узел обеспечивает два сервиса. Чтобы воспользоваться услугами того или иного сервиса, необходимо знать адрес узла, на котором работает нужный сервис,

и воспользоваться программой-клиентом для обеспечения взаимодействия с сервисом. Например, для просмотра Web-страницы следует запустить программу Internet Explorer, в которой указать адрес нужного ресурса.

Программа-клиент и программа-сервер, обеспечивающая определенный сервис, взаимодействуют по определенным правилам - протоколам - и через определенные порты. Порты используются для разделения информационных потоков на одном узле. Существуют договоренности о том, какие порты закреплены за каким протоколом. Так, например, WWW-сервера, обеспечивающие сервис WWW, работают с Web-клиентами по протоколу HTTP и используют порт 80. Для FTP-клиента и FTP-сервера, обеспечивающего сервис FTP, определен протокол с названием FTP и два порта - 20 и 21.

Итак, серверные узлы Интернет запускают определенные программы-сервисы. Те открывают определенные порты для своих клиентов и ждут обращения. Если клиент знает, по какому адресу, через какой порт и каким протоколом вести диалог с сервером, взаимодействие двух машин становиться возможным.

# IP-адресация

Для связки протоколов TCP/IP базовым является протокол IP, так как именно он занимается перемещением пакетов данных между компьютерами через сети, использующие различные сетевые технологии. Именно благодаря универсальным характеристикам протокола IP стало возможным само существование Интернета, состоящего из огромного количества разнородных сетей.

## Пакеты данных протокола IP

Протокол IP является службой доставки для всего семейства протоколов **TCP/IP**. Информация, поступающая от остальных протоколов, упаковывается в пакеты данных протокола IP, к ним добавляется соответствующий заголовок, и пакеты начинают свое путешествие по сети.

Заголовок пакета данных IP содержит следующие поля, позволяющие доставить его получателю:

- номер версии протокола IP;
- длина заголовка;
- тип службы;
- общая длина пакета;
- идентификатор фрагмента данных;
- флаги;
- смещение фрагмента данных;
- максимальное время жизни пакета;
- протокол, использующий службу доставки IP;

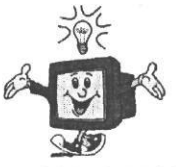
- контрольная сумма заголовка;
- IP-адрес отправителя;
- IP-адрес получателя.

Сразу после заголовка в пакете содержатся передаваемые данные.

## Система IP-адресации

Одними из важнейших полей заголовка пакета данных IP являются адреса отправителя и получателя пакета. Каждый IP-адрес должен быть уникальным в том межсетевом объединении, где он используется, чтобы пакет попал по назначению. Даже во всей глобальной сети Интернет невозможно встретить два одинаковых адреса.

*Адрес **IP** относится не ко всему компьютеру, а к его сетевому интерфейсу. В частности, компьютер, выполняющий функции маршрутизатора, имеет не менее двух сетевых интерфейсов и, соответственно — не менее двух IP-адресов.*



IP-адрес, в отличие от обычного почтового адреса, состоит исключительно из цифр. Он занимает четыре стандартные ячейки памяти компьютера - 4 байта. Так как один байт (Byte) равен 8 бит (Bit), то длина IP-адреса составляет 4 x 8 = 32 бита.

Бит представляет собой минимально возможную единицу хранения информации. В нем может содержаться только 0 (бит сброшен) или 1 (бит установлен). Чтобы пояснить сказанное, приведем конкретный пример IP-адреса (Рис. 1.19).

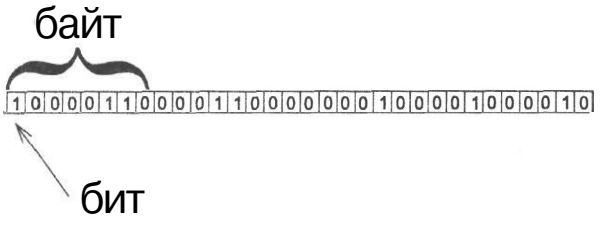



*Рис. 1.19. Пример IP-адреса*

Несмотря на то, что IP-адрес всегда имеет одинаковую длину, записывать его можно по-разному. Формат записи IP-адреса зависит от используемой системы счисления. При этом один и тот же адрес может выглядеть совершенно по-разному:

| Формат числовой записи | Значение |
|---|---|
| Двоичный (Binary) | 10000110000110000000100001000010 |
| Шестнадцатеричный (Hexadecimal) | 0x86180842 |
| Десятичный (Decimal) | 2249721922 |
| Точечно-десятичный (Dotted Decimal) | 134.24.8.66 |

Для преобразования адресов из двоичного в десятичный формат удобно пользоваться следующей таблицей, показывающей десятичные значения битов, начиная с крайнего правого (младший значащий бит).

| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

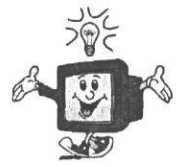
Например, двоичное число 10000110 преобразовывается в десятичное следующим образом: 128 + 0 + 0 + 0 + 0 + 4 + 2 + 0 =134.

Наиболее предпочтительным вариантом, с точки зрения удобства чтения человеком, является формат написания IP-адреса в точечно-десятичной нотации. Данный формат состоит из четырех десятичных чисел, разделенных точками. Каждое число, называемое октетом (Octet), представляет собой десятичное значение соответствующего байта в IP-адресе. Октет называется так потому, что один байт в двоичном виде состоит из восьми бит.

При использовании точечно-десятичной нотации записи октетов в адресе IP следует иметь ввиду следующие правила:

- допустимыми являются только целые числа;
- числа должны находиться в диапазоне от 0 до 255.

*Иногда при записи IP-адреса в двоичном формате также используются точки для разделения октетов, которые улучшают читаемость адреса, например: 10000110.00011000.00001000.01000010.*



Старшие биты в IP-адресе, расположенные слева, определяют класс и номер сети. Их совокупность называется идентификатором подсети или сетевым префиксом. При назначении адресов внутри одной сети префикс всегда остается неизменным. Он идентифицирует принадлежность IP-адреса данной сети.

Остальные младшие биты, расположенные справа, доступны для нумерации сетевых интерфейсов (Network Interfaces) в данной сети, которые также называются хостами (Hosts):

| сетевой префикс | | номер хоста |
|---|---|---|
| класс сети | номер сети | номер хоста |

Например, если IP-адреса компьютеров подсети 192.168.0.1 - 192.168.0.30, то первые два октета определяют идентификатор подсети - 192.168.0.0, а следующие два - идентификаторы хостов.

Сколько именно бит используется в тех или иных целях, зависит от класса сети. Если номер хоста равен нулю, то адрес указывает не на какой-то один конкретный компьютер, а на всю сеть в целом.

## Классификация сетей

Существует три основных класса сетей: A, B, C. Они отличаются друг от друга максимально возможным количеством хостов, которые могут быть подключены к сети данного класса.

Общепринятая классификация сетей приведена в следующей таблице, где указано наибольшее количество сетевых интерфейсов, доступных для подключения, какие октеты IP-адреса используются для сетевых интерфейсов (*), а какие — остаются неизменяемыми (N).

| Класс сети | Наибольшее количество хостов | Изменяемые октеты IP-адреса, используемые для нумерации хостов |
|---|---|---|
| A | 16777214 | N.*.*.* |
| B | 65534 | N.N.*.* |
| C | 254 | N.N.N.* |

Например, в сетях наиболее распространенного класса C не может быть более 254 компьютеров, поэтому для нумерации сетевых интерфейсов используется только один, самый младший байт IP-адреса. Этому байту соответствует крайний правый октет в точечно-десятичной нотации.

Возникает законный вопрос: почему к сети класса C можно подключить только 254 компьютера, а не 256? Дело в том, что некоторые внутрисетевые адреса IP предназначены для специального использования, а именно:

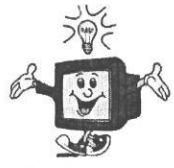
0 - идентифицирует саму сеть;

255 - широковещательный.

## Сегментирование сетей

Адресное пространство внутри каждой сети допускает разбиение на более мелкие по количеству хостов подсети (Subnets). Процесс разбиения на подсети называется также сегментированием.

> *Заметим, что маршруты из Интернета до любого хоста частной сети одинаковы, независимо от того, в какой подсети он расположен. Это позволяет администратору частной сети вносить любые изменения в ее логическую структуру без изменений таблиц маршрутизации в остальном Интернете.*



Например, если сеть 192.168.1.0 класса C разбить на четыре подсети, то их адресные диапазоны будут следующими:

- 192.168.1.0 – 192.168.1.63;
- 192.168.1.64 – 192.168.1.127;

- 192.168.1.128 – 192.168.1.191;
- 192.168.1.192 – 192.168.1.255.

В данном случае для нумерации хостов используется не весь правый октет из восьми бит, а только 6 младших из них. А два оставшихся старших бита определяют номер подсети, который может принимать значения от нуля до трех.

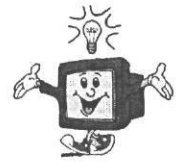
Класс и номер сети вместе с номером подсети образуют расширенный сетевой префикс:

| расширенный сетевой префикс | | | номер хоста |
|---|---|---|---|
| класс сети | номер сети | номер подсети | номер хоста |

Как обычный, так и расширенный сетевые префиксы можно идентифицировать с помощью маски подсети (Subnet Mask), которая позволяет также отделить в IP-адресе идентификатор подсети от идентификатора хоста, маскируя с помощью числа ту часть IP-адреса, которая идентифицирует подсеть.

Маска представляет собой комбинацию чисел, по внешнему виду напоминающую IP-адрес. Двоичная запись маски подсети содержит нули в разрядах, интерпретируемых как номер хоста. Остальные биты, установленные в единицу, указывают на то, что эта часть адреса является префиксом. Маска подсети всегда применяется в паре с IP-адресом.

*Не путайте сам IP-адрес и маску подсети, которая лишь позволяет провести четкую границу между двумя частями IP-адреса: сетевым префиксом и номером хоста.*



При отсутствии дополнительного разбиения на подсети, маски стандартных классов сетей имеют следующие значения:

| Класс сети | Маска | |
|---|---|---|
| | двоичная | точечно-десятичная |
| A | 11111111.00000000.00000000.00000000 | 255.0.0.0 |
| B | 11111111.11111111.00000000.00000000 | 255.255.0.0 |
| C | 11111111.11111111.11111111.00000000 | 255.255.255.0 |

Когда используется механизм разбиения на подсети, маска соответствующим образом изменяется. Поясним это, используя уже упомянутый пример с разбиением сети класса С на четыре подсети.

В данном случае два старших бита в четвертом октете IP-адреса используются для нумерации подсетей. Тогда маска в двоичной форме будет выглядеть следующим образом: 11111111.11111111.11111111.11000000,а точечно-десятичной - 255.255.255.192.

## Диапазоны адресов частных сетей

Каждый компьютер, подключенный к сети, имеет свой уникальный IP-адрес. Для некоторых машин, например, серверов, этот адрес не изменяется. Такой постоянный адрес называется статическим (Static). Для других, например, клиентов, IP-адрес может быть постоянным (статическим) или назначаться динамически, при каждом подключении к сети.

Чтобы получить уникальный статический, то есть постоянный адрес IP в сети Интернет, нужно обратиться в специальную организацию InterNIC - Internet Network Information Center (Сетевой информационный центр Интернета). InterNIC назначает только номер сети, а дальнейшей работой по созданию подсетей и нумерации хостов сетевой администратор должен заниматься самостоятельно.

Но официальная регистрация в InterNIC с целью получения статического IP-адреса обычно требуется для сетей, имеющих постоянную связь с Интернетом. Для частных сетей, не входящих в состав Интернета, специально зарезервировано несколько блоков адресного пространства, которые можно свободно, без регистрации в InterNIC, использовать для присвоения IP-адресов:

| Класс сети | Количество доступных номеров сетей | Диапазоны IP-адресов, используемые для нумерации хостов |
|---|---|---|
| A | 1 | 10.0.0.0 - 10.255.255.255 |
| B | 16 | 172.16.0.0 – 172.31.255.255 |
| C | 255 | 192.168.0.0 – 192.168.255.255 |
| LINKLOCAL | 1 | 169.254.0.0 – 169.254.255.255 |

Однако эти адреса используются только для внутренней адресации сетей и не предназначены для хостов, которые напрямую соединяются с Интернетом.

Диапазон адресов LINKLOCAL не является классом сети в обычном понимании. Он используется Windows при автоматическом назначении личных адресов IP компьютерам в локальной сети.

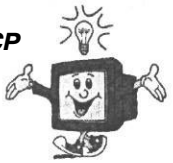
## Автоматическое назначение адресов

Операционная система Windows позволяет компьютерам автоматически получать IP-адреса при их подключении к локальной сети. Существуют две потенциальные возможности по автоматическому назначению адресов:

- с помощью сервера, поддерживающего протокол DHCP - Dynamic Host Configuration Protocol (Протокол динамической конфигурации хостов);
- благодаря механизму автоматического назначения личных IP-адресов с использованием адресного пространства LINKLOCAL.

Сервер DHCP имеет централизованную базу данных адресов IP, выделяемых компьютерам локальной сети при их включении.

*Поставщики услуг Интернета часто используют службу **DHCP** для назначения динамических IP-адресов компьютерам, подключающимся по модему. При каждом подключении к Интернету компьютерам назначаются разные, но уникальные номера.*



При отсутствии в сети сервера DHCP Windows производит широковещательный опрос других компьютеров и находит неиспользуемый адрес IP из диапазона **LINKLOCAL**, автоматически назначая первый свободный адрес своему сетевому интерфейсу.

Оба механизма автоматического выделения адресов значительно облегчают сетевое администрирование в одной сети, однако в случае межсетевого объединения не позволяют гибко настраивать маршрутизацию, поэтому мы не будем их использовать.

Кроме автоматического назначения IP-адресов, Windows позволяет вручную назначить каждому компьютеру локальной сети статический IP-адрес вида 192.168.0.*. Такой статический адрес всегда будет оставаться постоянным.

## Зарезервированные адреса

Некоторые IP-адреса зарезервированы для определенных целей и не могут присваиваться физическим сетевым устройствам:

| Сетевой префикс | Номер хоста | Предназначение | Пример |
|---|---|---|---|
| Все биты равны 0 | | Данное устройство | 0.0.0.0 |
| Номер сети | Все биты равны 0 | Данная сеть | 192.168.1.0 |
| Все биты равны 0 | Номер хоста | Устройство в данной сети | 0.0.0.2 |
| Все биты равны 1 | | Все устройства в данной сети | 255.255.255.255 |
| Номер сети | Все биты равны 1 | Все устройства в указанной сети | 192.168.3.255 |
| 127 (десятичное) | Что-либо (чаще 1) | Адрес обратной связи | 127.0.0.1 |

Как видно из таблицы, IP-адрес относится к данному устройству, когда все без исключения биты сброшены в ноль, или к данной сети, если обнулен только номер хоста.

Адреса IP, биты которых установлены в единицу, используются при широковещательной передаче информации. Если все без исключения биты установлены, то пакеты данных рассылаются всем компьютерам данной сети. При необходимости широковещательной передачи в другой сети указывается сетевой префикс, а биты номера хоста устанавливаются в единицу.

Номер сети 127.0.0.0 зарезервирован для обратной связи и используется для проверки взаимодействия сетевых интерфейсов программ, запущенных на одном компьютере. Чаще всего для этой цели используется IP-адрес 127.0.0.1. Когда приложение посылает пакеты данных на адрес обратной связи, они сразу же возвращаются обратно. При этом не происходит никакого физического перемещения информации по каналам связи.

# Доменная адресация и URL-адресация

Для облегчения пользователям запоминания адресов компьютеров существует возможность обращаться к серверам по более понятному символьному имени, называемому еще доменным именем. Так же, как и IP-адрес, доменное имя является уникальным для каждого компьютера, подключенного к Интернету. Но вместо цифровых значений адреса используются слова.

Доменное имя узла состоит из частей, написанных строчными латинскими символами и разделенных точками. Первая часть - обычно имя компьютера, следующая - имя домена компании и последняя - имя домена страны или одного из специальных доменов, обозначающих профиль деятельности организации:

com - коммерческие организации;

gov - правительственные организации;

edu - учреждения образования;

mil - военные организации;

net - организации, управляющие сетью и входящие в ее структуру;

org - прочие организации.

Каждой стране присвоено уникальное двухбуквенное обозначение: uk - Великобритания, jp - Япония, de - Германия, su - Советский Союз. После распада СССР его бывшие республики получили свои имена: ru - Россия, иа - Украина. Однако некоторые имена, сформировавшиеся прежде, сохранили обозначение **su.**

Исходя из описанных правил определения имен, доменным именем корпорации Microsoft будет microsoft.com, а Web-сервера корпорации - www.microsoft.com.

Из сказанного следует, что адреса образуют древоподобную структуру, благодаря которой ускоряется доступ к абонентам сети и выполняется поиск абонентов, В этой древоподобной структуре нет единого корня, но каждая страна образует свое поддерево. Так, в Украине доменами или узлами следующего, после **иа,** уровня являются домены городов, областей или регионов, например, kiev.ua, crimea.ua и т.д. Таким образом, адрес компьютера может состоять, по меньшей мере, из трех частей, разделенных точками: имя сервера, название города или региона, имя страны. Количество частей зависит от используемой локальной сети, количества серверов и т.д.

Для обозначения адреса электронной почты абонента сети обычно используется собственное полное или сокращенное имя или должность пользователя, отделенное от доменного имени символом @. Например, адрес E-mail главы корпорации Microsoft может быть таким: billg@microsoft.com.

Возможность использования доменных имен обеспечивается протоколом DNS (Domain Name System - Доменная система имен). Специальные серверы DNS преобразовывают символьное доменное имя компьютера в IP-адрес, отыскивая соответствующую запись в специальной базе данных, хранящейся на тысячах компьютеров. При необходимости выполняется также и обратное преобразование IP-адреса в DNS-имя.

Для быстрого доступа к информации, хранящейся на разных серверах Интернета, используется адрес URL (Uniform Resource Locators - Унифицированный указатель ресурсов), который определяет точное положение ресурса или объекта, к которому вы хотите получить доступ, и протокол для работы с ним. URL-адрес обычно начинается с названия протокола. Ресурсами или объектами Интернета обычно являются Web-страницы, файлы, почтовая корреспонденция, группы новостей и др. Например, URL-адрес **http://www.msu.ru** означает следующее: **http** - Web-сервер, использует протокол HTTP; www — узел находится в World Wide Web (Всемирная компьютерная паутина); **msu** - узел Московского государственного университета (МГУ); ru - узел находится в России.

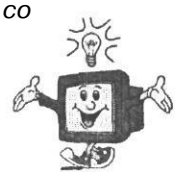
# ГЛАВА 2.
# Локальная сеть без сетевой карты

В предыдущей главе мы рассмотрели основные принципы построения и работы компьютерных сетей для предприятий малого бизнеса и общие принципы передачи данных через сеть Интернет, а также дали краткий обзор различных сетевых устройств, которые могут использоваться для организации таких сетей. Однако в домашних условиях, если нет необходимости в высоких скоростях передачи данных, можно построить полноценную сеть, не приобретая дорогостоящего сетевого оборудования. Тому, как связать два компьютера в единую сеть без применения специальных сетевых устройств, и будет посвящена эта глава. Конечно, скорости передачи данных в такой сети будет недостаточно для просмотра видеофильмов или прослушивания музыкальных файлов, но для передачи небольших файлов или организации сетевой компьютерной игры ее будет вполне достаточно.

## Локальная сеть за 25 рублей

Материнская плата современного персонального компьютера имеет несколько разъемов, которые обычно выводятся на заднюю панель его системного блока. Эти разъемы предназначены для подключения различных внешних устройств, таких как клавиатура, мышь, внешний модем, принтер и т.п. Уже давно стало стандартом, что на материнской плате существует как минимум два или три таких разъема. Один или два из них называются COM1 и COM2 (Communication Port - коммуникационный порт) и один LPT (Line PrinTer - порт принтера). COM-порты являются последовательными двунаправленными, т.е. обеспечивают побитную одновременную передачу и прием информации. LPT-порт является параллельным, т.е. передает информацию побайтно, и так же может как передавать, так и принимать данные.

*Многие современные материнские платы компьютеров со встроенной (интегрированной) видеосистемой вместо двух разъемов последовательных портов COM1 и COM2 имеют только один, который может быть либо COM1, либо COM2, в зависимости от настроек BIOS. Второй же разъем хоть внешне и очень похож на разъем последовательного порта, но используется для подключения монитора и обычно окрашен в синий цвет.*



Если для последовательных портов скорость передачи данных составляет 115 Кбит/сек, то для LPT она может достигать 1,5 Мбит/сек.

Как уже отмечалось выше, любой современный компьютер имеет, как минимум, два или три разъема портов ввода-вывода. Каждому порту присваивается свой номер, адрес (в виде шестнадцатеричного числа) и прерывание, с помощью которых операционная система или программа управляет передачей информации через порт. Стандартные базовые настройки портов приведены в таблице.

| Номер порта | Адрес | Прерывание |
|---|---|---|
| COM1 | 3F8 (Hex) | IRQ4 |
| COM2 | 2F8 (Hex) | IRQ3 |
| COM3 | 3E8 (Hex) | IRQ4 |
| COM4 | 2E8 (Hex) | IRQ3 |
| LPT1 | 378 (Hex) | IRQ7 |
| LPT2 | 278 (Hex) | IRQ5 |

Настройки портов, расположенных на системной плате компьютера, можно изменить с помощью программы BIOS Setup (Установки BIOS). Программу BIOS Setup (Установки BIOS) можно запустить, если в момент включения или перезагрузки компьютера нажать и удерживать клавишу Delete. Перенастройка параметров портов, расположенных на системной плате, может потребоваться, если вы используете дополнительные устройства, работающие через порты ввода-вывода. Например, используете внутренний модем, работающий через порт COM2, в этом случае необходимо отключить или перенастроить порт COM2 материнской платы, чтобы избежать системных конфликтов. Если все порты ввода-вывода компьютера уже заняты, а вам требуется еще, например, для соединения с соседним компьютером, то нужно приобрести мультипортовую карту. Такая карта устанавливается в свободный слот материнской платы, номера используемых портов и их прерывания обычно задаются перемычками или переключателями самой мультикарты. В комплекте поставки некоторых материнских плат с уменьшенным количеством портов ввода-вывода входит специальная планка с разъемами последовательных портов, которая устанавливается на задней панели системного блока и соединяется с материнской платой многожильным шлейфом. О подключении таких дополнительных разъемов вы можете более подробно узнать из описания, прилагающегося к вашей материнской плате.

Расположение и назначение разъемов материнской платы показаны на Рис. 2.1.

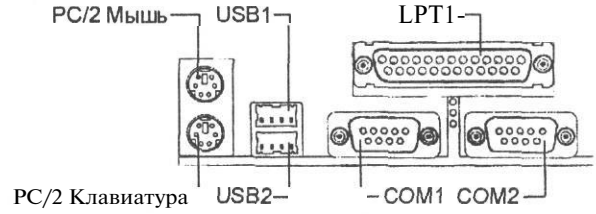



*Рис. 2.1 Расположение и назначение разъемов материнской платы*

В более старых моделях материнских плат разъемы портов выводятся на заднюю панель компьютера с помощью специальных кабелей. Разъем порта принтера LPT1 представляет собой разъем типа DB25-F, т.е. 25-контактную розетку, а COM1 - разъем типа **DB9-M** - 9- контактную вилку. Разъем порта COM2, в зависимости от модели материнской платы, может быть **DB9-M** или **DB25-M** (9- или 25- контактная вилка)[1]. На современных моделях материнских плат разъем LPT1 бывает красного цвета, а COM1 и COM2 - белого.

[1] 25-контактные вилки COM2 имеют обычно более старые модели материнских плат.

Любой из свободных портов ввода-вывода компьютера можно использовать для соединения с другим компьютером. Такое соединение называют прямым кабельным соединением, или нульмодемом. Достоинством такого соединения является его низкая стоимость, к недостаткам можно отнести низкую скорость передачи информации (особенно при использовании COM-портов) и ограниченная длина кабеля (для COM-портов около 30 метров, для LPT — 10 - 15 метров). Для соединения компьютеров, расположенных друг от друга дальше указанного расстояния, необходимо использовать дополнительные усилители.

## Кабели и разъемы для нульмодемов

Для соединения двух компьютеров с помощью нульмодема нужно приобрести 2 разъема и многожильный кабель необходимой длинны. Разъемы при использовании COM-портов должны быть розетками типа DB9-F или DB25-F, в зависимости от типа выходного разъема порта компьютера, а при соединении через LPT-порт - DB25-M (вилка). В качестве кабеля подойдет любой многожильный изолированный кабель, но лучше всего использовать ленточный многожильный кабель, причем распаять его таким образом, чтобы сигнальные провода чередовались с проводами заземления, в этом случае связь будет более защищенной от помех. Необходимо помнить об общем ограничении длины нульмодемного соединения.

Схема распайки кабеля для простого нульмодема, при использовании COM-портов, показана на Рис. 2.2. Номера контактов указаны для разъема типа DB9-F, а в скобках - для DB25-F. Все разъемы, которые вы приобретете, имеют цифровую маркировку контактов и поэтому могут быть легко определены.


*Рис. 2.2 Схема распаши кабеля простого нульмодема для COM-порта (минимальный вариант)*

На Рис. 2.3 приведена схема распайки полного нульмодемного кабеля для COM-портов.


*Рис. 2.3 Схема распайки кабеля стандартного нульмодема для COM-порта*

Схема нульмодемного кабеля для прямого соединения двух компьютеров через LPT-порты приведена на Рис. 2.4. Разъемы для изготовления такого нульмодемного кабеля должны быть вилками типа **DB25-M**.

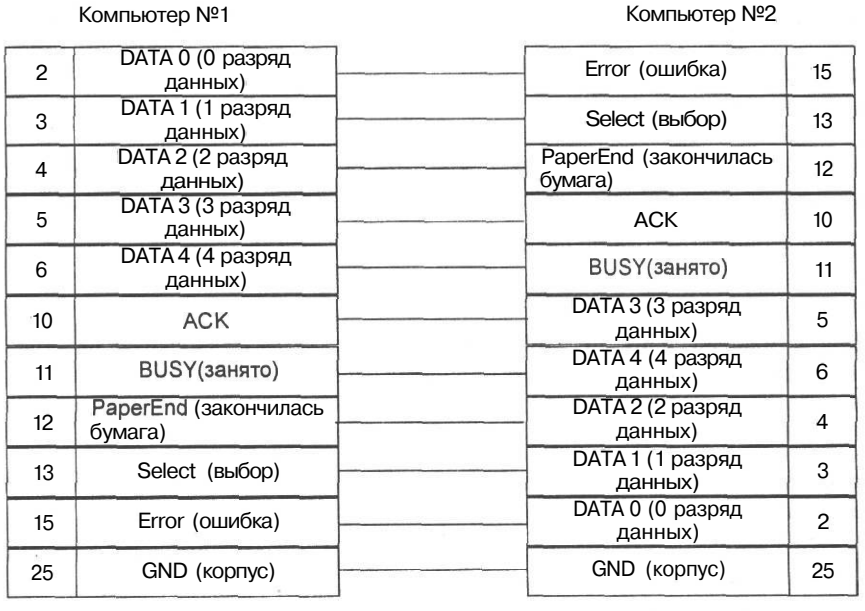



*Рис. 2.4 Схема распайки простого нульмодемного кабеля для LPT-порта*

Кабель, схема которого приведена на Рис. 2.4, часто называют LapLink (настольное соединение) и используют для переноса данных с переносного компьютера на стационарный. Скорость передачи информации по кабелю составляет до 1,5 Мбит/сек. Существуют также специальные кабели, рассчитанные на то, что LPT-порты обоих компьютеров будут работать в режиме ECP (Extended Capability Port - порт с расширенными возможностями), т.е. использовать двунаправленный канал DMA (Direct Memory Access - прямой доступ к памяти). Это позволит получить максимальную скорость передачи данных до 4 Мбит/с. Более полную информацию о кабеле DirectParallel® Universal Fast Cable (универсальный скоростной кабель фирмы DirectParallel®), обеспечивающем такую скорость передачи данных, вы можете получить в Интернете по адресу: http://www.lpt.com.

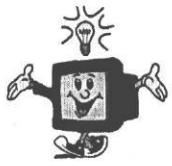
После того как кабель изготовлен или приобретен в магазине, остается только подключить его к соответствующим разъемам на задней панели системного блока компьютера. Перед подключением необходимо убедиться, что компьютер имеет свободный разъем COM- или LPT-порта. Необходимо помнить, что подключение кабеля нужно производить при отключенном электропитании компьютера.

Если у вас появилась необходимость перенастроить порты ввода-вывода материнской платы, то выполните приблизительно следующие действия, которые описываются на примере материнской платы ASUS P3BF.

- Включите питание компьютера, нажмите и удерживайте нажатой клавишу Delete до тех пор, пока на экране не появится главное меню программы BIOS Setup Utility (Утилиты установки базовой системы ввода-вывода).
- С помощью клавиш ↓, ↑, →, ← выберите команду меню Advanced (Дополнительно) и нажмите клавишу Enter. На экране появится дополнительное меню Advanced (Дополнительно).
- С помощью клавиш ↓, ↑, →, ← выберите команду дополнительного меню I/O Device Configuration (Конфигурация устройств ввода-вывода) и нажмите клавишу Enter. На экране появится меню с настройками устройств ввода-вывода.
- С помощью клавиш - и + в строках меню Onboard Serial **Port1** (Встроенный последовательный порт 1), Onboard Serial **Port2** (Встроенный последовательный порт 2), Onboard Parallel Port (Встроенный параллельный порт) установите необходимые значения адреса и прерывания с учетом рекомендаций, приведенных в начале знакомства.
- Если один из портов материнской платы необходимо отключить, то установите в параметрах порта опцию Disabled (Не используется).
- Если для связи двух компьютеров будет использоваться параллельный порт, то в строке меню Parallel Port Mode (Режим параллельного порта) установите ECP+EPP, а в строке ECP DMA Select (Выбор канала DMA для режима ECP) установите 3.
- По окончании настроек портов материнской платы дважды нажмите клавишу Esc, чтобы вернуться в главное меню программы BIOS Setup Utility (Утилиты установки базовой системы ввода-вывода).

- Нажмите клавишу И, чтобы сохранить настройки и выйти из программы. На экране появится диалог Save CMOS and Exit? (Сохранить настройки в энергонезависимой памяти и выйти?).
- Нажмите клавишу Y, чтобы сохранить изменения.

*Здесь описан способ изменения настроек портов ввода-вывода системной платы ASUS P3BF. Основное меню программы BIOS Setup Utility (Утилиты установки базовой системы ввода-вывода) других фирм-производителей может отличаться от описанного выше.*



После этого компьютер перезагрузится и конфигурация портов материнской платы компьютера изменится. Однако для установления прямого кабельного соединения между двумя компьютерами одной настройки портов ввода-вывода материнской платы недостаточно. Необходимо соответствующим образом подготовить операционную систему и произвести дополнительные настройки. Этим вопросам будет посвящено следующее знакомство.

## Настройка прямого кабельного соединения в Windows 98/ME/2000

Многие сетевые компьютерные игры имеют поддержку связи с другими игровыми компьютерами с помощью прямого кабельного соединения. Однако большинство сетевых программ и многие сетевые игры не поддерживают такое соединение. Абсолютное большинство сетевых программ и игр используют для связи с другими компьютерами протокол TCPЯP, который, как мы уже упоминали, является основным протоколом, используемым в сети Интернет. Тому, как установить этот протокол для нульмодемного соединения, и будет посвящено это знакомство.

Мы опишем вариант настройки соединения двух компьютеров через COM-порты.

Для того чтобы стало возможным использовать протокол TCPЯP при нульмодемном соединении, вам необходим файл mdmcisco.inf, который вы можете найти на компакт-диске, прилагаемом к книге.

- Скопируйте файл mdmcisco.inf в папку **C:\WINDOWS\INF**.
- Перезагрузите компьютер.
- Нажмите кнопку Пуск (Start). Откроется главное меню Windows 98.
- В главном меню выберите команду Настройка ◆ Панель управления (Settings ◆ Control Panel). На экране появится окно Панель управления (Control Panel) (Рис. 2.5).

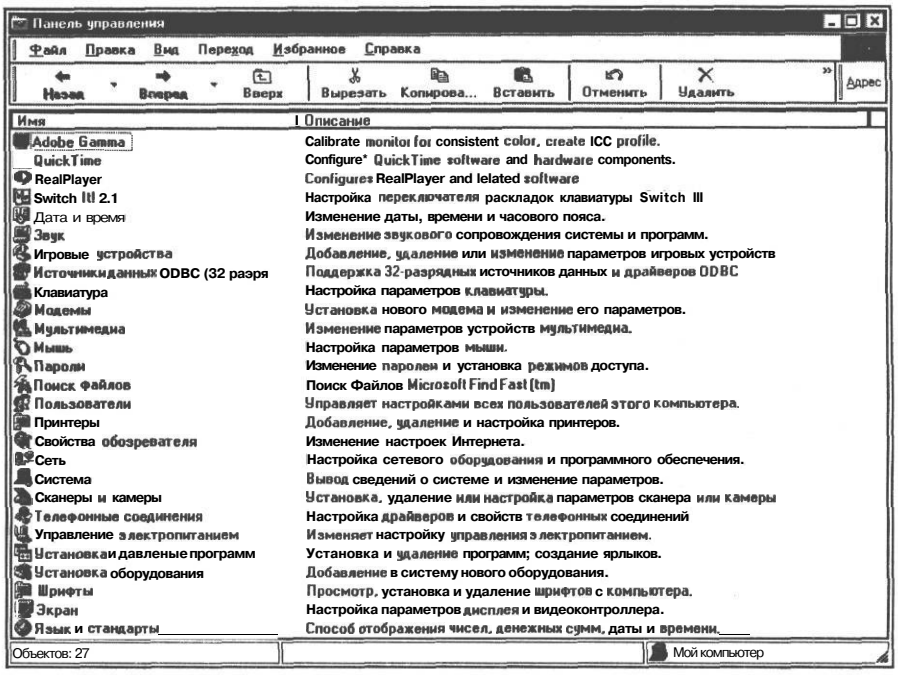



*Рис. 2.5 Окно **Панель управления** (Control Panel)*

> Дважды щелкните мышью на строке **Модемы** (Modems). На экране появится диалог **Свойства: Модемы** (Modems Properties) (Рис. 2.6).

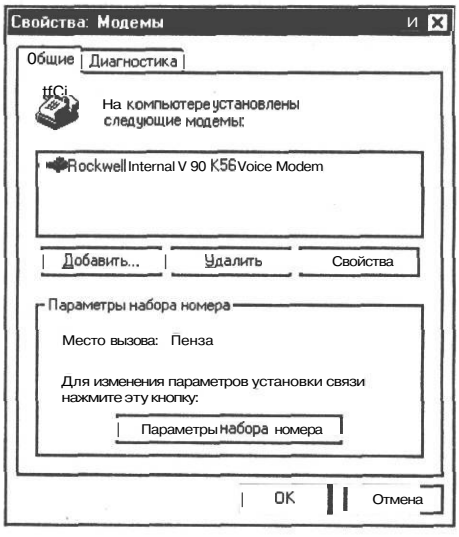



*Рис. 2.6 Диалог **Свойства: Модемы** (Properties Modems)*

> Нажмите кнопку **Добавить** (Add). На экране появится первый диалог мастера установки модема (Рис. 2.7).

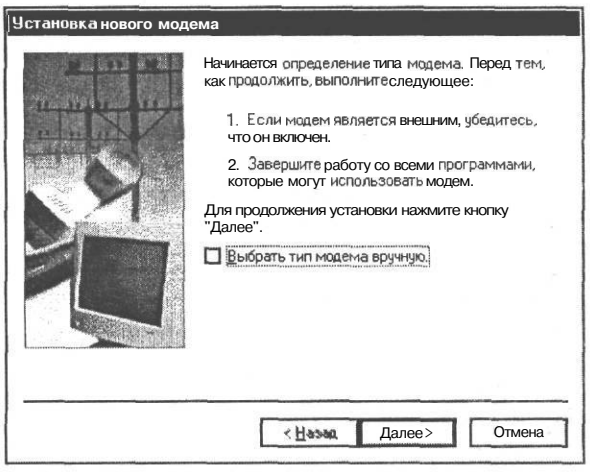



*Рис. 2.7 Первый диалог мастера установки модема*

- Установите флажок **Выбрать тип модема вручную** (Don't detect my modem; I'll select it from a list) и нажмите кнопку **Далее** (Next). Будет произведено обновление базы драйверов, после чего на экране на некоторое время появится окно **Создание базы драйверов** (Building drivers information database) (Рис. 2.8), а затем следующий диалог мастера установки модема (Рис. 2.9).

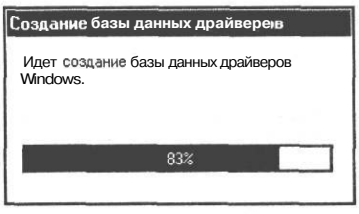



*Рис. 2.8 Окно **Создание базы драйверов** (Building drivers information database)*

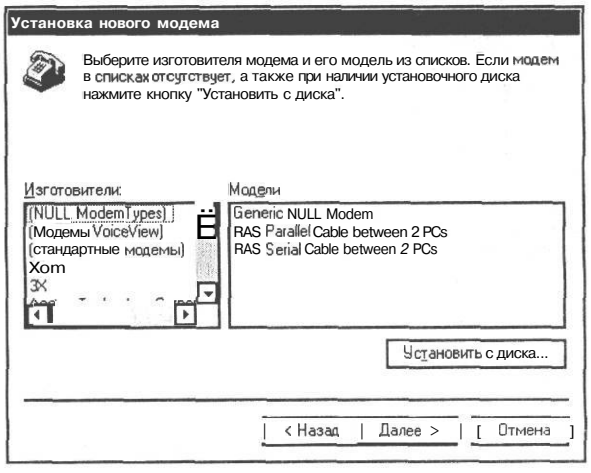



*Рис. 2.9 Второй диалог мастера установки модема*

- В списке Изготовители (Manufacturers) выберите строку (NULL Modem Types) (Типы нульмодемов), а в списке Модели (Models) - строку RAS Serial Cable between 2 PCs (Сервер удаленного доступа для последовательного кабеля между двумя компьютерами).
- Нажмите кнопку Далее (Next). На экране появится следующий диалог установки нового модема (Рис. 2.10).

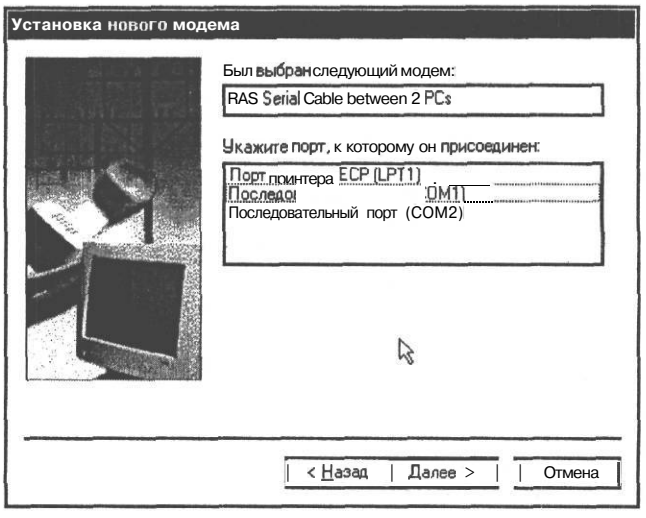



*Рис. 2.10 Третий диалог мастера установки модема*

- В списке Укажите порт, к которому он присоединен (Select the port to use wish this modem) щелкните мышью на строке с номером порта, к которому подключен нульмодемный кабель (COM1 - COM4) и нажмите кнопку Далее (Next). Через некоторое время, необходимое для установки нового модема, на экране появится диалог заключительный мастера установки нового модема (Рис. 2.11).

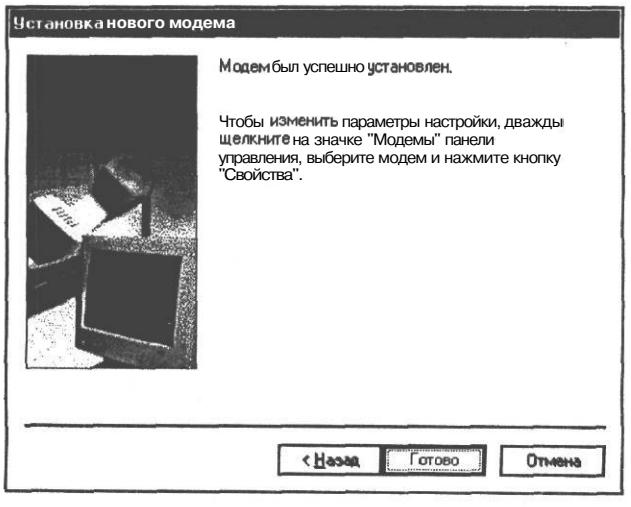



*Рис. 2.11 Заключительный диалог мастера установки модема*

➤ Нажмите кнопку Готово (Finish), заключительный диалог мастера установки нового модема будет закрыт, а в диалоге Свойства: Модемы (Modems Properties) появится запись о новом модеме.

> Нажмите кнопку OK, расположенную в нижней части диалога Свойства: Модемы (Modems Properties), чтобы закрыть его.

Далее необходимо установить на обоих компьютерах поддержку удаленного доступа к сети и сервер удаленного доступа, для этого выполните следующие действия.

> В окне Панель управления (Control Panel) выберите строку Установка и удаление программ (Add/Remove Programs) и нажмите кнопку Enter. На экране появится диалог Свойства: Установка и удаление программ (Add/Remove Programs Properties) (Рис. 2.12).

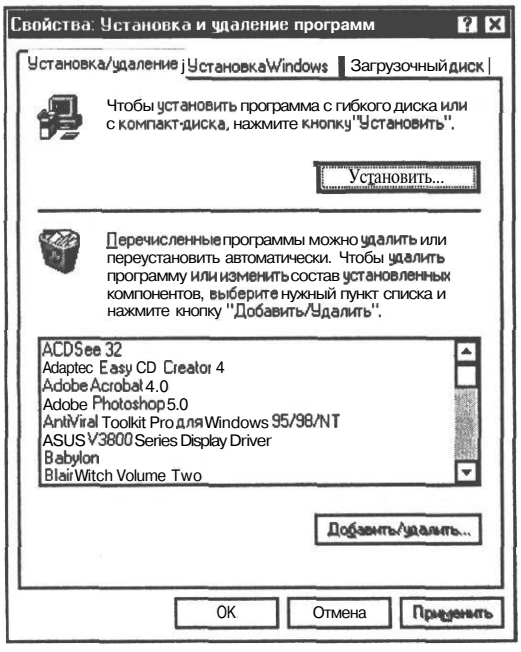



***Рис. 2.12 Диалог Свойства: Установка и удаление программ (Add/Remove Programs Properties)***

➤ Перейдите на вкладку Установка Windows (Windows Setup). На экране на короткое время появится окно Установка Windows (Windows Setup) (Рис. 2.13), после чего вид диалога Свойства: Установка и удаление программ (Add/Remove Programs Properties) изменится в соответствии с Рис. 2.14.

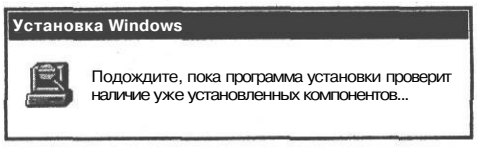



*Рис. 2.13 Окно Установка Windows (Windows Setup)*

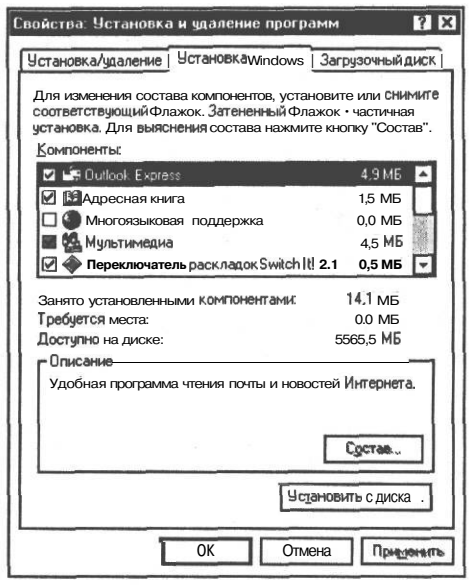



*Рис. 2.14 Вкладка* ***Установка Windows*** *(Windows Setup) диалога Свойства: Установка и удаление программ (Add/Remove Programs Properties)*

> С помощью кнопок [3 и [▲] прокрутите список установленных компонентов в списке **Компоненты** (Components) и щелкните мышью на строке **Связь** (Communications), чтобы выделить ее.

➤ Нажмите кнопку **Состав** (Details), расположенную в группе элементов управления **Описание** (Description). На экране появится диалог **Связь** (Communications) (Рис. 2.15).

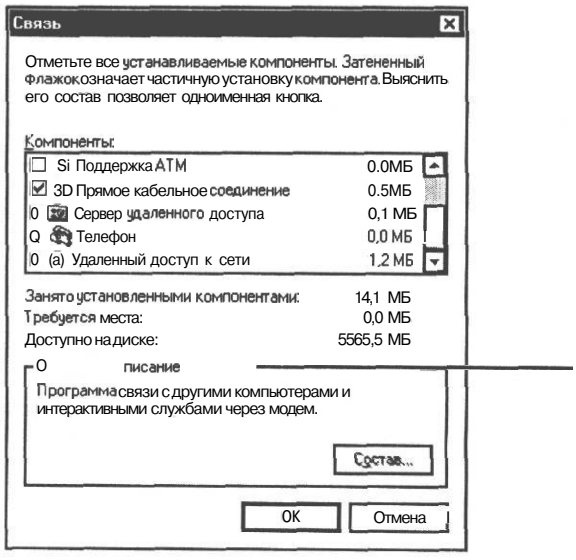



*Рис. 2.15Диалог* **Связь** *(Communications)*

> Установите флажки Сервер удаленного доступа (Dial-Up Server) и Удаленный доступ к сети (Dial-Up Networking) в списке Компоненты (Components). Для прокрутки списка используйте кнопки 0 и [▲].

➤ Нажмите кнопку OK, расположенную в нижней части диалога Связь (Communications), чтобы закрыть диалог.

> Нажмите кнопку Применить (Apply), расположенную в нижней части диалога Свойства: Установка и удаление программ (Add/Remove Programs Properties). Если установка операционной системы производилась с компакт-диска, то на экране появится диалог Вставка диска (Insert Disk) (Рис. 2.16).

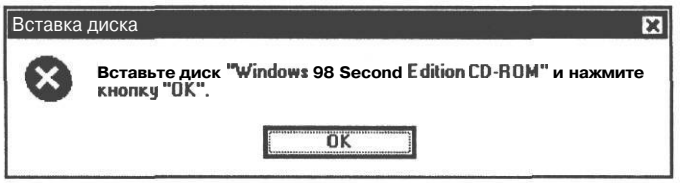



*Рис. 2.16 Диалог Вставка диска (Insert Disk)*

> Установите компакт-диск с операционной системой Windows в привод CD-ROM и нажмите кнопку OK.

Если все сделано правильно, то произойдет копирование необходимых файлов с компакт-диска на жесткий диск вашего компьютера. Если же операционная система не сможет найти на установленном компакт-диске нужные файлы, то на экране появится диалог Копирование файлов (Copying Files) (Рис. 2.17).

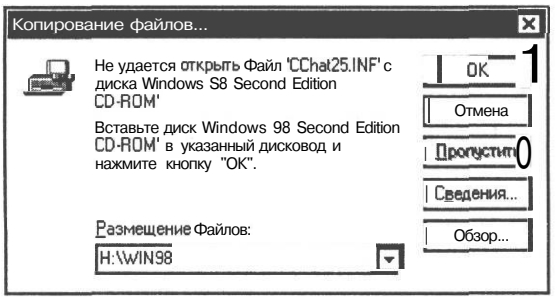



*Рис. 2.17 Диалог Копирование файлов (Copying Files)*

> В поле ввода со списком Размещение файлов (Copy files from) введите полный путь к папке, в которой содержатся файлы дистрибутива операционной системы и нажмите кнопку OK.

Для поиска необходимой папки в диалоге Копирование файлов (Copying Files) можно использовать кнопку Обзор (Browse), с помощью которой на экран выводится диалог Открытие файла (Open) (Рис. 2.18).

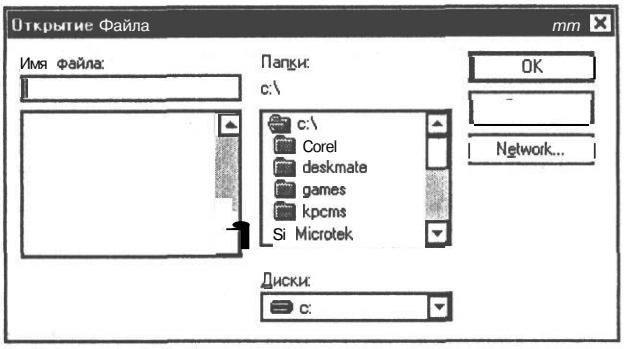



*Рис. 2.18 Диалог* ***Открытие файла*** *(Open)*

После того как установка необходимых компонентов завершится, необходимо установить протокол TCP/IP, для этого выполните следующие действия.

➤ Перейдите в окно **Панель управления** (Control Panel), выберите строку Сеть (Network) и нажмите клавишу Enter. На экране появится диалог Сеть (Network) (Рис. 2.19).

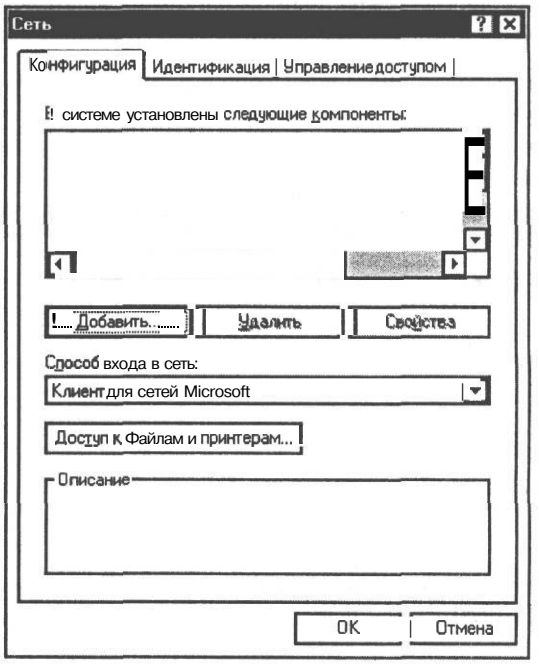



*Рис. 2.19 Диалог* ***Сеть*** *(Network)*

➤ На вкладке Конфигурация (Configuration) нажмите кнопку Добавить (Add). На экране появится диалог Выбор типа компонента (Select Network Component Type) (Рис. 2.20).

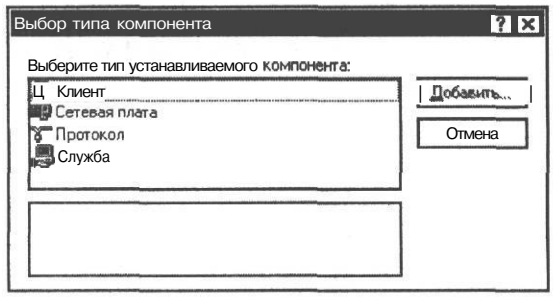



*Рис. 2.20 Диалог Выбор типа компонента (Select Network Component Type)*

> В списке Выберите тип устанавливаемого компонента (Click the type of network component you want to install) щелкните мышью на строке Клиент (Client) и нажмите кнопку Добавить (Add). На экране появится диалог Выбор: Клиент сети (Select Network Client) (Рис. 2.21).

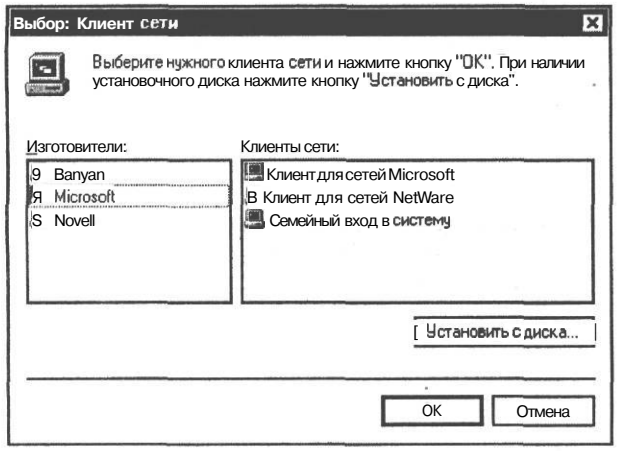



*Рис. 2.21 Диалог Выбор: Клиент сети (Select Network Client)*

> В списке Изготовители (Manufacturers) выберите строку Microsoft, а в списке Клиенты сети (Network Clients) строку Клиент для сетей Microsoft (Client for Microsoft Networks) и нажмите кнопку OK. Диалоги Выбор: Клиент сети (Select Network Client) и Выберите тип компонента (Select Network Component Type) будут закрыты.

➤ На вкладке Конфигурация (Configuration) диалога Сеть (Network) нажмите кнопку Добавить (Add). На экране снова появится диалог Выберите тип компонента (Select Network Component Type) (Рис. 2.20).

➤ **В списке Выберите тип устанавливаемого компонента** (Click the type of network component you want to install) щелкните мышью на строке **Протокол** (Protocol) и нажмите кнопку **Добавить** (Add). На экране появится диалог **Выбор: Сетевой протокол** (Select Network Protocol) (Рис. 2.22).

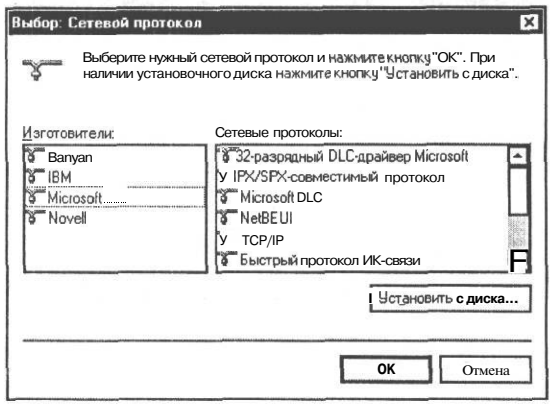



*Рис. 2.22 Диалог* ***Выбор: Сетевой протокол*** *(Select Network Protocol)*

> *В* списке **Изготовители** (Manufacturers) выберите строку **Microsoft,** а в списке **Сетевые протоколы** (Networks Protocols) строку **TCP/IP** (ТСРЛР) и нажмите кнопку OK. Диалоги **Выбор: Сетевой протокол** (Select Network Protocol) и **Выберите тип компонента** (Select Network Component Type) будут закрыты.

➤ В диалоге **Сеть** (Network) перейдите на вкладку **Идентификация** (Identification); вид диалога изменится в соответствии с Рис. 2.23.

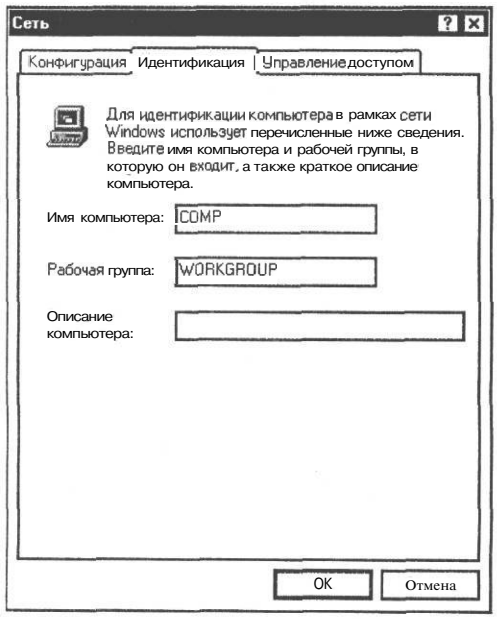



*Рис. 2.23 Вкладка* ***Идентификация*** *(Identification) диалога* ***Сеть*** *(Network)*

- В поле ввода **Имя компьютера** (Computer name) введите любое имя, различное для каждого из компьютеров, объединяемых в сеть, а в поле ввода **Рабочая группа** (Workgroup) одинаковое для обоих компьютеров имя рабочей группы, например **WORKGROUP.**
- Перейдите на вкладку **Конфигурация** (Configuration) и выберите из открывающегося списка **Способ входа в сеть** (Primary Network Logon) строку **Клиент для сетей Microsoft** (Client for Microsoft Network).
- Нажмите кнопку OK, чтобы закрыть диалог **Сеть** (Network).

После этого произойдет копирование необходимых файлов с компакт-диска или папки жесткого диска, где находится дистрибутив операционной системы Windows. После завершения операции копирования файлов на экран будет выведен диалог об изменении параметров системы (Рис. 2.24).

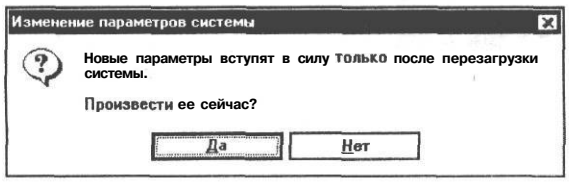



*Рис. 2.24 Диалог об изменении параметров системы*

- Нажмите кнопку Да (Yes). Диалог закроется, и произойдет перезагрузка операционной системы.

После перезагрузки на экране появится диалог **Ввод сетевого пароля** (Enter Network Password) (Рис. 2.25)

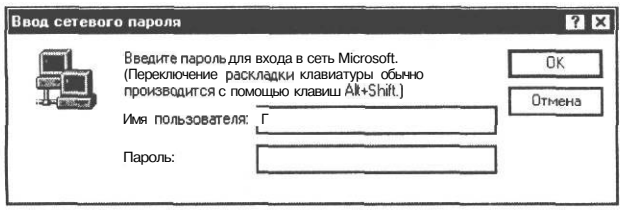
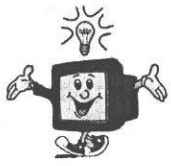



*Рис. 2.25 Диалог **Ввод сетевого пароля** (Enter Network Password)*

- Введите имя пользователя и пароль в поля ввода **Имя пользователя** (User name) и **Пароль** (Password). Если имя и пароль пользователя вводятся впервые, то на экране появится диалог с просьбой подтвердить пароль, в котором нзобходимо ввести пароль еще раз.

*Обратите внимание на то, что для работы с общими сетевыми ресурсами обязательно необходимо пройти аутентификацию (ввести имя пользователя и пароль). Если войти в систему минуя систему аутентификации (с помощью кнопки **Отмена** (Cancel) диалога **Ввод сетевого пароля** (Enter Network Password) или клавиши* Esc *). то сетевые ресурсы будут недоступны. Кроме того, компьютеры должны обязательно принадлежать одной рабочей группе.*



После прохождения аутентификации на экране появится окно **Панель управления** (Control Panel).

> Нажмите кнопку ☒, расположенную в правой части заголовка окна **Панель управления** (Control Panel), чтобы закрыть его.

Теперь все необходимые программы установлены, и можно перейти к настройке соединения. Для этого выполните следующие действия.

> На одном из компьютеров (компьютере клиенте) нажмите кнопку **Пуск** (Start). Откроется главное меню Windows 98.

➤ В главном меню выберите команду **Программы • Стандартные * Связь • Удаленный доступ к сети** (Programs ◆ Accessories ◆ Communications ◆ Dial-Up Networking). На экране появится окно **Удаленный доступ к сети** (Dial-Up Networking) (Рис. 2.26).

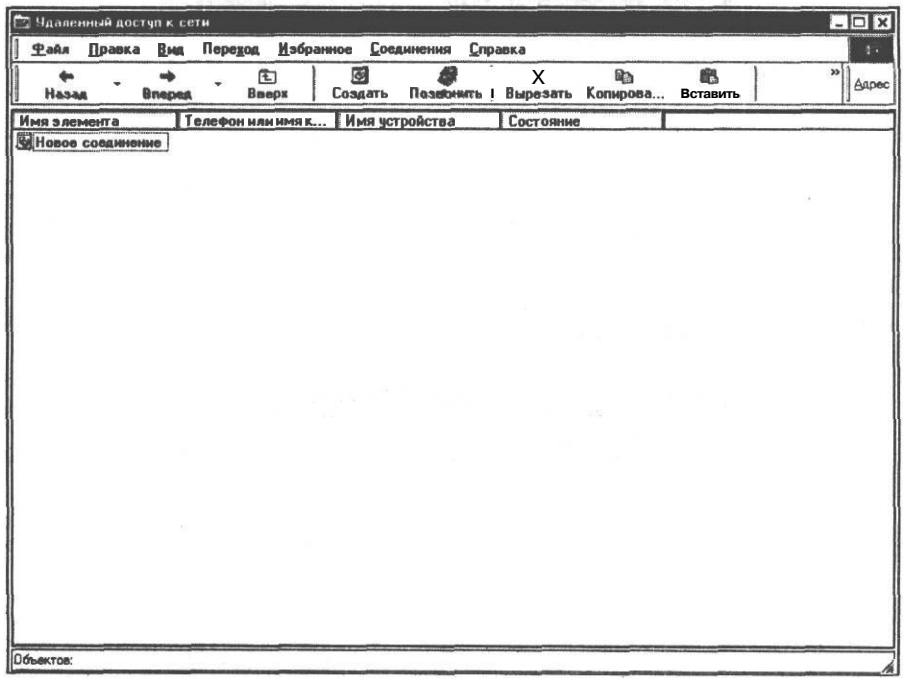



*Рис. 2.26 Окно* ***Удаленный доступ к сети*** *(Dial-Up Networking)*

➤ Дважды щелкните мышью на строке **Новое соединение** (Make New Connection). На экране появится первый диалог мастера создания нового соединения (Рис. 2.27).

➤ В поле ввода **Введите название соединения (например, имя компьютера, с которым устанавливается связь):** (Type a name for the computer you are dialing) введите имя соединения, например Нульмодем, а из открывающегося списка **Выберите модем** (Select a device) выберите строку **RAS Serial Cable between 2 PCs** (Сервер удаленного доступа последовательного кабеля между двумя компьютерами).

➤ Нажмите кнопку **Далее** (Next). На экране появится следующий диалог мастера создания нового соединения (Рис. 2.28).


*Рис. 2.27 Первый диалог мастера создания нового соединения*

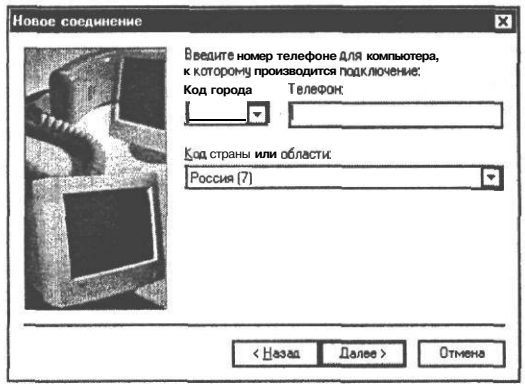



*Рис. 2.28 Второй диалог мастера создания нового соединения*

> В поле ввода Телефон (Telephone number) введите любой номер, а из открывающегося списка Код страны или области (Country code) выберите Россия (7) (Russia(7)).

➤ Нажмите кнопку Далее (Next). На экране появится заключительный диалог мастера установки нового соединения (Рис. 2.29).

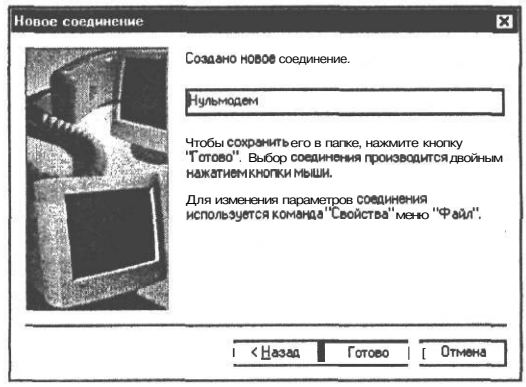



*Рис. 2.29 Заключительный диалог мастера создания нового соединения*

- Нажмите кнопку **Готово** (Finish), диалог закроется, а **в** окне **Удаленный доступ к сети** (Dial-Up Networking) появится строка **Нульмодем.**
- Щелкните правой кнопкой мыши на строке **Нульмодем и из** появившегося контекстного меню выберите команду **Свойства** (Properties). На экране появится диалог **Нульмодем** (Рис. 2.30).

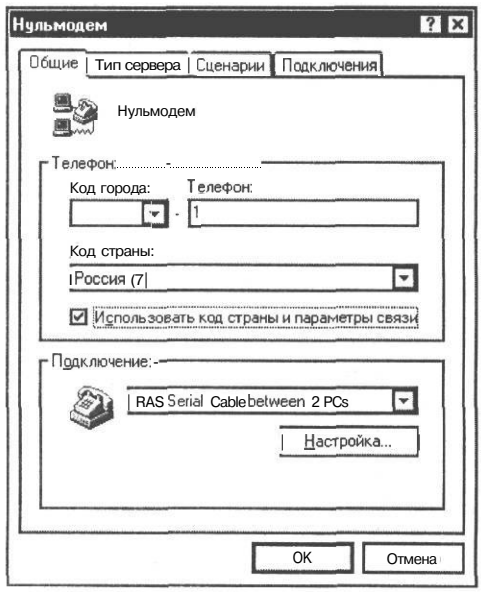



*Рис. 2.30Диалог Нульмодем*

- На вкладке **Общие** (General) сбросьте флажок **Использовать код страны и параметры связи** (Use area code and Dialing Properties),
- Выберите вкладку **Тип сервера** (Server Types), из открывающегося списка **Тип сервера удаленного доступа** (Type of Dial-Up Server) выберите строку **PPP: Интернет, Windows NT Server, Windows 98** (PPP: Internet, Windows NT Server, Windows 98).
- На той же вкладке **Тип сервера** (Server Types) установите флажки **Войти в сеть** (Log on to Network), **Программное сжатие данных** (Enable software compression) и **TCP/IP**.

Остальные параметры в диалоге **Нульмодем** можно оставить без изменения.

- Нажмите кнопку OK, чтобы зафиксировать изменения и закрыть диалог **Нульмодем.**
- Двойным щелчком мыши на строке **Нульмодем** запустите программу установки связи. На экране появится диалог **Установка связи** (Connect To) (Рис. 2.31).

На этом подготовка компьютера-клиента для связи через нульмодем закончена. Теперь необходимо подготовить компьютер-сервер, который будет принимать вызов через нульмодем. Для этого выполните следующие действия.

- Нажмите кнопку **Пуск** (Start). Откроется главное меню Windows 98.

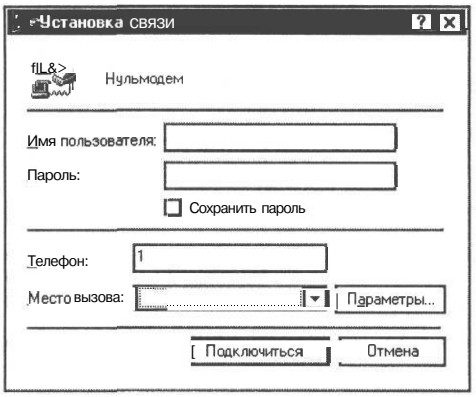



*Рис. 2.31 Диалог* ***Установка связи*** *(Connect To)*

> В главном меню выберите команду **Программы** ◆ **Стандартные** ◆ **Связь * Удаленный доступ к сети** (Programs ◆ Accessories ◆ Communications * Dial-Up Networking). На экране появится окно **Удаленный доступ к сети** (Dial-Up Networking) (Рис. 2.26).

➤ В окне **Удаленный доступ к сети** (Dial-Up Networking) выберите команду основного меню **Соединения** ◆ **Сервер удаленного доступа** (Communications ◆ Dial-Up Networking). На экране появится диалог **Сервер удаленного доступа** (Dial-Up Server) (Рис.2.32).

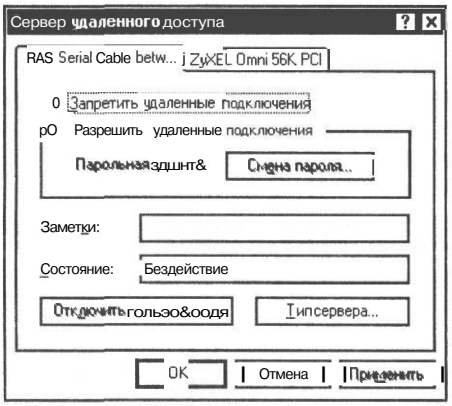



*Рис. 2.32 Диалог* ***Сервер удаленного доступа*** *(Dial-Up Server)*

Если у вас в компьютере установлены другие модемы, то диалог **Сервер удаленного доступа** (Dial-Up Server) будет содержать несколько вкладок по количеству подключенных модемов.

➤ Перейдите на вкладку **RAS Serial Cable between 2 PCs** (Сервер удаленного доступа для последовательного кабеля между двумя компьютерами) и нажмите кнопку **Тип сервера** (Server Type). На экране появится диалог **Тип сервера** (Server Type) (Рис. 2.33).

> Из открывающегося списка **Тип сервера удаленного доступа** (Type of Dial-Up Server) выберите строку **PPP: Интернет, Windows NT Server, Windows 98** (PPP: Internet, Windows NT Server, Windows 98).

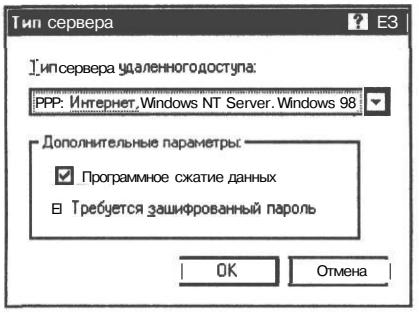



*Рис. 2.33 Диалог* ***Тип сервера*** *(Server Type)*

- *В* группе элементов управления **Дополнительные параметры:** (Advanced option) установите флажок **Программное сжатие данных** (Enable software compression) и сбросьте флажок **Требуется зашифрованный пароль** (Require encrypted password). Последнее действие необходимо для того, чтобы при установке соединения компьютер-сервер не запрашивал у компьютера-клиента пароль.
- Нажмите кнопку OK, чтобы закрыть диалог.
- В диалоге **Сервер удаленного доступа** (Dial-Up Server) установите переключатель в положение **Разрешить удаленные подключения** (Allow caller access) и нажмите кнопку Применить (Apply). В поле **Состояние** (Status) появится надпись **Наблюдение** (Monitoring), а на **панели задач** значок с экраном черного цвета. Это свидетельствует о том, что компьютер-сервер готов к установке соединения и находится в состоянии ожидания.
- На компьютере-клиенте в диалоге **Установка связи** (Connect To) (Рис. 2.31) в поле ввода **Пользователь** (User Name) введите свое имя или имя своего компьютера и нажмите кнопку **Подключиться** (Connect). На экране появится диалог **Установка связи с Нульмодем** (Connect to Нульмодем) (Рис. 2.34).


*Рис. 2.34 Диалог* ***Установка связи с Нульмодем*** *(Connect to Нульмодем)*

В этом диалоге будут последовательно появляться сообщения, отображающие этапы подключения к компьютеру-серверу. С помощью кнопки **Отмена** (Cancel) можно прервать установку соединения. На компьютере-сервере в строке **Состояние** (Status) диалога **Сервер удаленного доступа** (Dial-Up Server) также будет отображаться процесс установки соединения. После успешной установки связи на компьютере-клиенте диалог **Установка связи с Нульмодем** (Connect to Нульмодем) закроется, а на **панели задач** рабочего стола появится значок с экранами зеленого цвета. На компьютере-сервере в поле **Состояние** (Status) будет выведена информация об имени подключенного компьютера и времени подключения (Рис. 2.35), а на **панели задач** появится значок .

- Нажмите кнопку OK, чтобы закрыть диалог **Сервер удаленного доступа** (Dial-Up Server).

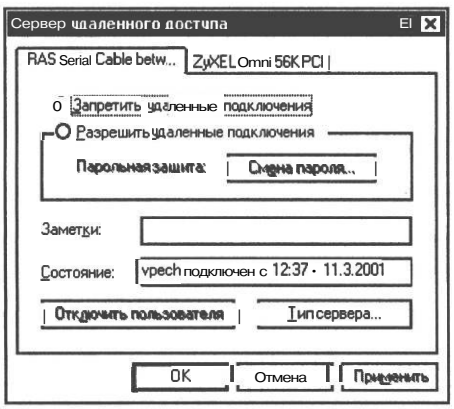



*Рис. 2.35 Вид диалога* ***Сервер удаленного доступа*** *(Dial-Up Server) после установки соединения*

Чтобы убедиться в нормальной работе установленного соединения, выполните следующие действия.

- Нажмите кнопку Пуск (Start) на **панели задач.** Откроется главное меню Windows 98.
- В главном меню выберите команду **Выполнить** (Run). На экране появится диалог **Запуск программы** (Run) (Рис. 2.36).

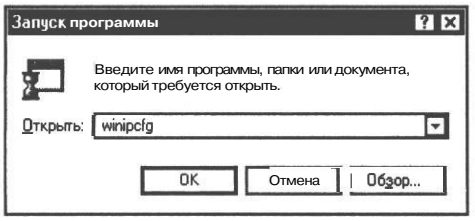



*Рис. 2.36 Диалог* ***Запуск программы*** *(Run)*

- В поле ввода **Открыть** (Open) введите текст:
  **winipcfg**
  и нажмите кнопку OK. На экране появится диалог **Конфигурация IP** (IP Configuration) (Рис. 2.37).

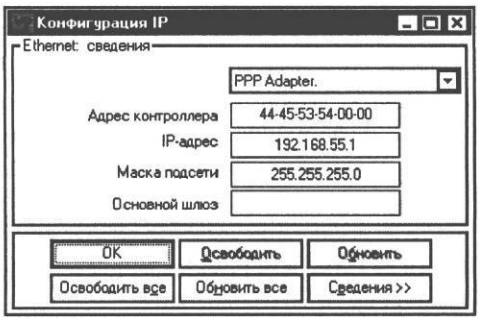



*Рис. 2.37 Диалог* ***Конфигурация IP*** *(IP Configuration)*

- Из открывающегося списка, расположенного в верхней части диалога, выберите строку **PPP Adapter** (Адаптер точка-точка), при этом в поле **IP-адрес** (IP Address) появится значение адреса, которое для компьютера-сервера будет равно **192.168.55.1**, а для компьютера-клиента **192.168.55.2.** Это свидетельствует о том, что оба компьютера теперь имеют IP-адреса.
- Нажмите кнопку OK, чтобы закрыть диалог **Конфигурация IP** (IP Configuration).

Чтобы проверить передачу данных по каналу связи от одного компьютера к другому, на обоих компьютерах выполните следующие действия.

- Нажмите кнопку **Пуск** (Start). Откроется главное меню Windows 98.
- В главном меню выберите команду **Программы * Сеанс MS-DOS** (Programs ◆ MS-DOS Prompt). На экране появится окно **Сеанс MS-DOS** (MS-DOS Prompt) (Рис. 2.38).

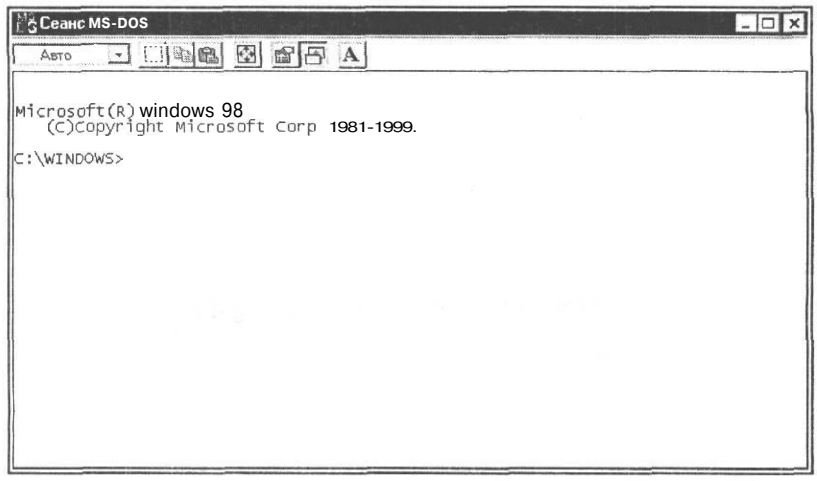



*Рис. 2.38 Окно **Сеанс MS-DOS (MS-DOS** Prompt)*

На компьютере-сервере введите в окне **Сеанс MS-DOS** (MS-DOS Prompt) команду:

**ping 192.168.55.2** Enter

А на компьютере-клиенте команду:

**ping 192.168.55.1** Enter

В окне будет выведена информация об обмене пакетами данных между компьютерами (Рис. 2.39).

Во время обмена пакетами данных между компьютерами в окне **Сеанс MS-DOS** (MS-DOS Prompt) будет выводиться информация об отклике удаленного компьютера, числе переданных байтов и времени задержки. По окончании сеанса обмена будет выведена статистическая информация о количестве посланных, принятых и потерянных пакетов. Мы видим, что потерянных пакетов нет, т.е. качество связи хорошее.

- Закройте окно **Сеанс MS-DOS** (MS-DOS Prompt) на обоих компьютерах, нажав кнопку ☒, расположенную в правой части заголовка окна.

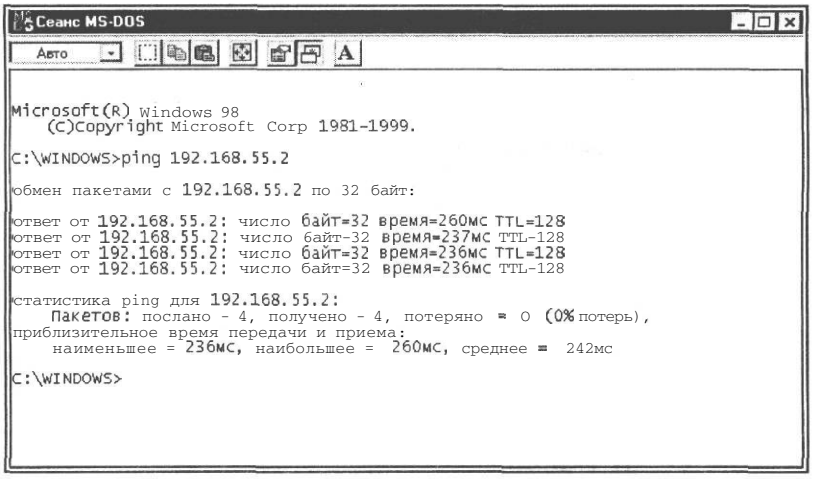



*Рис. 2.39 Окно* ***Сеанс*** *MS-DOS (MS-DOS Prompt) с информацией об обмене между компьютерами пакетами данных*

Если компьютерам не удалось установить соединение или при проверке обмена появляются потерянные пакеты данных, то попробуйте изменить скорость передачи данных через COM-порты компьютеров на более низкую. Для этого необходимо выполнить следующие действия на обоих компьютерах.

- Нажмите кнопку **Пуск** (Start). Откроется главное меню Windows 98.
- В главном меню выберите команду **Настройка * Панель управления** (Settings ◆ Control Panel). На экране появится окно **Панель управления** (Control Panel) (Рис. 2.5).
- Дважды щелкните мышью на строке **Модемы** (Modems). На экране появится диалог **Свойства: Модемы** (Modems Properties) (Рис. 2.40).

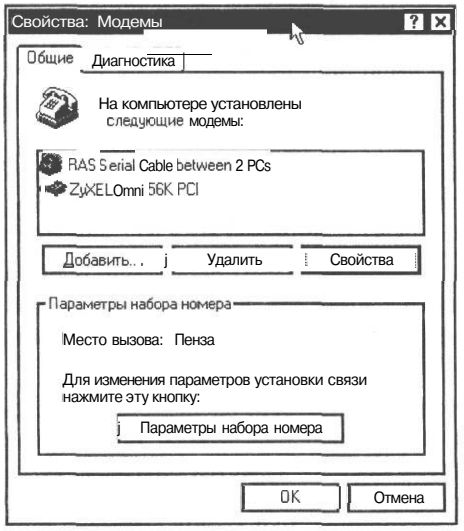



*Рис. 2.40 Диалог* ***Свойства: Модемы*** *(Modems Properties)*

➤ В списке **На компьютере установлены следующие модемы** (The following modems are set up on this computer) выберите строку **RAS Serial Cable between 2 PCs** и нажмите кнопку **Свойства** (Properties). На экране появится диалог **Свойства: RAS Serial Cable between 2 PCs** (RAS Serial Cable between 2 PCs Properties) (Рис. 2.41).

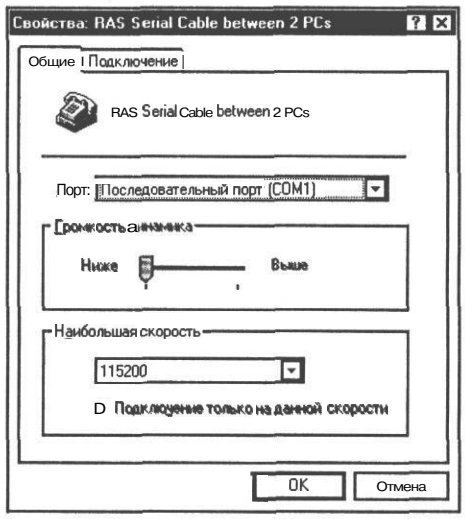



***Рис. 2.41 Диалог Свойства: RAS Serial Cable between 2 PCs***
*(RAS Serial Cable between 2 PCs Properties)*

> В группе элементов управления **Наибольшая скорость** (Maximum speed) из открывающегося списка выберите строку **9600** и нажмите кнопку OK, диалог будет закрыт.

➤ Закройте диалог **Свойства: Модемы** (Modems Properties) с помощью кнопки OK.

> Закройте окно **Панель управления** (Control Panel) с помощью кнопки ☒, расположенной в правой части заголовка окна.

➤ Повторите попытку еще раз установить связь и проверьте обмен данными между компьютерами, как это было описано ранее. Если и после этого соединение установить не удалось или появляются потерянные пакеты данных, то прозвоните нульмодемный кабель и проверьте надежность его подключения.

Если связь установилась и потерянных пакетов нет, то можно попробовать увеличить скорость соединения с помощью диалога **Свойства: RAS Serial Cable between 2 PCs** (RAS Serial Cable between 2 PCs Properties) (Рис. 2.41), как это было описано выше.

После успешной установки связи в сетевом окружении обоих компьютеров появятся их имена и станет возможно предоставить в совместное использование папки, файлы и принтеры, имеющиеся в распоряжении каждого из них, а также работать с различными сетевыми программами и играми.

Если на компьютере-клиенте используется операционная система Windows 2000/XP, то в настройке соединения никаких изменений не требуется. Однако, если компьютер с операционной системой Windows 2000/XP является сервером, т.е. к нему будет производиться подключение с помощью нульмодема, то необходимо настроить и разрешить прием входящих подключений. В операционной системе Windows XP это делается с помощью мастера новых подключений. Выполните следующие действия.

➤ Нажмите кнопку Пуск (Start). На экране появится главное меню Windows.

> Выберите команду меню **Панель управления** (Control Panel), на экране появится окно **Панель управления** (Control Panel) (Рис. 2.42).

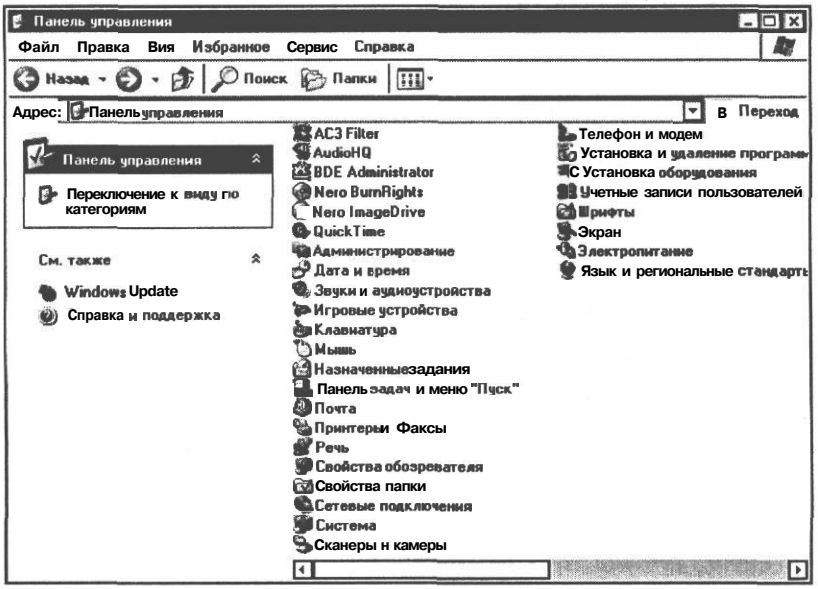



*Рис. 2.42 Окно **Панель управления** (Control Panel)*

> Дважды щелкните мышью на строке **Сетевые подключения** (Network Connection), на экране появится окно **Сетевые подключения** (Network Connection) (Рис. 2.43).

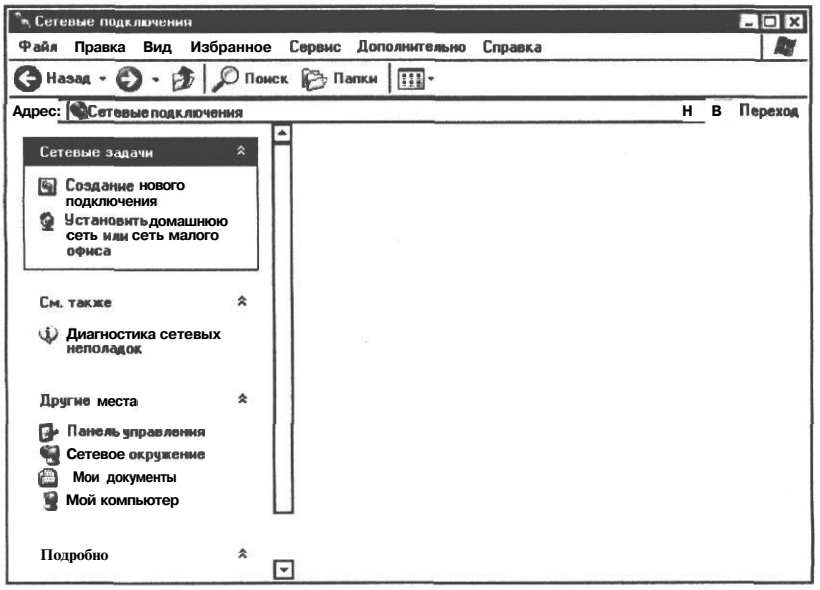



*Рис.* 2.43 *Окно **Сетевые подключения** (Network Connection)*

> Выберите команду меню **Файл ◆ Новое подключение** (File ◆ New connection), на экране появится первый диалог мастера новых подключений (Рис. 2.44).

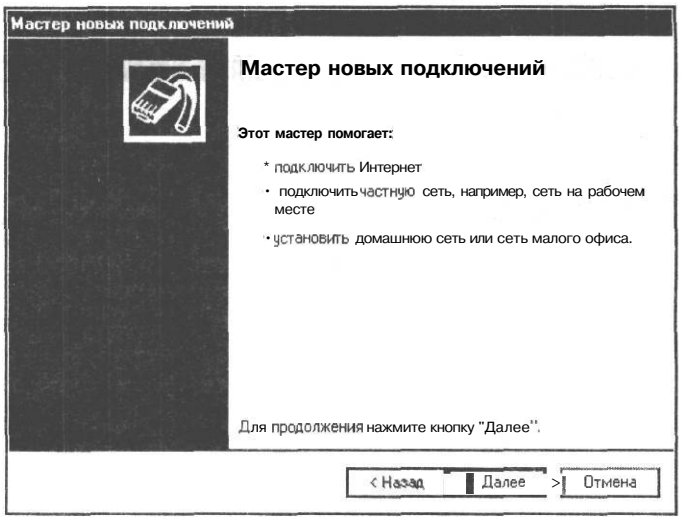



*Рис. 2.44 Первый диалог мастера новых подключений*

> Нажмите кнопку **Далее** (Next), на экране появится следующий диалог мастера новых подключений (Рис. 2.45).

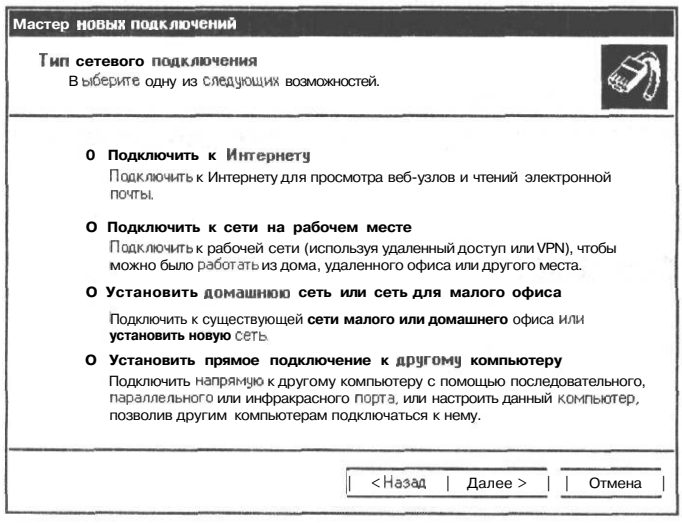



*Рис. 2.45 Второй диалог мастера новых подключений*

➤ Установите переключатель диалога в положение **Установить прямое подключение к другому компьютеру** (Set up an advanced connection) и нажмите кнопку **Далее** (Next). На экране появится следующий диалог мастера новых подключений (Рис. 2.46).

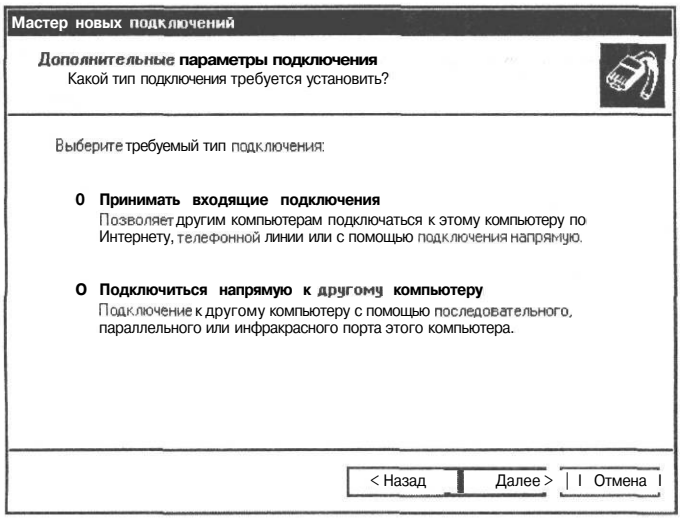



*Рис. 2.46 Третий диалог мастера новых подключений*

> Установите переключатель диалога в положение **Принимать входящие подключения** (Accept incoming connections) и нажмите кнопку **Далее** (Next). На экране появится следующий диалог мастера новых подключений (Рис. 2.47).

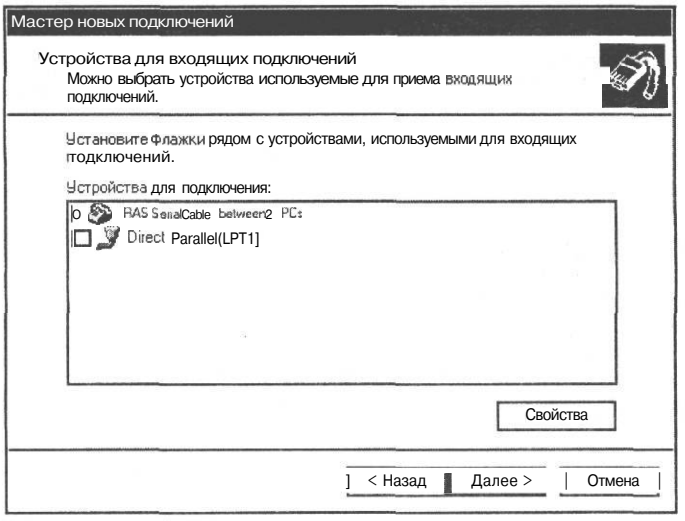



*Рис. 2.47 Четвертый диалог мастера новых подключений*

> В списке **Устройства для подключения** (Connection devices) установите флажок в строке **RAS Serial Cable between 2 PCs** и нажмите кнопку **Далее** (Next). На экране появится следующий диалог мастера новых подключений (Рис. 2.48).

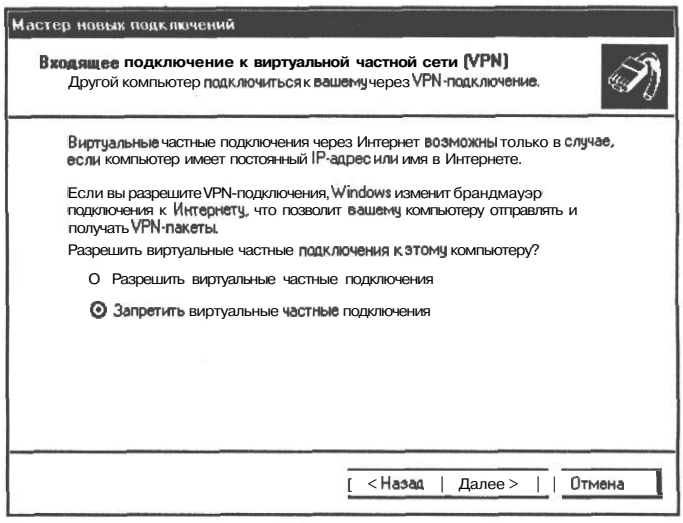



*Рис. 2.48 Пятый диалог мастера новых подключений*

> Установите переключатель диалога в положение **Запретить виртуальные частные подключения** (Do not allow virtual private connections) и нажмите кнопку **Далее** (Next). На экране появится следующий диалог мастера новых подключений (Рис. 2.49).

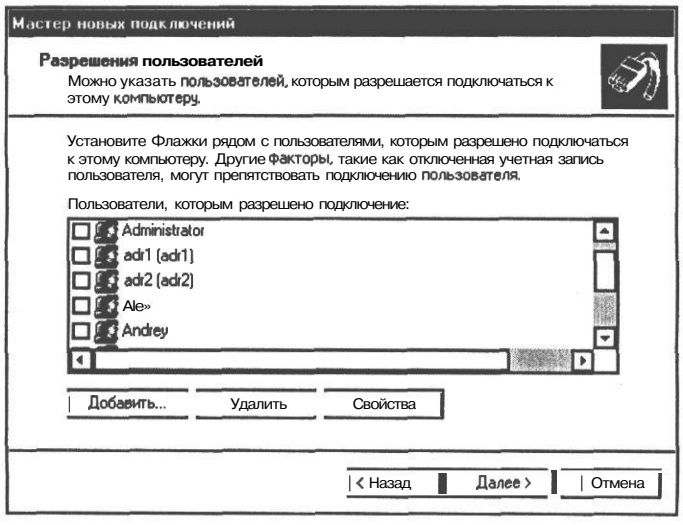



*Рис. 2.49 Шестой диалог мастера новых подключений*

> В списке **Пользователи, которым разрешено подключение** (Users allowed to connect) установите флажок в строке с именем пользователя, который будет указан

на компьютере-клиенте в диалоге Установка связи (Connect To) (Рис. 2.31). Если в списке пользователей, которым разрешено подключение, строка с нужным именем пользователя отсутствует, то нужно создать новую учетную запись с помощью диалога Новый пользователь (New User) (Рис. 2.50), который вызывается кнопкой Добавить (Add).

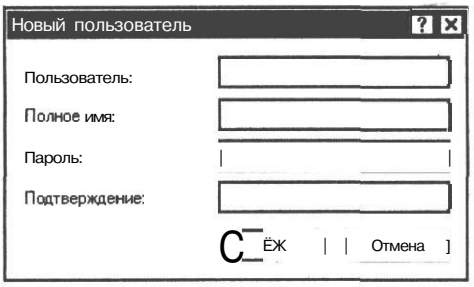



*Рис. 2.50 Диалога Новый пользователь (New User)*

➤ Нажмите кнопку Далее (Next), на экране появится следующий диалог мастера новых подключений (Рис. 2.51).

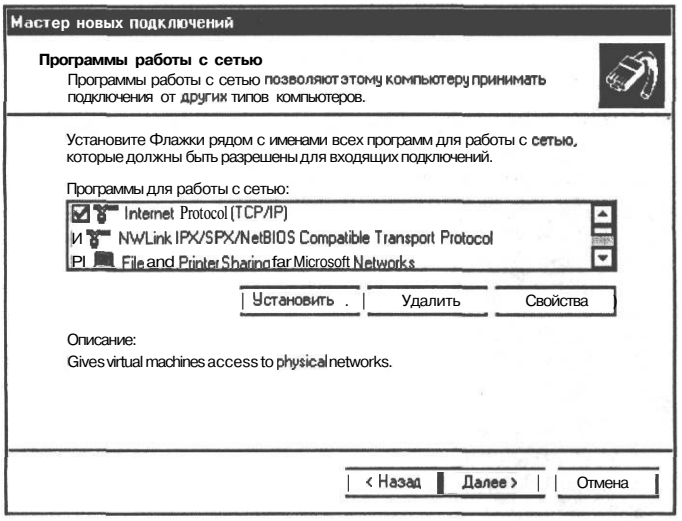



*Рис. 2.51 Седьмой диалог мастера новых подключений*

> В списке Программы для работы с сетью (Networking software) установите флажки в строках с именами сетевых протоколов и служб, которые будут вам нужны для работы (в большинстве случаев достаточно установить протокол TCP/IP и службу доступа к файлам и принтерам сети Microsoft (File and Printer Sharing for Microsoft Network)).

На этом этапе вы можете настроить параметры протокола TCP/IP. Для этого достаточно в списке Программы для работы с сетью (Networking software) щелкнуть мышью на имени протокола и нажать кнопку Свойства (Properties). При этом на экране появится

диалог **Свойства входящих вызовов TCP/IP** (Incoming TCP/IP Properties) (Рис. 2.52), в котором вы сможете настроить параметры IP-адреса, которые получит компьютер-клиент при установке связи.

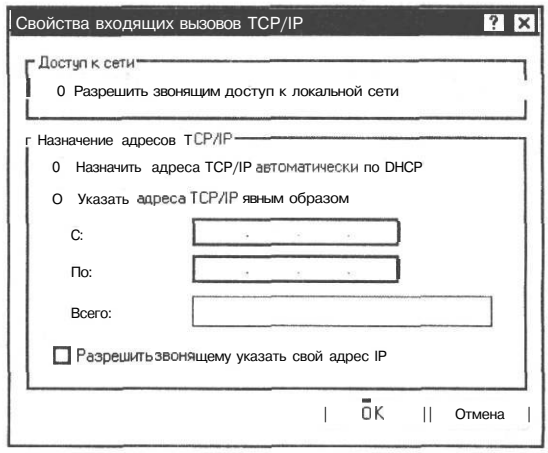



*Рис. 2.52 Диалог* ***Свойства входящих вызовов*** *TCP/IP (Incoming TCP/IPProperties)*

> После выбора и настройки сетевых протоколов нажмите кнопку Далее (Next), на экране появится заключительный диалог мастера новых подключений (Рис. 2.53).

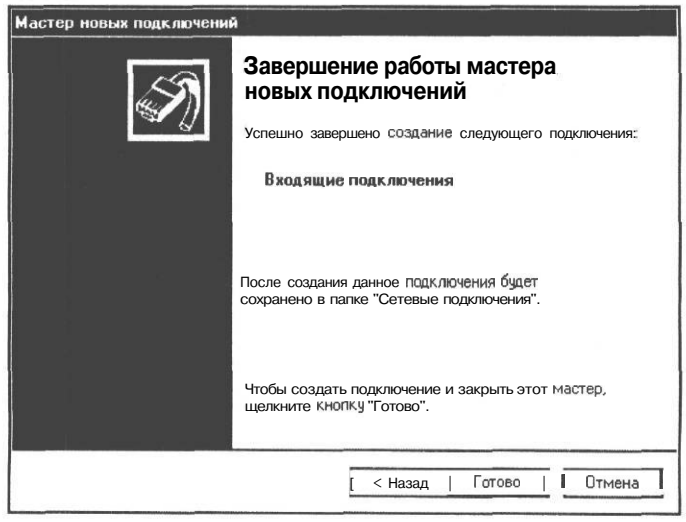



*Рис. 2.53 Заключительный диалог мастера новых подключений*

➤ Нажмите кнопку **Готово** (Finish), работа мастера новых подключений завершится, а в окне **Сетевые подключения** (Network Connection) появится строка **Входящие подключения** (Incoming connection).

С этого момента можно установить связь между компьютерами с помощью диалога **Установка связи** (Connect to) (Рис. 2.31) на компьютере-клиенте.

Если оба компьютера работают под управлением операционной системы Windows 2000/XP, то во избежание конфликтов, связанных с работой службы обозревателя компьютеров, на одном из компьютеров эту службу нужно отключить. Подробнее об обозревателе компьютеров и о разрешении связанных с его работой конфликтов вы сможете узнать в одной из следующих глав этой книги, поскольку этот вопрос является общим при организации сети любого вида и не зависит от количества компьютеров в сети или типа устройств, используемых для соединения компьютеров в сеть.

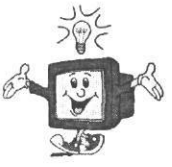
## Локальная сеть на основе USB

Описанный выше способ организации сетевого соединения между двумя компьютерами хоть и не требует больших материальных затрат, но по своим скоростным характеристикам оставляет желать много лучшего. Менее 10 лет назад была разработана универсальная последовательная шина - USB (Universal Serial Bus), которая должна была прийти на смену последовательному коммуникационному порту и предназначена для связи периферийных устройств с компьютером на скорости до 12 Мбит/сек в первоначальном своем варианте (USB 1.1). Практически все материнские платы, выпущенные за последние 5 лет, имеют поддержку этого интерфейса, а все современные материнские платы уже оснащаются универсальной последовательной шиной второй версии (USB 2.0), обеспечивающей скорость передачи данных до 480 Мбит/сек (при такой скорости становится возможной передача в реальном масштабе времени видеоинформации с дисководов DVD и цифровых видеокамер). Однако, поскольку изначально эта шина разрабатывалась для связи с различными внешними устройствами (модемы, принтеры, сканеры, цифровые фотоаппараты, видеокамеры и т.п.), она является несимметричной и в чистом виде не может быть использована для связи между двумя равноправными устройствами (компьютерами). Поэтому для связи между двумя компьютерами был разработан особенный кабель, оснащенный специальным устройством. Первоначально такие кабели обеспечивали лишь передачу файлов с одного компьютера на другой, что нельзя считать полноценной сетью (нет возможности использовать общие ресурсы или пользоваться сетевыми программами или играми). Но впоследствии задача была решена, и теперь все современные USB кабели, предназначенные для связи между двумя компьютерами, поддерживают полноценное сетевое соединение.

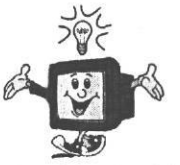
Объединение компьютеров в единую сеть с помощью шины USB идеально подходит, если стоит задача подключения переносного компьютера (ноутбука) к внутренней сети офиса, предприятия или домашнему компьютеру или связи двух компьютеров, расположенных в непосредственной близости друг от друга (длина стандартного USB-кабеля равна 2 метрам).

Мы покажем основные настройки, которые необходимо произвести для организации сетевого соединения двух компьютеров с помощью USB Network Link Cable (UANC11) (Кабель для сетевого соединения через USB 1.1).

*При приобретении кабеля обратите особое внимание на его тип, т.к. в продаже имеются внешне похожие кабели, предназначенные лишь для передачи данных с одного компьютера на другой. Например, кабель типа **UAU211** (USB to USB Laplink Cable — кабель для связи между компьютерами по шине USB) для организации сетевого соединения не подходит.*



*Внимание, если Вы соедините два компьютера обычным USB-кабелем, компьютеры могут сгореть.*



В комплекте с кабелем поставляется дискета с необходимым для нормальной работы программным обеспечением. Мы опишем настройку такого соединения для операционной системы Windows 98/Me.

- Соедините два компьютера кабелем UANC11, при этом не имеет значения в какой порт (обычно компьютер имеет 2 и более разъемов для подключения USB-устройств) будут подключены разъемы кабеля.
- Включите питание компьютера и дождитесь загрузки операционной системы.
- Соедините два компьютера кабелем UANC11, при этом не имеет значения в какой порт (обычно компьютер имеет 2 и более разъемов для подключения USB-устройств) будут подключены разъемы кабеля.
- Включите питание компьютера и дождитесь загрузки операционной системы.

После загрузки операционной системы на экране появится сообщение о том, что обнаружено новое устройство (Рис. 2.54).

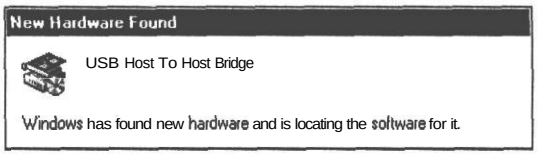



*Рис. 2.54 Диалог об обнаружении нового оборудования*

После чего на экране появится первый диалог мастера установки нового оборудования (Рис. 2.55).

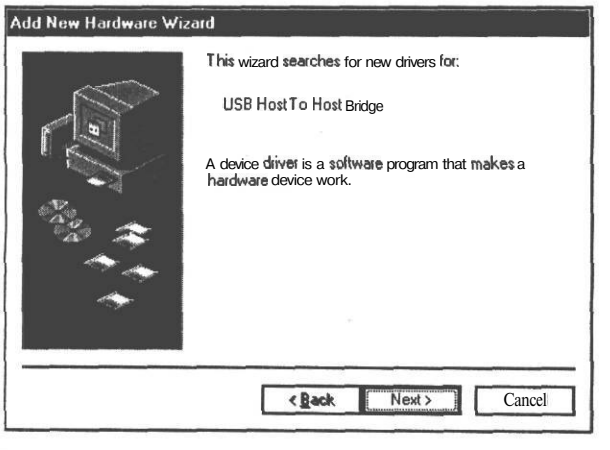



*Рис. 2.55 Первый диалог мастера установки нового оборудования*

➤ Нажмите кнопку **Next** (Далее), на экране появится следующий диалог мастера установки нового оборудования (Рис. 2.57).

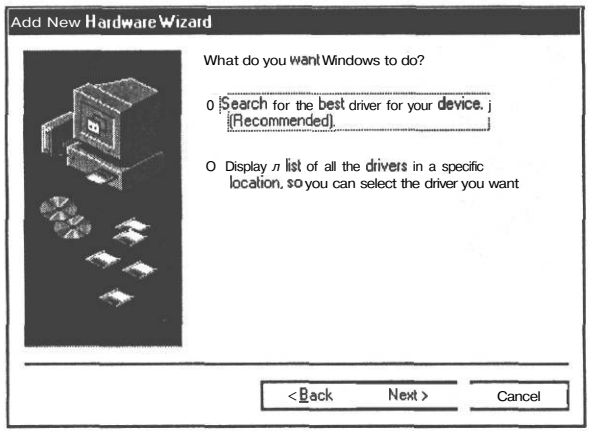



*Рис. 2.56 Второй диалог мастера установки нового оборудования*

В этом диалоге операционная система предлагает вам выбрать действие, которое она должна выполнить: произвести автоматический поиск размещения драйвера нового устройства или установить драйвер с указанного вами носителя информации.

> Установите переключатель диалога в положение **Search for the best driver for your device (Recommended)** (Произвести поиск наиболее свежего драйвера для устройства (Рекомендуется)). И нажмите кнопку **Next** (Далее), на экране появится следующий диалог мастера установки нового оборудования (Рис. 2.57).

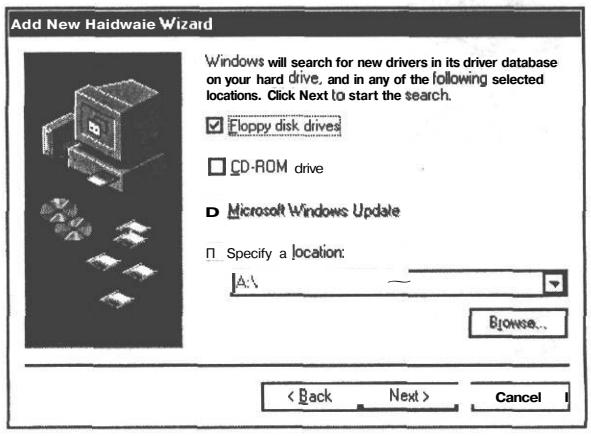



*Рис. 2.57 Третий диалог мастера установки нового оборудования*

В этом диалоге вам предлагается указать носитель, на котором находятся драйверы (управляющие программы) для нового устройства.

> Установите флажок **Floppy disk drives** (Гибкие диски), вставьте в дисковод 3,5-дюймовую дискету, которая входит в комплект поставки кабеля UANC11 и нажмите кнопку **Next** (Далее), на экране появится следующий диалог мастера установки (Рис. 2.58).

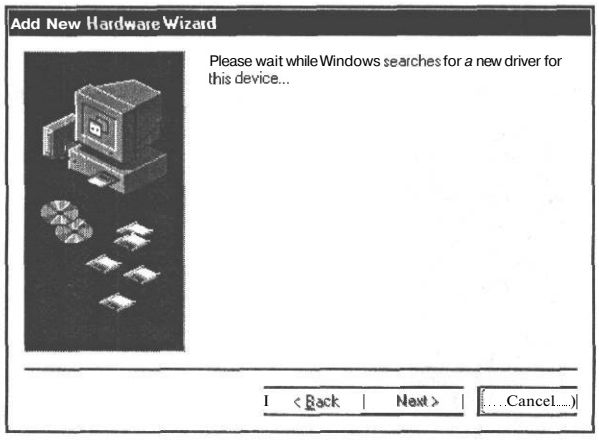



*Рис. 2.58 Четвертый диалог мастера установки оборудования*

В этом диалоге сообщается, что система производит поиск необходимых файлов на указанном диске. После чего на экране появится следующий диалог мастера установки оборудования с информацией о том, что обнаружен драйвер для подключенного устройства (Рис. 2.59).

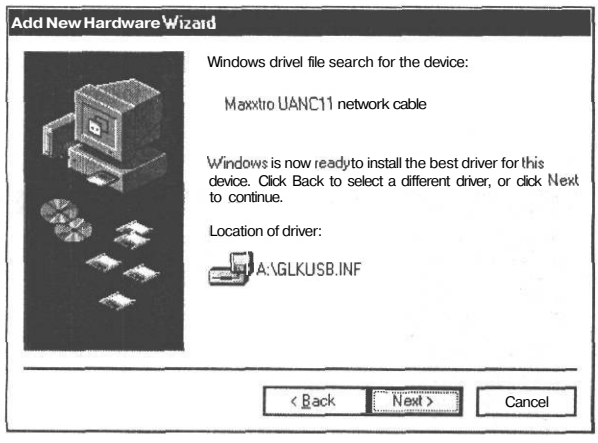



*Рис. 2.59 Пятый диалог мастера установки оборудования*

> Нажмите кнопку **Next** (Далее), на экране появится следующий диалог, отображающий процесс копирования файлов с дискеты во временную папку жесткого диска вашего компьютера (Рис. 2.60).

По окончании процесса копирования файлов на экране появится заключительный диалог мастера установки оборудования (Рис. 2.61).

➤ Нажмите кнопку **Finish** (Готово), заключительный диалог мастера установки нового оборудования будет закрыт, а на экране появится диалог установки программного обеспечения для работы с кабелем UANC11 (Рис. 2.62).

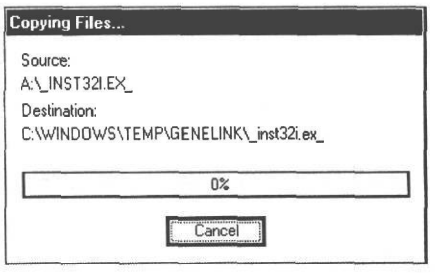



*Рис. 2.60 Диалог, отображающий процесс копирования файлов*

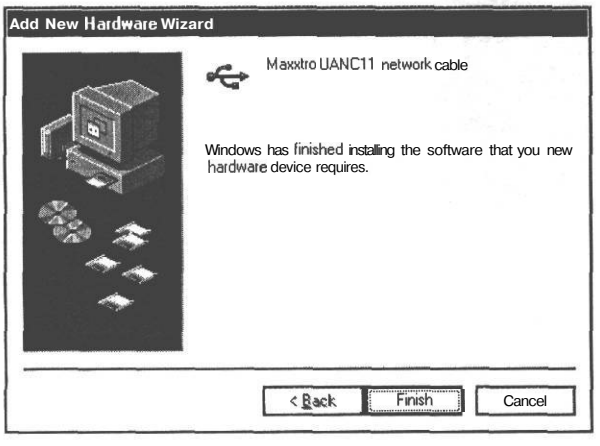



*Рис. 2.61 Заключительный диалог мастера установки оборудования*

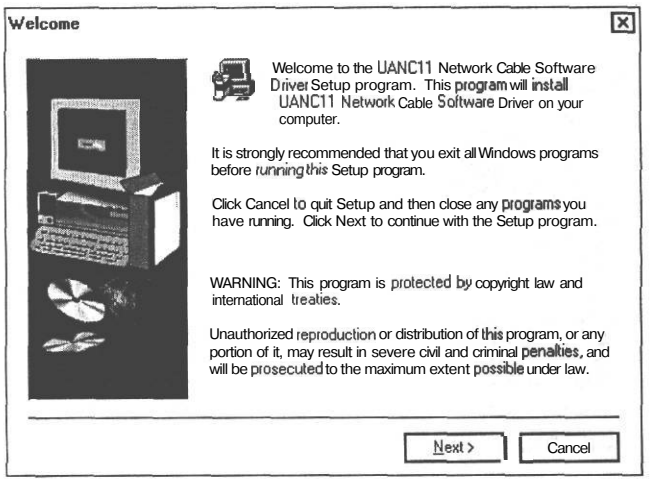



*Рис. 2.62 Первый диалог установки программного обеспечения для работы с кабелем UANC11*

В этом диалоге содержится приветствие от разработчиков программ и рекомендуется перед началом установки завершить работу других запущенных на компьютере программ.

➤ Нажмите кнопку **Next** (Далее), на экране появится следующий диалог мастера установки программного обеспечения (Рис. 2.63).

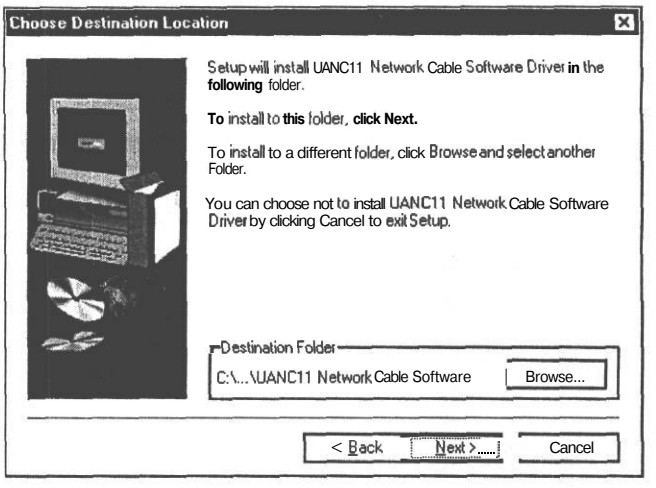



*Рис. 2.63 Второй диалог мастера установки программного обеспечения*

В этом диалоге вам предлагают выбрать папку, в которую будут скопированы файлы, необходимые для нормальной работы оборудования. Мы изменять папку назначения, предложенную по умолчанию, не будем. Вы можете указать другую папку с помощью диалога **Choose folder** (Выбор папки), который вызывается кнопкой **Browse** (Обзор).

➤ После выбора папки назначения нажмите кнопку **Next** (Далее). На экране появится следующий диалог мастера установки (Рис. 2.64).

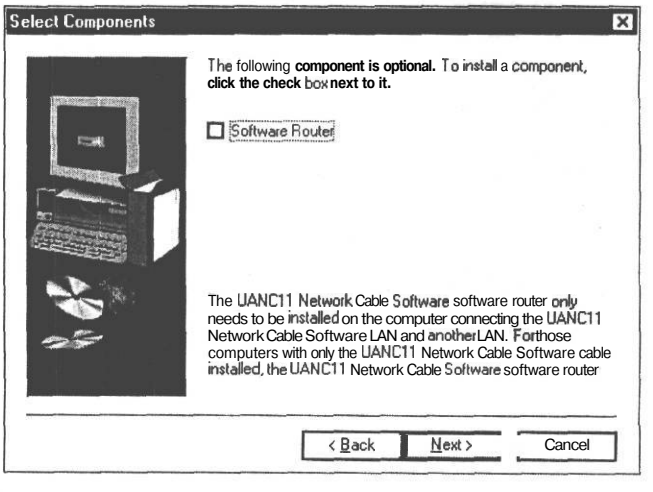



*Рис. 2.64 Третий диалог мастера установки программного обеспечения*

В этом диалоге говорится, что устанавливаемый компонент является не обязательным и, чтобы установить его, необходимо установить флажок **Software Router** (Программный маршрутизатор). Этот компонент понадобится вам, если ваш компьютер уже имеет сетевое соединение с другим компьютером или локальной сетью, в этом случае вновь создаваемое с помощью кабеля UANC11 соединение можно связать с уже существующим и получить таким образом единую компьютерную сеть. Мы устанавливать флажок **Software Router** (Программный маршрутизатор) не будем и покажем настройку соединения между двумя компьютерами.

> Нажмите кнопку **Next** (Далее). На экране появится диалог и индикатор установки, отображающий ход копирования необходимых файлов на жесткий диск вашего компьютера (Рис. 2.65).

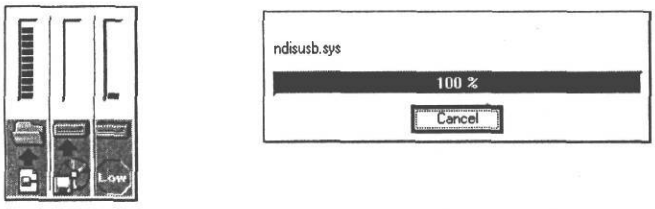



*Рис. 2.65 Диалог, отображающий ход копирования файлов*

В процессе копирования файлов может потребоваться установочный компакт-диск с операционной системой Windows 98. В этом случае на экране может появиться диалог о том, что не найден на исходный носитель (Рис. 2.66).

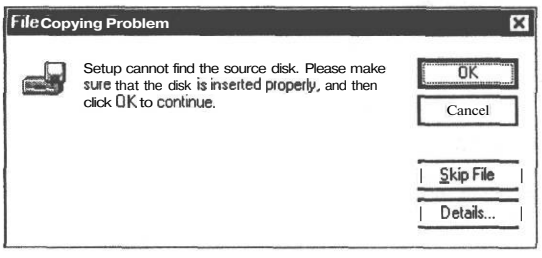



*Рис. 2.66 Диалог с предупреждением*

В этом случае нужно установить в привод для чтения компакт-дисков диск, содержащий дистрибутив операционной системы Windows 98, и нажать кнопку OK. Установка будет продолжена, о чем будет свидетельствовать диалог с прогресс-индикатором (Рис. 2.67).

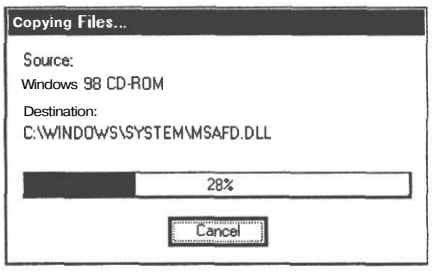



*Рис. 2.67 Диалог с прогресс-индикатором*

По окончании копирования файлов на экране может появиться информационный диалог (Рис. 2.68).

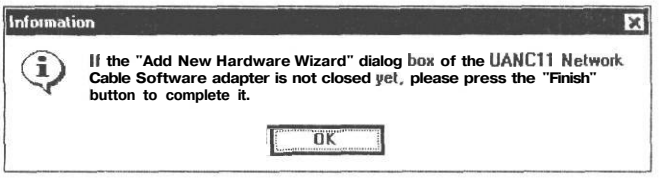



*Рис. 2.68 Информационный диалог*

В этом диалоге говорится о том, что если заключительный диалог мастера установки нового оборудования не был закрыт, то необходимо закрыть его с помощью кнопки **Finish** (Готово).

➤ Закройте заключительный диалог мастера установки нового оборудования с помощью кнопки **Finish** (Готово), если не сделали этого раньше, и нажмите кнопку OK в информационном диалоге, чтобы закрыть его. На экране появится заключительный диалог мастера установки программного обеспечения (Рис. 2.69).

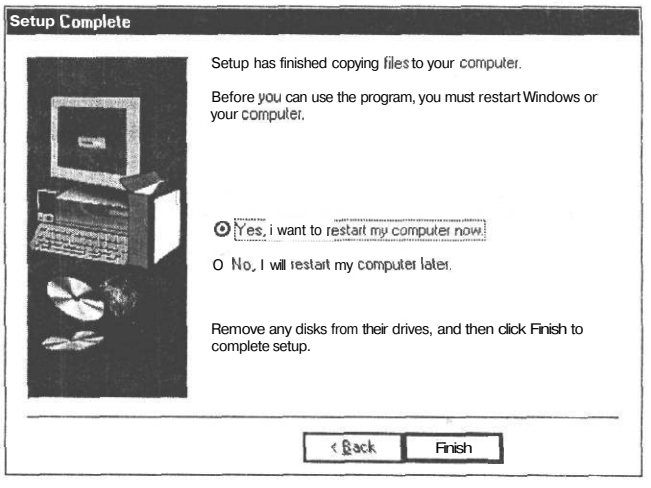



*Рис. 2.69 Заключительный диалог мастера установки программного обеспечения*

В этом диалоге сообщается, что установка программного обеспечения успешно завершена и перед тем как начать его использовать, необходимо выполнить перезагрузку компьютера.

> Установите переключатель диалога в положение **Yes, I want to restart my computer now** (Да, я хочу перезагрузить компьютер сейчас) и нажмите кнопку **Finish** (Готово). Заключительный диалог мастера установки программного обеспечения будет закрыт, а компьютер перезагружен.

После перезагрузки и входа в систему, для того чтобы убедиться в том, что установка прошла успешно, выполните следующие действия.

- Щелкните правой кнопкой мыши на ярлыке 

(сетевое окружение), расположенном на рабочем столе. На экране появится контекстное меню для сетевого окружения (Рис. 2.70).

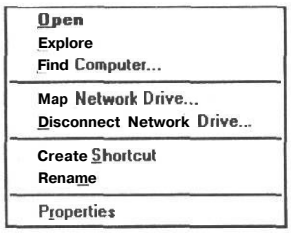



*Рис. 2.70 Контекстное меню для сетевого окружения*

- Выберите команду контекстного меню **Properties** (Свойства), на экране появится диалог Network (Сеть) (Рис. 2.71).

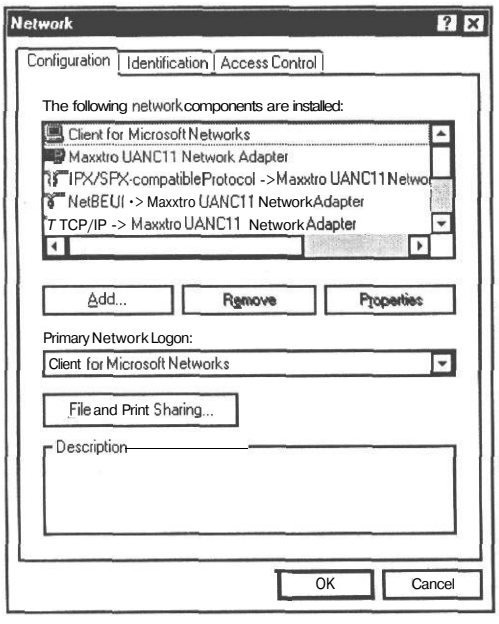



*Рис. 2.71 Диалог **Network** (Сеть)*

В списке **The following network components are installed** (В системе установлены следующие компоненты) появится строка **Maxxtro UANC11 Network Adapter,** свидетельствующая,

что в системе появился новый сетевой адаптер. Кроме того, в списке будут присутствовать строки, указывающие на установку для этого адаптера сетевых протоколов TCP/IP NetBEUI и IPX/SPX. Дальнейшая настройка сетевого соединения не отличается от настройки сети с использованием обычного сетевого адаптера. Выполните следующие действия.

- Убедитесь, что на вкладке **Identification** (Идентификация) диалога **Network** (Сеть) (Рис. 2.23) каждому компьютеру задано уникальное имя и общее имя рабочей группы (workgroup).
- Перейдите на вкладку **Configuration** (Конфигурация) и в списке **The following network components are installed** (В системе установлены следующие компоненты) щелкните мышью на строке TCP/IP -> **Maxxtro UANC11 Network Adapter,** чтобы выделить ее.
- Нажмите кнопку **Properties** (Свойства), на экране появится диалог **TCP/IP Properties** (Свойства TCP/IP) (Рис. 2.72).

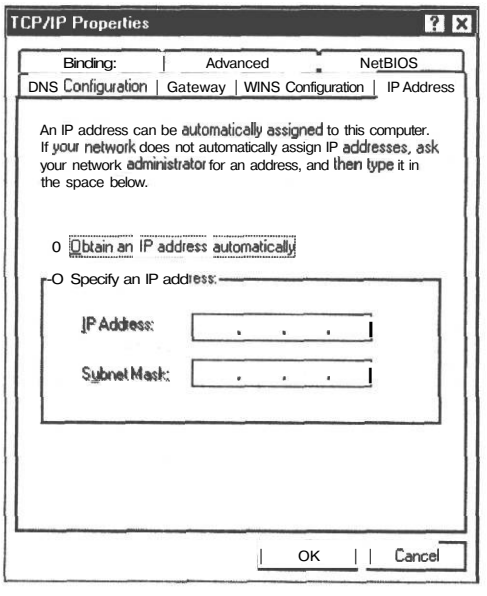



*Рис. 2.72 Диалог **TCP/IP Properties** (Свойства TCP/IP)*

- Установите переключатель диалога в положение **Specify an IP address** (Указать IP-адрес явным образом) и введите в поле ввода IP **Address** (IP Адрес) на одном компьютере число **192.168.0.1**, а на другом компьютере - **192.168.0.2**. В поле ввода **Subnet Mask** (Маска подсети) введите число 255.255.255.0, одинаковое для обоих компьютеров.
- Нажмите кнопку OK в диалогах **TCP/IP Properties** (Свойства TCP/IP) и Network (Сеть), чтобы закрыть их, на экране появится диалог **System Setting Change** (Изменение параметров системы) (Рис. 2.73).

В этом диалоге говорится о том, что настройки операционной системы были изменены и для того чтобы новые установки вступили в силу, требуется перезагрузка системы.

- Нажмите кнопку **Yes** (Да), диалог закроется, а компьютер перезагрузится.

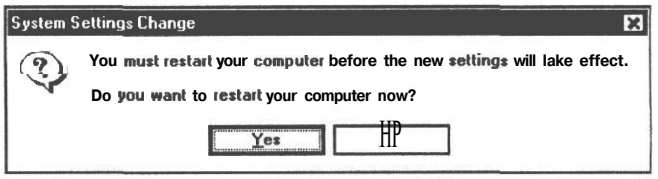



*Рис. 2.73Диалог System Setting Change (Изменение параметров системы)*

После перезагрузки и входа в операционную систему в сетевом окружении компьютеров появятся значки с именами связанных сетевым кабелем компьютеров и станет возможным использование общих папок, файлов и принтеров. Чтобы убедиться в работоспособности сети, выполните следующие действия.

- Нажмите кнопку Пуск (Start). Откроется главное меню Windows 98.
- В главном меню выберите команду Программы ◆ Сеанс MS-DOS (Programs ◆ MS-DOS Prompt). На экране появится окно Сеанс MS-DOS (MS-DOS Prompt) (Рис. 2.38).
- На компьютере с сетевым адресом 192.168.0.2 введите в окне Сеанс MS-DOS (MS-DOS Prompt) команду:

  **ping 192.168.0.1** Enter

  а на компьютере с IP адресом 192.168.0.1 команду:

  ping **192.168.0.2** Enter

В окне будет выведена информация об обмене пакетами данных между компьютерами (Рис. 2.39).

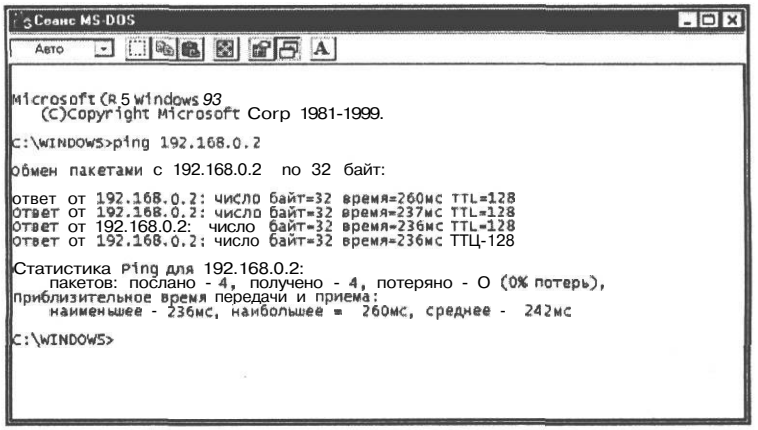



*Рис. 2.74. Окно* **Сеанс** ***MS-DOS*** *(MS-DOS Prompt) с информацией об обмене между компьютерами пакетами данных*

Во время обмена пакетами данных между компьютерами в окне **Сеанс MS-DOS** (MS-DOS Prompt) будет выводиться информация об отклике удаленного компьютера, числе переданных байтов и времени задержки. По окончании сеанса обмена будет выведена статистическая информация о количестве посланных, принятых и потерянных пакетов. Мы видим, что потерянных пакетов нет, т.е. качество связи хорошее.

➤ Закройте окно **Сеанс MS-DOS** (MS-DOS Prompt) на обоих компьютерах, нажав кнопку [×], расположенную в правой части заголовка окна.

Для организации сети из трех и более компьютеров с помощью USB-кабеля придется приобретать специальный хаб (концентратор), который является довольно дорогостоящим устройством. Еще одним недостатком сети на основе USB-кабеля является ограниченность ее применения только операционными системами семейства Windows, при переходе одного из компьютеров на другую операционную систему (Unix, FreeBSD, Linux и т.п.) вы рискуете остаться без сети.

## Локальная сеть на основе IEEE 1394 (FireWire)

Альтернативой связи через USB-шину является связь через шину IEEE 1394, или, как ее еще называют, FireWire («огненный провод»). Стандарт этой шины был разработан приблизительно в то же время, что и стандарт шины USB. Однако в отличие от стандарта USB стандарт IEEE 1394 сразу предполагал организацию передачи данных между двумя равноправными устройствами и скорость передачи данных до 400 Мбит/сек. Напомним, что такая скорость возможна только для шины USB-2.0, скорость передачи для шины USB-1.1 значительно ниже - 12 Мбит/сек. Операционные системы Windows Me/NT/2000/XP распознают контроллер (или адаптер) шины IEEE 1394 как дополнительный сетевой адаптер (или карту) (Рис. 2.75) и позволяют настроить сетевое соединение через него.

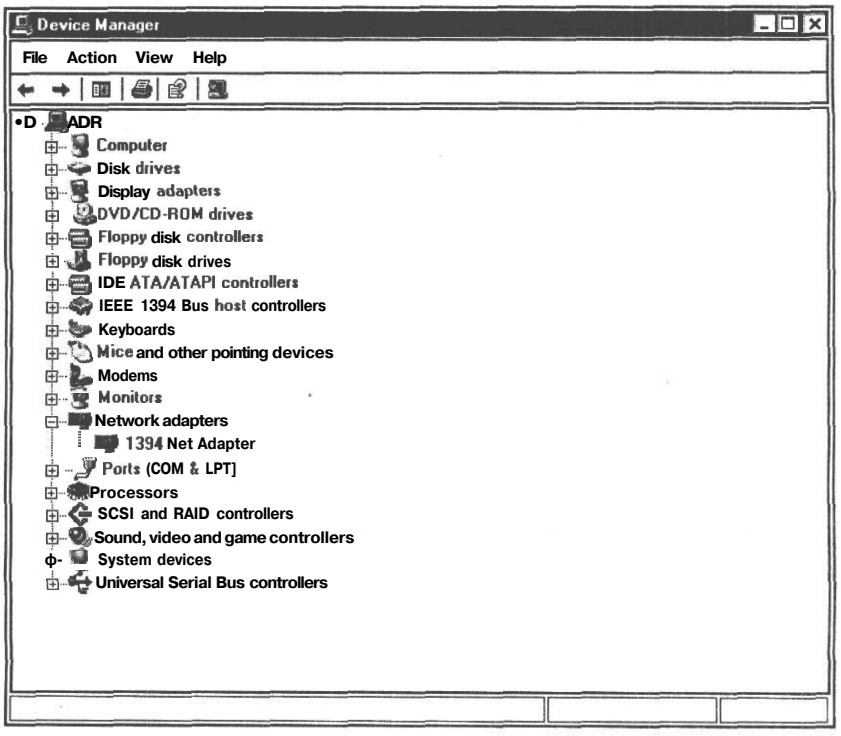



*Рис. 2.75 Диалог **Device** Manager (Диспетчер устройств), отображающий контроллер шины IEEE 1394 как сетевой адаптер*

Существует две основные модификации разъемов шины, показанные на Рис. 2.76, которые служат для организации связи по шине IEEE 1394.

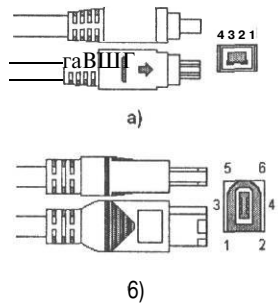



*Рис. 2.76 Разъемы шины IEEE1394*
*а) 4- контактный,*
*б) 6- контактный*

Адаптеры шины IEEE1394 обычно оснащаются 6-контактными розетками, а 4-контактные розетки, из-за своих малых габаритов, чаще всего устанавливаются на мобильных устройствах (цифровые фото- и видеокамеры, фотопринтеры, цифровые видеомагнитофоны, ноутбуки и т.п.). Назначение выводов 6-контактного разъема приведено в таблице.

| Контакт | Название сигнала | Описание |
|---|---|---|
| 1 | Power (Питание) | Нерегулируемый источник питания |
| 2 | Ground (общий) | Общий провод питания и экрана |
| 3 | TPB- | Витая пара B |
| 4 | TPB+ | Витая пара B |
| 5 | TPA- | Витая пара A |
| 6 | TPA+ | Витая пара A |
| Sheld | Экран | Экран кабеля |

Кабели IEEE 1394 выпускаются в разных модификациях в зависимости от их назначения. Существуют кабели, имеющие с каждой стороны по 4-контактной вилке, они используются для связи между двумя мобильными устройствами (например, двумя видеокамерами для перезаписи или видеокамерой и фотопринтером). Кабели, имеющие с одной стороны 4-х, а с другой стороны 6- контактную вилку, используются для подключения мобильных устройств к персональному компьютеру. Такие кабели обычно имеют дополнительное согласующее устройство. Кабели, имеющие с каждой стороны по 6-контактной вилке, можно использовать для организации сетевого соединения между двумя персональными компьютерами.

Для организации сетевого соединения между двумя компьютерами по шине IEEE1394 достаточно просто соединить выходные разъемы контроллеров кабелем и в операционной системе произвести настройку сетевого соединения, которая ничем не отличается от настройки сетевого соединения при использовании сетевых адаптеров Ethernet. Вам необходимо: проконтролировать наличие и при необходимости установить в диалоге

свойств сетевого соединения ШЕЕ 1394 необходимые протоколы (TCP/IP, IPX/SPX и др.) и сетевые службы (Клиент для сетей Microsoft или Netware, службу доступа к файлам и принтерам и т.п.), а также назначить IP-адрес для этого интерфейса. Все указанные шаги подробно описываются в следующей главе.

Многие материнские платы современных компьютеров имеют поддержку шины IEEE 1394, а наличие шины USB-2.0 уже стало стандартом, поэтому если у вас появится потребность в организации высокоскоростного сетевого соединения между двумя компьютерами или стационарным компьютером и ноутбуком, вам достаточно приобрести соответствующий кабель и настроить в операционной системе сетевое соединение. Единственным недостатком такого способа сетевого соединения компьютеров является небольшая длина соединительного кабеля, который в зависимости от исполнения может достигать 2,5 - 3 метра.

ГЛАВА 3.

# Создание локальной сети дома и в офисе

После завершения монтажа сетевого оборудования и кабельной системы необходимо на всех компьютерах локальной сети настроить программное обеспечение. Мы будем рассматривать построение сети на базе протокола TCP/IP, что позволит в дальнейшем легко подключить сеть к Интернету. Процедуры установки и настройки сетевого программного обеспечения несколько различаются в разных версиях операционной системы Windows, поэтому мы познакомимся с ними отдельно для Windows 98 и Windows 2000/XP.

## Динамический или статический IP-адрес?

Как уже отмечалось в первой главе, при построении локальной сети на основе протокола TCP/IP каждый компьютер получает уникальный IP-адрес, который может назначаться либо DHCP-сервером - специальной программой, установленной на одном из компьютеров сети, либо средствами Windows, либо вручную.

DHCP-сервер позволяет гибко раздавать IP-адреса компьютерам и закрепить за некоторыми компьютерами постоянные, статические IP-адреса. Встроенное средство Windows не имеет таких возможностей. Поэтому если в сети имеется DHCP-сервер, то средствами Windows лучше не пользоваться, установив в настройках сети операционной системы автоматическое (динамическое) назначение IP-адреса. Установка и настройка DHCP-сервера выходит за рамки этой книги.

Следует, однако, отметить, что при использовании для назначения IP-адреса DHCP-сервера или средств Windows загрузка компьютеров сети и операции назначения IP-адресов требует длительного времени, тем большего, чем больше сеть. Кроме того, компьютер с DHCP-сервером должен включаться первым.

Если же вручную назначить компьютерам сети статические (постоянные, не изменяющиеся) IP-адреса, то компьютеры будут загружаться быстрее и сразу же появляться в сетевом окружении. Для небольших сетей этот вариант является наиболее предпочтительным, и именно его мы будем рассматривать в данной главе.

## Настройка программного обеспечения в Windows 98

В Windows 98 настройка сетевого программного обеспечения включает:

- установку драйвера сетевой карты;
- установку сетевого протокола TCP/IP;
- назначение компьютеру статического IP-адреса;
- установку клиента сети Microsoft;

- задание имени компьютера и рабочей группы;
- обеспечение доступа к общим ресурсам.

Рассмотрим все эти операции по порядку.

## Установка драйвера сетевой карты

После установки сетевого оборудования и включения компьютера операционная система в процессе загрузки обычно автоматически определяет тип сетевой карты и подбирает соответствующий драйвер. Иногда приходится указывать диск и папку с драйвером самостоятельно.

Если Windows не смогла обнаружить сетевую карту, то следует установить ее драйвер вручную, выполнив последовательность действий, описанную ниже.

➤ Выберите команду меню Пуск ◆ Настройка ◆ Панель управления (Start ◆ Settings ◆ Control Panel). На экране появится окно Панель управления (Control Panel) (Рис. 3.1).

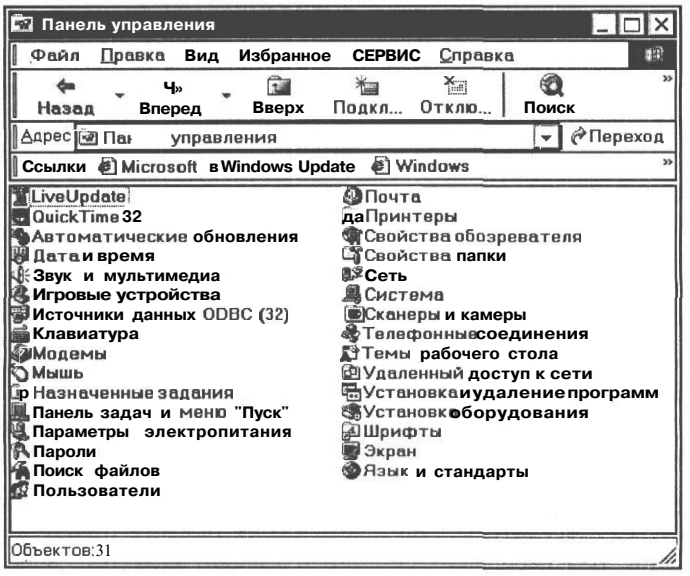


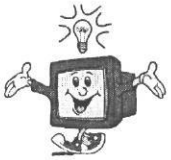

*Рис. 3.1. Окно **Панель управления** (Control Panel)*

> Дважды щелкните мышью на значке Установка оборудования (Add New Hardware). На экране появится первый диалог Мастера Установка оборудования (Hardware Installation Wizard) (Рис. 3.2).

Напомним, что Мастером называется программа, которая с помощью последовательности диалогов позволяет выполнить определенную задачу.

Первый диалог Мастера играет чисто информационную роль, поэтому прочитайте его и щелкните мышью на кнопке Далее (Next). Появится следующий диалог Мастера, информирующий о необходимости провести поиск новых подключенных устройств, поддерживающих стандарт самонастраивающегося оборудования - Plug and Play (Подключи и работай) (Рис. 3.3).

*Стандарт Plug and Play (Подключи и работай) поддерживают сетевые карты, подключающиеся к компьютеру через любые шины, кроме* ***ISA,*** *например PCI и USB.*



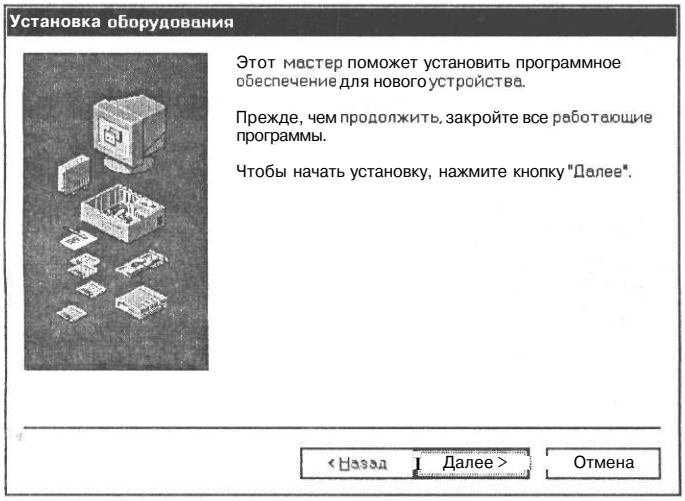



*Рис. 3.2. Первый диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard)*

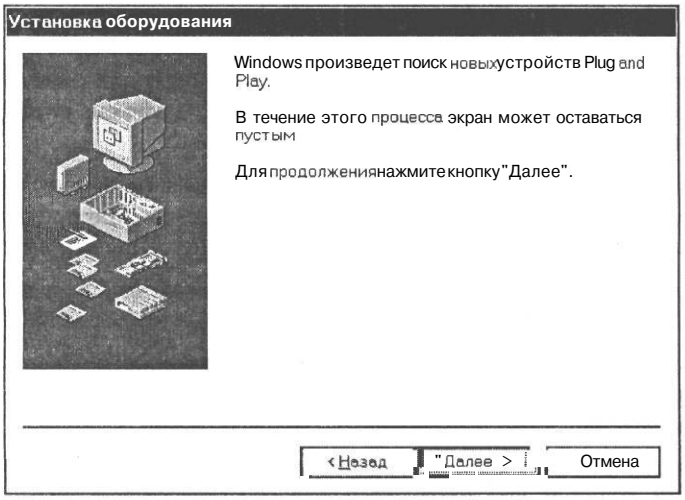
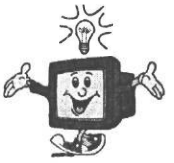



*Рис. 3.3. Второй диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard)*

*Желательно, чтобы в этот момент были выгружены из памяти компьютера все ненужные программы, особенно те, которые взаимодействуют с периферийным оборудованием.*



> Нажмите кнопку **Далее** (Next), чтобы инициировать процесс поиска новых подключенных устройств Plug and Play (Подключи и работай), о чем Мастер будет информировать с помощью линейного индикатора (Рис. 3.4).

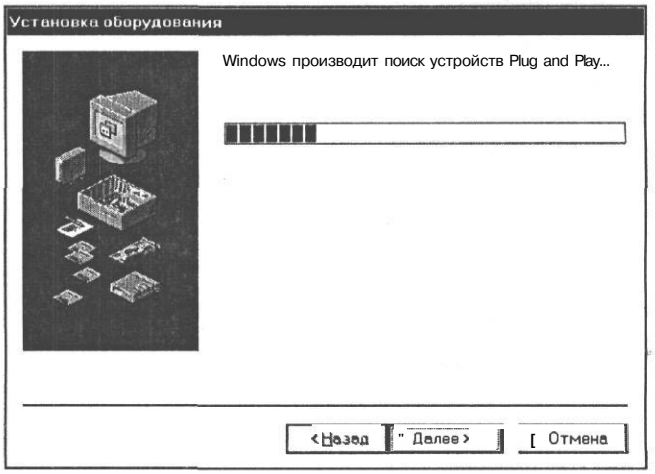


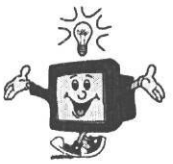

*Рис. 3.4. Третий диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard). Поиск новых устройств.*

Когда поиск завершится, Мастер отобразит список нового найденного оборудования. В данном случае таким устройством будет сетевая карта, название которой должно присутствовать в списке (Рис. 3.5).

- Если Мастер **Установка оборудования** (Hardware Installation Wizard) обнаружил и правильно определил тип сетевой карты, установленной на компьютере, щелкните мышью на кнопке **Далее** (Next), чтобы перейти к заключительному диалогу Мастера (Рис. 3.6).
- Нажмите кнопку **Готово** (Finish) для завершения работы Мастера **Установка оборудования** (Hardware Installation Wizard).

Иначе придется поступить, если в списке найденных устройств (Рис. 3.5) не окажется сетевой карты или ее тип определен неправильно.

*Впрочем, многие сетевые карты совместимы с популярной моделью* ***NE2000,*** *которая уже много лет служит стандартом де-факто. Поэтому стандартный драйвер* ***NE2000-Compatible*** *(NE2000-совместимая) часто подходит для большого количества типов сетевых карт. Хотя, конечно, лучше всего использовать «родной» драйвер карты.*



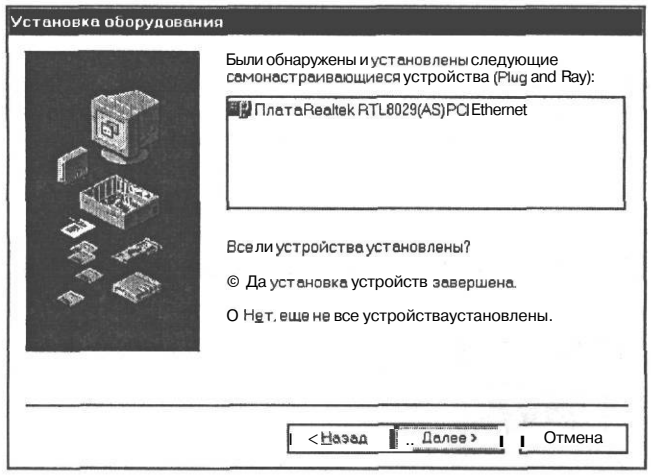



*Рис. 3.5. Четвертый диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard)*

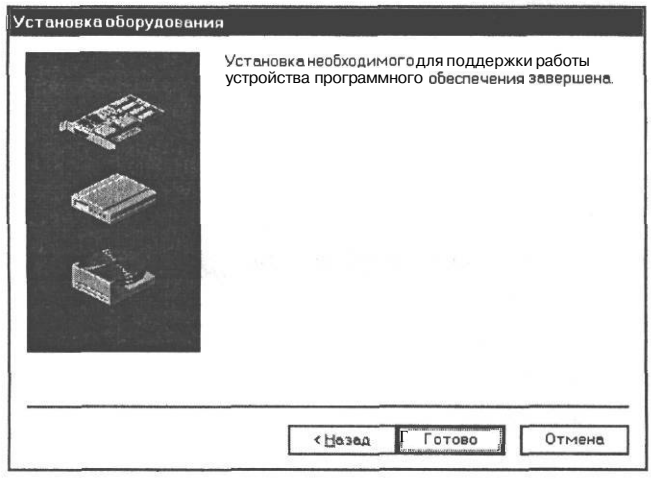
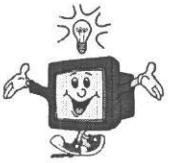



*Рис. 3.6. Заключительный диалог Мастера Установка оборудования (Hardware Installation Wizard)*

- Если сетевая карта не обнаружена автоматически, то в четвертом диалоге Мастера Установка оборудования (Hardware Installation Wizard) (Рис. 3.5) установите переключатель **Нет,** еще не все устройства установлены (No, not yet all devices are installed) и нажмите кнопку Далее (Next). Появится диалог мастера, где производится выбор режима поиска новых подключенных устройств, которые не поддерживают стандарт Plug and Play (Подключи и работай) (Рис. 3.7).
- Оставьте установленным переключатель Да (рекомендуется) (Yes (recommended)), чтобы подтвердить выбор режима автоматического поиска устройств, а затем нажмите кнопку Далее (Next). Появится диалог с сообщением о начале поиска (Рис. 3.8).

*Напоминаем, что в этот момент желательно выгрузить из памяти компьютера все ненужные программы, особенно те, которые взаимодействуют с периферийным оборудованием.*



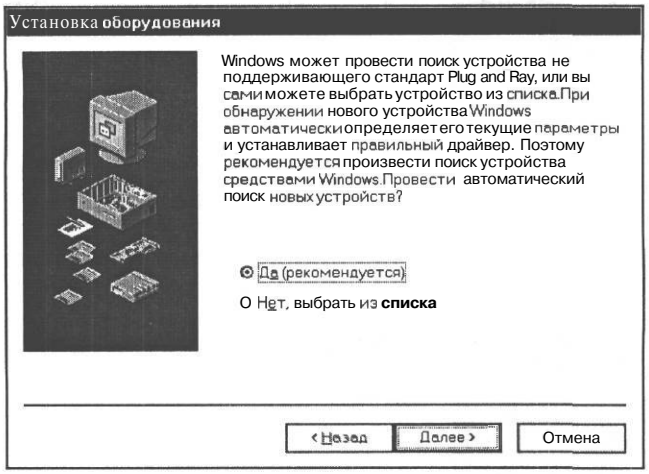



*Рис. 3.7. Диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard) для выбора режима поиска*

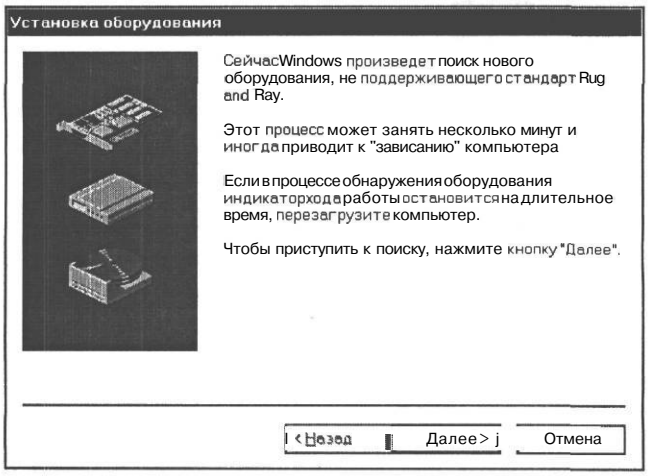



*Рис. 3.8. Диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard) с сообщением о начале поиска новых устройств, не поддерживающих стандарт Plug and Play (Подключи и работай)*

- Щелкните мышью на кнопке Далее (Next). Начнется поиск оборудования, не поддерживающего стандарт Plug and Play (Подключи и работай) (Рис. 3.9).
- Когда поиск завершится, нажмите кнопку **Готово** (Finish) в заключительном диалоге Мастера **Установка оборудования** (Hardware Installation Wizard) (Рис. 3.6).

В случае если мастер не сможет найти новые подключенные устройства, он предложит установить драйвер самостоятельно (Рис. 3.10).

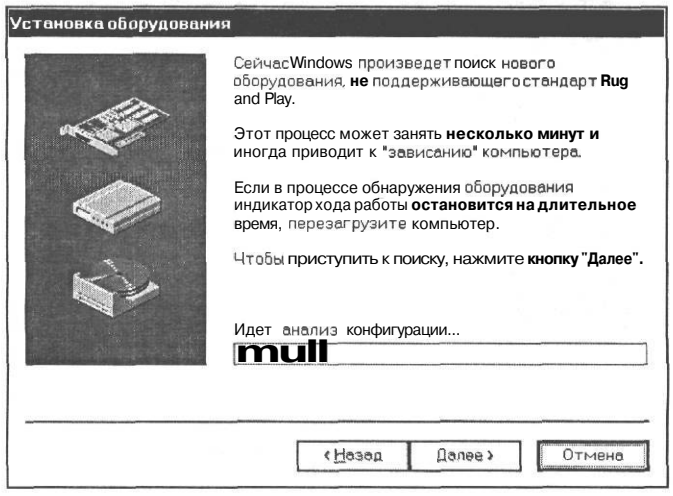



*Рис. 3.9. Диалог Мастера **Установка оборудования** (Hardware Installation Wizard), отображающий процесс поиска новых устройств, не поддерживающих стандарт Plug and Play (Подключи и работай)*

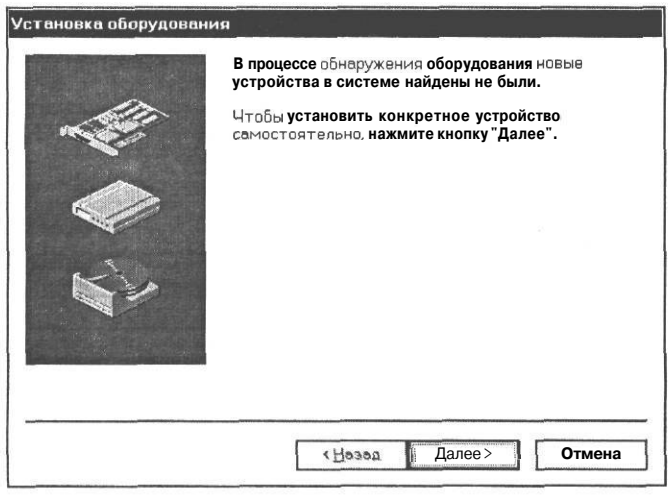



*Рис. 3.10. Диалог Мастера **Установка оборудования** (Hardware Installation Wizard) с сообщением о том, что новые устройства не найдены*

> Нажмите кнопку **Далее** (Next), чтобы в следующем диалоге **Установка оборудования** (Hardware Installation Wizard) (Рис. 3.11) произвести выбор типа устанавливаемого устройства.

> В поле списка выберите элемент **Сетевые платы** (Network Adapters) и щелкните мышью на кнопке **Далее** (Next). Появится диалог для выбора нужной модели устройства (Рис. 3.12).

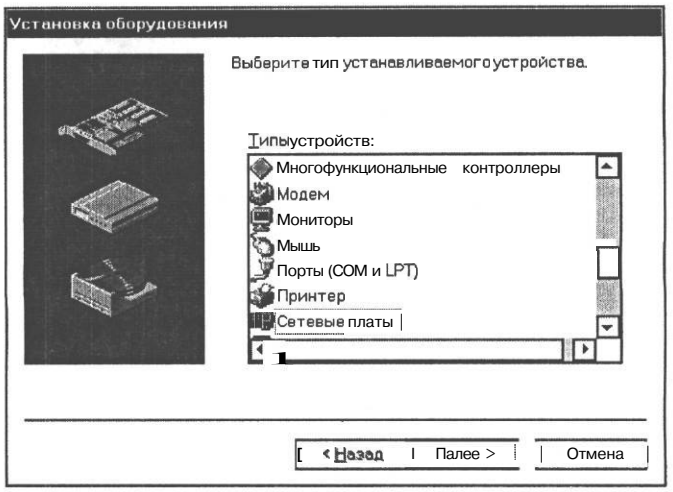



*Рис. 3.11. Диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard) для выбора типа устанавливаемого устройства*

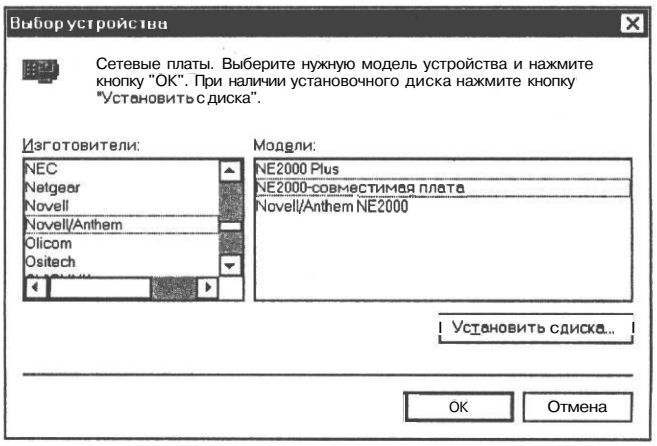
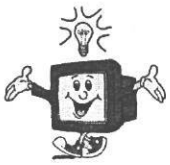



*Рис. 3.12. Диалог Мастера* ***Установка оборудования*** *(Hardware Installation Wizard) для выбора модели устройства*

➤ В списке **Изготовители** (Manufacturers) выберите название фирмы-производителя сетевой платы, затем **в** списке **Модели** (Models) выделите название конкретной модели сетевой платы.

***В** случае **отсутствия нужной модели и дискеты с драйвером, можно попробовать выбрать изготовителя Novell/Anthem и модель NE2000-совместимая плата (NE2000-Compatible Adapter).***



Если же у вас имеется дискета с драйвером сетевой карты, то лучше всего установить именно драйвер производителя.

➤ Для этого нажмите кнопку **Установить с диска** (Have Disk). Откроется диалог **Установка с диска** (Have Disk) (Рис. 3.13).

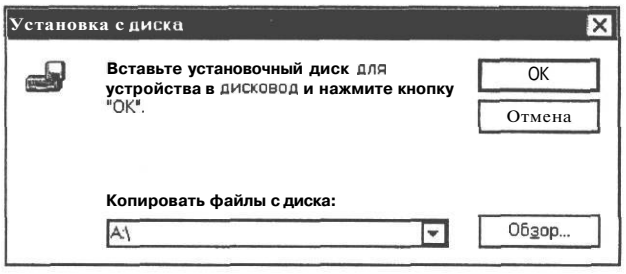



*Рис. 3.13. Диалог **Установка с диска** (Have Disk)*

> Вставьте установочную дискету или компакт-диск в дисковод и щелкните мышью на кнопке **Обзор** (Browse), чтобы найти файл драйвера сетевой карты. На экране появится диалог **Открытие файла** (Open File) (Рис. 3.14).

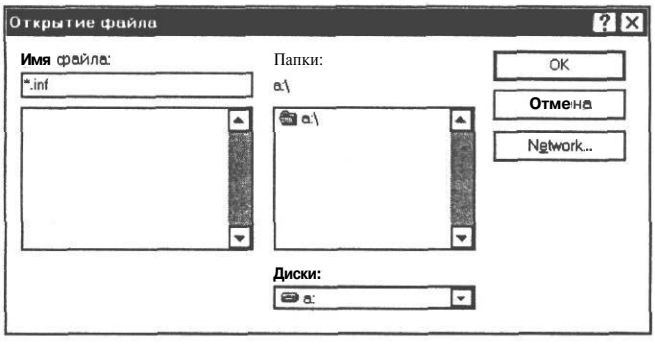
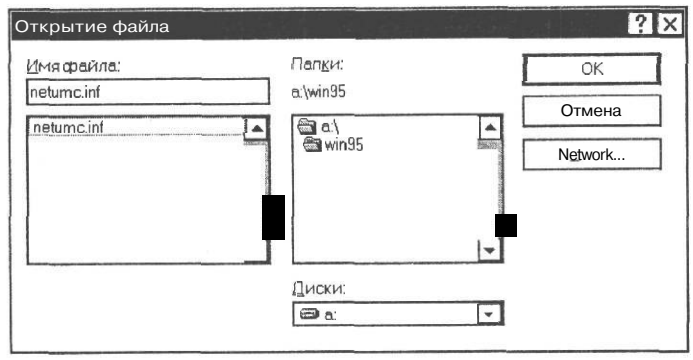



*Рис. 3.14. Диалог **Открытие файла** (Open File)*

> В списке **Папки** (Folders) найдите нужную, в которой находится драйвер сетевой карты, и откройте ее двойным щелчком мыши. После этого в поле Имя **файла** (File Name) должно появиться имя файла, имеющее расширение **INF** (Рис. 3.15).




*Рис, 3.15. Диалог **Открытие файла** (Open File) с найденным файлом*

> Нажмите кнопку OK для закрытия диалога **Открытие файла** (Open File). После этого в поле **Копировать файлы с диска** (Copy Files From Disk) диалога **Установка с диска** (Have Disk) появится путь к папке с драйвером (Рис. 3.16).

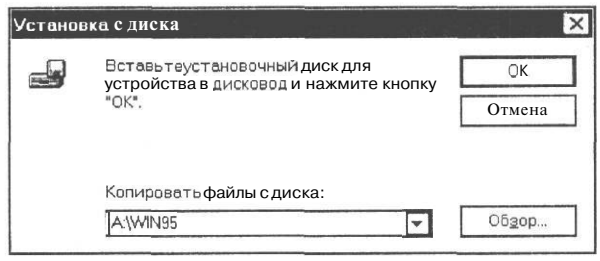



*Рис. 3.16. В диалоге **Установка с диска** (Have Disk) указан путь к папке с драйвером*

> Нажмите кнопку **OK** еще раз. Диалог **Установка с диска** (Have Disk) закроется, и появится новый диалог - **Выбор устройства** (Select Device) (Рис. 3.17).

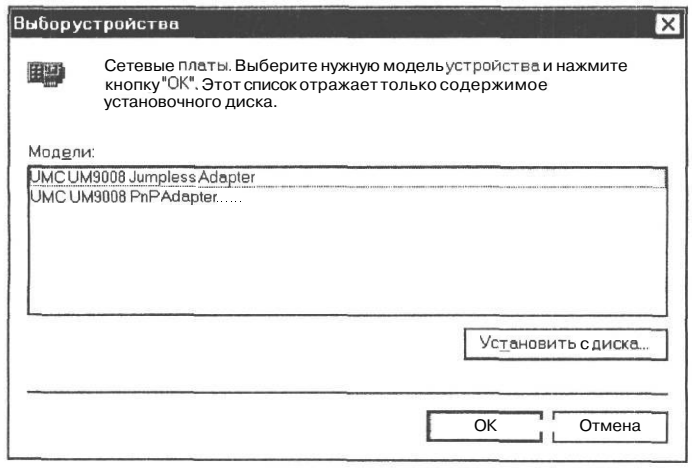



*Рис. 3.17. Диалог **Выбор устройства** (Select Device)*

➤ В списке Модели (Models) данного диалога выберите нужную модель сетевой карты и щелкните мышью на кнопке **OK.** Начнется процесс копирования файлов, после чего появится диалог **Изменение параметров системы** (System parameters was changed) (Рис. 3.18).

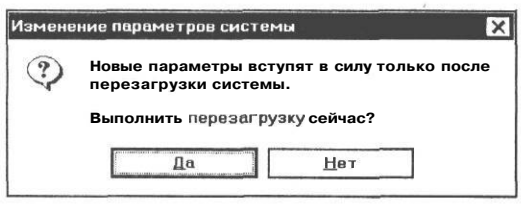



*Рис. 3.18. Диалог **Изменение параметров системы** (System parameters was changed)*

> Нажмите кнопку **OK**, подтверждая перезагрузку системы, чтобы сделанные изменения вступили в силу.

После перезагрузки драйвер сетевой карты будет установлен.

## Установка протокола TCP/IP

Теперь необходимо установить сетевой протокол TCP/IP.

> Выберите команду главного меню **Пуск** ◆ **Настройка** ◆ **Панель управления** (Start ◆ Settings ◆ Control Panel). На экране появится **Панель управления** (Control Panel) (Рис. 3.1).

> Дважды щелкните мышью на значке **Сеть** (Network). Появится диалог **Сеть** (Network) с открытой вкладкой **Конфигурация** (Configuration) (Рис. 3.19).

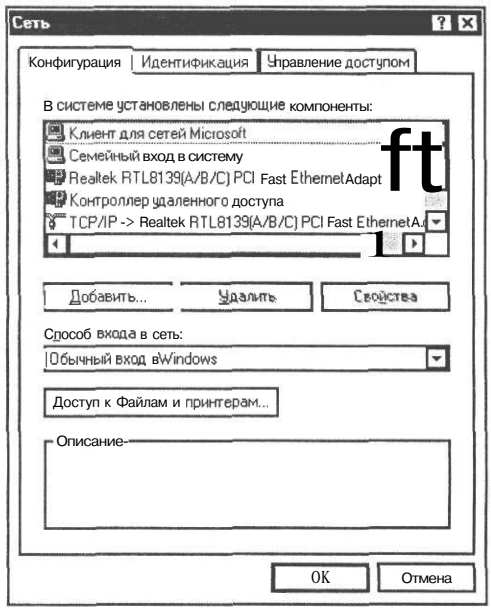
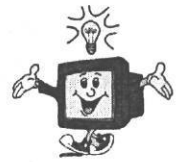



*Рис. 3.19. Вкладка **Конфигурация** (Configuration) диалога **Сеть** (Network)*

*Открыть диалог **Сеть** (Network) можно также, щелкнув правой кнопкой мыши на значке **Мое сетевое окружение** (My Network Neighbored), находящемся на **Рабочем столе** (Desktop), и выбрав в контекстном меню команду **Свойства** (Properties).*



Если в списке сетевых компонентов уже имеется протокол **TCP/IP,** связанный с сетевой картой, то раздел, описывающий его установку, можно пропустить. В противном случае необходимо сначала установить данный протокол.

> На вкладке **Конфигурация** (Configuration) диалога **Сеть** (Network) нажмите кнопку **Добавить** (Add). На экране появится диалог **Выбор типа компонента** (Select Component Type) (Рис. 3.20).

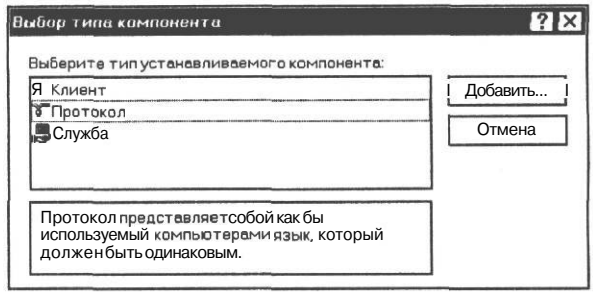



*Рис. 3.20. Диалог **Выбор типа компонента** (Select Component Type)*

> В списке устанавливаемых компонентов щелчком мыши выберите элемент **Протокол** (Protocol) и нажмите кнопку **Добавить** (Add). Откроется диалог **Выбор: Сетевой протокол** (Select: Network Protocol) (Рис. 3.21).

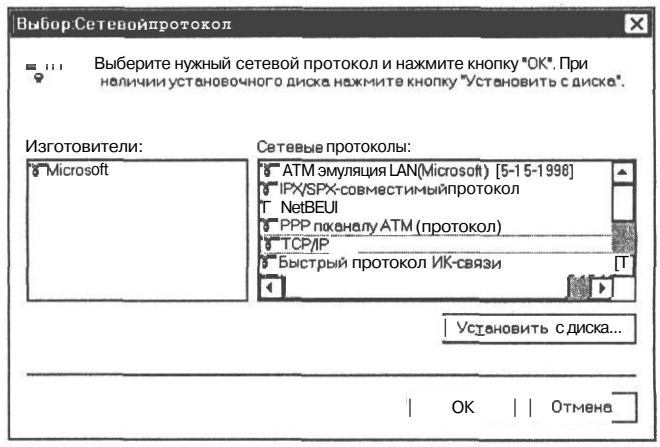


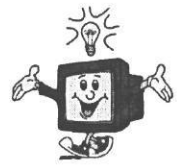

*Рис. 3.21. Диалог **Выбор: Сетевой протокол** (Select: Network Protocol)*

> Выберите в списке **Изготовители** (Manufacturers) фирму **Microsoft,** затем в списке **Сетевые протоколы** (Network Protocols) - протокол **TCP/IP,** после чего нажмите

кнопку OK для подтверждения вашего выбора и закрытия диалога **Выбор: Сетевой протокол** (Select: Network Protocol).

На вкладке **Конфигурация** (Configuration) диалога **Сеть** (Network) (Рис. 3.19) появится новый компонент - протокол **TCP/IP**.

*Аналогичным образом устанавливаются и другие сетевые протоколы, например, **IPX/SPX и NetBEUI.** Протокол **IPX/SPX** часто используется сетевыми играми, поэтому, если вы предполагаете запускать сетевые игры, его тоже следует добавить в систему.*



## Настройка протокола TCP/IP

После того, как протокол TCP/IP установлен, необходимо настроить его параметры, назначив каждому компьютеру сети, а точнее, каждому сетевому адаптеру статический IP-адрес вида 192.168.0.*. Благодаря такому адресу компьютеры смогут находить друг друга в сети.

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Настройка * Панель управления** (Settings ◆ Control Panel). На экране появится окно **Панель управления** (Control Panel) (Рис. 3.1).
- В окне **Панель управления** (Control Panel) дважды щелкните мышью на значке **Сеть** (Network). На экране появится диалог **Сеть** (Network) с открытой вкладкой **Конфигурация** (Configuration) (Рис. 3.19).

В поле списка в верхней части этого диалога перечислены все установленные сетевые адаптеры, протоколы, клиенты и службы, необходимые для обеспечения связи в сети. Заметьте, что в списке присутствуют два протокола TCP/IP: один связан с сетевым адаптером, а другой - с контроллером удаленного доступа.

- Щелчком мыши выделите в поле списка протокол **TCPJIP,** связанный с вашим сетевым адаптером. Соответствующая строка может иметь вид, например, **TCPJIP -> Realtek RTL8139(A/B/C) PCI Fast Ethernet Adapter.**
- Нажмите кнопку **Свойства** (Properties). Появится информационный диалог (Рис. 3.22) с рекомендацией указать параметры TCP/IP отдельно для каждого соединения удаленного доступа.

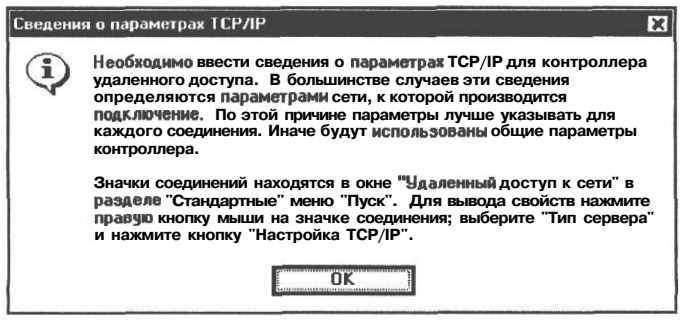



*Рис. 3.22. Информационный диалог с рекомендацией об указании параметров TCP/IP*

➤ Закройте этот диалог нажатием кнопки OK. Появится диалог Свойства: TCP/IP (TCPЯP Properties) с открытой вкладкой IP-адрес (IP address) (Рис. 3.23).

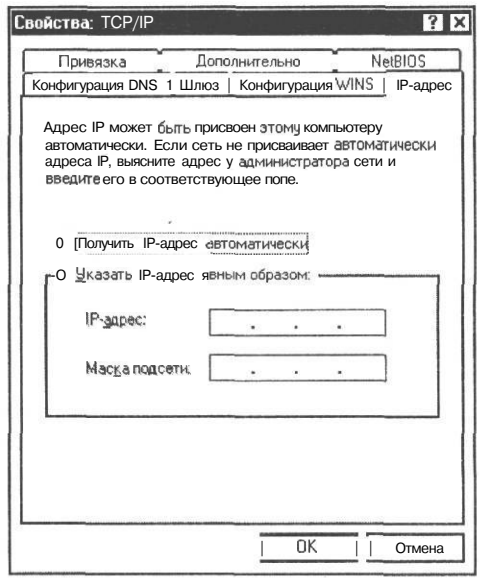



*Рис. 3.23. Вкладка* ***IP-адрес*** *(IP address) диалога Свойства: TCP/IP (TCP/IP Properties)*

> Установите переключатель Указать IP-адрес явным образом (Use the following IP address).

➤ В поле ввода IP-адрес (IP address) введите IP-адрес вида 192.168.0.*, который вы хотите присвоить данному компьютеру, например 192.168.0.1 или 192.168.0.2, т.е. вместо символа * следует указать целое число от 1 до 255. Число 0 (ноль) использовать нельзя, так как адрес **192.168.0.0** присваивается сети.

> В поле ввода Маска подсети (Subnet mask) введите маску 255.255.255.0.

➤ Закройте диалог Свойства: TCP/IP (TCP/IP Properties) нажатием кнопки OK. Вы возвратитесь к диалогу Сеть (Network).

> Нажмите кнопку OK, чтобы закрыть и этот диалог. Возможно, появится диалог с предложением вставить установочный диск Windows 98.

> Вставьте требуемый диск. После установки необходимых компонентов операционная система предложит перезагрузить компьютер (Рис. 3.18).

После перезагрузки указанные параметры протокола TCP/IP вступят в силу.

Описанным способом следует назначить статические IP-адреса всем компьютерам локальной сети. Но каждый компьютер должен иметь уникальный адрес вида 192.168.0.*, например, 192.168.0.1, 192.168.0.2 и т.д. Другими словами, в локальной сети не должно быть одинаковых статических адресов.

## Установка Клиента сетей Microsoft

Далее необходимо установить **Клиент сетей Microsoft** (Microsoft Network Client). Этот раздел можно пропустить, если данный компонент уже установлен и присутствует в списке на вкладке **Конфигурация** (Configuration) диалога **Сеть** (Network) (Рис. 3.19).

- Откройте диалог Сеть (Network), дважды щелкнув мышью в окне **Панель управления** (Control Panel) (Рис. 3.1).
- На вкладке **Конфигурация** (Configuration) диалога **Сеть** (Network) (Рис. 3.19) нажмите кнопку **Добавить** (Add). Откроется диалог **Выбор типа компонента** (Select Component Type) (Рис. 3.20).
- В списке устанавливаемых компонентов выберите элемент **Клиент** (Client) и нажмите кнопку **Добавить** (Add). Откроется диалог **Выбор: Клиент сети** (Select: Network Client) (Рис. 3.24).

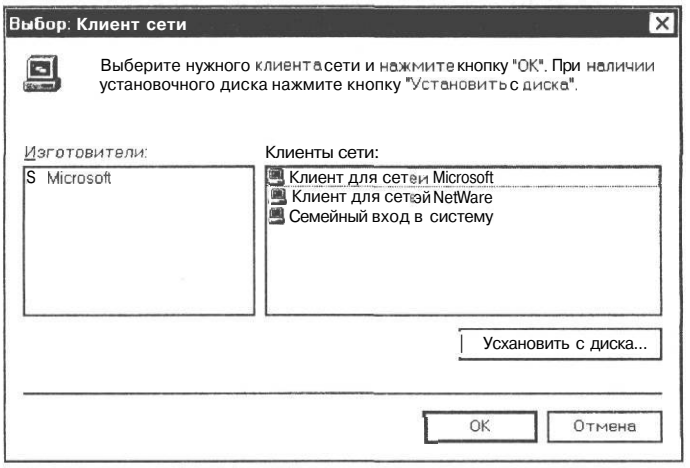



*Рис. 3.24. Диалог **Выбор: Клиент сети** (Select: Network Client)*

- В списке **Изготовители** (Manufacturers) выберите фирму **Microsoft,** затем в списке **Клиенты сети** (Network Clients) - элемент **Клиент для сетей Microsoft** (Microsoft Network Client).
- Нажмите кнопку **ОК** для подтверждения выбора. Диалог **Выбор: Клиент сети** (Select: Network Client) закроется. Появится диалог **Изменение параметров системы** (System parameters was changed) с предложением перезагрузить компьютер (Рис. 3.18).
- Нажмите кнопку Да (Yes).

После перезагрузки системы на вкладке **Конфигурация** (Configuration) диалога **Сеть** (Network) (Рис. 3.19) добавится новый компонент - **Клиент для сетей Microsoft** (Microsoft Network Client).

## Задание имени компьютера и рабочей группы

Наша следующая задача - задать сетевое имя компьютера и имя рабочей группы.

- Откройте диалог Сеть (Network), дважды щелкнув мышью на значке Сеть (Network) в окне Панель управления (Control Panel).
- Щелкните мышью на ярлыке Идентификация (Identification) для перехода на соответствующую вкладку (Рис. 3.25).
- В поле ввода Имя компьютера (Computer Name) введите название данного компьютера в качестве клиента сети Microsoft, например Manager.
- В поле Рабочая группа (Workgroup) введите имя рабочей группы сети Microsoft, в которой работает данный компьютер, например **MSHOME**. Это имя рабочей группы должно быть одинаковым для всех компьютеров локальной сети.

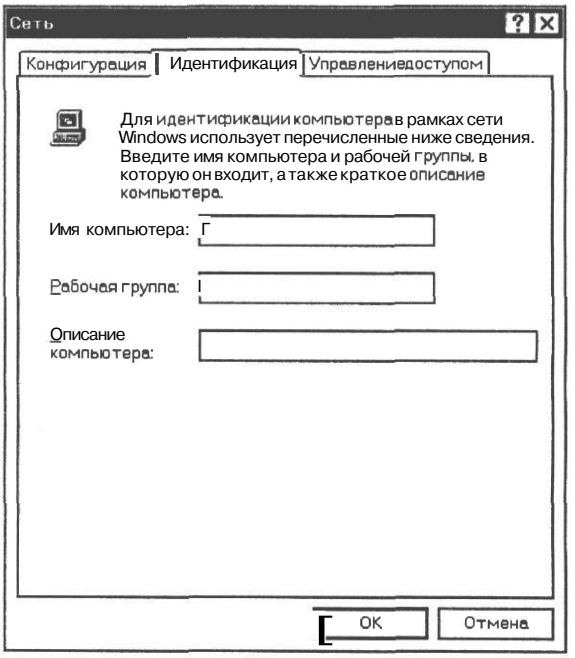



*Рис. 3.25. Вкладка Идентификация (Identification) диалога Сеть (Network),*

- Содержимое поля Описание компьютера (Description of Computer) заполните любой информацией, поясняющей основную роль этого компьютера, например Секретарь.
- Щелкните мышью на кнопке OK для закрытия диалога Сеть (Network). Система выполнит указанные изменения в настройках, а затем выдаст диалог Изменение параметров системы (System parameters was changed) (Рис. 3.18).

➤ В диалоге **Изменение параметров системы** (System parameters was changed) нажмите кнопку Да (Yes), подтверждая перезагрузку системы.

После перезагрузки сделанные изменения вступят в силу.

# Обеспечение доступа к общим ресурсам

Компьютеры локальной сети могут предоставлять свои ресурсы в совместное использование. Такими ресурсами могут быть:

- диски, папки и файлы;
- принтер;
- модем;
- факс и др.

Наиболее часто устанавливается общий доступ к дискам, папкам, отдельным файлам и принтерам.

## Установка службы доступа к файлам и принтерам

Чтобы сделать общими файлы и принтеры, необходимо установить службу доступа к файлам и принтерам, выполнив следующие действия.

> Щелкните правой кнопкой мыши на значке **Мое сетевое окружение** (My Network Neighborhood), находящемся на **Рабочем столе** (Desktop). На экране появится контекстное меню.

> Выберите в контекстном меню команду **Свойства** (Properties). Появится диалог **Сеть** (Network) с открытой вкладкой **Конфигурация** (Configuration) (Рис. 3.19).

> Щелкните мышью на кнопке **Доступ к файлам и принтерам** (Files and Printers Sharing). На экране появится диалог **Доступ к файлам и принтерам** (Files and Printers Sharing) (Рис. 3.26).

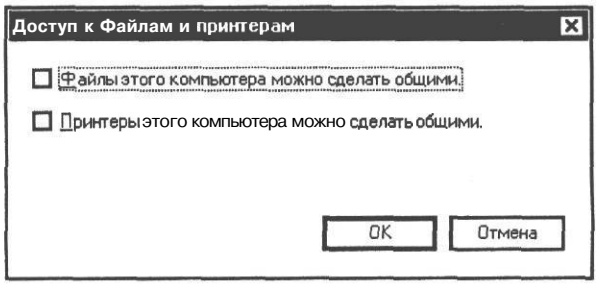



*Рис. 3.26. Диалог Доступ* ***к файлам и принтерам*** *(Files and Printers Sharing)*

> Установите оба флажка, чтобы разрешить возможность предоставления совместного доступа к файлам и принтерам этого компьютера.

Обратите внимание на то, что установка этих флажков только делает возможным общий доступ. О том, как фактически выделить в общее пользование диск, папку и принтер, будет рассказано далее.

- Нажмите кнопку **ОК** диалога **Доступ к файлам и принтерам** (Files and Printers Sharing), чтобы закрыть его.
- Затем щелкните мышью на кнопке **ОК** для закрытия диалога **Сеть** (Network). На экране появится диалог **Изменение параметров системы** (System parameters was changed) (Рис. 3.18).
- Нажмите кнопку **Да,** подтверждая перезагрузку системы.

После перезагрузки сделанные изменения вступят в силу.

## Как сделать диск или папку общими

Часто бывает необходимо предоставить в общее пользование диск или папку компьютера. Это можно сделать следующим образом.

- Щелкните правой кнопкой мыши на значке **Мой компьютер** (My Computer), находящемся на **Рабочем столе** (Desktop), и выберите команду контекстного меню **Проводник** (Windows Explorer). Запустится программа Проводник (Windows Explorer) (Рис. 3.27).
- В левой части окна выберите какой-нибудь диск или папку, например, **Мои документы** (My Documents), которую хотите предоставить в общее пользование, и щелкните на ней правой кнопкой мыши. На экране появится контекстное меню.

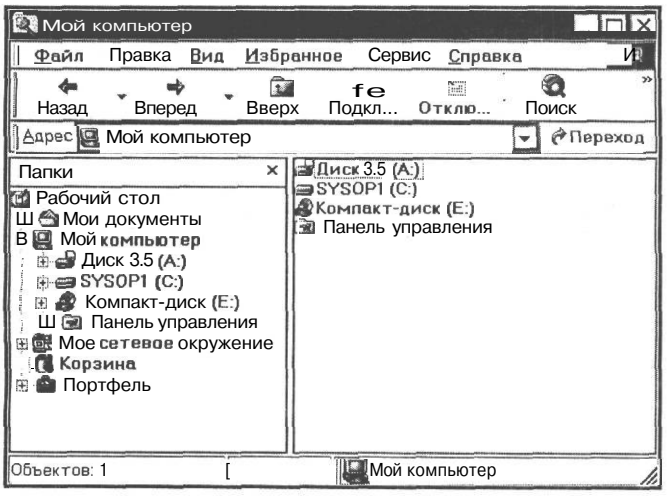



*Рис. 3.27. Окно программы Проводник (Windows Explorer) с открытой папкой **Мой компьютер** (My Computer)*

- В контекстном меню выберите команду **Свойства** (Properties). Появится диалог **Свойства: Мои документы** (Properties: My Documents) с открытой вкладкой **Общие** (General) (Рис. 3.28).

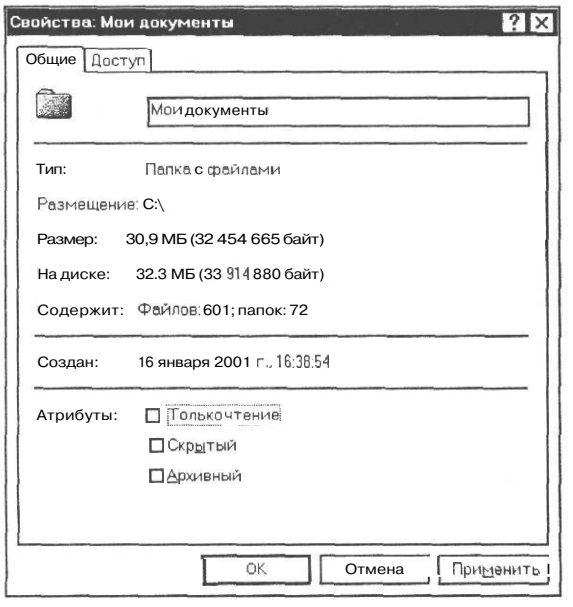



*Рис. 3.28. Вкладка **Общие (General)** диалога **Свойства: Мои документы** (Properties: My Documents)*

> Щелчком мыши на ярлыке **Доступ** (Sharing) перейдите на соответствующую вкладку (Рис. 3.29).

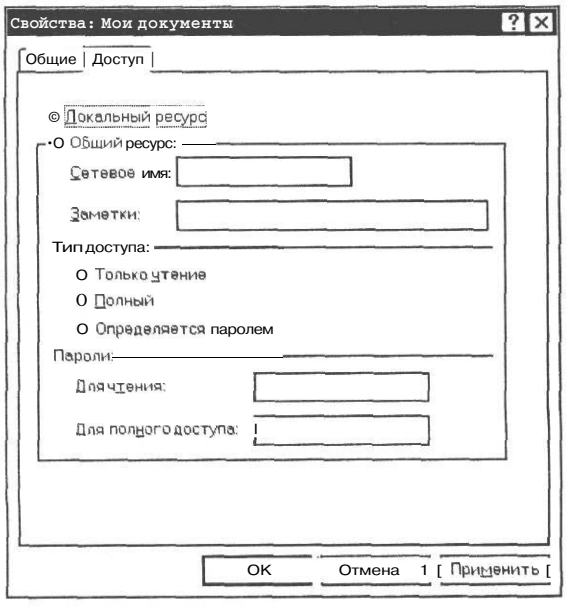
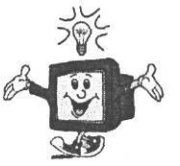


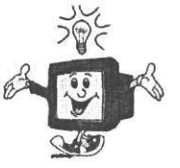

*Рис. 3.29. **Вкладка Доступ** (Sharing) диалога **Свойства: Мои документы** (Properties: My Documents)*

*Диалог **Свойства: Мои документы** (Properties: My Documents), открытый на вкладке **Доступ** (Sharing), можно также вызвать на экран командой контекстного меню Доступ (Sharing).*



➤ Чтобы разрешить общий доступ к выбранному ресурсу, установите переключатель **Общий ресурс** (Shared Resource). В поле ввода **Сетевое имя** (Network Name) появится автоматически сгенерированное имя сетевого ресурса, которое можно изменить по своему усмотрению.

*Если в конце имени сетевого ресурса добавить символ '$', данный ресурс становится невидимым в окне **Мое сетевое окружение** (My Network Neighborhood), однако доступным для тех, кто знает его название.*



Поле **Заметки** (Comments) можно оставить пустым или заполнить какой-то поясняющей информацией.

Переключатель **Тип доступа** (Access Type) можно установить в одно из трех положений:

**Только чтение** (Read Only) - предоставляется возможность только просмотра файлов в данной папке;

**Полный** (Full Access) - разрешается не только чтение, но и запись;

**Определяется паролем** (Defined By Password) - зависит от введенного пароля при попытке доступа к ресурсу.

В группе элементов управления **Пароли** (Passwords) находятся два поля ввода, в которых можно определить пароли для подключения к данному сетевому ресурсу: **Для чтения** (For Read) и **Для полного доступа** (For Full Access).

➤ Нажмите кнопку **Применить** (Apply).

➤ Щелкните мышью на кнопке **OK.** Диалог **Свойства: Мои документы** (Properties: My Documents) закроется.

Значок папки, ставшей общедоступной, изменится - появится рука, придерживающая его снизу .

## Как сделать общим принтер

Чтобы сделать общим принтер, выполните следующие действия.

➤ Выберите команду меню **Пуск • Настройка * Принтеры** (Start ◆ Settings ◆ Printers). На экране появится папка **Принтеры** (Printers) (Рис. 3.30).

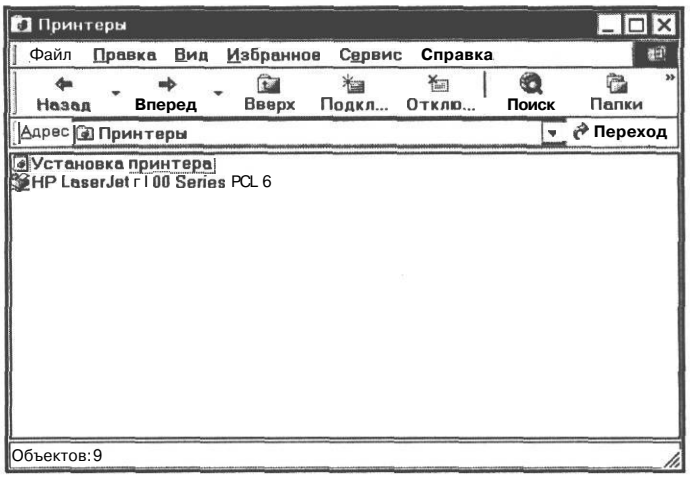



*Рис. 3.30. Папка **Принтеры** (Printers)*

> Щелкните правой кнопкой мыши на значке локального принтера, который вы хотите сделать общим. В нашем примере это **HP LaserJet 2100 Series PCL 6.** На экране появится контекстное меню.

> Выберите в контекстном меню команду **Доступ** (Sharing), Откроется диалог **Свойства: HP LaserJet 2100 Series PCL 6** (Properties: HP LaserJet 2100 Series PCL 6) (Рис. 3.31).

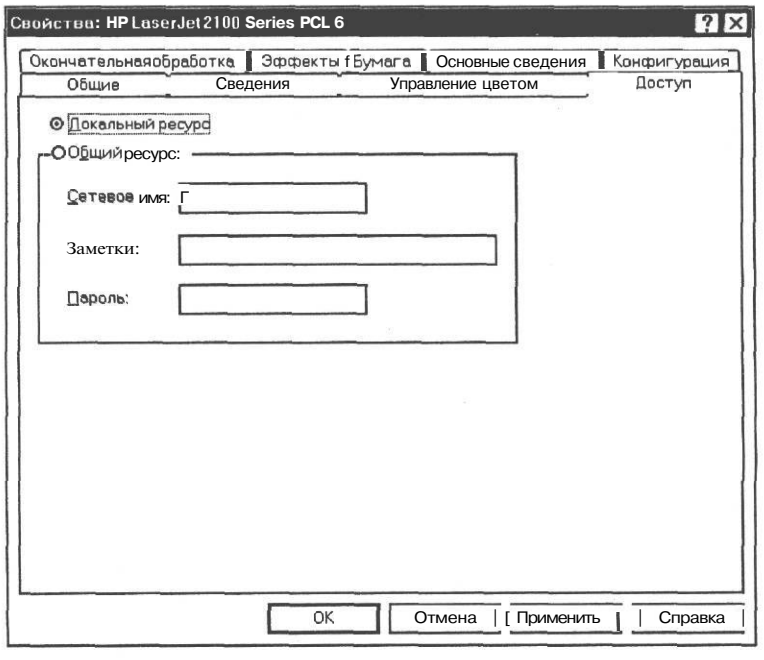



***Рис. 3.31. Вкладка Доступ (Sharing) диалога Свойства: HP LaserJet 2100 Series PCL 6*** *(Properties: HP LaserJet 2100 Series PCL 6)*

> Установите переключатель **Общий ресурс** (Shared Resource). В поле ввода **Сетевое имя** (Network Name) появится автоматически сгенерированное имя сетевого ресурса, которое можно изменить по своему усмотрению.

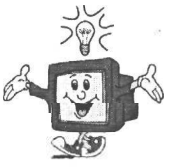
Поле Заметки (Comments) можно оставить пустым или заполнить какой-то поясняющей информацией.

Можно воспользоваться необязательным полем **Пароль** (Password) для ограничения доступа к данному сетевому принтеру.

➤ Закройте диалог **Свойства: HP LaserJet 2100 Series PCL 6** (Properties: HP LaserJet 2100 Series PCL 6), нажав кнопку **OK.**

Значок принтера, ставший общедоступным, изменится - появится рука, придерживающая его снизу.

*Аналогичным образом нужно настроить программное обеспечение остальных компьютеров. Для простой домашней сети выделять отдельный компьютер на роль сервера не требуется, достаточно создать одноранговую сеть.*



## Проверка работы локальной сети

После того как все компоненты локальной сети установлены и настроены, необходимо проверить ее работоспособность. Но сначала следует перезагрузить компьютер.

➤ Выберите в главном меню Windows команду **Завершение работы** (Shut Down). На экране появится диалог **Завершение работы Windows** (Shut Down Windows) (Рис. 3.32).

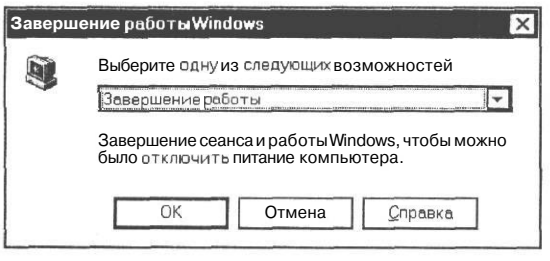



*Рис. 3.32. Диалог **Завершение работы Windows** (Shut Down Windows)*

> В открывающемся списке выберите **Перезагрузка** (Restart) и нажмите кнопку **OK.**

После завершения процесса перезагрузки должен появиться диалог **Ввод сетевого пароля** (Login to Network) (Рис. 3.33).

➤ В поле ввода **Имя пользователя** (User Name) введите имя, идентифицирующее пользователя Windows. Чтобы не было путаницы, будет лучше, если имя пользователя совпадает с содержимым поля **Имя компьютера** (Computer Name) вкладки **Идентификация** (Identification) диалога **Сеть** (Network), например, **LANGamer1**.

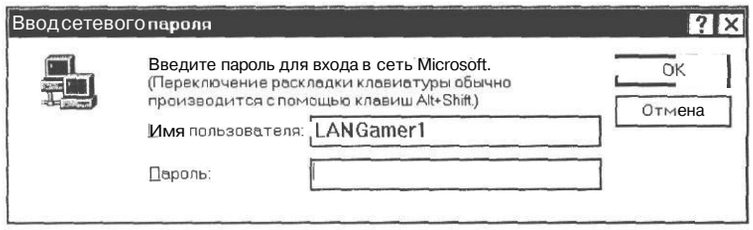
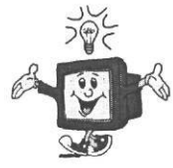



*Рис. 3.33. Диалог* ***Ввод сетевого пароля*** *(Login to Network)*

> Поле **Пароль** (Password) для заполнения не обязательно, но можно придумать данному пользователю любой пароль.

*В одноранговой сети Microsoft, где все рабочие станции имеют равные права, любой новый пользователь может войти в сеть без прохождения процедуры создания учетной записи.*



## Проверка связи между компьютерами

Теперь приступим к проверке работоспособности протокола TCP/IP и связи между компьютерами локальной сети. Для этого воспользуемся командой **ping,** которая посылает по указанному адресу эхо-запросы в виде 32-байтных пакетов и фиксирует время их возврата.

➤ Нажмите кнопку Пуск (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Программы * Сеанс MS-DOS** (Program ◆ MS-DOS Prompt). На экране появится окно **Сеанс MS-DOS** (MS-DOS Prompt) (Рис. 3.34).

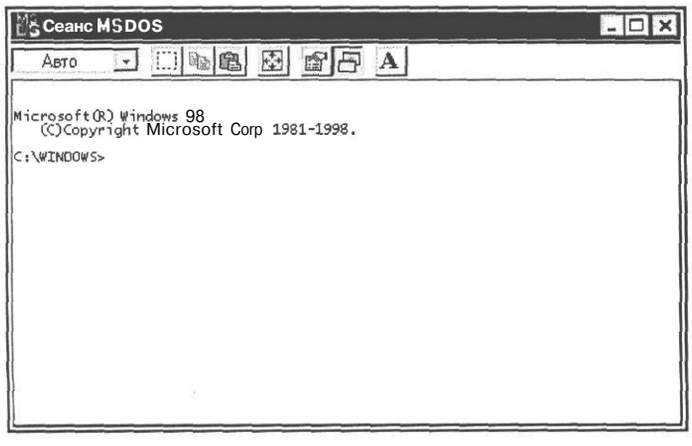



*Рис. 3.34. Окно* ***Сеанс*** *MS-DOS (MS-DOS Prompt)*

➤ В окне Сеанс MS-DOS (MS-DOS Prompt) введите команду ping, в качестве аргумента которой укажите статический IP-адрес компьютера, связь с которым хотите проверить, например ping **192.168.0.1**. Вместо IP-адреса можно указать сетевое имя компьютера, например ping LANGamer2. Этот компьютер должен быть включен и настроен для работы в сети.

> Нажмите клавишу Enter. Будет выполнен обмен четырьмя пакетами по 32 байта с указанным компьютером. После этого в окне Сеанс MS-DOS (MS-DOS Prompt) отобразится информация о времени, потребовавшемся на передачу и прием пакетов (Рис. 3.74).

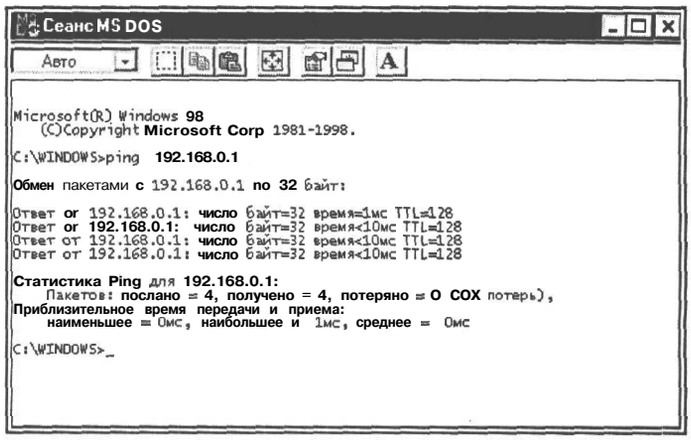



*Рис. 3.35. Окно Сеанс MS-DOS (MS-DOS Prompt) с результатом работы команды ping*

Если количество полученных и отправленных пакетов совпадает и потери составляют 0%, то все аппаратные и программные компоненты сети - сетевые карты, кабели, концентраторы, протоколы и т.д. - работают, настроены правильно и связь с указанным компьютером установлена.

Если же после такой команды появились сообщения Время ожидания запроса истекло (Timeout) и потери пакетов составляют 100%, то связь с указанным компьютером отсутствует либо указан неправильный IP-адрес или имя компьютера. В таком случае следует проверить:

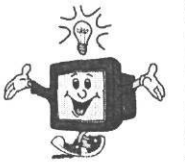
- правильность IP-адреса или имени компьютера;
- правильность монтажа кабеля, разъемов, сетевых карт и концентраторов;
- отсутствие разрывов и коротких замыканий;
- установку драйверов, сетевых протоколов и клиентов;
- связь между другими компьютерами сети.

Проверку связи между компьютерами командой ping следует выполнить на каждом компьютере локальной сети. Только в случае получения положительных результатов вы сможете быть уверены, что сеть работает.

## Сетевое окружение

После того, как вы убедились, что связь в сети установлена, можно увидеть компьютеры в сетевом окружении.

*Обратите внимание на то, что компьютеры в сетевом окружении появятся не сразу, а с задержкой в несколько минут, которые требуются на опознание клиентов сети и построение списков рабочих групп и имен компьютеров. Если IP-адрес назначается динамически, то задержка будет еще больше.*



➤ Найдите на рабочем столе значок **Мое сетевое окружение** (My Network Neighborhood) и дважды щелкните на нем мышью, чтобы открыть соответствующее окно (Рис. 3.36).

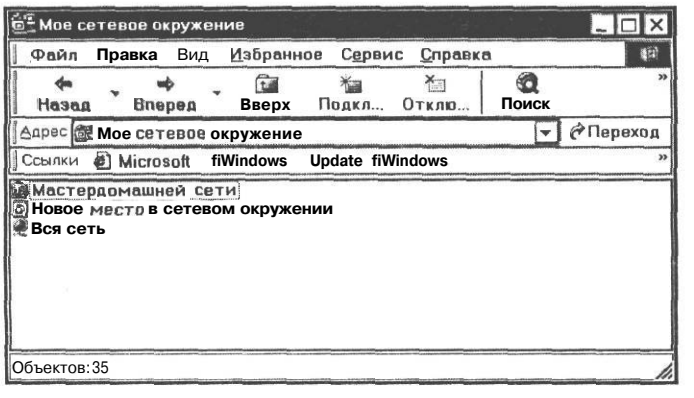



*Рис. 3.36. Окно **Мое сетевое окружение** (My Network Neighborhood)*

> В окне **Мое сетевое окружение** (My Network Neighborhood) дважды щелкните мышью на значке **Вся сеть** (Entire Network), показав ее содержимое (Рис. 3.37).

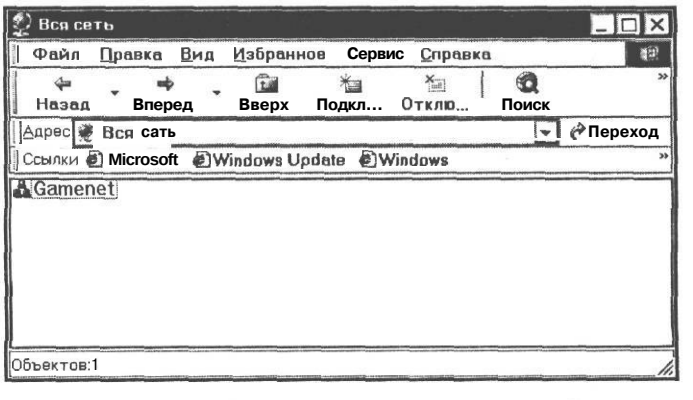



*Рис. 3.37. Окно **Вся сеть** (Entire Network)*

Вся сеть будет состоять из единственной рабочей группы. Имя рабочей группы для всех компьютеров сети должно быть одинаковым.

➤ Двойным щелчком мыши на значке рабочей группы откройте ее окно (Рис. 3.38).

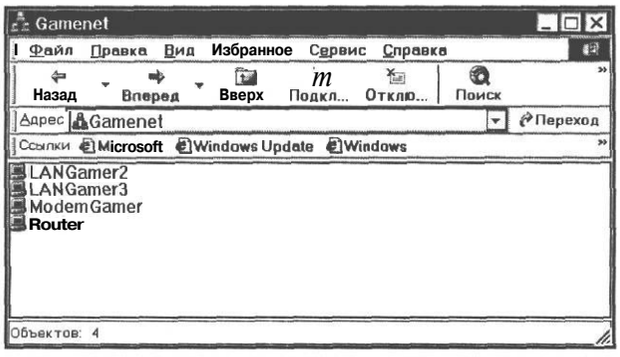
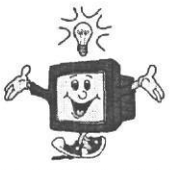



*Рис. 3.38. Окно рабочей группы*

В данном окне вы увидите компьютеры рабочей группы - клиентов сети Microsoft, с которыми установлена связь.

*Если один или несколько компьютеров подключились, когда окно* ***Мое сетевое окружение*** *(My Network Neighborhood) было уже открыто, следует обновить его содержимое, нажав клавишу* F5.



## Поиск компьютеров в сети

Чтобы окончательно убедиться в доступности (или недоступности) определенного клиента сети Microsoft, попробуйте найти его имя в сетевом окружении.

> Щелкните правой кнопкой мыши на значке **Мое сетевое окружение** (My Network Neighborhood) на **Рабочем столе** (Desktop). На экране появится контекстное меню.

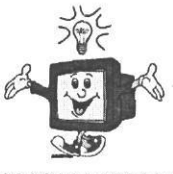
➤ Выберите команду контекстного меню **Поиск компьютеров** (Search Computers). Откроется окно **Результаты поиска - компьютеры** (Search Results - Computers) (Рис. 3.39).

➤ В поле ввода **Имя компьютера** (Computer Name), находящемся в левой части окна, введите имя какого-либо клиента сети Microsoft.

➤ Нажмите кнопку **Найти** (Search) для запуска процесса поиска. В случае успешного поиска имя компьютера появится в правой части окна.

На Рис. 3.40 вы видите, что найден компьютер с именем **LANGamer2,** поиск которого и осуществлялся.

*Для осуществления поиска сразу нескольких компьютеров в поле* ***Имя компьютера*** *(Computer Name) можно использовать подстановочные символы: ? и * Например, условию поиска* ***LANGamer**** *соответствуют все клиенты сети Microsoft, имена которых начинаются с* ***LANGamer.***



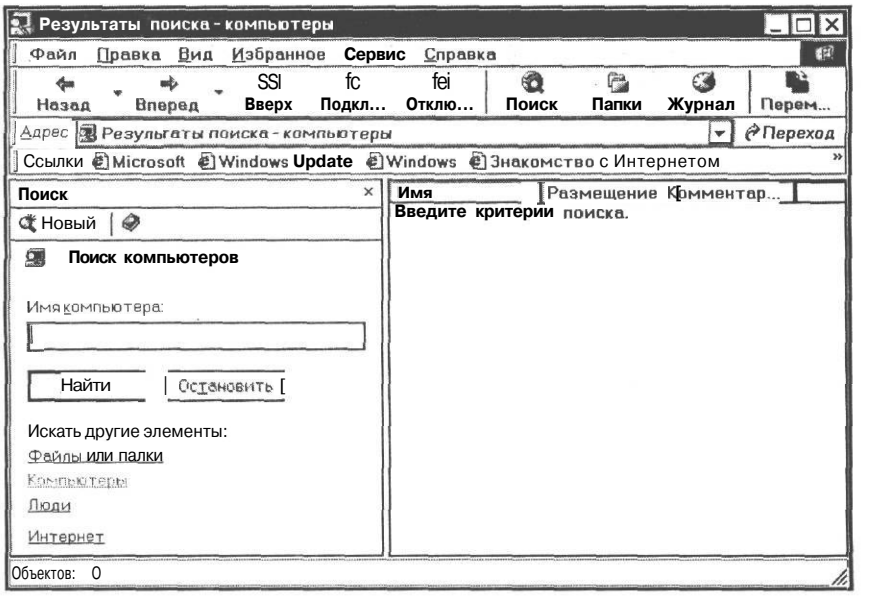



*Рис. 3.39. Окно* ***Результаты поиска - компьютеры*** *(Search Results — Computers)*

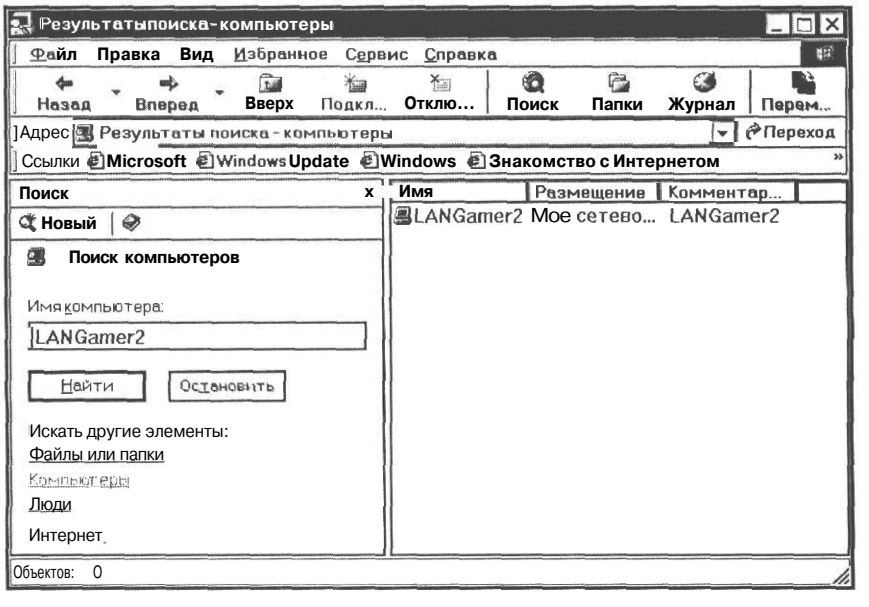



*Рис. 3.40. Окно* ***Результаты поиска - компьютеры*** *(Search Results — Computers). Поиск выполнен успешно*

Отрицательные результаты поиска будут свидетельствовать о том, что искомые компьютеры не подключены к сети.

# Настройка программного обеспечения в Windows 2000/XP

В отличие от Windows 98, в Windows 2000/XP сетевой протокол TCP/IP устанавливается автоматически вместе с операционной системой. Компонент «Клиент для сетей Microsoft», который позволяет компьютеру обращаться к ресурсам сети Microsoft, также устанавливается и включается автоматически. Поэтому в Windows 2000/XP после завершения монтажа сетевого оборудования и кабелей необходимо:

- установить драйвер сетевой карты;
- настроить в свойствах протокола TCP/IP статическое назначение IP-адреса и включить режим NetBIOS через TCP/IP;
- задать имена компьютера и рабочей группы;
- определить пользователей и группы;
- обеспечить доступ к общим ресурсам.

Рассмотрим указанные настройки для операционной системы Windows XP. В Windows 2000 они выполняются аналогично.

## Установка драйвера сетевой карты

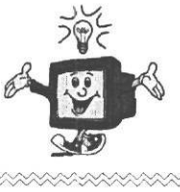
После установки сетевого оборудования и включения компьютера операционная система Windows 2000/XP должна автоматически определить тип сетевой карты и подобрать для нее драйвер. Иногда приходится указывать диск и папку с драйвером самостоятельно.

Если Windows XP не смогла обнаружить сетевую карту, следует установить драйвер карты вручную следующим образом.

➤ Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Панель управления** (Control Panel) в Windows XP или команду **Настройка** ◆ **Панель управления** (Settings ◆ Control Panel) в Windows 2000. На экране появится окно **Панель управления** (Control Panel).

➤ Дважды щелкните мышью на значке **Система** (System). На экране появится диалог **Свойства системы** (System Properties) с открытой вкладкой **Общие** (General) (Рис. 3.41).

*Диалог **Свойства системы** (System Properties) можно также вызвать, не обращаясь к **Панели управления** (Control Panel), а просто нажав комбинацию клавиш* ⊞ + Pause.



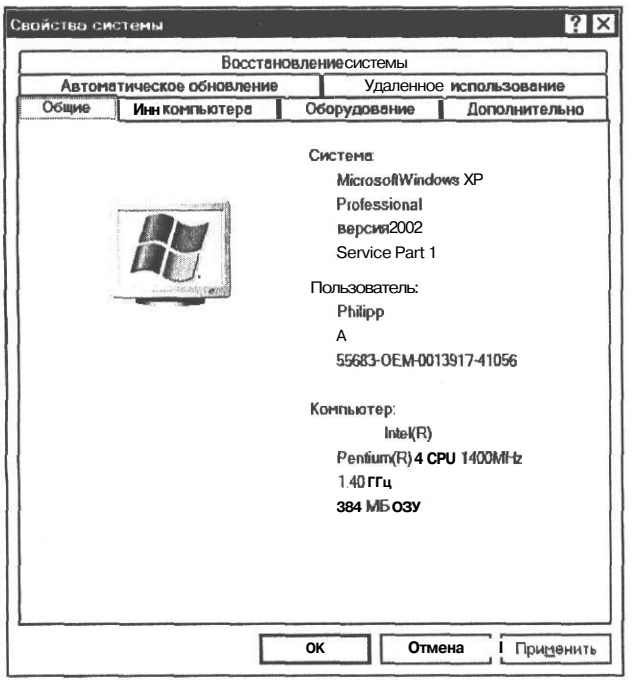



*Рис. 3.41, Вкладка* **Общие** *(General) диалога* ***Свойства системы*** *(System Properties)*

> В диалоге **Свойства системы** (System Properties) перейдите на вкладку **Оборудование** (Hardware) и нажмите кнопку **Установка оборудования** (Add Hardware Wizard). На экране появится первый диалог **Мастер установки оборудования** (Add Hardware Wizard) (Рис. 3.42) с информацией об его использовании.

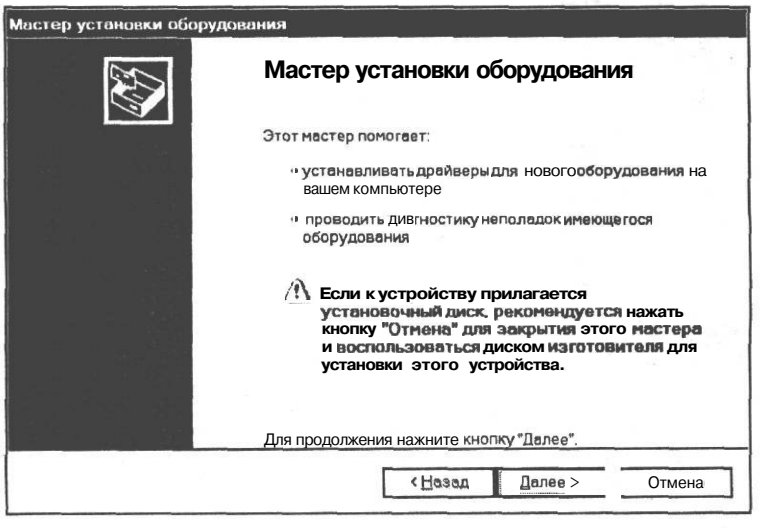



*Рис. 3.42. Первый диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard)*

➤ Нажмите кнопку **Далее** (Next), чтобы перейти к следующему диалогу Мастера, в котором осуществляется поиск новых устройств (Рис. 3.43).

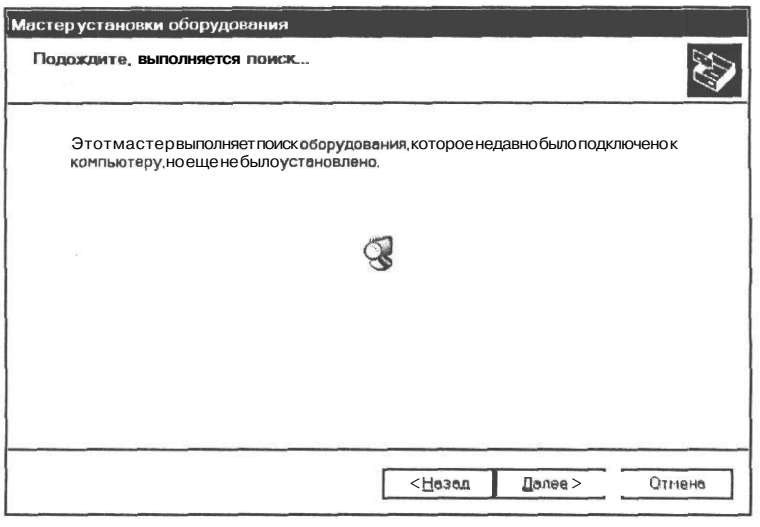



*Рис. 3.43. Диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard), в котором осуществляется поиск новых устройств*

Когда поиск завершится, мастер отобразит список нового найденного оборудования. В данном случае таким устройством будет сетевая карта, название которой должно присутствовать в списке (Рис. 3.44).

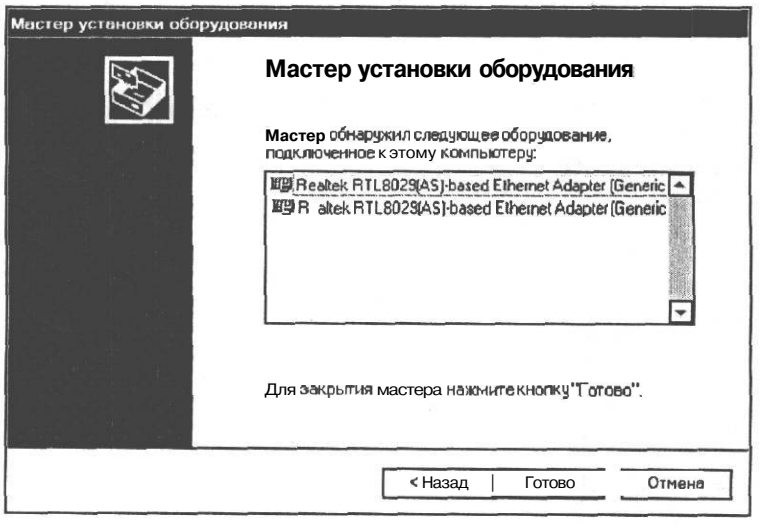
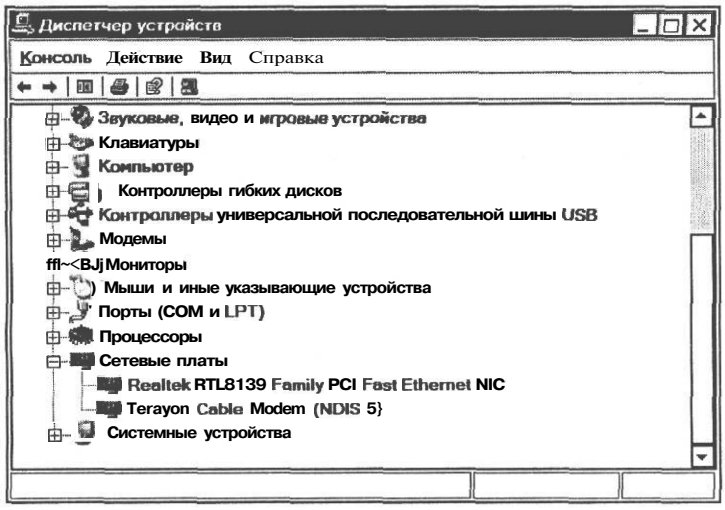



*Рис. 3.44. Диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard) со списком найденных новых устройств*

> Нажмите кнопку **Готово** (Finish), чтобы завершить работу мастера.

➤ Чтобы убедиться в том, что сетевая карта установлена, на вкладке **Оборудование** (Hardware) диалога **Свойства системы** (System Properties) нажмите кнопку **Диспетчер устройств** (Device Manager). На экране появится окно **Диспетчер устройств** (Device Manager) (Рис. 3.45).




PMC. 3.45. *Окно Диспетчер устройств (Device Manager)*

В окне Диспетчер устройств (Device Manager) перечислены все устройства, установленные в вашей системе. Имя устройства можно посмотреть, щелкнув на значке а, расположенном слева от названия типа устройства. Например, имя сетевой карты можно узнать, развернув компонент Сетевые платы (Network adapters).

➤ Закройте окно Device Manager (Диспетчер устройств), нажав кнопку ☒ в заголовке окна.

Как мы уже упоминали, многие сетевые карты совместимы с популярной моделью NE2000, которая уже много лет служит стандартом де-факто. Поэтому стандартный драйвер NE2000-CompatibIe (NE2000-совместимая) часто подходит для большого количества типов сетевых карт. Хотя, конечно, лучше всего использовать «родной» драйвер карты.

## Настройка протокола TCP/IP и других свойств сетевого соединения

После установки сетевой карты необходимо каждому компьютеру сети назначить статический IP-адрес, который позволит идентифицировать компьютер в сети, и определить некоторые свойства протокола TCP/IP. Эта операция выполняется в диалоге **Свойства: Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP) Properties).

➤ Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Панель управления** (Control Panel) в Windows XP или команду **Настройка ◆ Панель управления** (Settings ◆ Control Panel) в Windows 2000. На экране появится окно **Панель управления** (Control Panel).

> В окне Панель управления (Control Panel) дважды щелкните мышью на значке Сетевые подключения (Network Connections). Откроется окно Сетевые подключения (Network Connections). В Windows 2000 - значок и окно имеют название Сетевые и удаленные подключения (Network and Dial-up Connections).

> Щелкните правой кнопкой мыши на значке Подключение по локальной сети (Local Area Connection) и в появившемся контекстном меню выберите команду Свойства (Properties). На экране появится диалог Подключение по локальной сети - свойства (Local Area Connection Properties) с открытой вкладкой Общие (General) (Рис. 3.46).

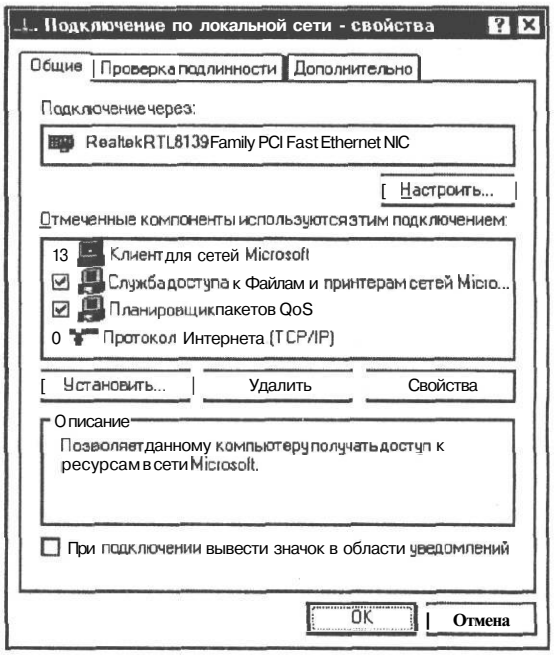



*Рис. 3.46. Вкладка Общие диалога Подключение по локальной сети - свойства (Local Area Connection Properties)*

В поле списка Отмеченные компоненты используются этим подключением (This connection uses the following items) этого диалога перечислены все установленные сетевые протоколы, клиенты и службы, используемые для связи в сети. По умолчанию все компоненты задействованы. На это указывают установленные для каждого из них флажки.

Если в этом списке отсутствуют компоненты Клиент для сетей Microsoft (Client for Microsoft Network) и Служба доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks), то их следует установить, нажав кнопку Установить (Install).

По умолчанию операционная система Window устанавливает сервис QoS (Quality of Service - Качество обслуживания) для обеспечения гарантированной полосы пропускания, например, для программ ввода-вывода потокового аудио и видео. Но в большинстве случаев этот сервис не нужен и даже вреден, так как уменьшает скорость соединения с Интернетом. В локальной сети он вообще бесполезен, и его следует удалить.

➤ На вкладке Общие (General) диалога Подключение по локальной сети - свойства (Local Area Connection Properties) (Рис. 3.46) щелчком мыши выделите компонент Планировщик пакетов QoS (QoS Packet Scheduler) и нажмите кнопку Удалить (Uninstall). На экране появится диалог с запросом подтверждения удаления (Рис. 3.47).

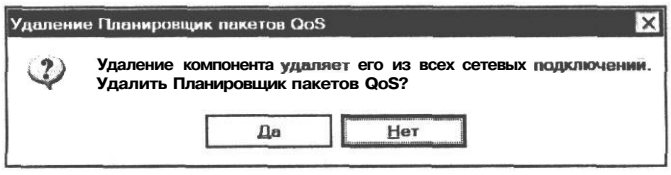



*Рис. 3.47. Запрос подтверждения удаления сервиса QoS*

> Нажмите кнопку Да (Yes), подтверждая необходимость удаления. Сервис QoS будет удален, и его имя исчезнет из списка Отмеченные компоненты используются этим подключением (This connection uses the following items).

Повторим еще раз, что удаление сервиса QoS не повлияет на работу сети.

Теперь зададим статический IP-адрес компьютера.

➤ Щелчком мыши выделите в этом диалоге компонент Протокол Интернета (TCP/IP) (Internet Protocol (TCP/IP)) и нажмите кнопку Свойства (Properties). Откроется диалог Свойства: Протокол Интернета (ТСРЛР) (Internet Protocol (TCP/IP) Properties) (Рис. 3.48).

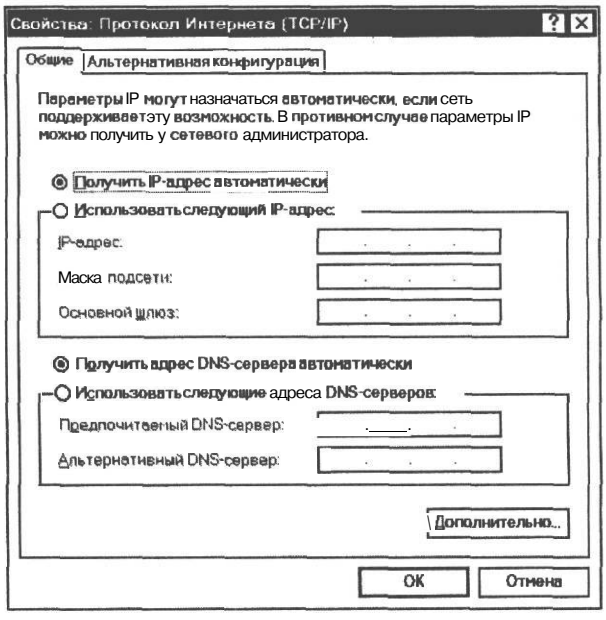



*Рис. 3.48. Вкладка Общие (General) диалога Свойства: Протокол Интернета (ТСРЛР) (Internet Protocol (TCP/IP) Properties)*

➤ Установите переключатель Использовать следующий IP-адрес (Use the following IP address).

- В поле ввода **IP-адрес** (IP address) введите IP-адрес вида 192.168.0.*, который вы хотите присвоить данному компьютеру, например **192.168.0.1**.
- В поле ввода **Маска подсети** (Subnet mask) введите маску **255.255.255.0.** Впрочем, когда вы щелкнете мышью в этом поле, данная маска появится автоматически.
- Нажмите кнопку **Дополнительно** (Advanced). Откроется диалог **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings).
- Щелкните мышью на ярлыке WINS, чтобы перейти на эту вкладку (Рис. 3.49).

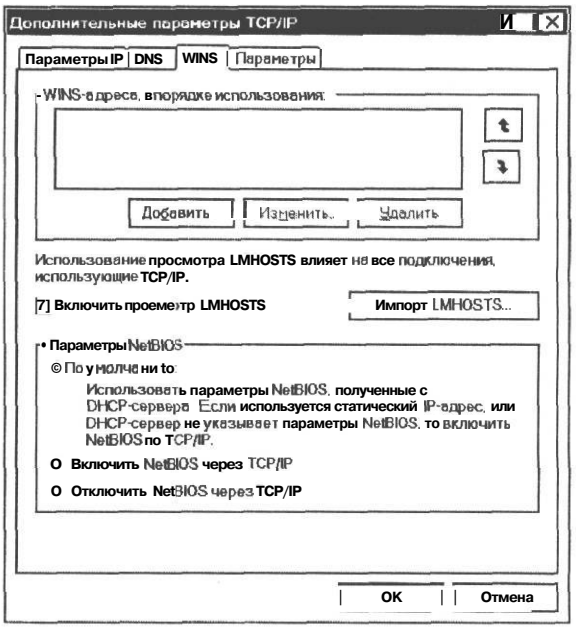



*Рис. 3.49. Вкладка WINS диалога Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)*

WINS (Windows Internet Naming Service - Служба имен Интернета Windows) - это сервис, обеспечивающий преобразование IP-адресов компьютера в понятные логические имена. Обычно задача такого преобразования возлагается на серверы DNS (Domain Name System - Система доменных имен), каждый из которых содержит информацию об адресах своей зоны (домена). Все вместе серверы DNS образуют иерархическую распределенную базу данных IP-адресов всех компьютеров в Интернете. Преимущество применения WINS-сервера перед DNS-сервером состоит в динамическом характере преобразования адресов, а также в возможности дополнительно различать имена компьютеров, которые они имеют не только в Интернете, но и в локальной сети - так называемые имена NetBIOS, и преобразовывать эти имена в IP-адреса.

- Установите переключатель **Включить NetBIOS через TCP/IP** (Enable NetBIOS over TCP/IP).
- Закройте диалог **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings) нажатием кнопки **OK.** Вы возвратитесь к диалогу **Свойства: Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP) Properties).

➤ Закройте также и этот диалог. На экране останется диалог **Подключение по локальной сети - свойства** (Local Area Connection Properties) (Рис. 3.46).

> В диалоге **Подключение по локальной сети - свойства** (Local Area Connection Properties) щелкните мышью на ярлыке **Проверка подлинности** (Authentication), чтобы перейти на эту вкладку (Рис. 3.50).

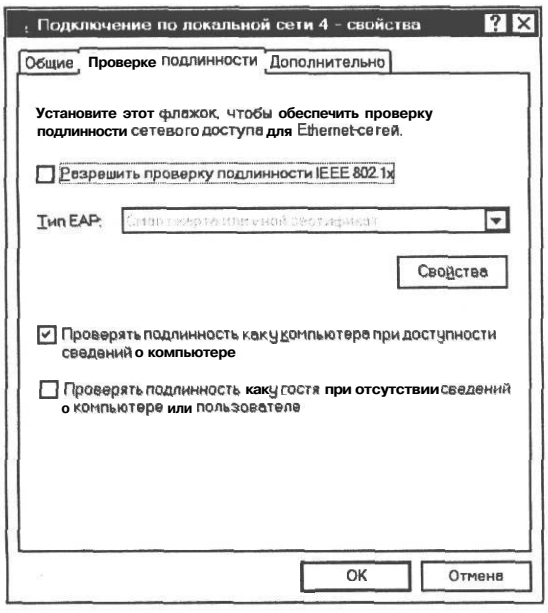



*Рис. 3.50. Вкладка **Проверка подлинности** (Authentication) диалога **Подключение по локальной сети - свойства** (Local Area Connection Properties)*

➤ Сбросьте флажок **Разрешить проверку подлинности IEEE 802.1 x** (Enable IEEE 802.lx authentication for this network), иначе компьютер не будет виден в сети.

➤ Закройте диалог **Подключение по локальной сети - свойства** (Local Area Connection Properties), нажав кнопку **OK.**

Описанным способом следует назначить статические IP-адреса, включить NetBIOS через TCP/IP и выключить проверку подлинности IEEE 802.1x для всех компьютеров локальной сети. Не забудьте только, что каждый компьютер должен иметь уникальный адрес вида 192.168.0.*, например 192.168.0.2, 192.168.0.3 и т.д.

## Задание имени компьютера и рабочей группы

Далее необходимо задать имена компьютера и рабочей группы. Для этого выполните следующие действия.

> В диалоге **Свойства системы** (System Properties) (Рис. 3.41) перейдите на вкладку **Имя компьютера** (Computer Name) (Рис. 3.51).

Содержимое поля **Описание** (Computer description) заполните любой информацией, поясняющей основную роль этого компьютера, например, № **1**.

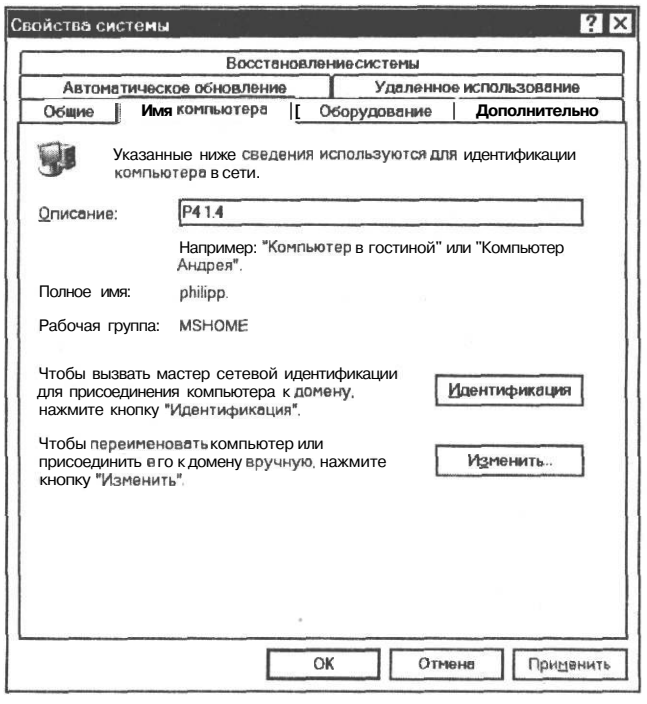



*Рис. 3.51. Вкладка **Имя компьютера** (Computer Name) диалога Свойства системы (System Properties)*

> Нажмите кнопку **Изменить** (Change). На экране появится диалог Изменение **имени компьютера** (Computer Name Changes) (Рис. 3.52).

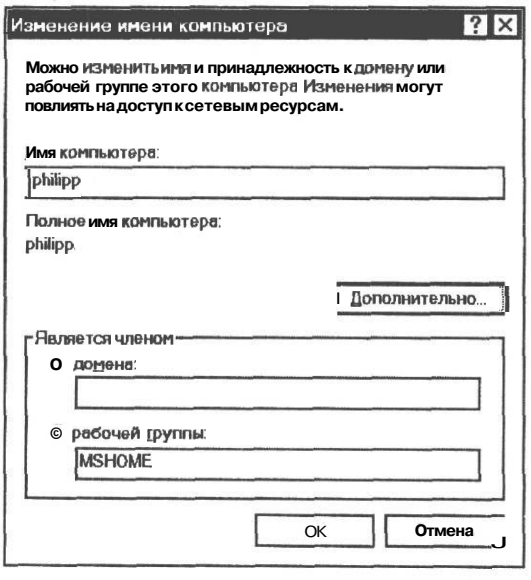



*Рис. 3.52. Диалог **Изменение имени компьютера** (Computer Name Changes)*

> В поле **Имя компьютера** (Computer name) введите название данного компьютера в качестве клиента сети Microsoft, например, **Manager.**

x Установите переключатель **рабочей группы** (Workgroup) и в поле ввода укажите имя рабочей группы сети Microsoft, в которой работает данный компьютер, например, **MSHOME**.

Напомним, что имя рабочей группы на всех компьютерах должно быть одинаковым.

> Нажмите кнопку **(Ж,** чтобы закрыть диалог **Изменение имени компьютера** (Computer Name Changes). На экране появится диалог, сообщающий о подключении к рабочей группе (Рис. 3.53).

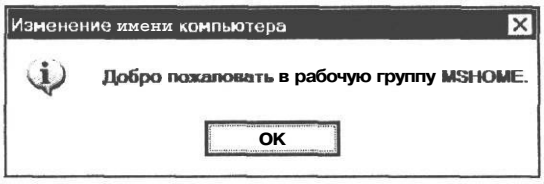



*Рис. 3.53. Диалог, сообщающий о подключении к рабочей группе*

➤ Нажмите кнопку **OK,** чтобы закрыть этот диалог. Появится диалог, информирующий о необходимости перезагрузить компьютер (Рис. 3.54).

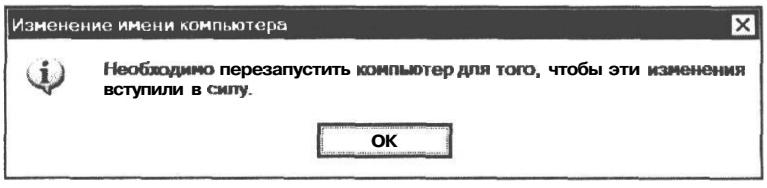



*Рис. 3.54. Диалог, информирующий о необходимости перезагрузить компьютер*

> Закройте этот диалог нажатием кнопки **OK.** Вы возвратитесь к диалогу **Свойства системы** (System Properties).

➤ Нажмите кнопку OK в диалоге **Свойства системы** (System Properties). На экране появится диалог **Изменение параметров системы** (System Settings Change) с предложением перезагрузить компьютер (Рис. 3.55).

➤ Нажмите кнопку Да (Yes), подтверждая перезагрузку системы.

Система перезагрузится, и сделанные изменения вступят в силу.

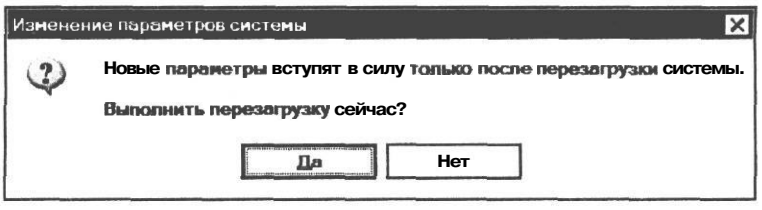



*Рис. 3.55. Диалог **Изменение параметров системы** (System Settings Change)*

## Управление пользователями и группами

Одним из элементов обеспечения безопасности Windows 2000/XP является создание учетных записей пользователей и групп. Назначая им права доступа, администратор сети получает возможность ограничить доступ к конфиденциальной информации, разрешить или запретить выполнять в сети определенные действия, например, архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом - файлом или папкой - и определяет возможность данного пользователя или группы получить доступ к объекту.

Учетная запись пользователя - это запись, содержащая все сведения, определяющие пользователя в операционной системе Windows. К этим сведениям относятся имя пользователя и пароль, требуемые для входа пользователя в систему, имена групп, членом которых является пользователь, а также права и разрешения, которые он имеет при работе в системе и доступе к ее ресурсам. Учетная запись пользователя определяет, какие действия пользователь может выполнять в Windows. На автономном компьютере или на компьютере, входящем в рабочую группу, учетная запись пользователя устанавливает полномочия каждого пользователя. На компьютере, являющемся частью сетевого домена, пользователь должен входить, по крайней мере, в одну группу.

Группа представляет собой набор учетных записей пользователей. При включении учетной записи пользователя в группу соответствующий пользователь получает все права и разрешения, предоставленные этой группе. Таким образом, вместо настройки системы защиты для каждой отдельной учетной записи можно сделать это сразу для целой группы пользователей. Разрешения и права, предоставленные группе, распространяются и на всех ее членов.

Для управления учетными записями пользователей и группами используется оснастка **Локальные пользователи и группы** (Local User Manager) консоли MMC (Microsoft Management Console - Консоль управления Microsoft). Консоль MMC - это своеобразная оболочка, обеспечивающая стандартный интерфейс и включающая инструменты, называемые оснастками, для выполнения различных административных задач. Оснастка **Локальные пользователи и группы** (Local User Manager) допускает создание новых пользователей и групп, добавление пользователей в группы, удаление пользователей из групп, отключение учетных записей пользователей и групп, а также сброс паролей.

Посмотрим, как использовать эту оснастку для управления учетными записями и группами.

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Панель управления** (Control Panel) в Windows XP или команду **Настройка ◆ Панель управления** (Settings ◆ Control Panel) в Windows 2000. На экране появится окно **Панель управления** (Control Panel).
- Дважды щелкните мышью на значке **Администрирование** (Administrative Tools). Появится окно **Администрирование** (Administrative Tools) (Рис. 3.56).
- Дважды щелкните мышью на значке **Управление компьютером** (Computer Management). Откроется окно консоли MMC **Управление компьютером** (Computer Management) (Рис. 3.57).

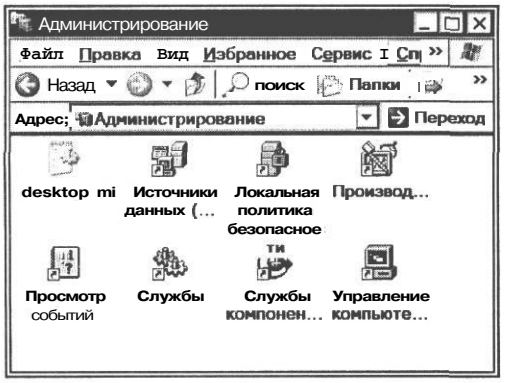



*Рис. 3.56. Окно Администрирование (Administrative Tools)*

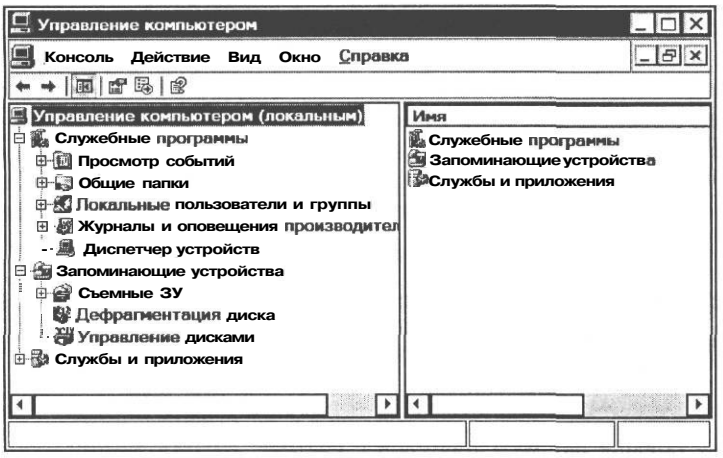



*Рис. 3.57. Окно Управление компьютером (Computer Management)*

В левой части этого окна располагается дерево оснасток, а в правой - содержимое выбранной оснастки.

➤ Дважды щелкните мышью в левой части окна на ветви **Локальные пользователи и группы** (Local User Manager). Данная ветвь развернется, и вы увидите две содержащиеся в ней папки - **Пользователи** (Users) и **Группы** (Groups) (Рис. 3.58).

Существует три типа учетных записей пользователей, доступных на компьютере, входящем в рабочую группу:

- учетная запись администратора компьютера;
- учетная запись с ограниченными правами;
- учетная запись гостя. Она доступна для пользователей, не имеющих собственных учетных записей на данном компьютере.

По умолчанию папка **Пользователи** (Users) содержит встроенные учетные записи. Вы можете увидеть их, открыв эту папку. Они создаются автоматически при установке Windows.

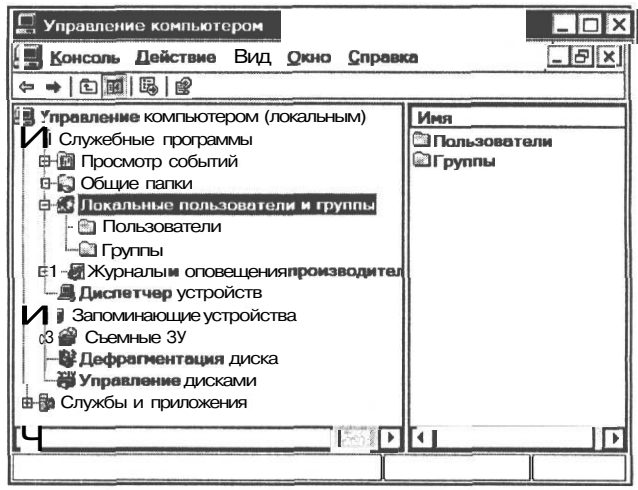



*Рис. 3.58. Папки **Пользователи** (Users) и **Группы** (Groups)*

**Администратор** (Administrator) - эта учетная запись используется при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть уничтожена, блокирована или удалена из группы **Администраторы** (Administrators), ее можно только переименовать. Пользователь с учетной записью администратора компьютера может:

- создавать и удалять учетные записи пользователей на компьютере;
- создавать пароли для других пользователей на компьютере;
- изменять в учетной записи имена пользователей, рисунки, пароли и типы учетных записей;
- не может изменить тип своей учетной записи на ограниченную в случае, когда на компьютере больше нет пользователей с учетной записью администратора компьютера. Таким образом обеспечивается наличие на компьютере, по крайней мере, одного пользователя с учетной записью администратора.

**Учетная запись с ограниченными правами** предназначается для пользователей, которым должно быть запрещено изменять большинство настроек компьютера и удалять важные файлы. Пользователь с учетной записью с ограниченными правами не может:

- устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;
- изменять имя или тип собственной учетной записи. Такие изменения должны выполняться пользователем с учетной записью администратора компьютера;
- может создавать, изменять или удалять собственный пароль.

**Гость** (Guest) - учетная запись, предназначенная для пользователей, не имеющих собственных учетных записей на компьютере. Данная учетная запись не имеет пароля. Это позволяет быстро входить на компьютер для проверки электронной почты или просмотра Интернета. Пользователь, вошедший с учетной записью гостя, не может:

- устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;

- изменить тип учетной записи гостя.

Учетная запись **Гость** (Guest) является членом одноименной группы. Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Существует несколько фундаментальных уровней защиты, предоставляемых пользователям через членство в группах.

Папка Группы (Groups) по умолчанию содержит такие встроенные группы, создаваемые автоматически при установке системы. Вы можете увидеть их, щелкнув мышью на этой папке в левой части окна консоли. Эти группы имеют следующие свойства.

**Администраторы** (Administrators). Члены данной группы обладают полным доступом ко всем ресурсам системы. Это - единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав.

**Операторы архива** (Backup Operators). Члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архивации могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности.

**Опытные пользователи** (Power Users). Члены этой группы могут создавать учетные записи пользователей, и имеют право модифицировать настройки безопасности только созданных ими пользователей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами **Пользователи** (Users), **Гости** (Guests) **и Опытные пользователи** (Power Users), но не могут модифицировать членство в группах **Администраторы** (Administrators) и **Операторы архива** (Backup Operators). Они не могут быть владельцами файлов, архивировать и восстанавливать каталоги, загружать и выгружать драйверы устройств, модифицировать настройки безопасности и журнал событий.

**Пользователи** (Users). Члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов, но не могут получить доступ к общей папке или создать локальный принтер.

**Гости** (Guests). Эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи **Гости** (Guests) и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут завершать работу системы.

**Репликатор** (Replicator). Членом этой группы должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи.

## Создание учетной записи

Для каждого нового пользователя необходимо создать учетную запись. Это делается следующим образом.

➤ В окне **Управление компьютером** (Computer Management) (Рис. 3.57) щелкните правой кнопкой мыши на значке папки **Пользователи** (Users) и в появившемся контекстном меню выберите команду **Новый пользователь** (New User). На экране появится диалог **Новый пользователь** (New User) (Рис. 3.59).

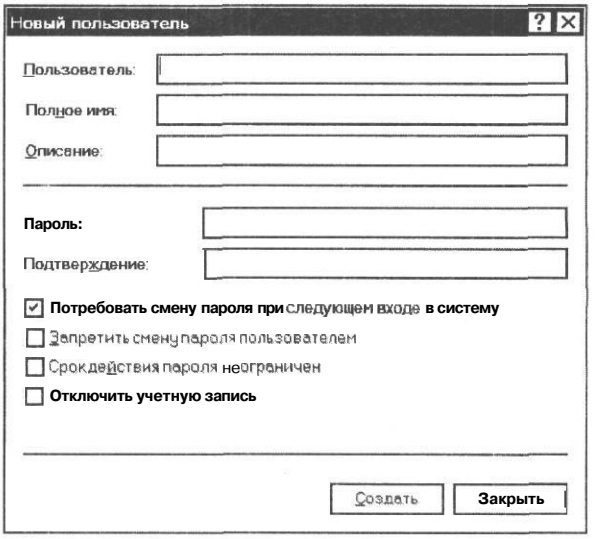



*Рис. 3.59. Диалог **Новый пользователь** (New User)*

- В поле ввода **Пользователь** (User name) введите имя создаваемого пользователя.
- В поле вода **Полное имя** (Full name) введите полное имя пользователя.
- В поле ввода **Описание** (Description) введите описание пользователя или его учетной записи.
- В поле ввода **Пароль** (Password) укажите пароль пользователя и подтвердите его правильность вторичным вводом в поле ввода **Подтверждение** (Confirm password).

При установленном флажке **Потребовать смену пароля при следующем входе в систему** (User must change password at next logon) система потребует изменить пароль при следующем входе в Windows. Если, например, при создании учетной записи указан какой-нибудь стандартный, небезопасный пароль типа «admin», то при следующем входе система потребует заменить его.

Установка флажка **Запретить смену пароля пользователем** (User cannot change password) не позволит пользователю изменять пароль. Это используется в том случае, когда в целях безопасности администратор сам задает безопасные пароли пользователей.

Если установить флажок **Срок действия пароля не ограничен** (Password never expires), то заданный пароль будет использоваться постоянно, без ограничения во времени. Но такая установка снижает защищенность системы. В целях безопасности необходимо регулярно менять пароли.

При установленном флажке **Отключить учетную запись** (Account disabled) данная учетная запись блокируется.

- Нажмите кнопку **Создать** (Create). Учетная запись будет зарегистрирована, и в папке **Пользователи** (Users) появится вновь созданный пользователь.

Но диалог **Новый пользователь** (New User) не закроется, а только очистятся его поля, и вы сможете продолжать создание учетных записей. После того как все учетные записи будут созданы, можно закрыть этот диалог нажатием кнопки **Закрыть** (Close).

## Модификация и удаление учетных записей

Изменять, переименовывать и удалять учетные записи пользователей можно с помощью контекстного меню (Рис. 3.60), вызываемого щелчком правой кнопкой мыши на имени пользователя, либо, обратившись к меню **Действие** (Action) окна **Управление компьютером** (Computer Management) (Рис. 3.57).

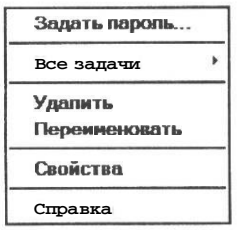



*Рис. 3.60. Контекстное меню учетной записи*

С помощью команды **Свойства** (Properties) можно определить **Членство в группах** (Member of) и **Профиль пользователя** (Profile).

Поскольку переименованная учетная запись сохраняет свой уникальный идентификатор, она сохраняет и все свои свойства, например, описание, полное имя, пароль, членство в группах и т.д.

В Windows XP возможен еще один способ создания и модификации учетных записей - с помощью Мастера **Учетные записи пользователей** (User Accounts) (Рис. 3.61), который запускается из **Панели управления** (Control Panel). Но этот Мастер предоставляет ограниченные возможности администрирования, позволяя только создавать, переименовывать и назначать пароли учетным записям.

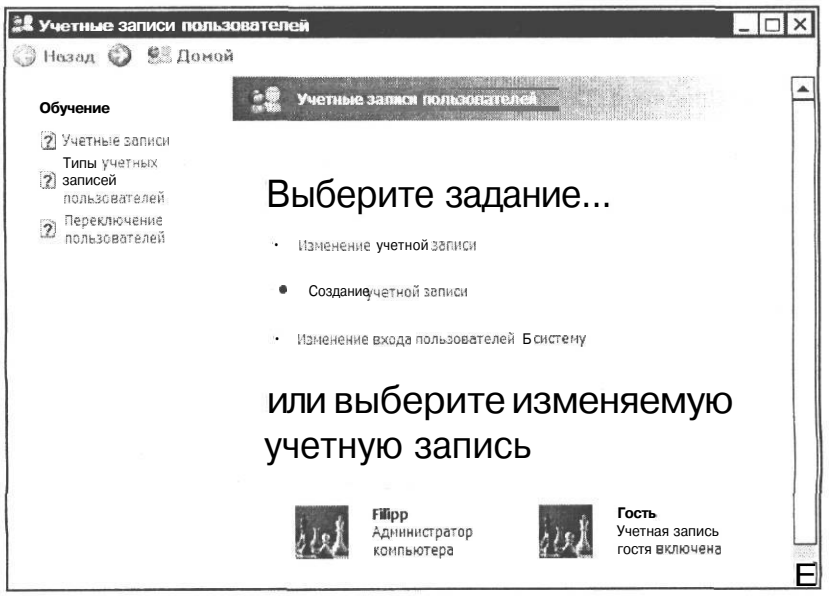



*Рис. 3.61. Мастер **Учетные записи пользователей (User Accounts)***

## Создание локальной группы

Для создания новой локальной группы выполните следующие действия.

➤ В окне **Управление компьютером** (Computer Management) (Рис. 3.57) щелкните правой кнопкой мыши на значке папки **Группы** (Groups) и в появившемся контекстном меню выберите команду Создать группу (New Group). На экране появится диалог **Новая группа** (New Group) (Рис. 3.62).

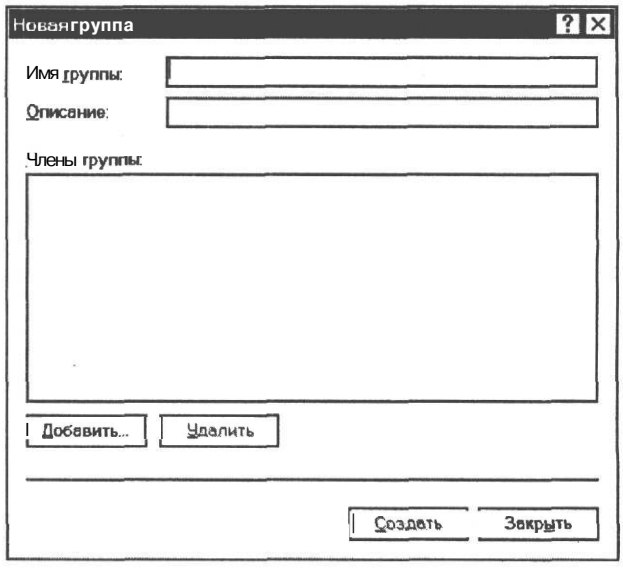



*Рис. 3.62. Диалог **Новая группа** (New Group)*

> В поле ввода **Имя группы** (Group name) введите имя новой группы.

> В поле ввода **Описание** (Description) введите описание создаваемой группы.

Нажав кнопку **Добавить** (Add), вы сможете добавить в группу учетные записи пользователей. Добавленные записи отобразятся в поле списка **Члены группы** (Members). Чтобы удалить пользователей из группы, следует выделить в этом списке их учетные записи и нажать кнопку Удалить (Remove).

После нажатия кнопки **Создать** (Create) новая группа будет создана и помещена в папку **Группы** (Groups). Поля ввода диалога очистятся для создания следующей группы. Когда создание групп будет закончено, нажатием кнопки **Закрыть** (Close) закройте диалог **Новая группа** (New Group).

Чтобы добавить новых членов в ранее созданную группу, следует щелкнуть правой кнопкой мыши на названии группы в папке **Группы** (Groups) и в появившемся контекстном меню выбрать команду **Добавить в группу** (Add to Group) или **Свойства** (Properties). В появившемся диалоге **Свойства** (Properties) (Рис. 3.63) следует нажать кнопку **Добавить** (Add) и найти нужные учетные записи.

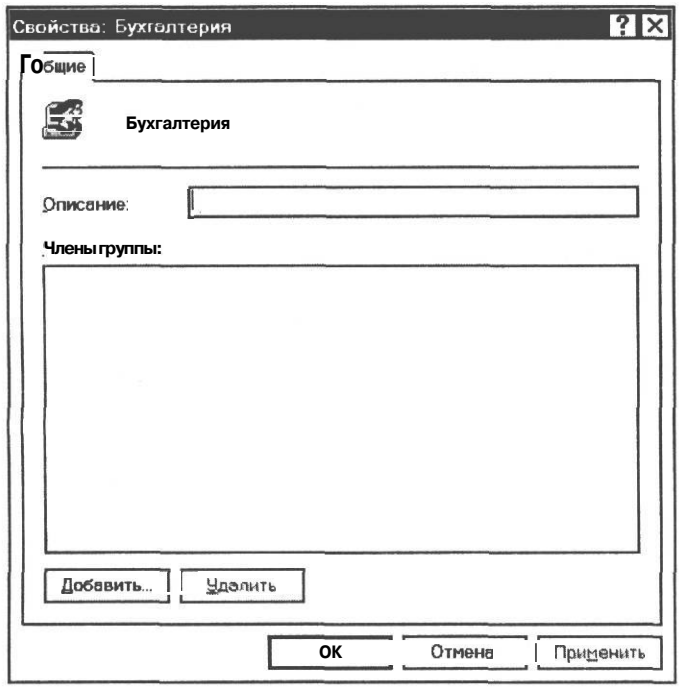



*Рис. 3.63. Диалог* ***Свойства*** *(Properties) группы*

Следует помнить, что встроенные группы не могут быть удалены, а созданные вами и удаленные группы не могут быть восстановлены. При удалении групп их члены сохраняются.

## Обеспечение доступа к общим ресурсам

Как уже упоминалось ранее, компьютеры локальной сети могут предоставлять свои ресурсы, такие как диски, папки и файлы, принтер, модем, факс и т.д., в совместное использование. Наиболее часто устанавливается общий доступ к дискам, папкам, отдельным файлам и принтерам.

Компонент Windows «Служба доступа к файлам и принтерам сетей Microsoft» позволяет другим сетевым компьютерам обращаться к ресурсам данного компьютера по сети Microsoft. Этот компонент в Windows 2000/XP устанавливается и включается автоматически.

### Как выделить в общее пользование папку или диск

Чтобы сделать общими диск или папку, выполните следующие действия:

- Щелкните правой кнопкой мыши на кнопке **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся контекстном меню выберите команду **Проводник** (Explorer). Запустится программа Проводник (Windows Explorer) (Рис. 3.64).
- В левой части окна выберите диск или папку, которые вы хотите выделить в общее пользование, и щелкните на соответствующем значке правой кнопкой мыши. На экране появится контекстное меню.

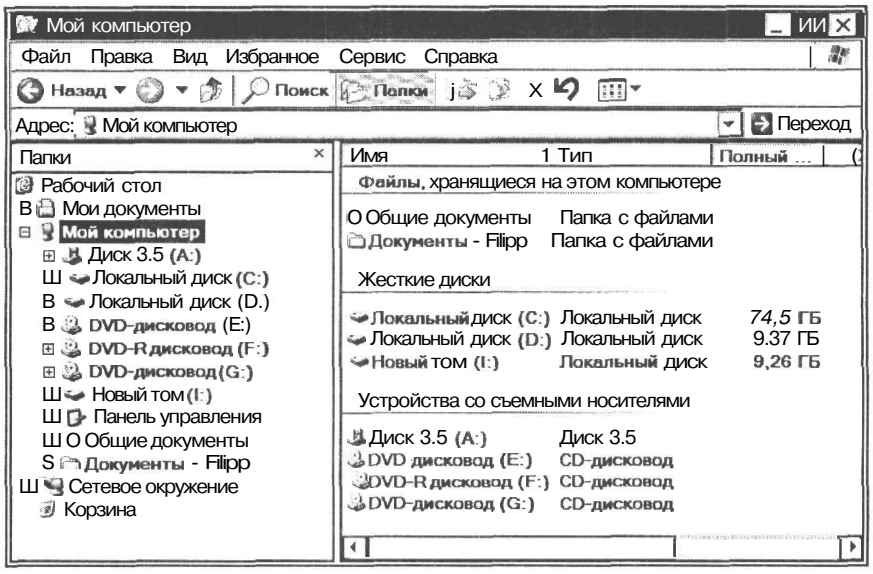



*Рис. 3.64. Окно программы Проводник (Windows Explorer) с открытой папкой **Мой компьютер** (My Computer)*

> В контекстном меню выберите команду **Свойства** (Properties). Появится диалог **Свойства** (Properties) выбранного объекта с открытой вкладкой **Общие** (General) (Рис. 3.65).

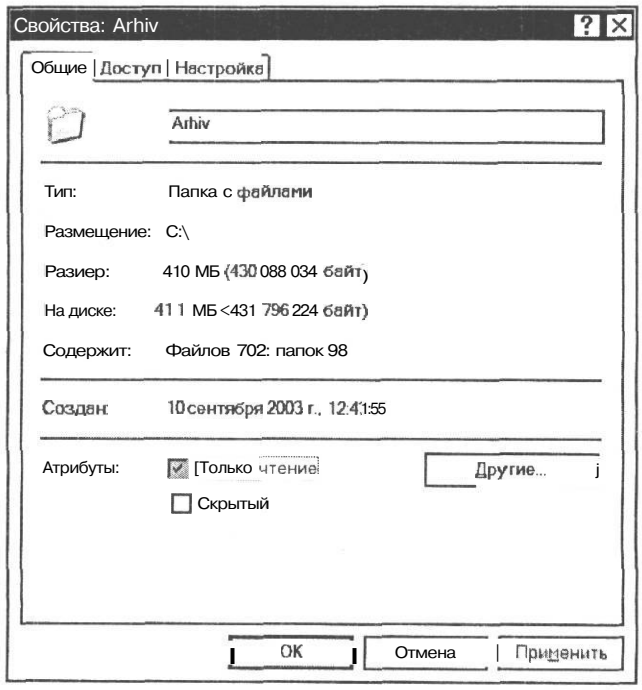



*Рис. 3.65. Вкладка **Общие** (General) диалога **Свойства** (Properties)*

➤ Перейдите на вкладку **Доступ** (Sharing). Если был выбран диск, то эта вкладка будет иметь вид, как на Рис. 3.66, а если папка - то как на Рис. 3.67.

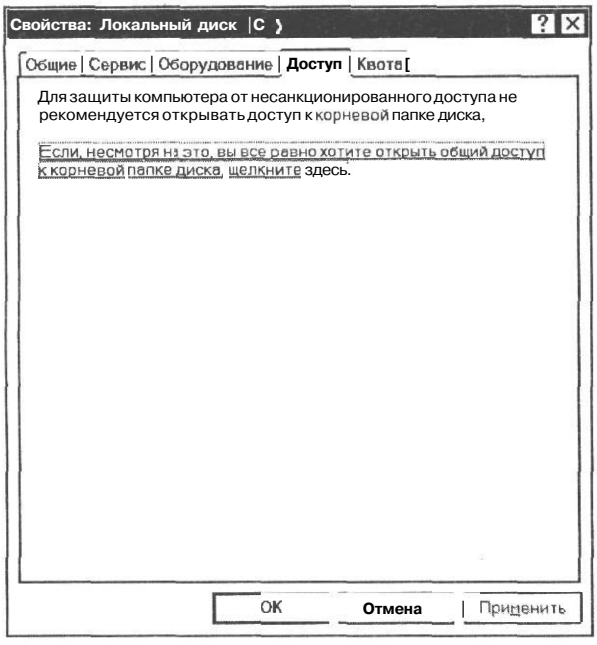



*Рис. 3.66. **Вкладка Доступ** (Sharing) диалога **Свойства** (Properties) диска*

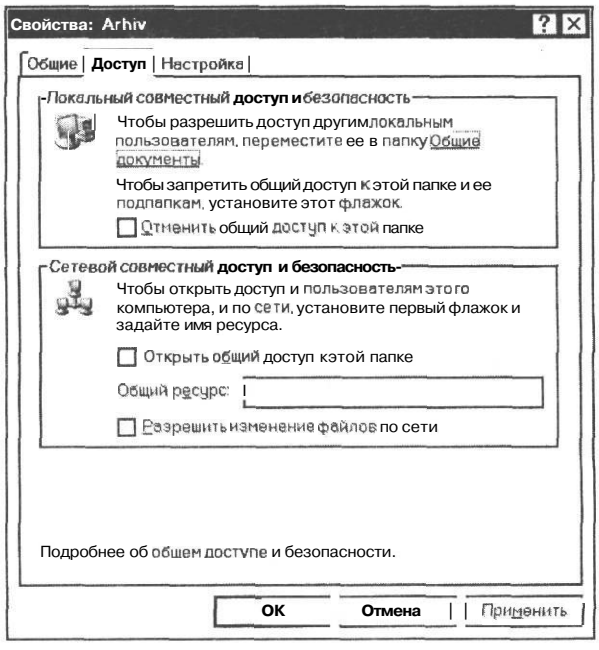
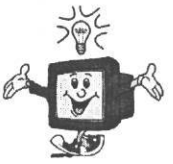



*Рис. 3.67. Вкладка **Доступ** (Sharing) диалога **Свойства** (Properties) папки*

*Диалог **Свойства** (Properties), открытый на вкладке **Доступ** (Sharing), можно также вызвать на экран командой контекстного меню **Общий доступ и безопасность** (Sharing and Security).*



> Если требуется общий доступ к диску, на вкладке Доступ (Sharing) щелкните мышью на ссылке Если, несмотря на это, вы все равно хотите открыть общий доступ к корневой папке диска, щелкните здесь (If you understand the risk but still want to share the root of the drive, click here). Вкладка примет вид, как на Рис. 3.67, т.е. появятся элементы управления для настройки общего доступа.

➤ Чтобы разрешить общий доступ к выбранному ресурсу, установите флажок Открыть общий доступ к этой папке (Share this folder on the network). В поле ввода Общий ресурс (Share name) вы увидите автоматически сгенерированное имя сетевого ресурса, которое можно изменить по своему усмотрению.

Если установить флажок Разрешить изменение файлов по сети (Allow network users to change my files), то другие пользователи сети смогут не только читать файлы, но и редактировать их.

➤ Нажмите кнопку Применить (Apply), чтобы применить установленные параметры.

➤ Нажмите кнопку OK, чтобы закрыть диалог Свойства (Properties).

После такой настройки выбранная папка или диск станут общими.

## Специальные разрешения доступа к файлам и папкам

Общий доступ к папкам и дискам, установленный описанным выше способом, является простым и применяется по умолчанию на компьютерах, не являющихся членами домена. При простом доступе в диалоге Свойства (Properties) отсутствует вкладка Безопасность (Security) а также дополнительные параметры на вкладке Доступ (Sharing).

В операционных системах Windows 2000/XP вы можете применять также специальные разрешения доступа к файлам и папкам, расположенным в томах NTFS. Специальные разрешения доступа представляют собой настраиваемые наборы правил, используемых для управления доступом пользователей к ресурсам сетевого компьютера.

Разрешения определяют тип доступа к объекту или его свойству, допустимый для пользователя или группы. Например, группе сотрудников бухгалтерии можно предоставить разрешения на чтение и запись файла ведомости начисления зарплаты. Разрешения могут быть предоставлены любому пользователю, группе или компьютеру. Рекомендуется назначать разрешения не отдельным пользователям, а группам.

При установке разрешений необходимо определить уровень доступа для групп и пользователей. Например, одному пользователю можно разрешить читать содержимое некоторого файла, другому - вносить изменения в файл, а всем остальным пользователям вообще запретить доступ к этому файлу. Так же можно устанавливать разрешения на доступ к принтерам, чтобы одни пользователи могли настраивать принтер, а другие - только печатать на нем.

Возможности ограничения доступа пользователей к файлам и папкам зависят от того, какая файловая система используется. В операционных системах Windows 2000/XP могут

использоваться файловые системы FAT, FAT32 и NTFS. Последняя является более предпочтительной, так как обладает характеристиками надежности и защищенности, поддерживая контроль доступа к данным и привилегии владельца, играющие исключительно важную роль в обеспечении целостности жизненно важных конфиденциальных данных. Папки и файлы NTFS могут иметь назначенные им права доступа вне зависимости от того, являются ли они разделяемыми или нет. NTFS - единственная файловая система в Windows, которая позволяет назначать права доступа к отдельным файлам. Однако, если файл будет скопирован из раздела или тома NTFS в раздел FAT, все права доступа и другие уникальные атрибуты, присущие NTFS, будут утеряны. Файловая система NTFS позволяет определить также, какие пользователи и группы имеют доступ к общим ресурсам, а также настроить доступ к файлам и пакам для локальных пользователей, работающих на одном компьютере поочередно, что абсолютно недоступно в FAT и FAT32. Если к системе предъявляются повышенные требования в отношении безопасности, то реализовать их можно только при использовании файловой системы NTFS.

## Выключение режима простого доступа к файлам

Чтобы иметь возможность задать, просмотреть, изменить и удалить особые разрешения для файлов и папок в NTFS, следует сначала выключить включенный по умолчанию режим простого доступа к файлам. Сделайте это следующим образом.

➤ В окне программы Проводник (Windows Explorer) (Рис. 3.64) выберите команду меню **Сервис * Свойства папки** (Tools ◆ Folder Options). На экране появится диалог **Свойства папки** (Folder Options).

> Перейдите на вкладку Вид (View) (Рис. 3.68).

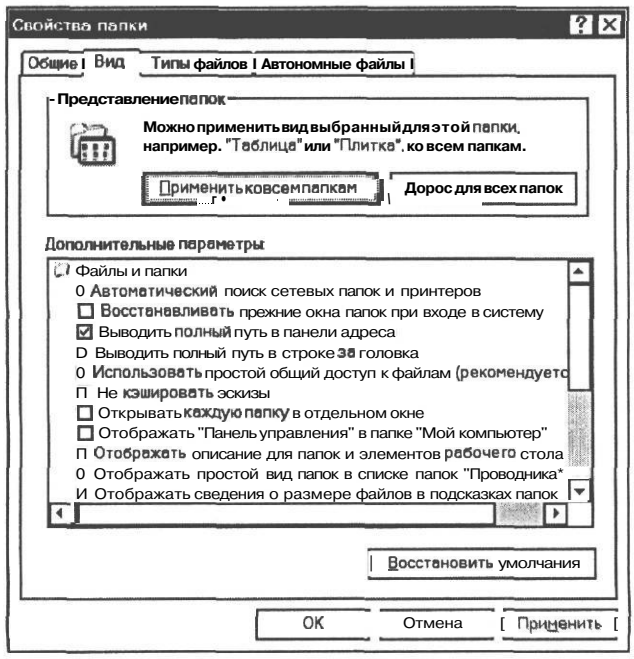



*Рис. 3.68. Вкладка Вид (View) диалога* ***Свойства папки*** *(Folder Options).*

- **Сбросьте флажок Использовать простой общий доступ к файлам (рекомендуется)** (Use simple file sharing (Recommended)).
- Нажмите кнопку **Применить** (Apply).
- Закройте диалог **Свойства папки** (Folder Options), нажав кнопку **OK.**

## Задание разрешений для доступа к файлам и папкам

Теперь можно использовать разрешения для доступа к файлам и папкам. Посмотрим, как это сделать.

- В окне программы Проводник (Windows Explorer) (Рис. 3.64) щелкните правой кнопкой мыши на папке или файле, для которого необходимо установить разрешения. Появится контекстное меню.
- Выберите в контекстном меню команду **Свойства** (Properties). На экране появится диалог **Свойства** (Properties) выбранного объекта (Рис. 3.65).
- Перейдите на вкладку **Безопасность** (Security) (Рис. 3.69).

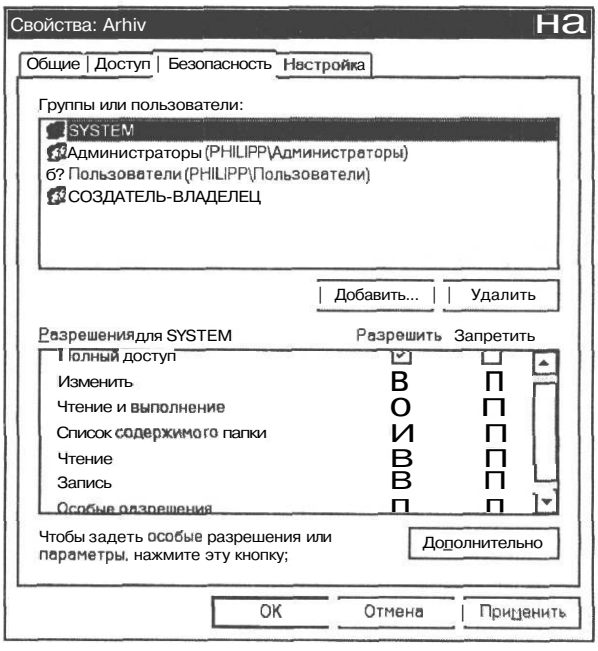



*Рис. 3.69. Вкладка **Безопасность** (Security) диалога **Свойства** (Properties) папки*

В верхней части этой вкладки перечислены пользователи и группы, которым уже предоставлены разрешения для данного объекта.

В поле списка **Разрешения для** ... (Permissions for ...) отображаются стандартные разрешения для выделенной группы или выделенного пользователя: **Полный доступ** (Full control), **Изменить** (Modify), **Чтение и выполнение** (Read&Execute), **Список содержимого папки** (List folder contents) - только для папок, **Чтение** (Read), **Запись** (Write), **Особые разрешения** (Special Permissions). Чтобы явно **Разрешить** (Allow) или **Запретить** (Deny)

доступ к объекту, следует установить соответствующий флажок. Чтобы задать **Особые разрешения** (Special Permissions), следует нажать кнопку **Дополнительно** (Advanced).

Вы можете добавить новых пользователей или группы, нажав кнопку **Добавить** (Add) или удалить их из верхнего списка, нажав кнопку **Удалить** (Remove).

После установки разрешений необходимо нажать кнопку **Применить** (Apply) и закрыть диалог **Свойства** (Properties) нажатием кнопки **OK.**

При установке разрешений следует руководствоваться следующими принципами:

- старайтесь устанавливать разрешения для групп, а не для отдельных пользователей;
- поскольку непосредственное сопровождение учетных записей пользователей, как правило, неэффективно, назначать разрешения отдельным пользователям следует лишь в исключительных случаях;
- устанавливайте разрешения, которые могли бы наследоваться дочерними объектами, т.е. вложенными папками и файлами, созданными в папке, для которой установлено разрешение;
- лучше назначать не индивидуальные разрешения, а разрешения **Полный доступ** (Full control), если это допустимо.

Запретить доступ может потребоваться в следующих случаях:

- чтобы исключить каких-либо пользователей из группы, которой предоставлены определенные разрешения;
- чтобы отменить какое-либо особое разрешение, если пользователю или группе уже предоставлен полный доступ.

## Как сделать общим принтер

В домашней или офисной сети значительно удобнее использовать для всех компьютеров один общий принтер, чем приобретать несколько. Чтобы выделить принтер в общее пользование, выполните следующие действия.

➤ Нажмите кнопку Пуск (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows XP выберите команду **Принтеры и факсы** (Printers and Faxes), а в меню Windows 2000 - команду Настройки ◆ Принтеры (Settings ◆ Printers). В Windows XP появится окно **Принтеры и факсы** (Printers and Faxes), а в Windows 2000 - окно **Принтеры** (Printers) с перечнем всех установленных в системе принтеров (Рис. 3.70).

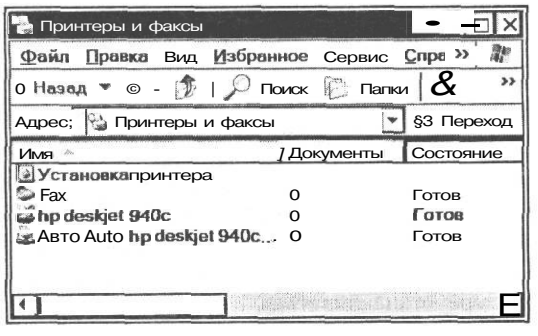



*Рис. 3.70. Папка **Принтеры и факсы** (Printers and Faxes)*

➤ Щелкните правой кнопкой мыши на значке локального принтера, который вы хотите выделить в общее пользование. На экране появится контекстное меню.

> Выберите в контекстном меню команду Общий доступ (Sharing). Откроется диалог Свойства (Properties) выбранного принтера (Рис. 3.71).

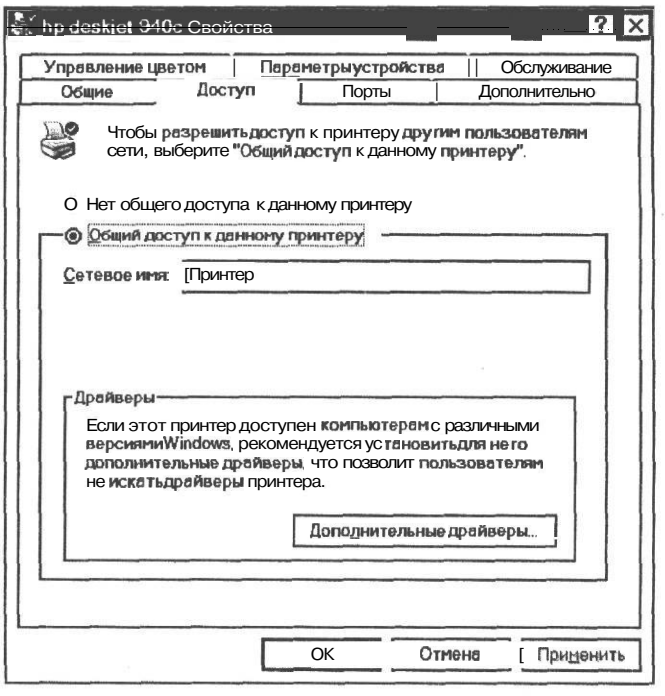



*Рис. 3.71. Вкладка Доступ (Sharing) диалога Свойства (Properties) принтера*

> Установите переключатель Общий доступ к данному принтеру (Share this printer).

> В поле ввода Сетевое имя (Share name) появится автоматически сгенерированное имя сетевого ресурса, которое можно изменить по вашему усмотрению.

Если принтер, выделяемый в общее пользование, будет доступен компьютерам с разными операционными системами, то следует установить для него дополнительные драйверы, что позволит пользователям сети автоматически зафузить их при подключении к этому принтеру.

> Нажмите кнопку Дополнительные драйверы (Additional Drivers). На экране появится диалог Дополнительные драйверы (Additional Drivers) (Рис. 3.72).

Здесь приведен перечень доступных драйверов для разных версий Windows, работающих на компьютерах с разными процессорами - Alpha, IA64, Intel. Сброшенный флажок означает, что драйверы для данной операционной системы и платформы не установлены. Установленный флажок означает, что драйверы выбраны для установки. Если установленный флажок затенен (серого цвета) и не доступен, то это означает, что драйверы уже установлены и не будут переустанавливаться.

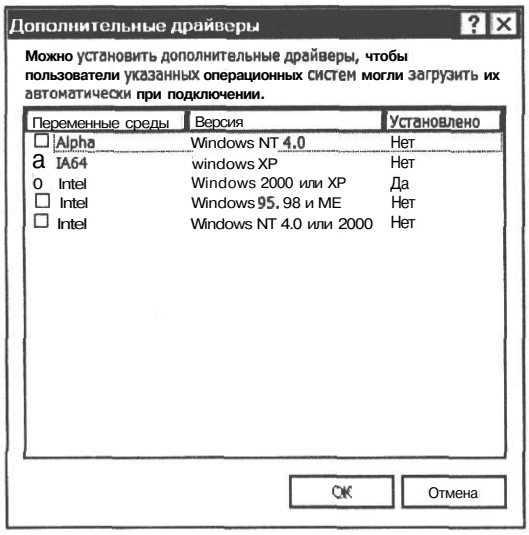



*Рис. 3.72. Диалог Дополнительные драйверы (Additional Drivers)*

> Установите флажки для тех операционных систем и платформ, которые будут использовать этот принтер.

> Закройте диалог Дополнительные драйверы (Additional Drivers), нажав кнопку OK. Вы возвратитесь к вкладке Доступ (Sharing) диалога Свойства (Properties).

➤ Нажмите кнопку Применить (Apply) в этом диалоге, чтобы применить установленные параметры.

➤ Нажмите кнопку OK, чтобы закрыть диалог Свойства (Properties).

В окне Принтеры и факсы (Printers and Faxes) значок принтера, ставшего общедоступным, изменится - на нем появится изображение руки.

> Закройте окно Принтеры и факсы (Printers and Faxes), нажав кнопку ☒ в его заголовке.

Чтобы на других компьютерах локальной сети можно было использовать принтер, выделенный в общее пользование, его необходимо установить как сетевой. При установке автоматически будут загружены необходимые драйверы.

## Проверка работы локальной сети

Когда настройка локальной сети завершена, прежде всего следует убедиться, что протокол TCP/IP работает и связь между компьютерами установлена. Следует помнить, что после настройки сетевых компонентов, компьютеры в сетевом окружении появляются не сразу, а спустя некоторое время, измеряемое минутами, которое зависит от размеров и конфигурации сети.

### Проверка связи между компьютерами

Для проверки работоспособности протокола TCP/IP и связи между компьютерами используется команда **ping.**

x Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Выполнить** (Run). На экране появится диалог **Запуск программы** (Run) (Рис. 3.73).

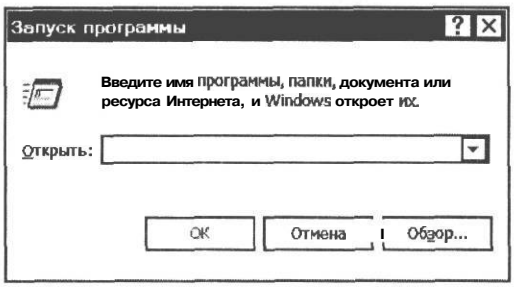



*Рис. 3.73. Диалог **Запуск программы** (Run)*

- *В* поле ввода **Открыть** (Open) введите команду: **cmd** и нажмите кнопку **ОК.** На экране появится окно **Командная строка** (Command Prompt).
- В окне **Командная строка** (Command Prompt) введите команду **ping** и в качестве ее аргумента - статический IP-адрес компьютера, связь с которым проверяется, например **ping 192.168.0.1**. Вместо IP-адреса можно указать сетевое имя компьютера. Этот компьютер должен быть включен и его сетевые компоненты настроены.
- Нажмите клавишу Enter. Будут посланы эхо-запросы, после чего вы увидите время их приема-передачи (Рис. 3.74).

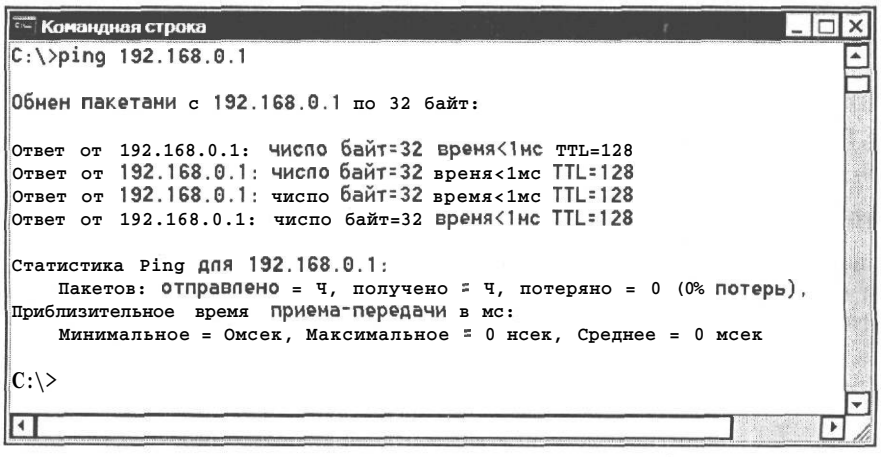



*Рис. 3.74. Окно **Командная строка** (Command Prompt) с результатом работы команды **ping***

Если все 4 отправленных пакета были получены без потерь, то протокол TCP/IP настроен правильно и связь с проверяемым компьютером установлена.

Если же после такой команды появились сообщения **Превышен интервал ожидания для запроса** (Timeout), то это свидетельствует об отсутствии связи с указанным компьютером либо о неправильном IP-адресе.

В таком случае следует проверить:

- правильность IP-адреса или имени компьютера;
- правильность монтажа кабеля, разъемов, сетевых карт и концентраторов;
- отсутствие разрывов и коротких замыканий;
- установку драйверов, сетевых протоколов и клиентов;
- связь между другими компьютерами сети.

## Сетевое окружение

Когда вы убедились, что связь с компьютерами сети установлена, можно увидеть компьютеры в сетевом окружении и доступность сетевых ресурсов.

➤ В Windows XP нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и выберите команду главного меню **Сетевое окружение** (My Network Places). В Windows 2000 дважды щелкните мышью на значке **Сетевое окружение** (My Network Places) на **Рабочем столе** (Desktop). На экране появится окно **Сетевое окружение** (My Network Places) (Рис. 3.75).

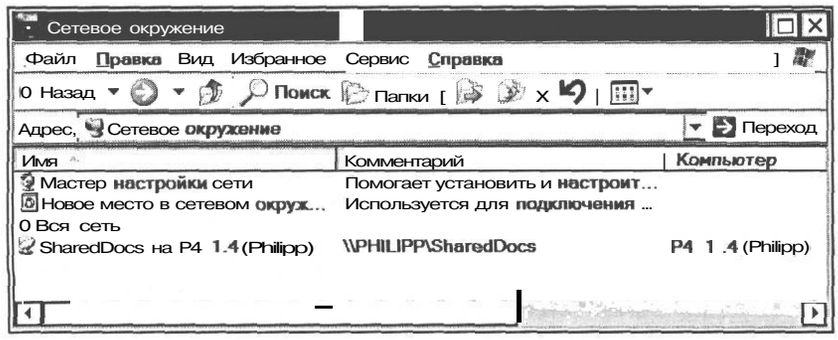



*Рис. 3.75. Окно **Сетевое окружение** (My Network Places)*

В этом окне, кроме прочего, перечислены все файлы и папки компьютера, к которым открыт общий доступ. На вашем компьютере данный список может отличаться от того, который приведен на рисунке.

> Дважды щелкните мышью в окне **Сетевое окружение** (My Network Places) на значке **Вся сеть** (Entire Network). Откроется окно папки **Вся сеть** (Entire Network) (Рис. 3.76).

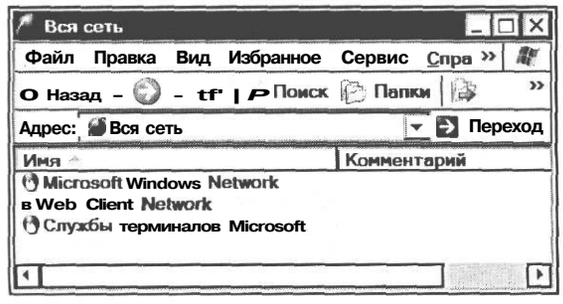



*Рис. 3.76. Окно папки **Вся сеть** (Entire Network)*

➤ Дважды щелкните мышью в окне Вся сеть (Entire Network) на значке **Microsoft Windows Network.** Откроется окно с таким же названием, в котором вы увидите значок с названием рабочей группы (Рис. 3.77).

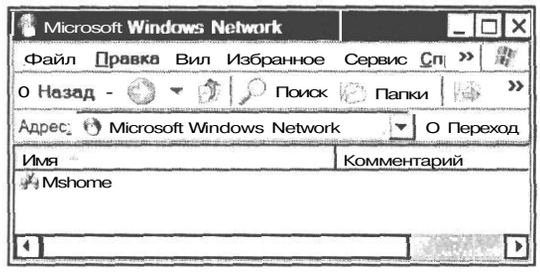



*Рис. 3.77. Окно папки* ***Microsoft Windows Network***

> Дважды щелкните мышью в окне **Microsoft Windows Network** на значке рабочей группы. Откроется окно рабочей группы, в котором будут перечислены все включенные компьютеры (Рис. 3.78).

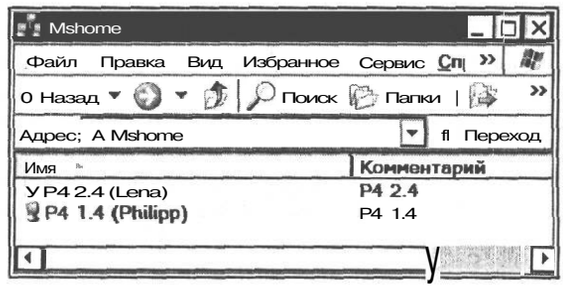



*Рис. 3.78. Окно папки рабочей группы с перечнем включенных компьютеров*

С помощью двойного щелчка мышью на имени любого компьютера можно отобразить его общие ресурсы (Рис. 3.79).

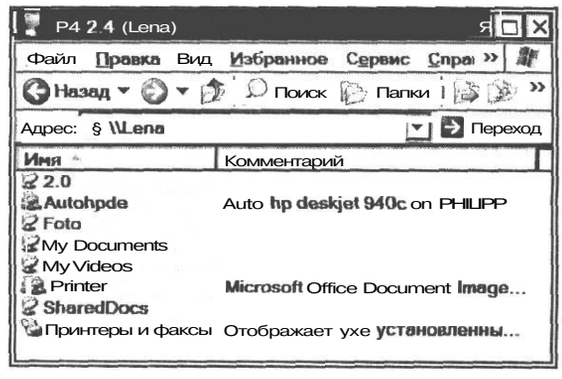



*Рис. 3.79. Окно папки сетевого компьютера с перечнем его общих ресурсов*

С этими ресурсами, которыми могут быть диски, папки, принтеры, вы можете работать, как со своими собственными.

## Подключение сетевого диска

Но значительно удобнее назначить каждой сетевой папке букву диска. После этого к ним можно будет обращаться, как к диску, из окна папки **Мой компьютер** (My Computer) или из программы **Проводник** (Windows Explorer).

Для этого в окне любой папки или программы **Проводник** (Windows Explorer) выберите команду меню **Сервис** ◆ **Подключить сетевой диск** (Tools ◆ Map Network Drive). В открывающемся списке **Диск** (Drive) появившегося диалога **Подключение сетевого диска** (Map Network Drive) (Рис. 3.80) выберите букву диска. Затем нажмите кнопку **Обзор** (Browse) и выберите сетевую папку, имя которой отобразится в поле открывающегося списка **Папка** (Folder). При установленном флажке **Восстанавливать при входе в систему** (Reconnect at logon) эта папка будет автоматически загружаться при входе в Windows. После нажатия кнопки **Готово** (Finish) подключение будет установлено, и в дальнейшем открыть эту сетевую папку можно будет, щелкнув мышью на букве назначенного ей диска в окне папки **Мой компьютер** (My Computer) или программы Проводник (Windows Explorer).

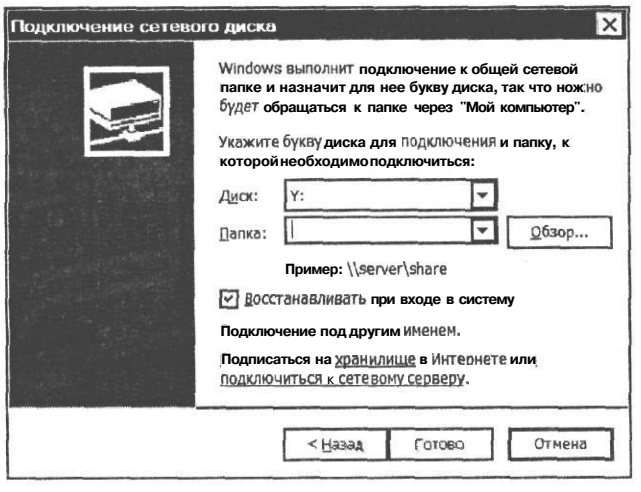



*Рис. 3.80. Диалог **Подключение сетевого диска** (Map Network Drive)*

## Поиск компьютера в сети

Чтобы окончательно убедиться в доступности (или недоступности) определенного клиента локальной сети, попробуем найти его имя в сетевом окружении.

- Нажмите кнопку **Поиск** (Search) на панели инструментов окна рабочей группы (Рис. 3.78). В левой части этого окна появится панель **Помощник по поиску** (Search Companion) (Рис. 3.81). В Windows 2000 эта панель называется **Поиск** (Search).
- В поле ввода **Имя компьютера** (Computer name), находящееся в левой части окна, введите имя какого-либо клиента локальной сети.
- Нажмите кнопку **Найти** (Search) для запуска процесса.

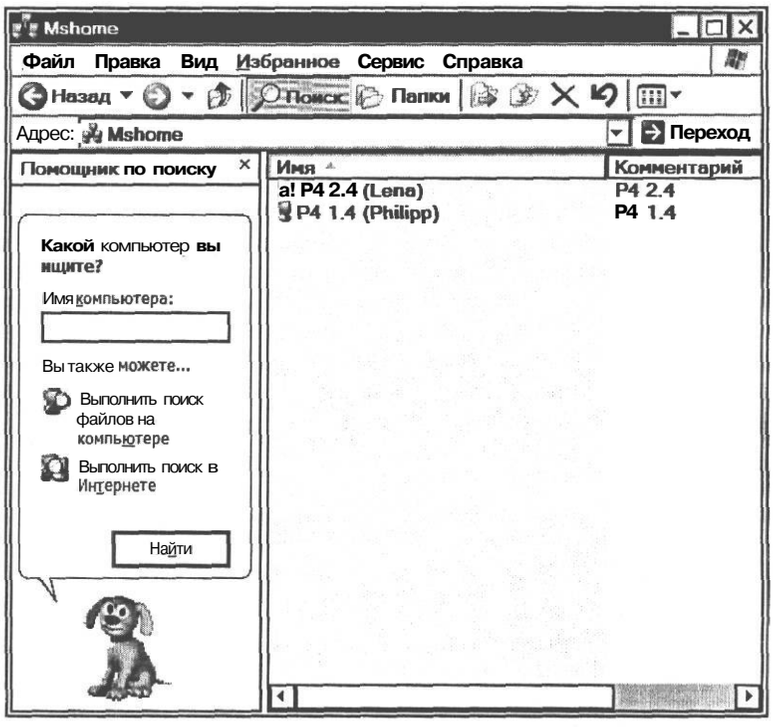



*Рис. 3.81. Окно рабочей группы с панелью* ***Помощник по*** *поиску (Search Companion)*

В случае успешного поиска имя компьютера появится в правой части окна рабочей группы, которое теперь будет называться **Результаты поиска - компьютеры** (Search Results - Computers).

ГЛАВА 4.

# Подключение локальной сети к Интернету

Когда локальная сеть создана и работает, возникает естественное желание подключить ее к Интернету, чтобы все пользователи сети могли на своих компьютерах в любое время беспрепятственно просматривать Web-страницы, получать и отправлять сообщения по электронной почте и пользоваться всеми другими ресурсами Интернета. Чтобы осуществить подключение локальной сети к Интернету, прежде всего следует решить, каким способом это сделать.

## Способы подключения локальной сети к Интернету

Существует несколько способов подключения домашних или малых офисных сетей к Интернету:

- с использованием средства общего доступа к подключению Интернета (Internet Connection Sharing, ICS) в операционной системе Windows XP;
- соединение компьютеров и модема (DSL или кабельного) непосредственно с концентратором Ethernet;
- через частный шлюз (маршрутизатор, роутер).

### Общий доступ к подключению Интернета

При использовании общего доступа один компьютер играет роль узла, предоставляя свое подключение к Интернету в общий доступ всем компьютерам локальной сети (Рис. 4.1). Модем подключается непосредственно к узловому компьютеру. Трафик Интернета, идущий от компьютеров сети и в обратном направлении, проходит через этот узел.

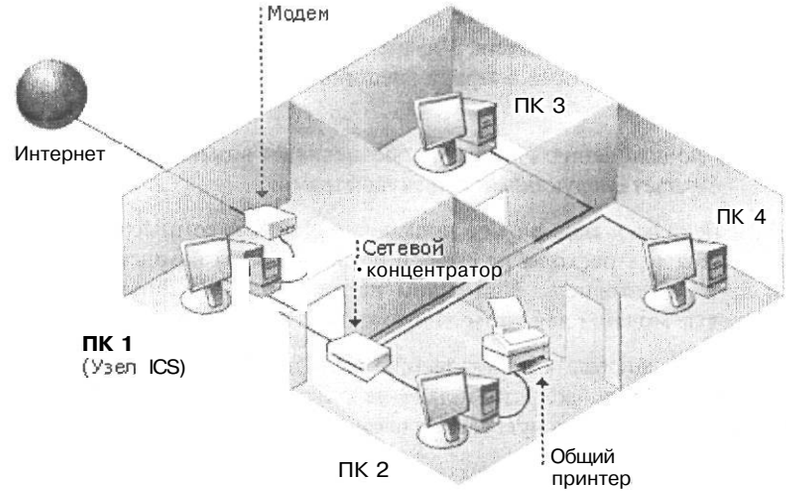



*Рис. 4.1. Локальная сеть с общим доступом к подключению Интернета*

Таким образом, служба общего доступа к подключению Интернета (Internet Connection Sharing, ICS) в Windows XP позволяет компьютерам домашней или небольшой офисной сети входить в Интернет, используя только одно общее подключение. Например, предположим, что в сети есть компьютер, который подключается к Интернету с помощью модема по коммутируемой телефонной линии. Если на этом компьютере включить средство общего доступа, остальные компьютеры сети смогут получать доступ в Интернет по этому же подключению.

Сеть с такой конфигурацией можно также создать, используя адаптеры HPNA (Home Phoneline Network Adapter - адаптер домашней сети на базе телефонной линии) или адаптеры беспроводной сети.

Узловой компьютер общего доступа соединяется с Интернетом через обычный модем с пропускной способностью 28.8 или 56 Кбит/с, модем ISDN, внешний модем DSL или кабельный модем.

Самый дешевый и популярный метод подключения к Интернету - через обычный модем, который может быть внутренним или внешним. Внутренние модемы подключаются к гнезду PCI на системной плате компьютера. На некоторых компьютерах модем встроен непосредственно в системную плату. Внешние модемы подключаются к последовательному порту, параллельному порту или к порту USB компьютера.

Модемы ISDN во многом напоминают обычные модемы; они также могут быть внутренними и внешними. Модем ISDN подключается к обычной телефонной линии. ISDN - это высокоскоростная цифровая линия связи, устанавливаемая телефонной компанией или телекоммуникационным оператором.

Модем DSL обеспечивает широкополосное подключение к Интернету через имеющиеся телефонные линии; он также может быть внутренним и внешним. Внутренние модемы DSL вставляются в гнезда расширения на системной плате и не требуют сетевого адаптера. Подключение к компьютерам внешних модемов DSL осуществляется либо через порт USB, либо через сетевой адаптер.

Кабельные модемы обеспечивают широкополосное подключение к Интернету через инфраструктуру кабельного телевидения; они используют специальную полосу частот, не создающую помех для телепередачи. Внутренние модемы вставляются в гнезда расширения на системной плате компьютера, а внешние подключаются к порту USB или к сетевому адаптеру.

Общий доступ к подключению Интернета обеспечивает возможности безопасной работы Windows XP и обладает следующими преимуществами:

- совместное использование одного подключения всеми компьютерами сети дает возможность сократить расходы на связь и позволяет всем компьютерам одновременно иметь доступ к Интернету. При таком подключении можно использовать сравнительно дешевые модемы для коммутируемой телефонной линии;
- средство общего доступа к подключению Интернета Windows XP позволяет ограничиться контролем безопасности только на одном, узловом компьютере и защитить домашнюю или малую офисную сеть от несанкционированного доступа из Интернета;

Если локальная сеть устанавливается в данной конфигурации, ее безопасность можно обеспечить, используя средство общего доступа к подключению Интернета Windows XP

(ICS) в сочетании с брандмауэром подключения к Интернету (ICF). Кроме того, можно работать с общими файлами и принтерами, не опасаясь, что сведения частного характера будут доступны из Интернета.

Брандмауэр (Internet Connection Firewall, ICF) - это система безопасности, действующая как защитный барьер между сетью и внешним миром. Брандмауэр подключения к Интернету представляет собой программное средство, используемое для настройки ограничений, регулирующих обмен данными между Интернетом и локальной сетью.

Большинство компьютерных систем организаций и отдельные домашние компьютеры используют брандмауэры для защиты от постороннего вмешательства. В целях безопасности компьютеры, использующие широкополосное подключение к Интернету, например, кабельное или по технологии DSL, также защищаются брандмауэром.

Если в сети используется служба общего доступа к подключению Интернета (Internet Connection Sharing, ICS), обеспечивающая доступ в Интернет сразу для нескольких компьютеров, на этом общем подключении к Интернету активизируется брандмауэр. Брандмауэр целесообразно устанавливать для любого компьютера, имеющего прямое подключение к Интернету. Если компьютер подключен к Интернету с помощью кабельного модема, модема DSL или модема удаленного доступа, брандмауэр обеспечивает защиту также и этого подключения.

Недостатком конфигурации сети с общим доступом к подключению Интернета является то, что узловой компьютер должен быть постоянно включен, чтобы остальные компьютеры имели доступ в Интернет.

## Подключение через сетевой концентратор

Внешний модем DSL или кабельный модем можно подключить к сетевому концентратору Ethernet и к нему же подключить все компьютеры (Рис. 4.2). При этом каждый компьютер локальной сети получает прямой доступ в Интернет через сетевой концентратор, который функционирует как центральное устройство подключения к Интернету.

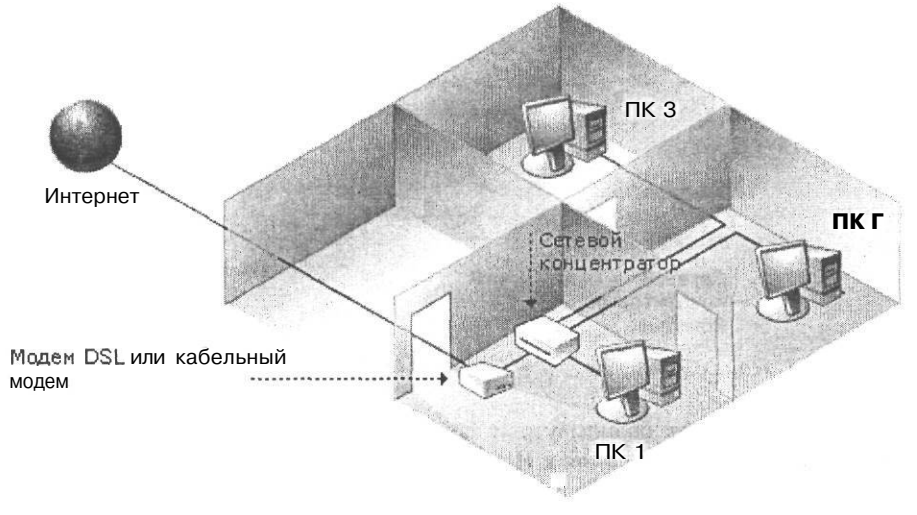



*Рис. 4.2. Подключение локальной сети к Интернету через сетевой концентратор*

Основное преимущество этого способа в том, что для доступа в Интернет не нужно держать один компьютер все время включенным.

Эта конфигурация имеет ряд недостатков:

- необходимо контролировать безопасность на каждом компьютере сети. Сетевые компьютеры, работающие под управлением Windows XP, должны использовать брандмауэр подключения к Интернету на каждом соединении с сетевым концентратором.
- если не установить брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) или другой брандмауэр на каждом подключении к Интернету, общие файлы и папки могут быть видны из Интернета. Брандмауэр подключения к Интернету Windows XP (или другой применяемый брандмауэр) может помешать совместному использованию файлов и принтеров компьютерами сети.
- В некоторых вариантах настройки сети невозможен общий доступ к файлам и принтерам.

## Подключение через частный шлюз

Домашняя или малая офисная сеть может быть подключена к Интернету через специальное устройство, которое называется частным шлюзом, или маршрутизатором. Подобно средству общего доступа к подключению Интерната в Windows XP, такой шлюз позволяет всем компьютерам сети совместно использовать подключение к Интернету через кабельный модем или модем DSL. Частный шлюз располагается между модемом (DSL или кабельным) и локальной сетью (Рис. 4.3).

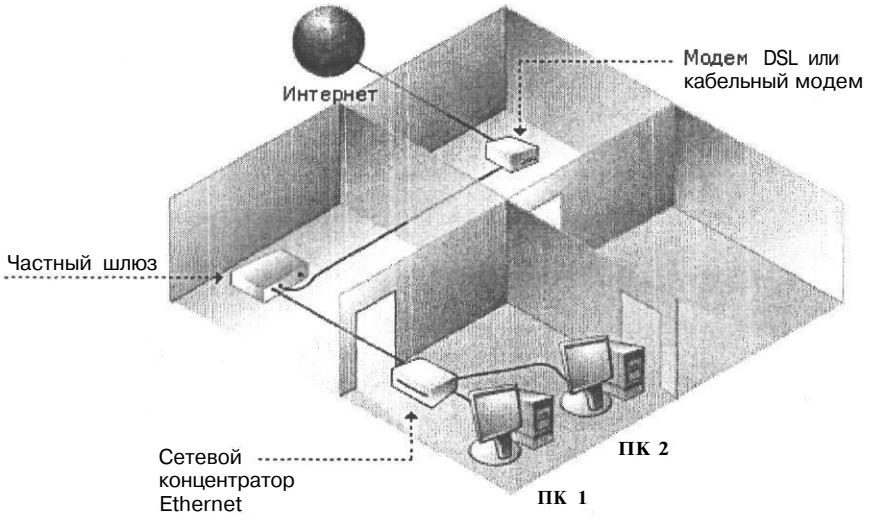



*Рис. 4.3. Подключение локальной сети к Интернету через частный шлюз*

Частный шлюз включает брандмауэр и заменяет узловой компьютер в качестве центрального блока для подключения к Интернету. Так как шлюз не содержит файлов, папок или других данных и не используется для управления компьютерами сети, он имеет более надежную степень защиты, чем узловой компьютер. И поэтому, если какой-то

неуполномоченный пользователь захочет обойти брандмауэр, то единственное, что он получит, это доступ к пустому устройству.

Конфигурация с частным шлюзом обладает следующими преимуществами:

- шлюз выступает в Интернете в качестве компьютера, скрывая компьютеры домашней или малой офисной сети;
- подключение к Интернету используется совместно всеми компьютерами в сети;
- нет необходимости держать один компьютер все время включенным для доступа в Интернет;

Недостатком использования частного шлюза являются дополнительные расходы на оборудование.

Из всего вышесказанного можно сделать вывод, что для создания дешевого и безопасного подключения домашней или малой офисной сети к Интернету следует воспользоваться средством общего доступа к подключению Интернета, имеющимся в Windows XP, а само подключение осуществлять с помощью модема по коммутируемой телефонной линии.

Напомним, что с помощью средства общего доступа один компьютер, называемый узловым, предоставляет свое подключение к Интернету в общий доступ для остальных компьютеров сети. При наличии общего доступа к подключению Интернета вы можете просматривать Web-страницы, в то время как ваш коллега на другом компьютере работает со своей электронной почтой.

В этой главе мы рассмотрим именно такое подключение.

## Выбор узлового компьютера общего доступа для подключения к Интернету

В домашней или малой офисной сети следует выбрать компьютер, который будет предоставлять свое подключение к Интернету в общее пользование всем остальным компьютерам сети. Такой компьютер, как уже отмечалось, называется узловым компьютером общего доступа к подключению Интернета (Internet Connection Sharing, ICS).

На узловом компьютере необходимо установить два сетевых подключения. Подключение по локальной сети, автоматически создаваемое в результате установки сетевого адаптера, обеспечивает соединение с компьютерами локальной сети. Второе подключение, использующее модем с пропускной способностью 56 Кбит/с, линию ISDN, DSL или кабельный модем, связывает эту сеть с Интернетом. Необходимо убедиться, что служба общего доступа к Интернету включена на втором подключении, обеспечивающем выход в Интернет. Таким образом, общее подключение соединит локальную сеть с Интернетом.

Чтобы определить, какой компьютер должен стать узловым компьютером, руководствуйтесь следующими соображениями.

- Этот компьютер должен работать под управлением Windows XP.
- Компьютер должен быть включен, чтобы остальные компьютеры сети могли получать доступ к Интернету. Если компьютер выключен, подключение к Интернету будет недоступно.

## Что нужно для подключения локальной сети к Интернету?

Чтобы осуществить подключение локальной сети к Интернету через модем с использованием средства общего доступа, вам нужно будет:

- заключить договор на обслуживание с поставщиком услуг Интернета и получить учетную запись;
- подобрать модем и установить его на узловом компьютере;
- создать на узловом компьютере подключение к Интернету;
- включить на узловом компьютере средство общего доступа к подключению Интернета;
- настроить все компьютеры локальной сети для доступа к общему подключению Интернета.

Далее мы подробно рассмотрим все вышеперечисленные шаги.

# Получение учетной записи у провайдера Интернета

Интернет представляет собой глобальную сеть - объединение большого количества компьютерных сетей. Хотя они и функционируют вместе как единый организм, но подключиться к Интернету можно, только соединившись по модему с одной из таких сетей.

Организации, имеющие компьютерную сеть, входящую в состав Интернета, и предоставляющие услуги доступа в остальную его часть, называются **провайдерами**,или **поставщиками услуг Интернета** (Internet Service Provider). Для получения возможности доступа в глобальную сеть необходимо заключить договор с одним из Интернет-провайдеров, который создаст для вас **учетную запись** (Internet Account). Учетная запись идентифицирует конкретного пользователя сетевых услуг и позволяет провайдеру контролировать объем предоставленного сервиса, чтобы определить сумму денег, которую пользователь должен заплатить.

## Советы по выбору провайдера

В каждом городе, как правило, существует несколько поставщиков услуг Интернета, из которых вам необходимо выбрать для себя наилучшего. Обычно услуги доступа в Интернет являются платными, но большинство провайдеров предоставляют несколько часов или дней для бесплатного доступа, что позволяет опробовать качество связи и сделать правильный выбор.

При выборе поставщика услуг Интернета следует руководствоваться следующей информацией, характеризующей его деятельность:

- стоимость подключения, форма оплаты - ежемесячная или почасовая, размер ежемесячной абонентской платы или стоимость 1 часа работы в Интернете;

- пропускная способность канала связи, по которому происходит подключение к другим, в первую очередь зарубежным провайдерам, обеспечивающим доступ к мировым ресурсам, и уровень загрузки канала. Чем выше пропускная способность канала и чем ниже уровень его загрузки, тем качественнее будет связь;
- качество телефонных линий АТС, по которым будет осуществляться подключение к серверу удаленного доступа поставщика услуг Интернета;
- степень загруженности модемов провайдера или, другими словами, насколько легко дозвониться до модема сервера удаленного доступа;
- наличие льготных тарифов на подключение в различное время суток, в частности, в ночное время, и их размер;
- возможность и уровень технической поддержки пользователей; получение консультаций, организация обучения, выезд специалиста к заказчику и т.д.

Многие поставщики услуг Интернета за небольшую плату или бесплатно предоставляют возможность пробного или тестового подключения в течение нескольких дней или нескольких часов. Такое пробное подключение позволяет практически оценить качество услуг данного провайдера, после чего заключить с ним постоянный договор или поискать другого провайдера.

Перечни предоставляемых услуг и их стоимость легко сравнить по прейскурантам. Следует не просто механически сравнивать перечни услуг, а учитывать их полезность применительно к вашим требованиям. Вполне вероятно, что вас мало интересует поддержка работы Perl-скриптов на сервере провайдера, зато требуется возможность читать и посылать сообщения в группы новостей **fido7.***.

Выбор оптимального тарифного плана значительно сократит ваши расходы. Например, если вы предполагаете подключаться к Интернету после работы, то выгоднее выбрать схему оплаты за доступ в вечернее или ночное время, когда цены обычно ниже.

Что же касается скорости и надежности связи с конкретными провайдерами Интернета, то проверить это можно только опытным путем, потому что тут многое зависит от качества физических каналов коммутируемой телефонной связи.

## Регистрация и получение информации для настройки доступа в Интернет

Итак, вы решили заключить договор с одним из поставщиков услуг Интернета. Зарегистрируйтесь у него и получите необходимую информацию, на основании которой вы сможете настроить программное обеспечение своего компьютера для связи с Интернетом.

Обязательная информация, предоставляемая пользователю провайдером Интернета, должна включать:

- имя пользователя (UserName, или Login) - имя, под которым вы зарегистрированы на сервере удаленного доступа провайдера. Обычно это имя вы можете выбрать сами;
- пароль (Password) - пароль для входа на сервер, который «работает» только вместе с вводом имени пользователя;
- телефонный номер для доступа по модему (Access Phone Number), по которому следует звонить для подключения к серверу удаленного доступа.

Кроме того, провайдер может предоставить дополнительную информацию, необходимую для настройки доступа в Интернет:

- имя хоста (Host Name) - имя Web-сервера вашего провайдера, на котором вы можете получить дополнительные сведения об услугах, расценках и др.;
- имя домена (Domain Name) - доменное имя, т.е. символьный адрес узла вашего провайдера в Интернете;
- протокол (Protocol) - тип протокола для связи с сервером удаленного доступа. Чаще всего это PPP. Использовавшийся ранее протокол SLIP теперь применяется редко;
- адреса DNS (DNS Server Address) - IP-адреса серверов DNS. Эти серверы преобразуют доменный адрес компьютера в IP-адрес и определяют местоположение узла с данным адресом. Например, доменный адрес Web-сервера фирмы ЮМ www.ibm.com будет преобразован сервером DNS в такой IP-адрес: 207.68.137.53;
- IP-адрес (IP Address) - IP-адрес вашего компьютера в Интернете. Указывается только в том случае, если вам предоставляется статический IP-адрес;
- адрес электронной почты (E-mail address) - ваш адрес электронной почты, на который вы будете получать почтовую корреспонденцию. Этот адрес состоит из имени пользователя и доменного имени узла провайдера, разделенных символом @;
- сервер входящей почты (POP3) - имя сервера входящей почты;
- сервер исходящей почты (SMTP) - имя сервера исходящей почты;
- сервер новостей (NNTP) — имя сервера новостей;
- сценарий для подключения к серверу удаленного доступа.

Следует отметить, что в полученной от провайдера информации могут отсутствовать некоторые из перечисленных сведений, например IP-адрес сервера DNS, или присутствовать некоторые другие сведения, например статический IP-адрес или отдельный пароль для электронной почты или новостей. Ответы на возникшие вопросы по поводу параметров подключения лучше получить у провайдера.

Получили нужную информацию от провайдера? Пора приобретать модем и настраивать доступ в Интернет.

## Выбор модема

Компьютер сам по себе может обрабатывать только цифровые данные и не приспособлен для их передачи по обычным аналоговым каналам связи. Поэтому для связи компьютеров друг с другом через телефонную сеть используются специальные устройства, называемые модемами.

Слово **модем** (Modem) представляет собой сокращение от словосочетания «модулятор-демодулятор». При передаче данных модем преобразует (модулирует) цифровые компьютерные данные в аналоговый звуковой сигнал. При приеме данных происходит обратный процесс - модем преобразует (демодулирует) аналоговый звуковой сигнал в цифровые компьютерные данные.

Если в тот момент, когда модем передает или принимает данные, подключиться к линии, например, с помощью параллельного телефонного аппарата, то можно услышать писки и шипение. Это и есть аналоговый сигнал, который передает или принимает модем. Естественно, каждый компьютер, участвующий в приме/передаче данных, должен иметь свой модем.

Кроме Интернета, модемы позволяют компьютерам связываться друг с другом и с различными глобальными сетями, например Фидонет, Спринт и другими.

Обычно консультацию по вопросу качества конкретных типов модемов можно получить, позвонив в службу поддержки любого Интернет-провайдера. Здесь же мы расскажем о том, что необходимо знать для правильного выбора модема для коммутируемой телефонной линии.

## Сравнительная характеристика модемов

В настоящее время существует огромное количество моделей модемов. Все они отличаются друг от друга следующими основными характеристиками:

- фирма-производитель;
- параметры конкретной модели (в основном это максимальная скорость приема/передачи данных);
- конструктивный вариант исполнения;
- стоимость.

### Фирмы-производители модемов

От фирмы-производителя во многом зависит качество модема. Вот примерный перечень фирм, производящих наиболее дорогие и качественные модемы:

- Zyxel;
- US Robotics;
- Rockwell;
- MultiTech;
- Motorola.

Особенно высоким качеством отличаются модемы первой тройки производителей, которые уже много лет выпускают модемы, стабильно работающие на наших отечественных, сильно зашумленных телефонных линиях.

Немного ниже по качеству, но значительно более дешевые модемы выпускаются фирмами:

- Acer;
- Acorp;
- Genius.

Фирма Eline производит продукцию весьма невысокого качества. Модемы других малоизвестных фирм тоже лучше не покупать.

## Скорость и надежность связи

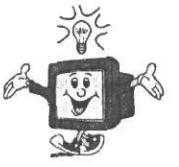
Имеет немаловажное значение и конкретная модель модема. Например, из модемов фирмы Zyxel несколько худшее качество имеет модель Omni российской сборки.

Максимальная скорость передачи данных у всех современных модемов для коммутируемых телефонных линий составляет около 56 килобит в секунду, сокращенно - 56 Кбит/с, или просто 56K.

В принципе, если определяющим фактором является цена, можно купить модем со скоростью передачи данных 14,4-33,6K. Но тогда, сэкономив на покупке быстрого модема, вы будете переплачивать из-за более медленного доступа в Интернет.

Фирмы-производители модемов создали три независимые технологии, обеспечивающие передачу данных через модем со скоростью 56K: K56Flex, V90 и X2. В последнее время появились модемы, поддерживающие модификацию протокола V90 - протокол V92.

*Следует заметить, что не все поставщики услуг Интернета могут обеспечить максимальную скорость 56K, а только те, которые на своих модемных входах используют технологию K56Flex, V90 (V92) или X2.*



Важнейшим параметром, определяющим продолжительность времени непрерывной работы на линии, служит надежность удержания несущей частоты при возникновении помех. Но данная характеристика модемов поддается определению, в основном, лишь практическим путем. Поэтому рекомендуется ориентироваться на фирму-производителя и рекомендации специалистов.

## Внешний и внутренний варианты конструктивного исполнения

Теперь рассмотрим характеристики модемов, не влияющие на скорость и качество связи, но которые могут повлиять на ваш выбор конкретной модели.

Модемы изготавливаются в двух основных вариантах конструктивного исполнения:

- внешний - коробка размером чуть побольше мыльницы со светодиодными лампочками-индикаторами, подключаемая к последовательному или параллельному порту;
- внутренний - представляет собой модемную карту, вставляемую в один из слотов расширения на материнской плате компьютера.

Полезно сравнить различные характеристики внешнего и внутреннего модема одной фирмы, имеющие одинаковую скорость передачи данных.

| Характеристика | Внешний модем | Внутренний модем |
|---|---|---|
| Скорость передачи данных | одинаковая | |
| Надежность связи | одинаковая | |
| Возможность приема и передачи факсимильных сообщений | имеется у обоих | |

| Характеристика | Внешний модем | Внутренний модем |
|---|---|---|
| Возможность приема и передачи голосового сигнала (Voice) при подключении микрофона и наушников | имеется у обоих | |
| Компактность | выполнен в виде отдельного устройства | находится внутри корпуса компьютера |
| Наличие блока питания, подключаемого в отдельную розетку | да | нет |
| Стоимость | выше стоимости внутреннего модема примерно в два раза | ниже стоимости внешнего модема примерно вдва раза |

Из приведенной таблицы видно, что различия между внутренним и внешним модемом не очень значительные. Каждый из них имеет свои плюсы и минусы, так что в данном случае выбор остается за вами.

## Аппаратные и программные модемы

Важно знать, что внутренние модемы бывают двух разновидностей:

- аппаратные (hardware-модемы);
- программные (software- или win-модемы).

Обычные, или аппаратные модемы самостоятельно занимаются обработкой данных, используя вычислительные мощности микросхем, расположенных на плате модема.

В противоположность им программные модемы перекладывают эти функции на центральный процессор компьютера, что может быть чревато замедлением работы, зависаниями и невозможностью работы в других операционных системах, кроме Windows (именно поэтому они еще называются win-модемами). Поэтому программные модемы лучше не использовать, хотя они и самые дешевые из всех существующих разновидностей модемов.

## Соотношение цены и качества

Такую характеристику, как стоимость модемов, нельзя рассматривать отдельно. Скорее всего, следует производить сравнительную оценку их с точки зрения наилучшего соотношения: цена/качество.

В этом рейтинге лидируют модемы фирмы Acorp со скоростью передачи данных 56K. Данные модемы выпускаются во внешнем и внутреннем исполнении. Оба варианта неплохо работают на наших телефонных линиях. Что же касается цены, то она очень невысока: внешний модем стоит около $55, а внутренний - вдвое дешевле.

Мы рассмотрели основные характеристики модемов, которые производятся в настоящее время, и теперь вы сами сможете сделать правильный выбор.

Хотелось бы только дать последний совет: не покупайте изделия плохого качества, иначе вы не сможете нормально работать в Интернете из-за постоянных разрывов связи.

# Физическое подключение модема к компьютеру

Способы подключения к компьютеру внутреннего и внешнего модемов существенно различаются. Рассмотрим каждый из них.

## Внешний модем

Проще всего подключить к компьютеру внешний модем, хотя и здесь могут встретиться определенные трудности, поэтому лучше расскажем обо всем по порядку.

> Откройте коробку с модемом и распакуйте все принадлежности к нему.

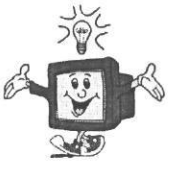
➤ Выключите компьютер.

➤ Соедините последовательные порты компьютера и модема с помощью кабеля, имеющего подходящие разъемы. Последовательные порты обычно располагаются на задней стенке компьютера и имеют штырьковые разъемы по 9 или 25 штырьков. В случае необходимости там же можно найти параллельный порт и USB.

> Вытащите из телефонного аппарата кабель телефонной линии и подключите его в гнездо модема **Line** (Линия).

➤ Возьмите такой же кабель из комплекта модема и подключите с его помощью телефонный аппарат в гнездо **Phone или Telephone** (Телефон) модема.

*Если у вас старый отечественный телефонный аппарат, то придется купить универсальную телефонную розетку, куда можно будет параллельно подключить модем и этот телефон, или заняться творческим процессом обрезки, зачистки и соединения импортных телефонных проводов с отечественными. В последнем случае вам следует знать, что модем для соединения с линией использует только два средних контакта (обычно это красный и зеленый провода).*



➤ Поднимите трубку телефонного аппарата для проверки правильности соединения. Должен быть слышен длинный гудок телефонной станции.

➤ Подключите блок питания к модему с помощью провода с пальчиковым разъемом, вставив его в круглое гнездо **Power** (Питание) модема.

➤ Подключите блок питания к электрической розетке (220 вольт).

➤ Измените текущее положение выключателя питания на модеме с Off (Выключено) на On (Включено). На передней панели модема должны загореться несколько светодиодных индикаторов.

## Внутренний модем

Подключение внутреннего модема требует разборки компьютера. Если вы делаете это впервые, то можете позвать кого-нибудь на помощь. Однако можно попробовать все сделать и самому.

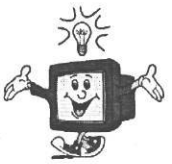
> Откройте коробку с модемом и распакуйте все принадлежности к нему.

➤ Выключите компьютер.

➤ Вытащите вилку питания системного блока компьютера из электрической розетки.

> Снимите крышку системного блока компьютера, открутив с помощью крестообразной отвертки несколько болтов на задней панели.

*Если у вас современный корпус, то, может быть, крышка системного блока открывается и без отвертки. Чаще всего требуется нажать на кнопку, отодвигающую защелку, а затем снять крышку. Подробности об этом можно узнать в техническом руководстве к компьютеру.*

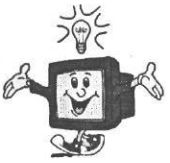


> Выберите подходящий по размеру свободный шинный разъем на материнской плате (MotherBoard или MainBoard). Современные модемные платы обычно вставляются в разъем системной шины PCI, а старые - в разъем ISA.

➤ Открутите и вытащите заглушку на задней панели системного блока напротив выбранного разъема. Если же она закреплена «намертво» без болтов, то выломайте ее.

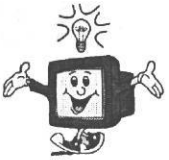
➤ Если модем имеет перемычки, установите их в режим Plug and Play для Windows XP или, если этот режим недоступен, - для вашей операционной системы. Инструкции по установке перемычек ищите в документации модема.

*На старых моделях внутренних модемов нужно еще установить переключатели (Jumpers), которые определяют номер используемого последовательного порта (COM) и прерывания (IRQ). Лучше всего использовать режим автоматического определения, а если он не предусмотрен - выбрать комбинацию: COM 4 и IRQ 3. Подробности о выборе номера порта и прерывания можно узнать в техническом руководстве к модему.*



➤ Слегка покачивая, вставьте модемную плату в разъем и убедитесь, что она вошла туда до упора.

*При установке модема в разъем не прилагайте чрезмерных усилий, чтобы не повредить материнскую плату. Лучше вытащите модем и попробуйте вставить его снова.*



➤ Прикрутите модемную плату болтом к корпусу системного блока в том месте, где раньше была закреплена заглушка.

➤ Наденьте и закрепите болтами крышку системного блока компьютера.

➤ Вытащите из телефонного аппарата кабель телефонной линии и подключите его в гнездо модема **Line** (Линия).

- Возьмите такой же кабель из комплекта модема и подключите с его помощью телефонный аппарат в гнездо **Phone** или **Telephone** (Телефон) модема.

После подключения поднимите трубку телефонного аппарата для проверки правильности соединения. Должен быть слышен длинный гудок телефонной станции.

# Установка драйвера модема в Windows XP

Теперь следует включить компьютер и установить драйверы модема - специальные программы, управляющие работой устройства.

## Установка модемов Plug and Play

Большинство современных модемов имеют функцию автоматической конфигурации, называемую Plug and Play (Включай и работай). Это значит, что устройство при включении сообщает операционной системе информацию о себе, после чего выполняется автоматическая его настройка. Если у вас именно такой модем, то, как только Windows обнаружит его, на экране появится сообщение: **Обнаружено новое устройство** (Windows detects a new hardware), а вслед за ним - диалог **Мастер нового оборудования** (New Hardware Wizard) (Рис. 4.4), в котором будет указано название вашего модема и предложено несколько вариантов установки драйвера.

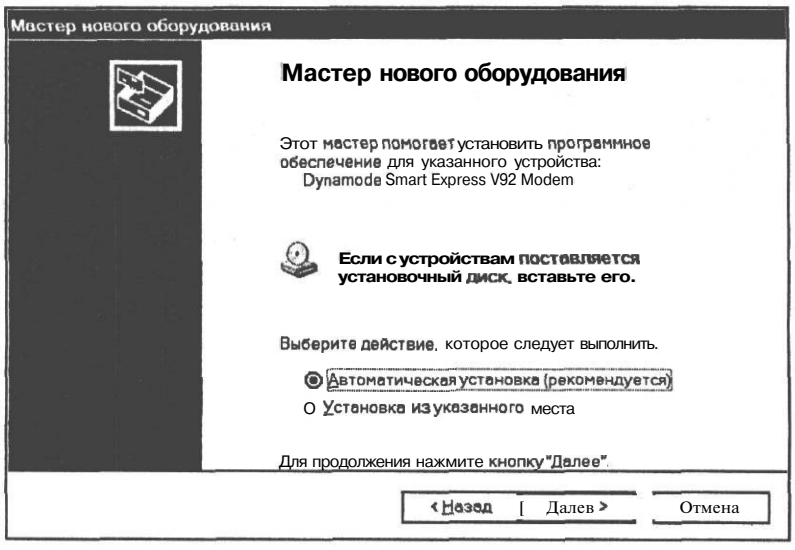



*Рис. 4.4. Диалог **Мастер нового оборудования** (New Hardware Wizard)*

Напомним, что мастером называется программа, которая с помощью последовательности диалогов позволяет выполнить определенную задачу.

- Если в комплект поставки вашего модема входит дискета или диск с драйверами, выберите в следующем диалоге Мастера вариант установки драйвера изготовителя (Manufacturer driver) и нажмите кнопку OK. Вам будет предложено вставить диск с драйверами модема. Выполнив это, следуйте дальнейшим указаниям программы.
- Если же у вас нет дискеты с драйверами, то выберите вариант установки драйвера Microsoft, входящего в поставку операционной системы и следуйте указаниям программы.

## Установка модема «вручную»

Но, возможно, что ваш модем не является устройством Plug and Play и операционная система при загрузке не обнаружит его. В таком случае драйвер модема придется установить вручную, как описано далее на примере операционной системы Windows XP.

Если у вас внешний модем, то убедитесь, что он включен. На передней панели модема должны светиться несколько светодиодных индикаторов. Внутренний модем включается вместе с компьютером.

- Включите компьютер и дождитесь окончания загрузки Windows.
- Убедитесь, что не запущены программы, использующие модемы и последовательные порты компьютера, в том числе: HyperTerminal, Прямое кабельное соединение (Direct Cable Connection), Телефон (Phone Dialer), Установка связи (Connection).
- Выберите команду меню Пуск * Панель управления (Start ◆ Control Panel). На экране появится окно Панель управления (Control Panel) (Рис. 4.5).

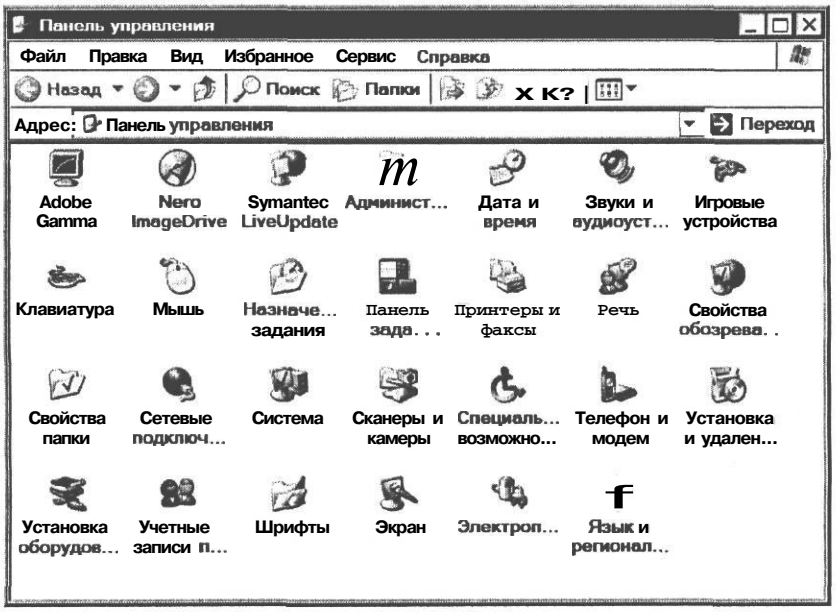



*Рис. 4.5. Окно **Панель управления** (Control Panel)*

> В окне **Панель управления** (Control Panel) дважды щелкните мышью на значке **Телефон и модем** (Phone and Modem Options) и в появившемся диалоге **Телефон и модем** (Phone and Modem Options) выберите вкладку **Модемы** (Modems) (Рис. 4.6).

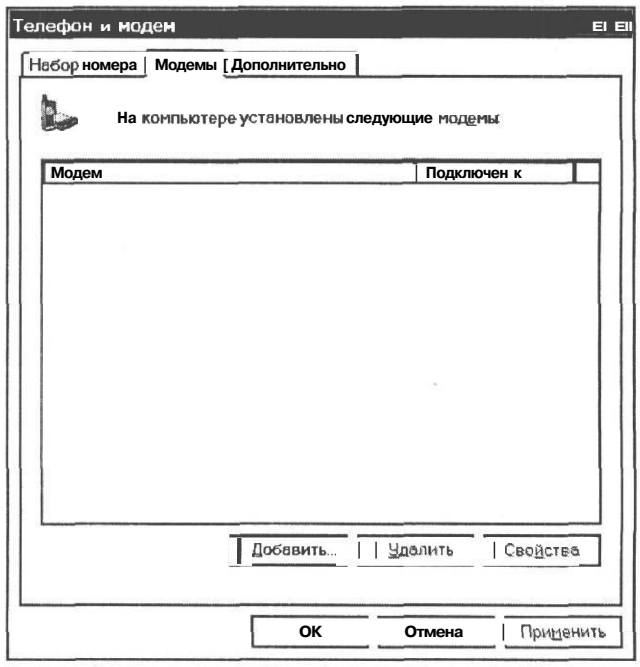
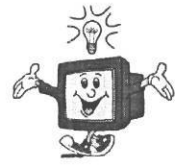



*Рис. 4.6. Вкладка **Модемы** (Modems) диалога **Телефон и модем** (Phone and Modem Options)*

*Если у вас на компьютере модемы раньше не устанавливались, то список модемов будет пуст. В противном случае в списке могут присутствовать один или несколько модемов. Как вы, наверное, уже догадались, их можно безболезненно удалить, для чего выделите название модема щелчком мыши и нажмите кнопку **Удалить** (Remove).*



➤ На вкладке **Модемы** (Modems) диалога **Телефон и модем** (Phone and Modem Options) нажмите кнопку **Добавить** (Add). На экране появится первый диалог **Мастер установки оборудования** (Add Hardware Wizard) (Рис. 4.7).

В этом диалоге предлагается выбрать автоматический или ручной режим определения типа модема. Поскольку мы рассматриваем случай, когда модем не определился системой сразу, то будем выбирать тип модема сами.

> Установите флажок **Не определять тип модема (выбор из списка)** (Don't detect my modem: I will select it from a list) и нажмите кнопку **Далее** (Next). На экране появится второй диалог мастера **Мастер установки оборудования** (Add Hardware Wizard), позволяющий вручную выбрать изготовителя и модель модема (Рис. 4.8).

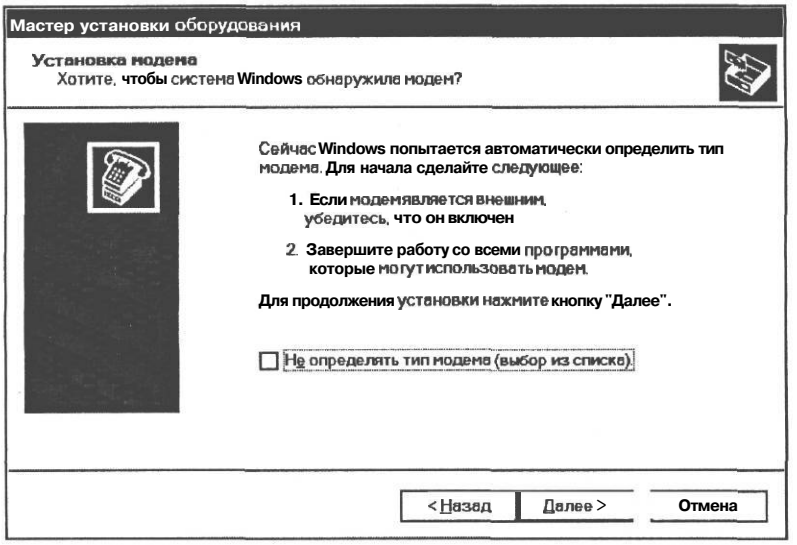



*Рис. 4.7. Первый диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard)*

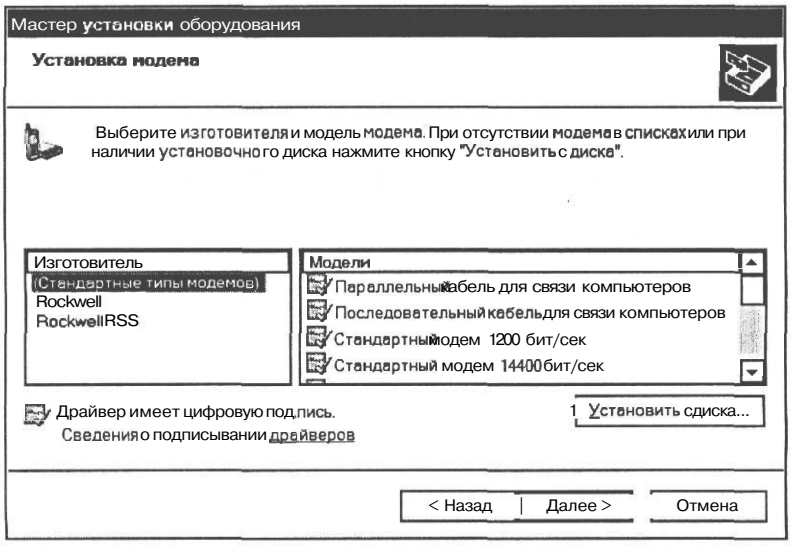



*Рис. 4.8. Второй диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard)*

В этом диалоге имеются две возможности по установке драйвера модема:

- выбрать модем из списка драйверов, имеющихся в Windows;
- указать путь к диску, на котором записан драйвер модема.

Обычно новый модем комплектуется диском с драйвером, разработанным для этого модема самим изготовителем, поэтому рекомендуется установить именно его. Если же модем не новый или диск изготовителя отсутствует, то можно выбрать тип модема из списка.

При установке модема, для которого нет диска с драйверами, во втором диалоге мастера **Мастер установки оборудования** (Add Hardware Wizard) (Рис. 4.8) выполните следующие действия.

- Передвигаясь по списку **Изготовитель** (Manufacturer) с помощью полосы прокрутки, найдите фирму-производитель модема и щелчком мыши выделите ее. После этого в списке **Модели** (Models) отобразится перечень модемов данного изготовителя.
- В списке Модели (Models) найдите и щелчком мыши выделите конкретную модель вашего модема.

***Если в списке Модели (Models) нужная модель модема отсутствует, и диска с драйвером тоже нет в наличии, в списке Изготовитель (Manufacturer) выделите элемент Стандартные типы модемов (Standard Modem Types) и подберите подходящую модель с требуемой скоростью обмена данными.***

- Нажмите кнопку **Далее** (Next). На экране появится диалог **Мастер установки оборудования** (Add Hardware Wizard), в котором предлагается выбрать для модема коммуникационный порт (Рис. 4.12).

При установке модема, для которого есть диск с драйверами, во втором диалоге **Мастер установки оборудования** (Add Hardware Wizard) (Рис. 4.8) выполните следующие действия.

- Щелкните мышью на кнопке **Установить с диска** (Have Disk). На экране появится диалог **Установка с диска** (Install From Disk) (Рис. 4.9).

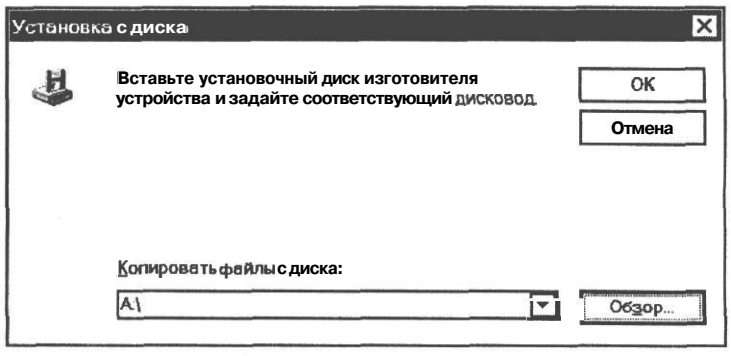



*Рис. 4.9. Диалог* ***Установка с диска*** *(Install From Disk)*

- В поле ввода **Копировать файлы с диска** (Copy manufacturer's files from) с помощью клавиатуры введите имя диска и путь к папке с драйвером.
- Если вы не знаете точный путь, нажмите кнопку **Обзор** (Browse), чтобы выбрать нужный диск и папку. На экране появится диалог **Поиск файла** (Locate File) (Рис. 4.10).
- В диалоге **Поиск файла** (Locate File) выберите диск и папку и нажмите кнопку **Открыть** (Open) для подтверждения вашего выбора.

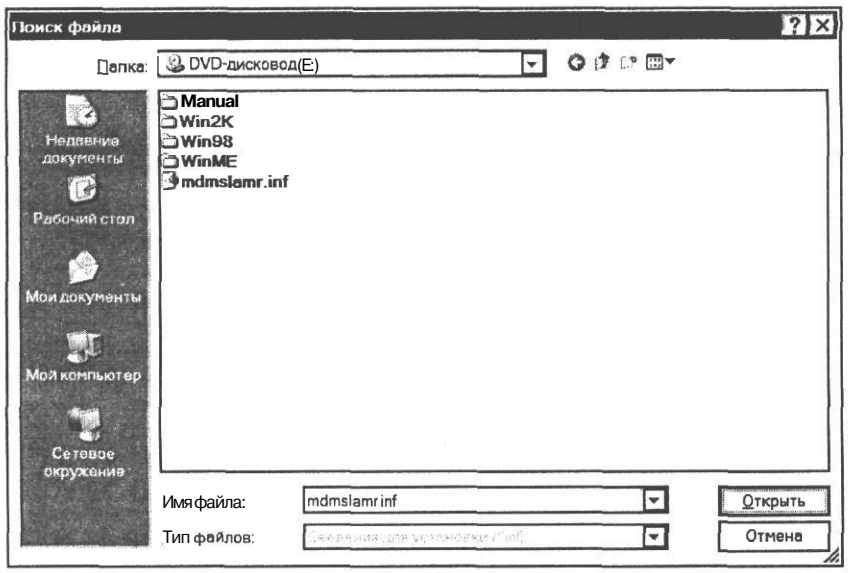



*Рис. 4.10. Диалог* ***Поиск файла*** *(Locate File)*

> Нажмите кнопку OK в диалоге **Установка с диска** (Install From Disk). На экране появится следующий диалог **Мастер установки оборудования** (Add Hardware Wizard), в котором предлагается выбрать модель модема (Рис. 4.11).

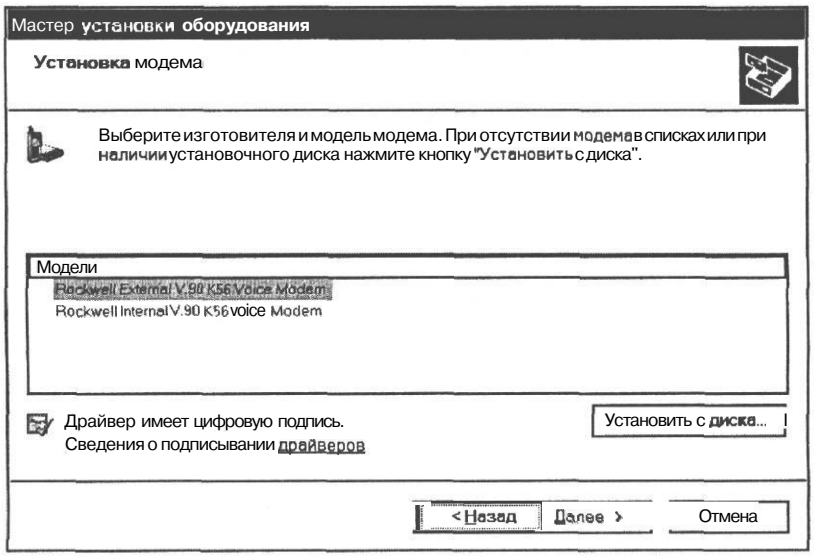



*Рис. 4.11. Диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard) для выбора модели модема*

➤ В списке **Модели** (Models) выберите модель модема и нажмите кнопку **Далее** (Next). На экране появится следующий диалог **Мастер установки оборудования** (Add Hardware Wizard), в котором предлагается выбрать для модема коммуникационный порт (Рис. 4.12).

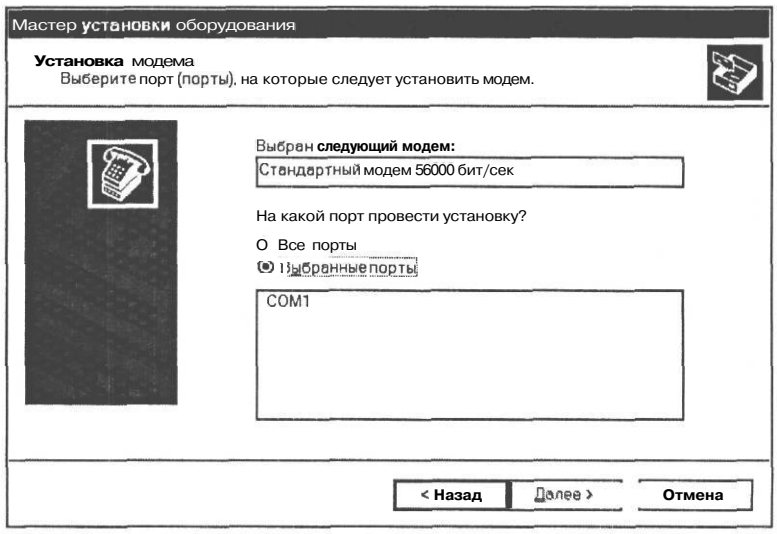



*Рис. 4.12. Диалог **Мастер установки оборудования** (Add Hardware Wizard) для выбора коммуникационного порта*

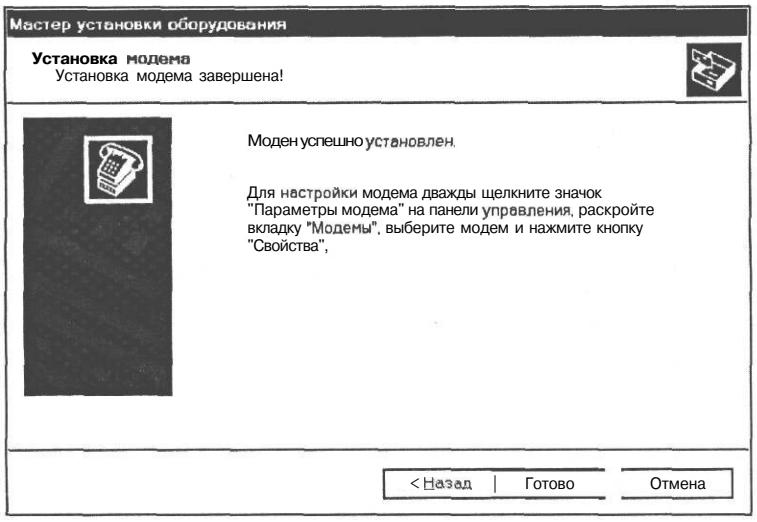
> Щелчком мыши выберите коммуникационный порт **COM1**, **COM2** или **COM3** для подключения модема и нажмите кнопку **Далее** (Next).

На экране может появиться диалог, в котором предупреждается о несовместимости выбранного вами драйвера с операционной системой. В случае появления такого сообщения вы можете либо вернуться к предыдущим диалогам мастера и выбрать для вашего модема другой драйвер, либо попытаться использовать выбранный, нажав кнопку **Все равно продолжить** (Continue Anyway).

После выбора коммуникационного порта на экране появится заключительный диалог **Мастер установки оборудования** (Add Hardware Wizard), в котором сообщается об успешной установке модема (Рис. 4.13).

➤ Нажмите в этом диалоге кнопку **Готово** (Finish). **Мастер установки оборудования** (Add Hardware Wizard) завершит работу, а в списке модемов диалога **Телефон и модем** (Phone and Modem Options) появится новый модем (Рис. 4.14).

Теперь, когда модем установлен в системе, желательно проверить работоспособность подключенного устройства.




*Рис, 4.13. Заключительный диалог* ***Мастер установки оборудования*** *(Add Hardware Wizard)*

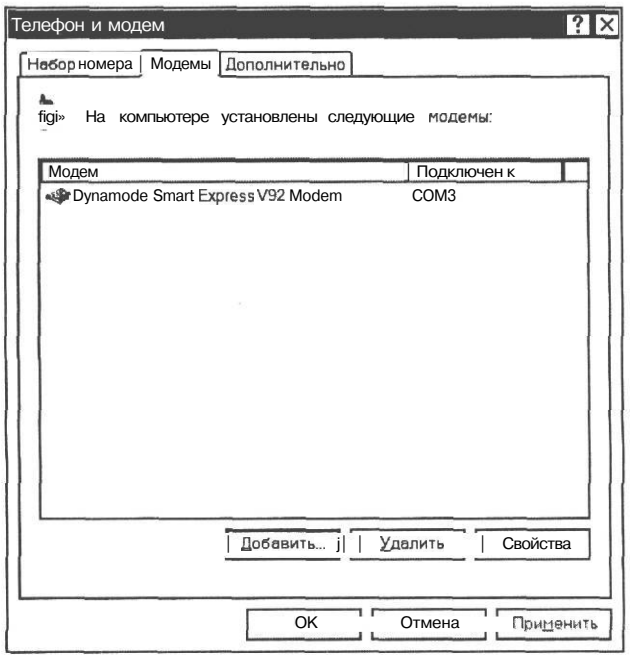



*Рис. 4.14. Новый модем установлен*

## Проверка модема

Проверка модема выполняется с помощью диалога **Свойства** (Properties).

➤ В диалоге **Телефон и модем** (Phone and Modem Options) (Рис. 4.14) выберите установленный модем в списке модемов и нажмите кнопку **Свойства** (Properties). На экране появится диалог Свойства (Properties) с именем выбранного модема в заголовке (Рис. 4.15).

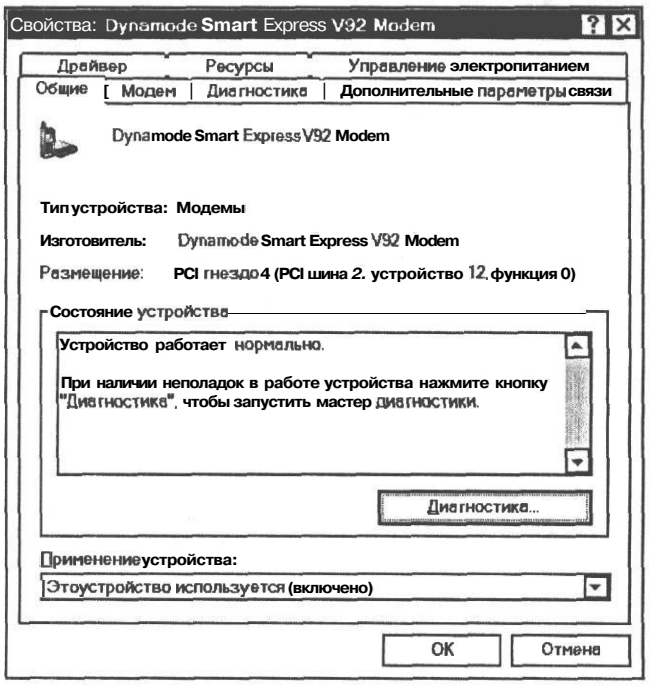



*Рис. 4.15. Диалог* ***Свойства*** *(Properties)*

Как мы видим из сообщения в текстовом поле диалога, устройство работает нормально.

➤ Щелкните мышью на ярлыке **Диагностика** (Diagnostics) для перехода на соответствующую вкладку (Рис. 4.16).

➤ Нажмите кнопку **Опросить модем** (Examine Modem). В течение нескольких секунд произойдет обмен данными с модемом, и в нижней части диалога появятся результаты опроса модема (Рис. 4.17).

В таблице результатов можно увидеть посылаемые драйвером команды и ответы модема на них.

➤ Прокручивая таблицу с помощью полосы прокрутки, просмотрите ответы модема на AT-команды. В ответах модема не должно содержаться ошибок.

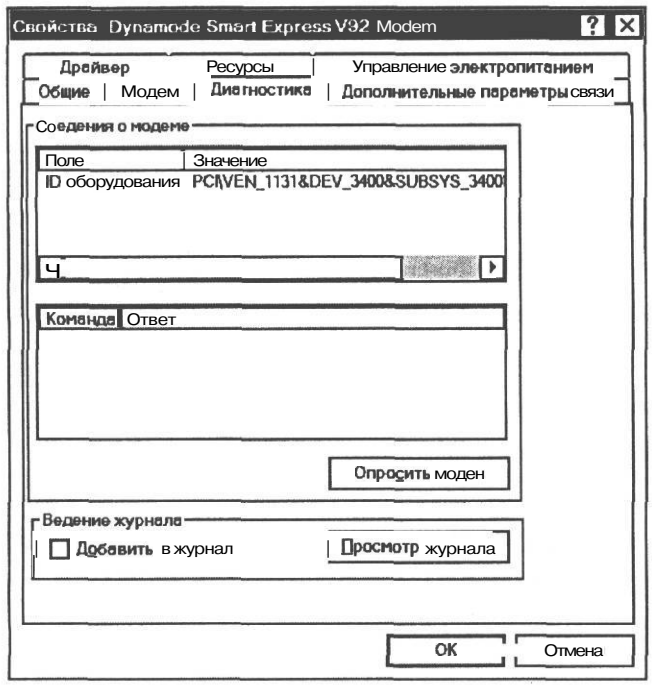



*Рис. 4.16.* ***Вкладка Диагностика*** *(Diagnostics) диалога* ***Свойства*** *(Properties)*

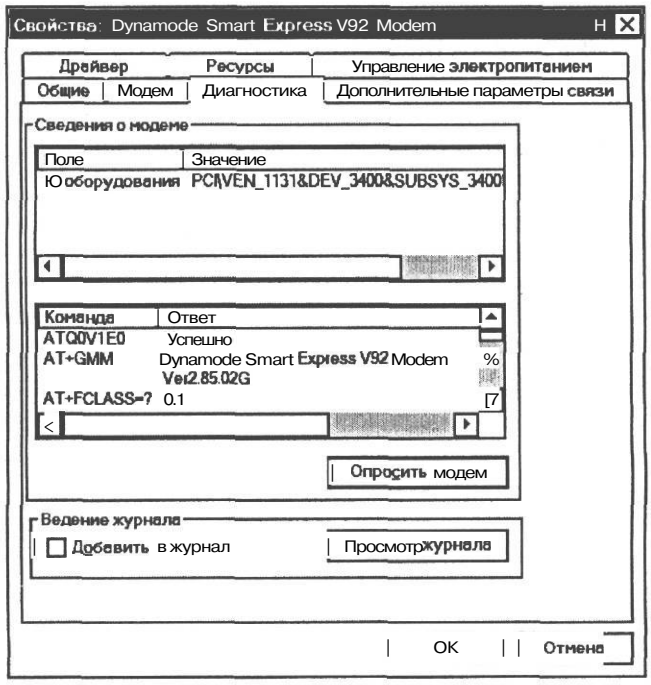



*Рис. 4.17. Результаты опроса модема*

Если вы обнаружили хотя бы одну команду, завершившуюся неуспешно (неподдерживаемые команды не в счет), это может быть вызвано следующими причинами:

- установленный драйвер не подходит для данного модема;
- неисправно оборудование: модем, соединительный кабель или коммуникационный порт.

> Щелкните мышью на кнопке OK, чтобы закрыть диалог Свойства (Properties).

➤ Закройте также диалог Телефон и модем (Phone and Modem Options).

Чтобы исправить ошибки, попробуйте сделать следующее:

- заменить драйвер;
- подключить модем к другому коммуникационному порту;
- заменить модем с соединительным кабелем.

## Создание и настройка удаленного подключения для доступа в Интернет в Windows XP

Чтобы узловой компьютер вашей локальной сети мог подключаться к Интернету, необходимо создать подключение к провайдеру. Подключение по своей сути представляет собой совокупность параметров, необходимых Windows для инициирования и поддержания модемной связи с другими компьютерами или сетями. После того как подключение будет создано, модем сможет звонить на сервер удаленного доступа вашего провайдера, открывая таким образом доступ в Интернет. Напомним еще раз, что подключение следует создать на узловом компьютере с операционной системой Windows XP.

Создание подключения осуществляется с помощью Мастера новых подключений (New Connection Wizard). Эта программа входит в состав Windows XP и устанавливается по умолчанию, чтобы обеспечить быстрое подключение к сети.

> Нажмите кнопку Пуск (Start) на Панели задач (Taskbar) и в появившемся главном меню Windows XP выберите команду Все программы ◆ Стандартные ◆ Связь ◆ Мастер новых подключений (All Programs * Accessories ◆ Communications * New Connection Wizard). На экране появится первый диалог Мастер новых подключений (New Connection Wizard) (Рис. 4.18).

Мастер новых подключений (New Connection Wizard) с помощью последовательных диалогов поможет нам создать новое подключение и выполнить все необходимые настройки. *В* первом диалоге описывается его назначение.

> Нажмите кнопку Далее (Next). На экране появится следующий диалог Мастера новых подключений (New Connection Wizard), в котором предлагается выбрать тип сетевого подключения (Рис. 4.19).

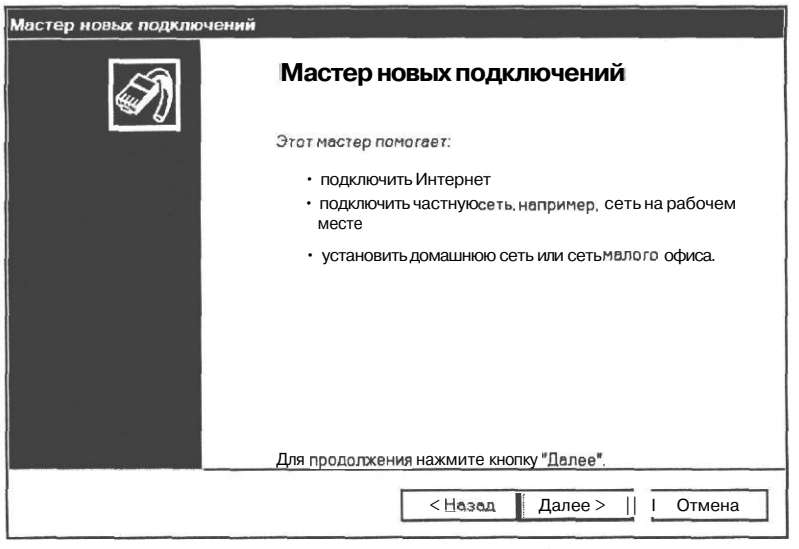



*Рис. 4.18. Первый диалог* ***Мастер новых подключений*** *(New Connection Wizard)*

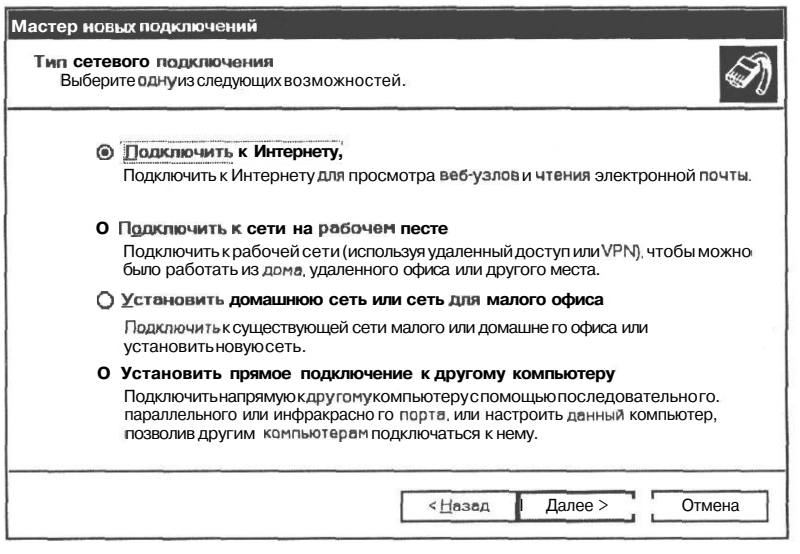



*Рис. 4.19. Второй диалог* ***Мастер новых подключений*** *(New Connection Wizard)*

Так как мы создаем подключение к Интернету, следует выбрать именно этот вариант.

> Установите переключатель **Подключить к Интернету** (Connect to the Internet) и нажмите кнопку **Next** (Далее). На экране появится третий диалог **Мастер новых подключений** (New Connection Wizard) (Рис. 4.20).

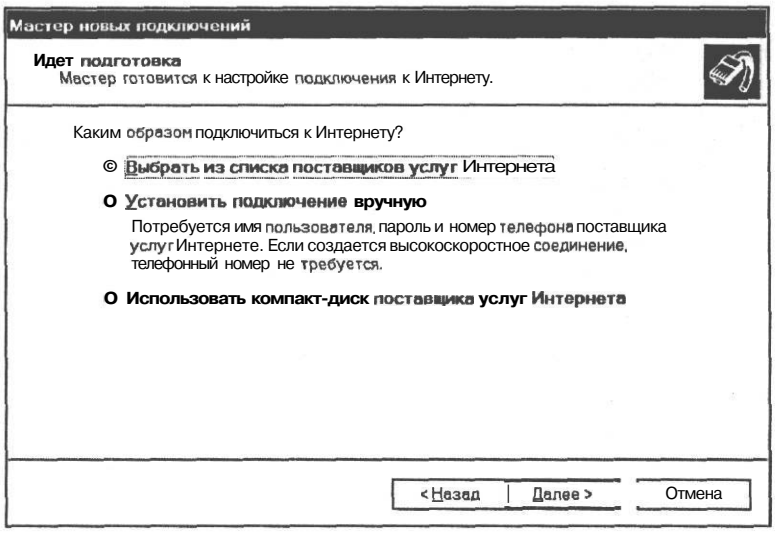



*Рис. 4.20. Третий диалог* ***Мастер новых подключений*** *(New Connection Wizard)*

В этом диалоге необходимо выбрать способ подключения. Для подключения мы будем использовать информацию, полученную от провайдера Интернета.

➤ Установите переключатель **Установить подключение вручную** (Set my connection manually) и нажмите кнопку **Далее** (Next). На экране появится следующий диалог **Мастер новых подключений** (New Connection Wizard) (Рис. 4.21).

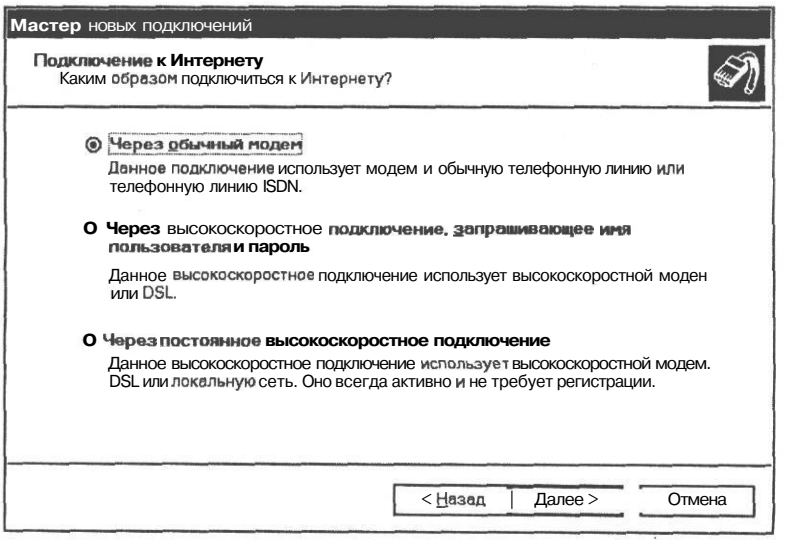



*Рис. 4.21. Четвертый диалог* ***Мастер новых подключений*** *(New Connection Wizard)*

Теперь следует выбрать тип подключения. Здесь мы рассматриваем только подключение через обычный модем.

➤ Убедитесь в том, что установлен переключатель **Через обычный модем** (Connect using a dial-up modem), и нажмите кнопку **Далее** (Next). На экране появится пятый диалог **Мастер новых подключений** (New Connection Wizard) (Рис. 4.22).

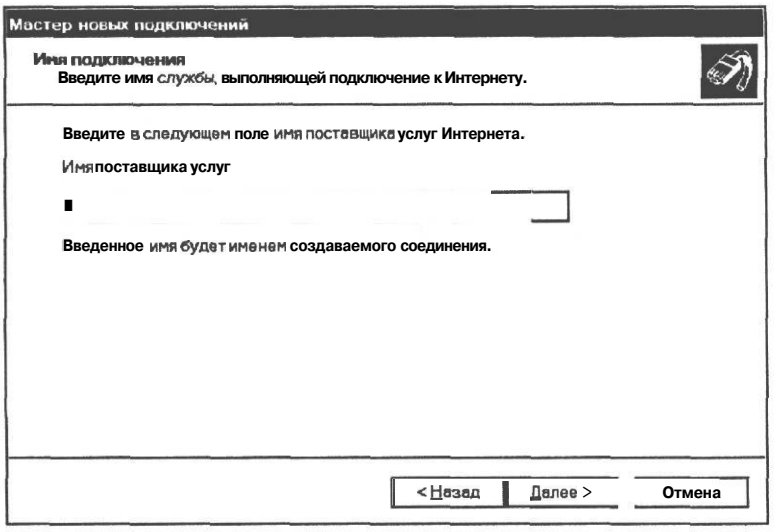



*Рис. 4.22. Пятый диалог* ***Мастер новых подключений*** *(New Connection Wizard)*

*В* этом диалоге следует указать имя вашего поставщика услуг Интернета. Это имя будет указано на значке подключения.

➤ В поле ввода **Имя поставщика услуг** (ISP name) введите имя вашего провайдера, например **Мой провайдер,** и нажмите кнопку **Далее** (Next). На экране появится шестой диалог **Мастер новых подключений** (New Connection Wizard), предлагающий ввести номер телефона провайдера (Рис. 4.23).

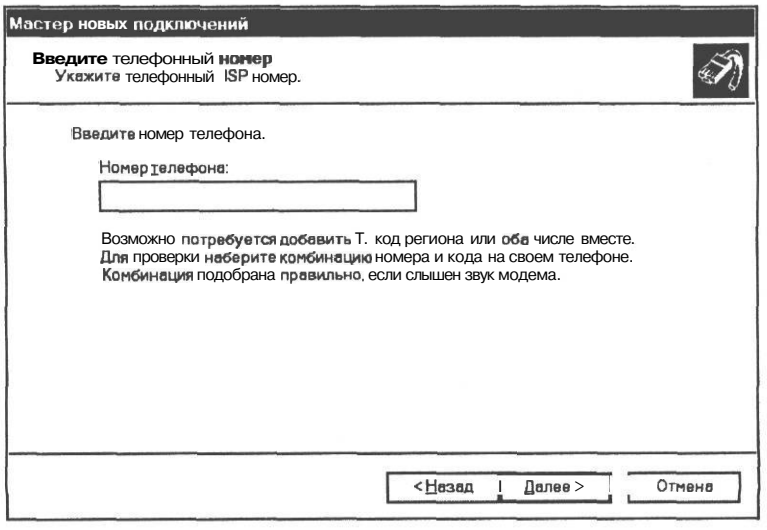



*Рис. 4.23. Шестой диалог* ***Мастер*** **новых** ***подключений*** *(New Connection Wizard)*

Здесь следует указать номер телефона, по которому модем будет звонить на сервер удаленного доступа вашего провайдера. Ввести нужно только один номер. Если вы получили у провайдера несколько телефонных номеров, то мы укажем их позднее.

Операционная система Windows XP по умолчанию использует тоновый набор номера. Но так как в телефонных сетях России и стран СНГ используется импульсный набор, следует перед номером обязательно поставить английский символ p, например **p555-25-69.**

➤ В поле ввода **Номер телефона** (Phone number) введите основной номер телефона, если их несколько, и нажмите кнопку **Далее** (Next). На экране появится седьмой диалог **Мастера новых подключений** (New Connection Wizard) (Рис. 4.24).

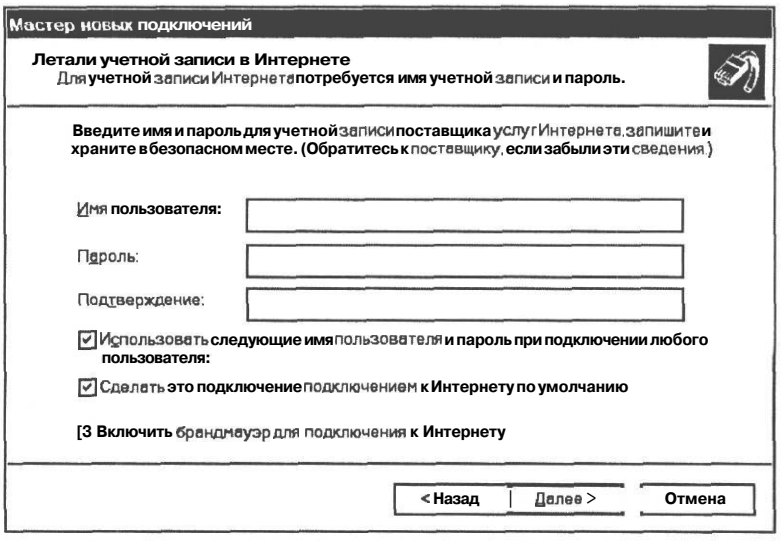



*Рис. 4.24. Седьмой диалог* ***Мастера новых подключений*** *(New Connection Wizard)*

В этом диалоге необходимо ввести сведения, которые будут идентифицировать вас на сервере удаленного доступа поставщика услуг Интернета - имя пользователя и пароль. Эту информацию вы получили у провайдера.

➤ В поле ввода **Имя пользователя** (User name) введите имя, указанное провайдером.

> В поле ввода **Пароль** (Password) введите пароль для доступа, предоставленный провайдером.

➤ В поле ввода **Подтверждение** (Confirm password) повторите указанный пароль.

Будьте внимательны при вводе имени и пароля. Большинство ошибок подключения происходят именно из-за неправильного указания этой информации.

При установленном флажке **Использовать следующее имя пользователя и пароль при подключении любого пользователя** (Use this account name and password when anyone connects to the Internet from this computer) данная информация будет использоваться при подключении любого пользователя, работающего на данном компьютере.

Если установлен флажок **Сделать это подключение подключением к Интернету по умолчанию** (Make this the default Internet connection), то данное подключение будет использоваться по умолчанию. Другими словами, при попытке запустить браузер или доставить почту для установки связи с провайдером будет использовано данное подключение.

Когда установлен флажок **Включить брандмауэр для подключения к Интернету** (Turn on Internet Connection Firewall for this connection), создаваемое подключение будет защищено брандмауэром.

> Нажмите кнопку **Далее** (Next). На экране появится заключительный диалог **Мастера новых подключений** (New Connection Wizard) (Рис. 4.25), информирующий об успешном создании подключения.

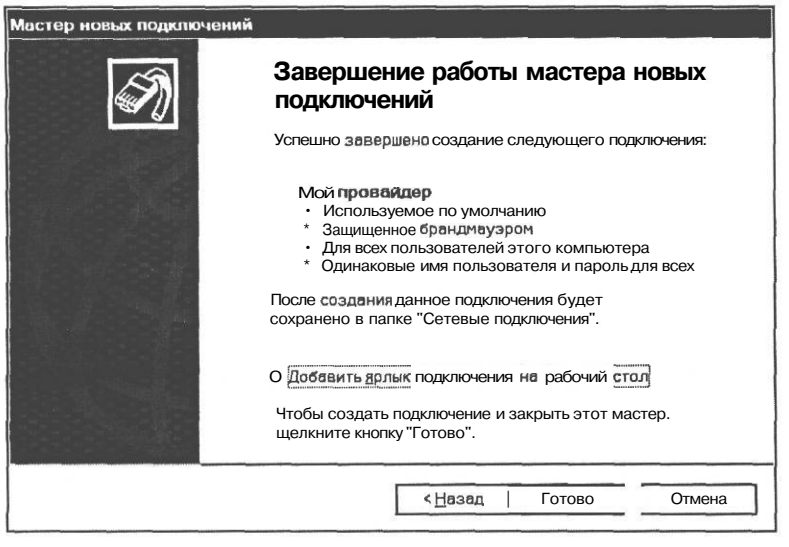



*Рис. 4.25. Заключительный диалог Мастера новых подключений (New Connection Wizard)*

Если установить флажок Добавить ярлык подключения на рабочий стол (Add a shortcut to this connection to my desktop), то после закрытия Мастера на Рабочем столе (Desktop) появится ярлык данного подключения, и вы сможете соединяться с провайдером, дважды щелкнув мышью на этом ярлыке.

➤ Нажмите кнопку Готово (Finish). Мастер создаст подключение с заданным параметрами и закончит свою работу.

На экране появится диалог Подключение к Мой провайдер (Connect to Мой провайдер) (Рис. 4.26).

С помощью этого диалога уже можно подключиться к серверу удаленного доступа провайдера.

Если вы создали первое подключение, то в главном меню Windows появится вложенное меню Подключение (Connect To) и в нем команда для подключения к вашему провайдеру - Мой провайдер.


*Рис. 4.26. Диалог* ***Подключение к Мой провайдер*** *(Connect to Мой провайдер)*

## Настройка дополнительных параметров подключения

Прежде чем звонить на сервер удаленного доступа провайдера, настроим некоторые дополнительные параметры созданного нами подключения **Мой провайдер.**

> Нажмите кнопку **Свойства** (Properties) в диалоге **Подключение к Мой провайдер** (Connect to Мой провайдер). На экране появится диалог **Мой провайдер - свойства** (Мой провайдер Properties) с открытой вкладкой **Общие** (General) (Рис. 4.27).

Этот диалог можно вызывать также, выбрав в главном меню Windows команду Подключения (Connect To), щелкнув правой кнопкой мыши на строке **Мой провайдер** и в появившемся контекстном меню выбрав команду **Свойства** (Properties).

В верхней части диалога в поле ввода **Подключаться через** (Connect using) указано название установленного модема. Вы можете изменить настройку его параметров, нажав кнопку **Настроить** (Configure).

В поле ввода **Номер телефона** (Phone number) указан телефонный номер провайдера, который вы ввели при создании соединения. Вы можете также заполнить поле ввода **Код города** (Area code) и поле ввода Код **страны или региона** (Country/region code). Чтобы сделать эти поля активными, необходимо установить флажок **Использовать правила набора номера** (Use dialing rules). Чтобы создать новое размещение или внести изменения, следует нажать кнопку **Правила** (Dialing rules).

Если вы получили у провайдера несколько телефонных номеров для дозвона на сервер удаленного доступа, то их можно добавить сейчас.

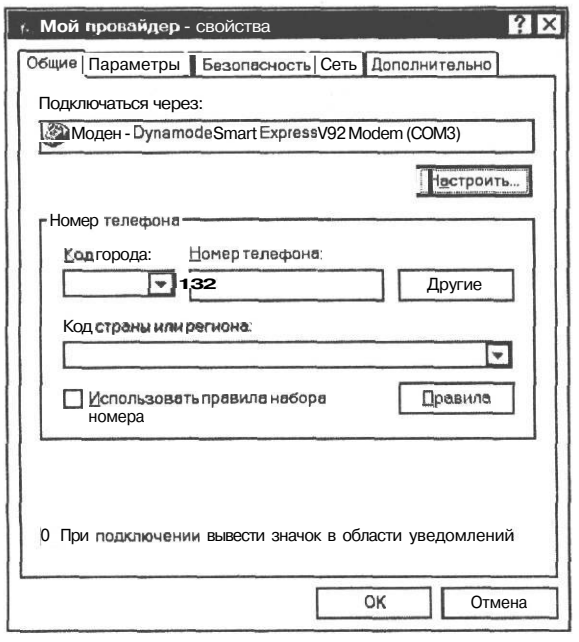



*Рис. 4.27. Вкладка **Общие** (General) диалога **Свойства** (Properties) соединения*

➤ Нажмите кнопку **Другие** (Alternates). На экране появится диалог **Дополнительные номера телефонов** (Alternate phone numbers) (Рис. 4.28).

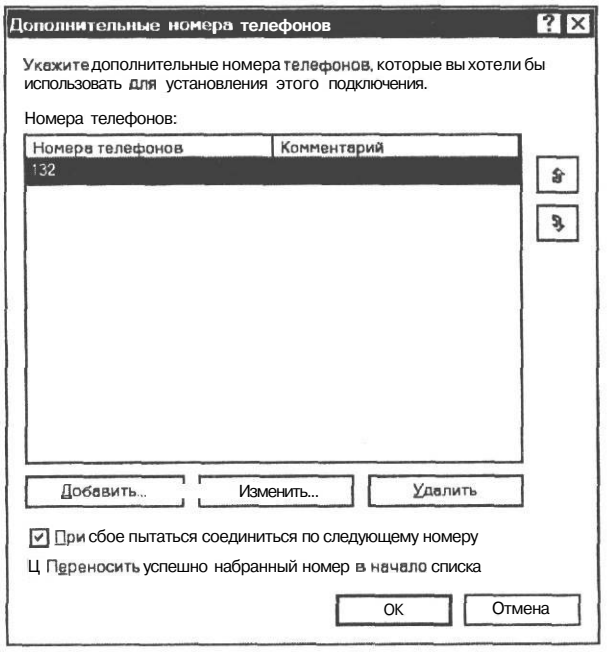



*Рис. 4.28. **Диалог Дополнительные номера телефонов** (Alternate phone numbers)*

> Нажмите кнопку **Добавить** (Add). На экране появится диалог **Добавить дополнительный номер телефона** (Add alternate phone number) (Рис. 4.29).

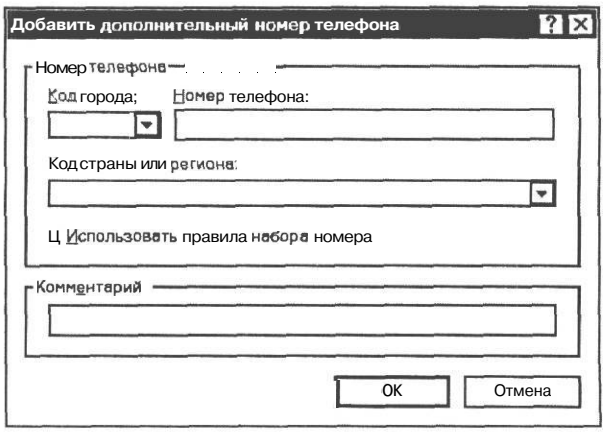



***Рис. 4.29. Диалог Добавить дополнительный номер телефона*** *(Alternate phone numbers)*

> В поле ввода **Номер телефона** (Phone number) введите один из альтернативных телефонных номеров из числа полученных у провайдера. Не забудьте перед номером вести английский символ р, чтобы осуществлять импульсный набор, например **p221-85-35**.

➤ Если для подключения к серверу удаленного доступа будет использоваться междугородняя связь, укажите также код города в открывающемся списке Код города (Area code) и код страны, выбрав название страны в открывающемся списке **Код страны или региона** (Country/region code), предварительно установив флажок **Использовать правила набора номера** (Use dialing rules).

В поле ввода **Комментарий** (Comment) вы можете ввести дополнительные сведения о данном телефонном номере.

> Нажатием кнопки OK закройте диалог **Добавить дополнительный номер телефона** (Add alternate phone numbers). Программа вернет вас к диалогу **Дополнительные номера телефонов** (Alternate phone numbers), в поле списка которого **Номера телефонов** (Phone numbers) отобразится введенный номер.

> Нажимая кнопку **Add** (Добавить), повторите описанные шаги, чтобы ввести остальные альтернативные телефонные номера, полученные у провайдера.

В дальнейшем при необходимости вы сможете изменить любой номер, щелчком мыши выделив его в списке и нажав кнопку **Изменить** (Edit), или удалить, нажав кнопку **Удалить** (Delete).

> Убедитесь, что установлен флажок **При сбое пытаться соединиться по следующему номеру** (If number fails, try next number). Это позволит автоматически звонить по альтернативным номерам при неудачной попытке связи с первым номером.

**Если установить флажок Переносить успешно набранный номер в начало списка** (Move successful number to top of list), то телефонный номер, с которым было установлено последнее соединение, будет автоматически перемещен в начало списка.

Вы можете также вручную переместить любой номер в любое место списка, выделив нужный и нажимая кнопки | ⇧ | и | ⇩ |. Модем будет поочередно звонить по каждому номеру, начиная с первого, до тех пор, пока связь не будет установлена.

- Закройте диалог **Дополнительные номера телефонов** (Alternate phone numbers), нажав кнопку **ОК.** Программа вернет вас к диалогу **Свойства** (Properties) выбранного соединения.
- Убедитесь, что установлен флажок **При подключении вывести значок в области уведомлений** (Show icon in notification area when connected). При этом после подключения к провайдеру в правой части **Панели задач** (Taskbar) будет отображаться значок соединения. Подведя к нему указатель мыши или дважды щелкнув на нем мышью, вы сможете увидеть информацию о состоянии соединения.
- Щелкните мышью на ярлыке **Параметры** (Options), чтобы перейти на следующую вкладку (Рис. 4.30).

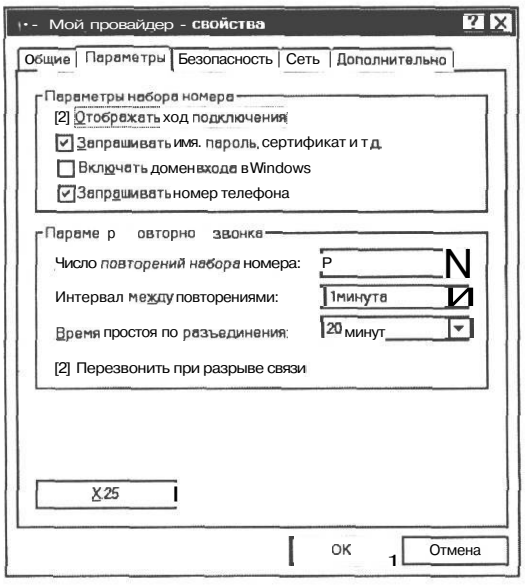



*Рис. 4.30. Вкладка **Параметры** (Options) диалога **Свойства** (Properties) соединения*

На данной вкладке определяются параметры дозвона.

- Убедитесь, что установлен флажок **Отображать ход подключения** (Display progress while connecting). Это позволит в диалоге подключения наблюдать за процессом подключения к серверу удаленного доступа провайдера.
- Убедитесь, что установлен флажок **Запрашивать имя, пароль, сертификат и т.д.** (Prompt for name and password, certificate, etc.). В таком случае перед подключением на экране появится диалог, в котором можно будет ввести нужную информацию или изменить параметры соединения.

> Сбросьте флажок **Включать домен входа в Windows** (Include Windows logon domain), чтобы в диалоге перед подключением не запрашивались сведения для регистрации в Windows. Эта информация не требуется при подключении к провайдеру.

> Если вы получили от провайдера несколько телефонных номеров, установите флажок **Запрашивать номера телефона** (Prompt for phone number). Это позволит вам при необходимости выбирать номер телефона для подключения из открывающегося списка.

Если вы получили только один телефонный номер для подключения к провайдеру и хотите, чтобы программа автоматически повторяла попытки дозвона в тех случаях, когда номер занят или не отвечает, то следует в группе элементов управления **Параметры повторного звонка** (Redialing options) установить **Число повторений набора номера** (Redial attempts), **Интервал между повторениями** (Time between redial attempts) и **Время простоя до разъединения** (Idle time before hanging up).

> Убедитесь, что установлен флажок **Перезвонить при разрыве связи** (Redial if line is dropped). В этом случае программа удаленного доступа автоматически предпримет попытки восстановления связи при ее разрыве.

Указанная возможность становится доступной, только если запущен сервис **Диспетчер автоподключений удаленного доступа** (Remote Access Auto Connection Manager). По умолчанию в Widows XP он должен быть уже запущен. Проверим это.

➤ Не закрывая диалог **Свойства** (Properties) выбранного соединения, щелкните правой кнопкой мыши на значке fejj - **Мой компьютер** (My Computer) на **Рабочем столе** (Desktop) или на команде **Мой компьютер** (My Computer) главного меню. На экране появится контекстное меню.

➤ В контекстном меню выберите команду **Управление** (Manage). На экране появится окно **Управление компьютером** (Computer Management), разделенное на левую и правую части.

➤ Выберите в левой части окна, в группе **Службы и приложения** (Services and Applications) компонент **Службы** (Services). На правой панели отобразится таблица с перечнем всех доступных служб.

➤ Воспользовавшись полосой прокрутки правой панели, найдите строку с названием сервиса **Диспетчер автоподключений удаленного доступа** (Remote Access Auto Connection Manager). Если сервис запущен, в колонке **Состояние** (Status) строки таблицы с названием выбранного сервиса стоит отметка **Работает** (Started) (Рис. 4.31).

Connection Manager) отключен, то колонка **Состояние** (Status) строки таблицы с его названием пуста. Запустим его.

Щелкните правой кнопкой мыши на строке с названием сервиса **Диспетчер автоподключений удаленного доступа** (Remote Access Auto Connection Manager) и в появившемся контекстном меню выберите команду **Пуск** (Start). Сервис будет запущен. В колонке **Status** (Состояние) строки таблицы с названием выбранного сервиса появится отметка **Работает** (Started).

> Если сервис **Диспетчер автоподключений удаленного доступа** (Remote Access Auto

> Закройте окно папки **Управление компьютером** (Computer Management), нажав кнопку ☒ в правом верхнем его углу. Вы возвратитесь к диалогу **Свойства** (Properties) созданного соединения.

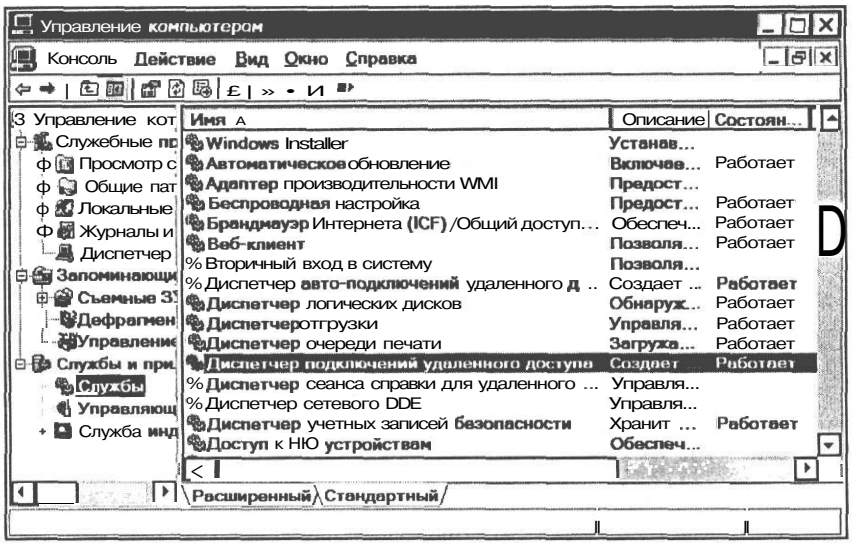



*Рис. 4.31. Окно папки* ***Управление компьютером*** *(Computer Management)*

> Щелкните мышью на ярлыке **Безопасность** (Security). В диалоге отобразятся элементы управления данной вкладки (Рис. 4.32).

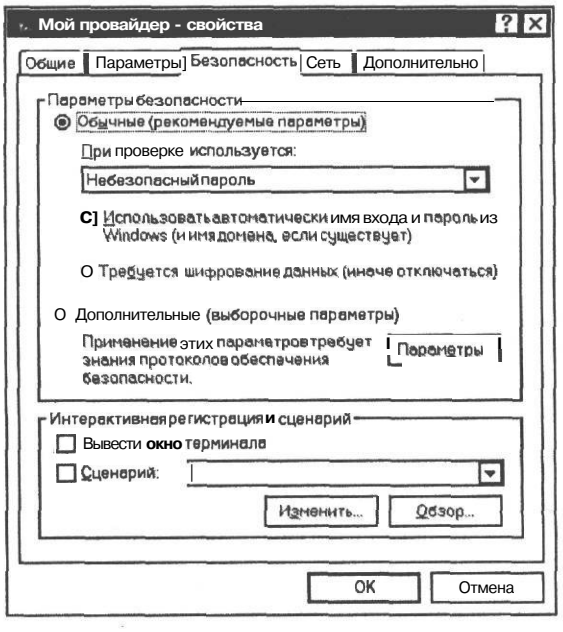



*Рис. 4.32. Вкладка* ***Безопасность*** *(Security) диалога* ***Свойства*** *(Properties) соединения*

Если для соединения с вашим провайдером требуется файл-сценарий и вы еще не подключили его, то это можно сделать на данной вкладке, установив флажок **Сценарий** (Run script), а затем нажав кнопку **Обзор** (Browse) и выбрав нужный файл с расширением **.scp,** который предварительно следует скопировать в удобную для вас папку на жестком

диске. Имя выбранного сценария отобразится в поле открывающегося списка справа от флажка Сценарий (Run script).

> Щелкните мышью на ярлыке Сеть (Networking), чтобы перейти на следующую вкладку (Рис. 4.33).

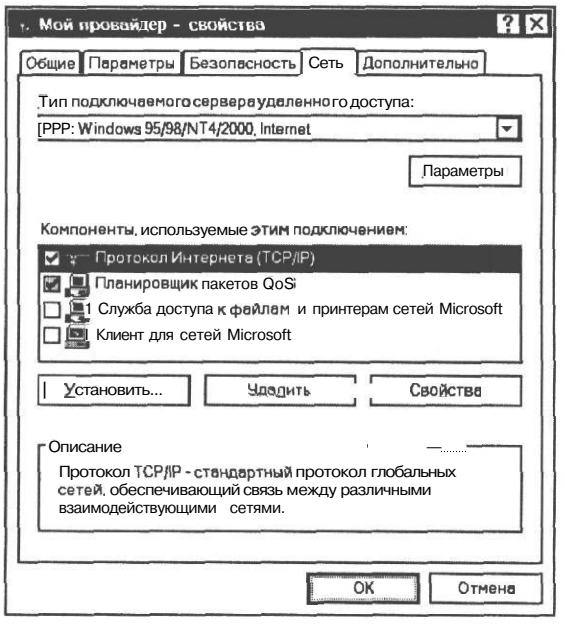



*Рис. 4.33. Вкладка Сеть (Networking) диалога Свойства (Properties) соединения*

> Убедитесь, что в поле открывающегося списка Тип подключаемого сервера удаленного доступа (Type of dial-up server I am calling) правильно указан тип сервера удаленного доступа провайдера и протокол связи с ним. В большинстве случаев этот протокол - PPP: Windows **95/98/NT4/2000,** Internet.

Чтобы компьютеры разных типов с различными операционными системами могли общаться друг с другом и обмениваться информацией, они должны использовать один «язык», который называется протоколом. Для работы в сети Интернет применяется семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol - Протокол управления передачей данных/Протокол Интернета), поддерживающее связь между объединенными сетями, состоящими из компьютеров различной архитектуры с различными операционными системами. Протокол TCP/IP включает в себя стандарты для связи между компьютерами и соглашения о соединении сетей и правилах маршрутизации сообщений.

➤ Убедитесь, что в поле списка Компоненты, используемые этим подключением (This connection uses the following items) присутствует и отмечен флажком компонент Протокол Интернета **(TCP/IP)** (Internet Protocol (TCP/IP)). Если же флажок сброшен, установите его.

➤ Если Планировщик пакетов QoS (QoS Packet Scheduler) не был удален ранее, при настройке сети, удалите его сейчас, выделив и нажав кнопку Удалить (Uninstall). В появившемся диалоге с запросом подтвердите необходимость удаления.

➤ Закройте диалог **Мой провайдер - свойства** (Мой провайдер Properties) нажатием кнопки **OK.** На экране останется диалог **Подключение к Мой провайдер** (Connect to Мой провайдер) (Рис. 4.26), который появился после завершения работы **Мастера новых подключений** (New Connection Wizard).

Диалог **Подключение к Мой провайдер** (Connect to Мой провайдер) позволяет установить соединение с провайдером Интернета. Этот диалог можно вызвать, нажав кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выбрав команду **Подключение * Мой провайдер** (Connect To * Мой провайдер) или дважды щелкнув мышью на значке созданного подключения на **Рабочем столе** (Desktop).

# Проверка связи с Интернетом

Теперь все готово для соединения с Интернетом, а точнее - для проверки связи с провайдером и тестирования работы всего сетевого сервиса.

## Подключение к серверу удаленного доступа провайдера

Для подключения к серверу удаленного доступа провайдера выполните следующие действия.

> Убедитесь, что в поле ввода **Пользователь** (User Name) диалога **Подключение к Мой провайдер** (Connect to Мой провайдер) (Рис. 4.26) указано правильное имя, а в открывающемся списке **Набрать** (Phone Number) - корректный номер телефона. При необходимости исправьте их.

Чтобы изменить сохраненный пароль, следует щелкнуть мышью в поле ввода **Пароль** (Password) и ввести новый пароль доступа.

Нажав кнопку **Свойства** (Properties), вы откроете диалог **Свойства** (Properties) (Рис. 4.27) для данного подключения, в котором сможете изменить ранее настроенные параметры.

Теперь можно подключиться к серверу удаленного доступа.

➤ Нажмите кнопку **Вызов** (Connect) в диалоге **Подключение к Мой провайдер** (Connect to Мой провайдер). Этот диалог закроется, и на экране появится новый диалог, отображающий процесс установки связи (Рис. 4.34).

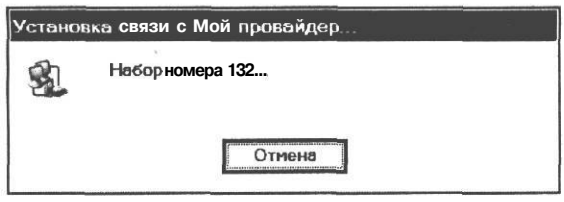



*Рис. 4.34. Процесс установки связи*

Если модемы на обоих концах линии успешно установили связь между собой, то начнется проверка имени пользователя и пароля, которая происходит на сервере провайдера (Рис. 4.35).

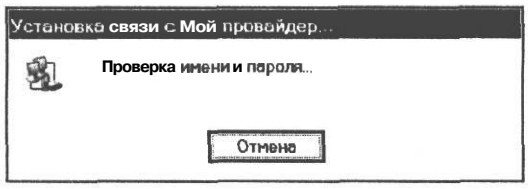


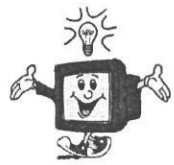

*Рис. 4.35. Проверка имени пользователя и пароля*

В случае удачного прохождения процесса аутентификации пользователя ваш компьютер будет зарегистрирован в сети (Рис. 4.36).


*Рис. 4.36. Регистрация компьютера в сети*

Затем диалог отображения процесса установки связи закроется.

*Внимание! Начиная с данного момента, у поставщика услуг Интернета включается отсчет времени, проведенного вами в сети Интернете, со всеми вытекающими из этого последствиями. О том, что компьютер подключен к Интернету, информирует специальный значок на* ***Панели задач*** *(Taskbar) в виде двух соединенных компьютеров* .



# Проверка протокола TCP/IP

Итак, мы подключились к серверу удаленного доступа провайдера. Но это еще не означает, что успешно установлена связь с Интернетом. Ведь возможны ошибки в настройках протокола **TCP/IP**. Поэтому теперь следует проверить связь с каким-нибудь из серверов Интернета, например, с узлом www.ru. Для проверки связи воспользуемся командой ping, которая, отправляя сообщения с эхо-запросом, проверяет соединение с другим компьютером на уровне протокола TCP/IP.

> Откройте диалог Запуск программы (Run), нажав кнопку Пуск (Start) на Панели задач (Taskbar) и в появившемся главном меню Windows выбрав команду Выполнить (Run).

> В поле ввода Открыть (Open) введите команду cmd и нажмите кнопку OK. На экране появится окно Командная строка (Command Prompt).

> В окне Командная строка (Command Prompt) при установленной связи с провайдером Интернета введите команду ping www.ru и нажмите клавишу Enter. По указанному адресу будут посланы четыре пакета данных по 32 байта каждый, после чего вы увидите число полученных пакетов, процент потерянных и время приема-передачи эхо-запросов (Рис. 4.37).

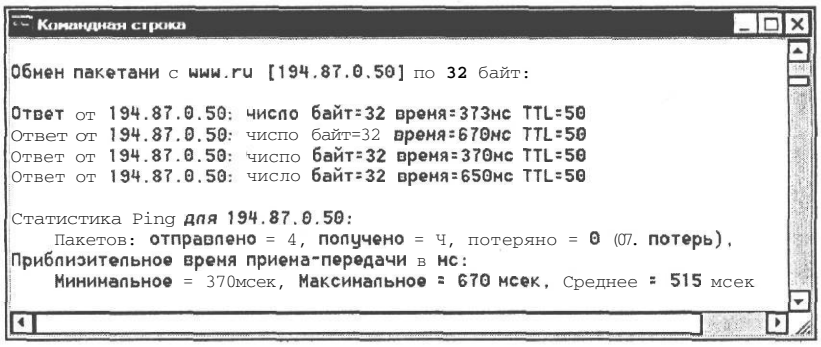
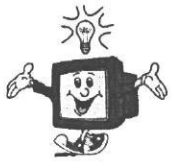



*Рис. 4.37. Окно Командная строка (Command Prompt) с результатами работы команды ping*

Если полученный результат не содержит сообщений об ошибках и вы видите информацию о времени прохождения эхо-запросов для четырех посланных пакетов данных, то все в порядке, подключение к Интернету успешное.

Если же после ввода команды ping вы видите сообщения об ошибках: Превышен интервал ожидания для запроса (Timeout), Сеть недоступна (Network unreachable) или если число потерянных пакетов составит 100%, то это указывает на отсутствие связи или ошибки в настройке протокола TCP/IP. Сообщение Bad IP (Неправильный IP) указывает на неправильный сетевой адрес.

*В некоторых случаях отсутствие доступа к узлам Интернета может быть обусловлено нарушением связи в самой глобальной сети или неработоспособностью опрашиваемого сервера. На всякий случай попробуйте «пропинговать» адреса нескольких серверов Интернета, включая своего провайдера.*



## Состояние подключения

Когда связь с Интернетом установлена, в правой части Панели задач (Taskbar), рядом с часами появляется значок действующего подключения, который представляет собой два связанных компьютера. Если установить на нем указатель мыши, то вы увидите название подключения, а также объем отправленных и полученных данных в байтах.

➤ Щелкните мышью на значке. Откроется информационный диалог, отображающий Состояние (Status) связи (Рис. 4.38).

Данный диалог отображает текущие параметры связи:

Состояние: Подключено (Status: Connected);

Длительность (Duration) связи (часы:минуты:секунды);

Скорость (Speed) подключения (Кбит/с);

Отправлено (Send) (байт);

Принято (Receive) (байт).


*Рис. 4.38. Диалог с информацией о состоянии связи*

Для просмотра дополнительной информации о состоянии связи, щелкните мышью на ярлыке **Сведения** (Information). Вы увидите дополнительные сведения о подключении (Рис. 4.39).

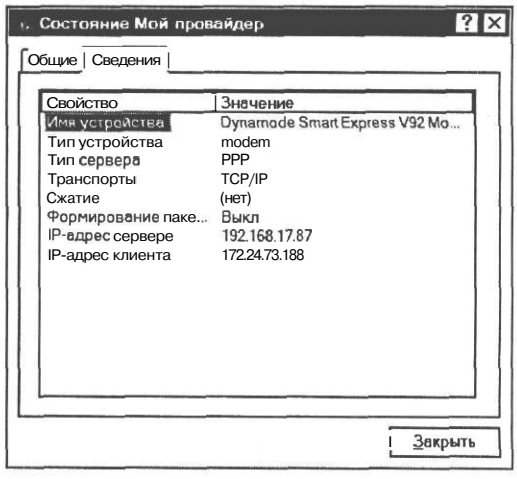


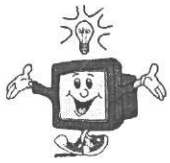

*Рис. 4.39. Дополнительные сведения о состоянии связи*

Здесь приводится дополнительная информация:

- название и тип устройства, установившего текущее подключение;
- тип удаленного сервера;
- список работающих сетевых протоколов;
- IP-адреса сервера и клиента и другие.

Чтобы разорвать текущее удаленное подключение, нажмите кнопку **Отключить** (Disconnect) на вкладке **Общие** (General) диалога **Состояние** (Status) (Рис. 4.38).

*Разорвать связь можно и по-другому. Щелкните правой кнопкой мыши на значке удаленного подключения, затем в появившемся контекстном меню выберите команду* ***Отключить*** *(Disconnect).*



## Возможные сообщения об ошибках установки связи

Случается, что с первой попытки не удастся установить связь с поставщиком услуг Интернета. Это может быть вызвано разными причинами. Ниже перечислены наиболее распространенные ошибки и варианты их устранения.

### Нет отклика от модема (Error 630)

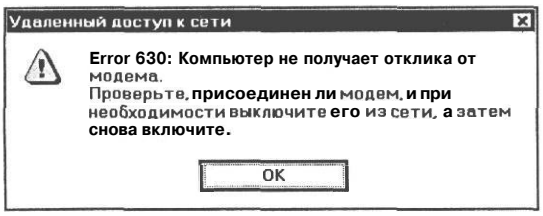



*Рис. 4.40. Диалог с сообщением об ошибке: Компьютер не получает отклика от модема*

Ваши действия:

- Выключите, а затем снова включите модем.
- Проверьте надежность подключения модема к компьютеру.
- Повторите попытку установки соединения.

### Нет сигнала в линии (Error 680)


*Рис. 4.41. Диалог с сообщением об ошибке: Нет сигнала в линии*

Ваши действия:

- Поднимите трубку на параллельном телефоне и проверьте наличие длинного гудка.
- Проверьте надежность подключения модема к телефонной линии и убедитесь, что кабель телефонной линии подключен в гнездо модема **Line** (Линия).
- Повторите попытку установки соединения.

## Линия занята (Error 676)

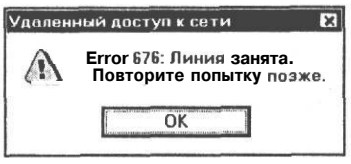



*Рис. 4.42. Диалог с сообщением об ошибке: Линия занята*

Ваши действия:

> Повторите попытку установки соединения позднее.

## Удаленный компьютер не отвечает (Error 678)

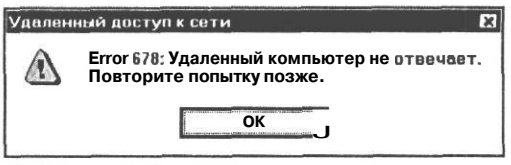



*Рис. 4.43. Диалог с сообщением об ошибке: Удаленный компьютер не отвечает*

➤ Повторите попытку подключения позднее.

## Не удалось подобрать совместимый протокол (Error 720)

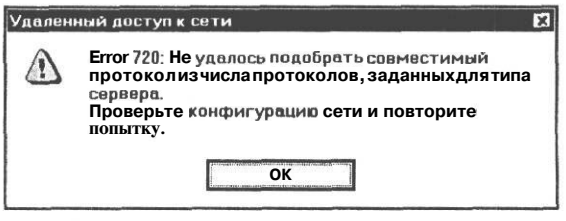



*Рис. 4.44. Диалог с сообщением об ошибке: Не удалось подобрать совместимый протокол*

Ваши действия:

➤ Откройте диалог настройки свойств удаленного подключения на вкладке **Сеть** (Networking) (Рис. 4.33) и убедитесь, что открывающийся список **Тип подключаемого сервера удаленного доступа** (Type of dial-up server I am calling) содержит значение **PPP: Windows 95/98/NT4/2000, Internet,** а **в** группе элементов управления **Компоненты, используемые этим подключением** (This connection uses the following items) установлен флажок **Протокол Интернета TCPJIP** (Internet Protocol (TCP/IP)).

➤ Повторите попытку установки соединения.

### Невозможно установить удаленное подключение (Error 691)

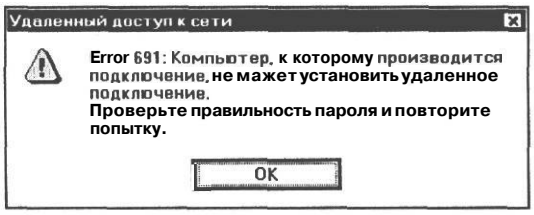



*Рис. 4.45. Диалог с сообщением об ошибке: Невозможно установить удаленное подключение*

Ваши действия:

- Полностью очистите и заново введите информацию в поля ввода **Имя пользователя** (User Name) и **Пароль** (Password) диалога **Подключение к Мой провайдер** (Connect to Мой провайдер) (Рис. 4.26).
- Узнайте у провайдера Интернета, не заблокирована ли ваша учетная запись.
- Повторите попытку установки соединения.

## Настройка узлового компьютера для общего доступа к подключению Интернета

После того как вы убедились, что узловой компьютер локальной сети может беспрепятственно подключаться к Интернету, следует настроить на нем параметры общего доступа всех компьютеров к данному подключению. Это можно сделать либо автоматически с помощью **Мастера настройки сети** (Network Setup Wizard), который запускается из окна **Сетевые подключения** (Network Connections), либо вручную на вкладке **Дополнительно** (Advanced) диалога **Свойства** (Properties) соответствующего подключения. В нашем примере - это диалог **Мой провайдер - свойства** (Мой провайдер Properties). Доступ к этому диалогу осуществляется из контекстного меню для значка соответствующего подключения (Мой провайдер) в окне **Сетевые подключения** (Network Connections) или нажатием кнопки **Свойства** (Properties) в диалоге **Подключение к Мой провайдер** (Connect To Мой провайдер) (Рис. 4.26).

Посмотрим практически, как вручную настроить общий доступ к подключению Интернета на узловом компьютере локальной сети, который, напомним, должен работать под управлением операционной системы Windows XP. Для выполнения этой процедуры необходимо войти в систему с учетной записью «Администратор» или члена группы «Администраторы».

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Панель управления** (Control Panel). На экране появится окно **Панель управления** (Control Panel).
- В окне **Панель управления** (Control Panel) дважды щелкните мышью на значке **Сетевые подключения** (Network Connections). Откроется окно **Сетевые подключения** (Network Connections) (Рис. 4.46).

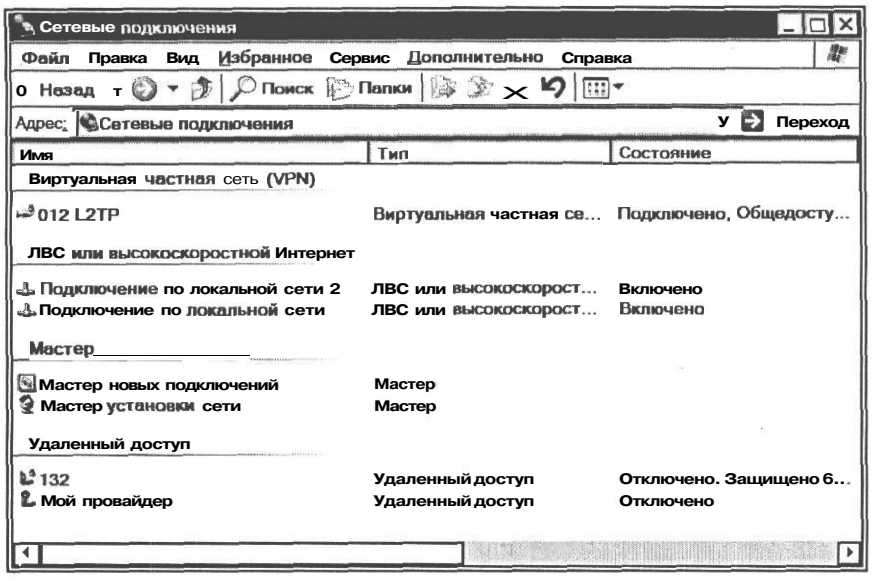



*Рис. 4.46. Окно* ***Сетевые подключения*** *(Network Connections)*

> Щелкните правой кнопкой мыши на значке подключения удаленного доступа Мой **провайдер** и в появившемся контекстном меню выберите команду **Свойства** (Properties). На экране появится диалог **Мой провайдер - свойства** (Мой провайдер Properties).

> Щелкните мышью на ярлыке **Дополнительно** (Advanced), чтобы перейти на эту вкладку (Рис. 4.47).

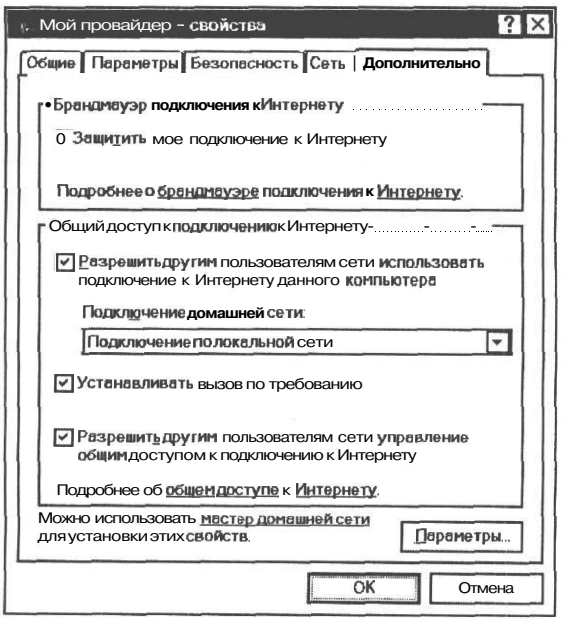



*Рис. 4.47.* ***Вкладка Дополнительно*** *(Advanced) диалога* ***Свойства*** *(Properties)*

Установка флажка **Защитить мое подключение к Интернету** (Protect my computer and network by limiting or preventing access to this computer from the Internet) включает брандмауэр, обеспечивающий защиту от просмотра ресурсов вашего компьютера и доступа к ним с компьютеров, расположенных за пределами вашей локальной сети. Но защита, которую обеспечивает встроенный брандмауэр Windows XP, не является полноценной, и вместо него лучше использовать брандмауэры сторонних разработчиков. В главе «Защита сети от вирусов и атак через Интернет» мы рассмотрим лучшую из таких программ - Agnitum Outpost Firewall Pro. А пока брандмауэр Windows XP следует отключить.

➤ Сбросьте флажок **Защитить мое подключение к Интернету** (Protect my computer and network by limiting or preventing access to this computer from the Internet).

Установка флажка **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера** (Allow other network users to connect through this computer's Internet connection) разрешает общий доступ к подключению Интернета, а в поле открывающегося списка под ним выбирается локальная сеть, которой предоставляется общий доступ.

➤ Установите флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера** (Allow other network users to connect through this computer's Internet connection).

> Если на компьютере установлено несколько сетевых адаптеров, в открывающемся списке **Подключение домашней сети** (Home networking connection) выберите локальную сеть, которой предоставляется общий доступ к Интернету. Другими словами, здесь надо выбрать название соединения Ethernet-карты, с помощью которой данный компьютер подсоединен к локальной сети.

После активизации службы общего доступа к подключению Интернета сетевому адаптеру, подключенному к локальной сети, присваивается новый статический IP-адрес - 192.168.0.1. Как следствие, все подключения TCP/IP между компьютерами сети и главным компьютером общего доступа, которые уже были установлены ранее, будут разорваны и потребуют повторной установки посредством включения на каждом компьютере режима автоматического получения IP-адреса. В следующем разделе мы покажем, как это сделать в операционных системах Windows 98 и Windows 2000/XP.

Установка флажка **Устанавливать вызов по требованию** (Establish a dial-up connection whenever a computer on my network attempts to access the Internet) позволит использовать данное подключение автоматически, когда другой компьютер сети попытается получить доступ в Интернет.

> Установите флажок **Устанавливать вызов по требованию** (Establish a dial-up connection whenever a computer on my network attempts to access the Internet). Теперь, если кто-либо в сети запустит браузер или почтовую программу, на узловом компьютере автоматически начнется набор номера для подключения к провайдеру.

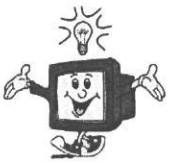
Если установить флажок **Разрешить другим пользователям сети управление общим доступом к подключению к Интернету** (Allow other network users to control or disable the shared Internet connection), то пользователи сети смогут управлять состоянием данного подключения к Интернету, устанавливая и разрывая его. Данный флажок следует устанавливать только в том случае, когда вы действительно хотите дать право клиентам сети по своему усмотрению разрывать связь с провайдером и снова подключаться к нему.

Для нормальной работы в Интернете может потребоваться дополнительная настройка компьютера с общим подключением. Предоставляемые службы должны быть настроены так, чтобы пользователи Интернета могли к ним обращаться. Например, если в локальной сети размещается Web-сервер и нужно обеспечить доступ к нему для пользователей Интернета, необходимо настроить на узловом компьютере общего доступа службу Web-сервера и обеспечить доступ к нему, нажав кнопку **Параметры** (Settings) и выполнив соответствующие настройки.

➤ Закройте диалог **Мой провайдер - свойства** (Мой провайдер Properties) нажатием кнопки OK.

Доступ к подключению Интернета на узловом компьютере будет активизирован и выделен в общее пользование. Теперь все компьютеры сети смогут совместно использовать подключение к Интернету, а также другие ресурсы узлового компьютера, такие, как файлы и принтеры. Но сначала нужно настроить для доступа к Интернету каждый компьютер сети.

*Обратите внимание на то, что узловой компьютер с общим доступом к подключению Интернета всегда должен включаться первым и выключаться последним. В противном случае другие компьютеры сети не смогут подключаться к Интернету.*



## Настройка компьютеров сети для общего доступа к подключению Интернета

Как было отмечено выше, после установки общего доступа к подключению Интернета сетевому адаптеру узлового компьютера присваивается новый статический IP-адрес 192.168.0.1. В результате все ранее установленные подключения между узловым компьютером и другими компьютерами сети будут разорваны. Чтобы восстановить связь между компьютерами сети, необходимо на каждом из них, кроме узлового, включить для сетевого адаптера режим автоматического получения IP-адреса.

Напомним, что при настройке локальной сети мы назначили каждому компьютеру статический IP-адрес. Такая настройка обеспечивала быструю загрузку сетевых компьютеров и практически моментальное появление их в сетевом окружении. Однако средство общего доступа к подключению Интернета Windows XP не предусматривает использование статических IP-адресов для компьютеров локальной сети, а требует их автоматического назначения. Именно поэтому мы теперь должны на каждом компьютере локальной сети включить для сетевого адаптера режим автоматического назначения IP-адреса.

Это можно выполнить либо с помощью **Мастера настройки сети** (Network Setup Wizard), либо вручную. На компьютерах, работающих под управлением операционных систем Windows XP Home Edition и Windows XP Professional, можно запустить **Мастер настройки сети** (Network Setup Wizard) из окна **Сетевые подключения** (Network Connections) (Рис. 4.46). На компьютерах, работающих под управлением операционных систем Windows 98, Windows 98 Second Edition, Windows Millennium Edition, следует воспользоваться

либо установочным компакт-диском Windows XP, либо диском настройки сети, созданным при запуске **Мастера настройки сети** (Network Setup Wizard) на узловом компьютере.

Мы же рассмотрим ручной способ настройки компьютеров сети для общего доступа к подключению Интернета в операционных системах Windows 98 и Windows 2000/XP. Это позволит лучше понять логику работы протокола TCP/IP.

## Настройка компьютеров с операционной системой Windows 98

Включение режима автоматического назначения IP-адреса в Windows 98 выполняется на вкладке IP-адрес (IP address) диалога Свойства: TCP/IP (TCP/IP Properties).

- Откройте окно Панель управления (Control Panel) и дважды щелкните мышью на значке Сеть (Network). Появится диалог Сеть (Network) с открытой вкладкой Конфигурация (Configuration).
- Щелкните мышью в поле списка этого диалога на строке протокола TCPЛP, связанного с сетевым адаптером. Эта строка может быть, например, такой: TCP/IP -> Realtek **RTL8139(A/B/C)** PCI Fast Ethernet Adapter.
- Нажмите кнопку Свойства (Properties). Появится диалог Свойства: TCPЛP (TCP/IP Properties) с открытой вкладкой IP-адрес (IP address) (Рис. 4.48).
- Закройте диалог Свойства: TCPЛP (TCP/IP Properties) нажатием кнопки OK. Вы возвратитесь к диалогу Сеть (Network).

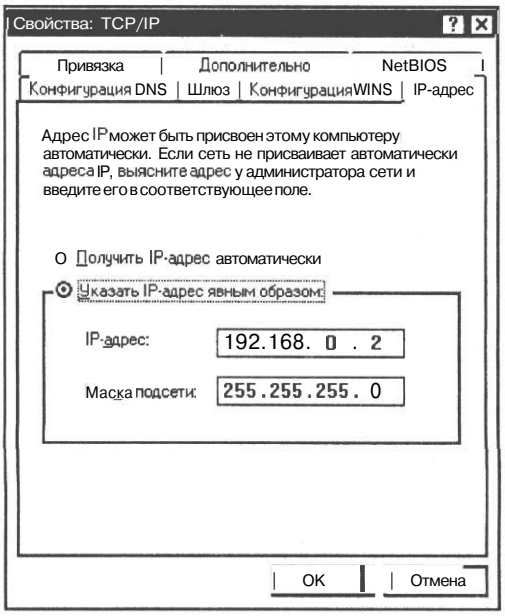



*Рис. 4.48. Вкладка* ***IP-адрес*** *(IP address) диалога* ***Свойства:*** *TCP/IP (TCP/IP Properties)*

> Закройте также диалог **Сеть** (Network) нажатием кнопки OK. На экране появится диалог **Изменение параметров системы** (System parameters was changed) с предложением перезагрузить компьютер (Рис. 4.49).

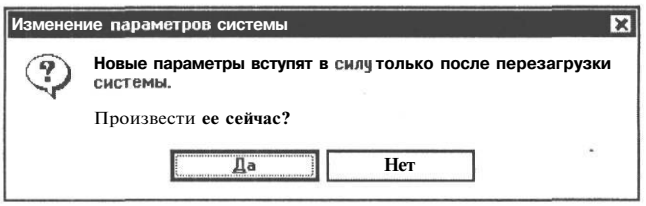



*Рис. 4.49. Диалог **Изменение параметров системы** (System parameterswas changed)*

> Нажмите кнопку Да (Yes), чтобы выполнить перезагрузку.

После перезагрузки будет включен режим автоматического назначения IP-адреса.

Таким же способом следует задать автоматическое назначение IP-адреса всем компьютерам локальной сети.

## Настройка компьютеров с операционной системой Windows 2000/XP

Для выполнения настройки сети необходимо войти в систему в качестве администратора. Процедура настройки выполняется в диалоге **Свойства: Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP) Properties).

- Откройте окно **Панель управления** (Control Panel), нажав кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выбрав команду **Панель управления** (Control Panel).
- Откройте окно **Сетевые подключения** (Network Connections), дважды щелкнув мышью на значке **Сетевые подключения** (Network Connections) в окне **Панель управления** (Control Panel).
- Щелкните правой кнопкой мыши на значке **Подключение по локальной сети** (Local Area Connection) и в появившемся контекстном меню выберите команду **Свойства** (Properties). Откроется диалог **Подключение по локальной сети - свойства** (Local Area Connection Properties). Вкладка **Общие** (General) будет активна (Рис. 4.50).
- Щелкните мышью на компоненте **Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP)), чтобы выделить его, и нажмите кнопку **Свойства** (Properties). Появится диалог **Свойства: Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP) Properties) (Рис. 4.51).
- Установите переключатель **Получить IP-адрес автоматически** (Obtain an IP address automatically). При этом поля ввода IP-адрес (IP address) и **Маска подсети** (Subnet mask), в которых был указан установленный ранее статический IP-адрес и маска подсети, очистятся.
- Закройте диалог **Свойства: Протокол Интернета (TCP/IP)** (Internet Protocol (TCP/IP) Properties) нажатием кнопки **OK.**

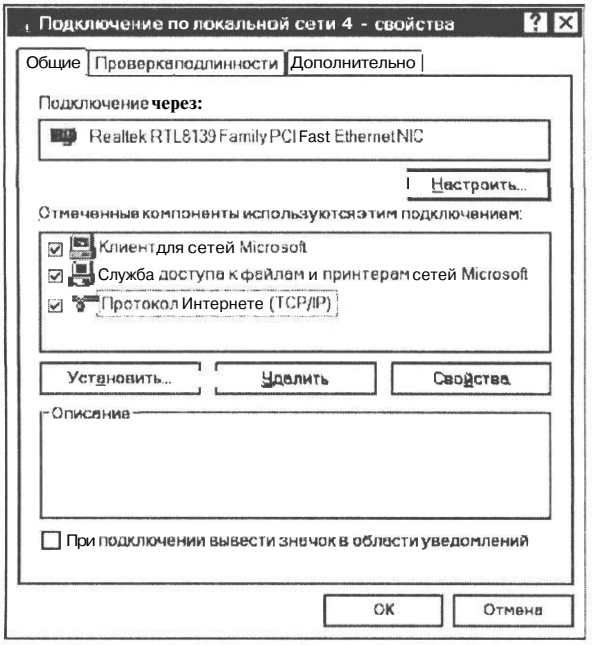



*Рис. 4.50. Вкладка Общие диалога* ***Подключение по локальной сети — свойства*** *(Local Area Connection Properties)*

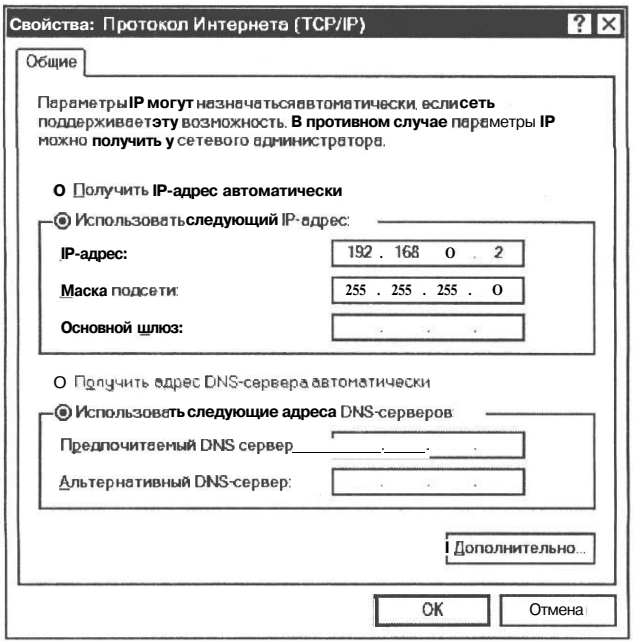



*Рис. 4.51. Вкладка* ***Общие*** *(General) диалога* ***Свойства: Протокол Интернета*** *(TCP/IP) (Internet Protocol (TCP/IP) Properties)*

> Закройте также диалог **Подключение по локальной сети - свойства** (Local Area Connection Properties) (Рис. 4.50).

Подобным же образом необходимо выполнить настройку всех компьютеров вашей локальной сети с операционной системой Windows 2000/XP.

## Проверка общего доступа к подключению Интернета

Чтобы протестировать работу сетевых соединений и подключения к Интернету, сначала воспользуйтесь командой **ping,** посылая сигнал с каждого компьютера сети на узловой командой **ping 192.168.0.1**, так как адрес узлового компьютера всегда остается постоянным. Затем проверьте, доступны ли на всех компьютерах файлы других компьютеров сети, выделенные для совместного использования, и все ли компьютеры могут подключаться к Интернету.

Включив общий доступ к подключению Интернета и убедившись, что все компьютеры могут обмениваться данными друг с другом и имеют доступ в Интернет, можно пользоваться программами Internet Explorer, Outlook Express и любыми другими так, как будто компьютеры сети непосредственно подключены к поставщику услуг Интернета. При отправке запроса в Интернет с любого компьютера сети узловой компьютер соединяется с провайдером и создает подключение, позволяющее другим компьютерам получить доступ к указанному Web-адресу, электронной почте и любому другому ресурсу Интернета.

# ГЛАВА 5.
# Защита сети от вирусов и атак через Интернет

Каждый, кто пользуется компьютером, знает, что конфиденциальности, целостности и доступности данных угрожает множество опасностей, начиная с атак хакеров и кончая сетевыми вирусами-червями. Причем нарушение безопасности чревато серьезными потерями. Получая доступ к ресурсам многих миллионов компьютеров в Интернете, вы одновременно, в той или иной степени, открываете другим компьютерам Интернета доступ к ресурсам компьютеров вашей локальной сети. Перечислим основные опасности, которым подвергается ваша сеть:

- вместе с почтой, в виде вложений в компьютеры сети, кроме вирусов, могут проникнуть Интернет-черви. Некоторые почтовые программы, а также неопытные пользователи, не сознавая угрозы, открывают вложения сами. Если такое послание открыть, то выполняющийся «червь» стремительно поражают систему;
- на ваших компьютерах могут исполняться, например, при отображении Web-страниц, содержащих элементы ActiveX или Java-апплеты, поступившие извне программы, которые, в общем случае, могут выполнять любые опасные действия, например, передавать файлы с вашей частной информацией другим компьютерам в сети или просто удалять ваши данные, причем управлять работой этих программ вы не имеете возможности;
- при неправильной настройке системы другие компьютеры Интернета могут получить или попытаться получить доступ к файлам ваших винчестеров, в которых хранится конфиденциальная информация;
- ваш компьютер может использоваться для атаки другого компьютера, так что вы не будете знать об этом;
- многие Web-узлы могут размещать на ваших компьютерах файлы (cookies или referrers), по которым они смогут определять, к какой информации вы обращались и, напротив, кто обращался к вашему компьютеру;
- на ваши машины могут попасть «троянские кони», т.е. программы, которые передают частную информацию (например, пароли доступа в Интернет или номера кредитных карточек) с вашего компьютера на компьютер злоумышленника. Распространенным вариантом вторжения является установка на компьютере различных серверов для удаленного управления (Backdoor). Если подобная программа оказалась в вашей системе, то ее хозяин сможет работать на вашем компьютере почти как на своем собственном. Основным отличием «троянца» от вируса является именно то, что вирус, попавший на ваш компьютер, никак не связан со своим создателем, а «троянский конь» как раз и предназначен для последующего взаимодействия с пославшим его злоумышленником;
- на ваших компьютерах без вашего ведома может быть размещена специальная программа-шпион (spyware), которая передает своему разработчику информацию о владельце компьютера, его пристрастиях, например, информацию о получаемых из сети файлах, посещаемых сайтах, установленном программном обеспечении. Шпионские программы используют в основном фирмы-разработчики программного обеспечения в маркетинговых целях;

## Установка обновлений с узла Windows Update

Самый простой способ установить обновления операционной системы - это запустить Windows Update и следовать инструкциям, появляющимся на экране. Посмотрим, как это сделать практически.

Значок Windows Update обычно находится в меню кнопки Пуск (Start). Если значка Windows Update в этом меню нет, можно выбрать в главном меню команду Справка и поддержка (Help and Support), после чего в открывшемся окне Центр справки и поддержки (Help and Support Center) после подключения к Интернету щелкнуть мышью на ссылке Обновление системы с помощью веб-узла Windows Update (Keep your computer up-to-day with Windows Update) или же обратиться по адресу windowsupdate.microsoft.com.

После соединения с Web-узлом Windows Update одним из указанных способов вы увидите его первую страницу (Рис. 5.1).

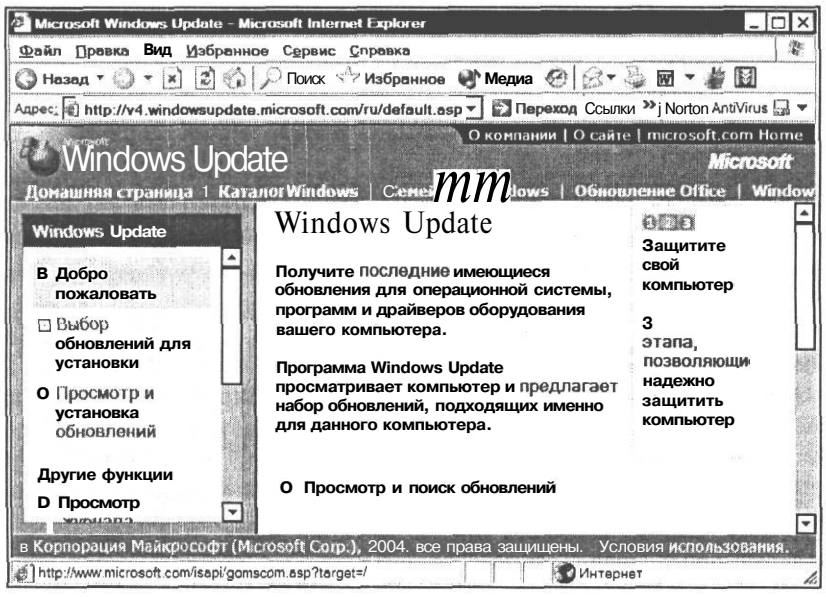



*Рис. 5.7. Первая страница Web-узла Windows Update*

> Щелкните мышью на ссылке Просмотр и поиск обновлений (Scan for Updates).

Программа выполнит поиск доступных обновлений для вашего компьютера. Это может занять некоторое время.

Когда поиск будет закончен, на экране появится сообщение о количестве найденных критических обновлений (Рис. 5.2). Напомним, что критические обновления предназначены для исправления обнаруженных ошибок и защиты компьютера от известных неполадок безопасности. Вы увидите также информацию о других обновлениях для вашей операционной системы и драйверов. Количество дополнительных обновлений указывается в левой части окна.

➤ Щелкните мышью на ссылке Просмотр и установка обновлений (Review and install updates).

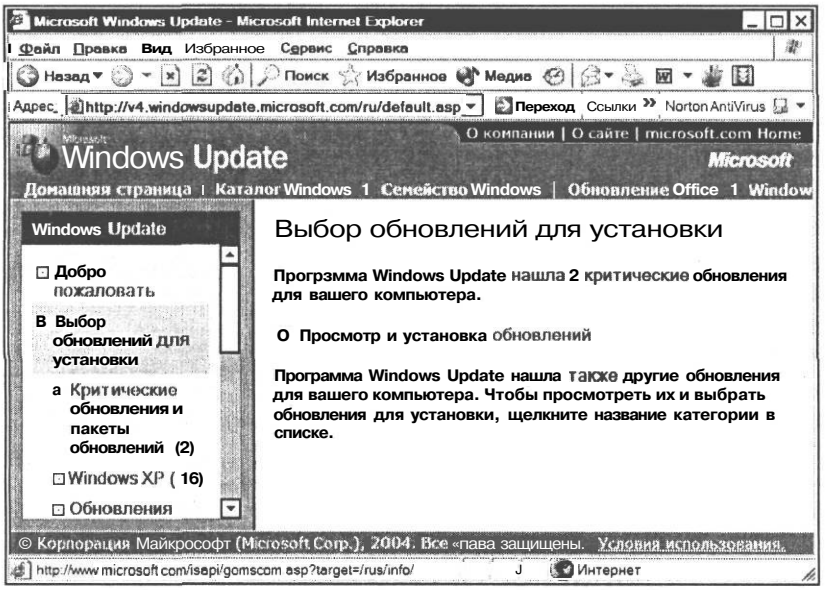



*Рис. 5.2. Выбор обновлений для установки*

На появившейся странице будет представлена информация обо всех обнаруженных критических обновлениях: их описание, размер файла, время зафузки (Рис. 5.3). Вы можете удалить любое обновление, нажав кнопку Удалить (Remove), расположенную под описанием.

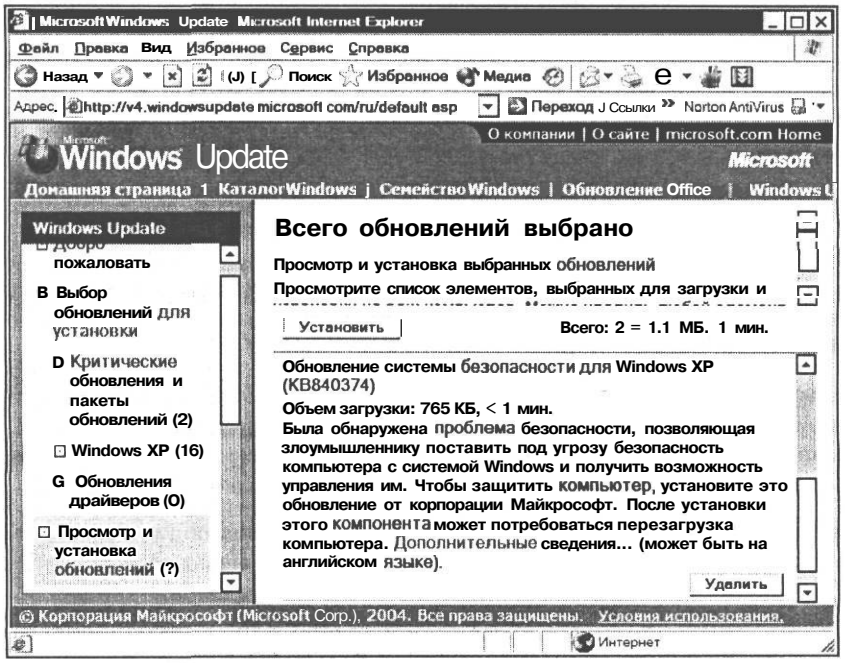



*Рис. 5.3. Информация о критических обновлениях*

➤ Нажмите кнопку **Установить** (Install Now). Программа выполнит загрузку и установку критических обновлений. Этот процесс будет отображаться в диалоге **Windows Update** (Обновление Windows) (Рис. 5.4).

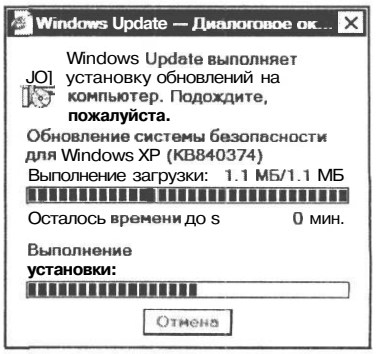



*Рис. 5.4. Диалог **Windows Update** (Обновление Windows)*

Чтобы просмотреть и установить прочие обновления, не являющиеся критическими, следует использовать ссылки в левой части Web-страницы.

Если вы ранее не выполняли обновлений, то может потребоваться загрузить большой объем данных - 100-500 Мбайт. В таком случае лучше загружать обновления по частям: сначала - наиболее важные критические обновления, чтобы закрыть самые опасные «дыры» в системе безопасности, потом, со временем - менее важные. Чтобы выбрать наиболее важные обновления, следует воспользоваться Анализатором основных элементов защиты Microsoft (Microsoft Baseline SecurityAnalyzer).

## Анализатор безопасности системы

Для оценки уязвимости компьютеров с операционной системой Windows, определения наличия свежих патчей и обновлений систем безопасности корпорация Microsoft разработала специальную программу - Microsoft Baseline Security Analyzer, MBSA (Анализатор основных элементов защиты). Эта программа обеспечивает возможность сканирования как отдельного компьютера, так и всех машин сети с целью оценки уровня безопасности, получения отчета и рекомендаций о необходимых действиях. MBSA определяет, какие патчи уже установлены, и дает рекомендации о необходимости установки других критических обновлений. Запустить программу можно на компьютерах с операционной системой Windows 2000 Professional, Windows 2000 Server, Windows XP Home или Windows XP Professional.

Программа Microsoft Baseline Security Analyzer 1.2 записана на диске CD-ROM, прилагаемом к этой книге. Установите ее, подключитесь к Интернету и запустите, дважды щелкнув мышью на значке с таким же именем, находящемся на **Рабочем столе** (Desktop), или выбрав команду главного меню **Программы * Microsoft Baseline Security Analyzer 1.2** (Programs * Microsoft Baseline Security Analyzer 1.2). На экране появится рабочее окно **Microsoft Baseline Security Analyzer** (Рис. 5.5).

В левой части этого окна находится меню ссылок, для выбора задачи, а в правой - элементы управления текущей задачи — ссылки: **Scan a computer** (Сканирование компьютера), **Scan more than one computer** (Сканирование более одного компьютера), **View existing security reports** (Просмотр существующего отчета о безопасности).

MBSA может выполнять проверку компьютеров, работающих под управлением операционных систем Windows NT 4, Windows 2000, Windows XP Professional и Windows XP Home Edition. Для запуска сканирования необходимо иметь права администратора.

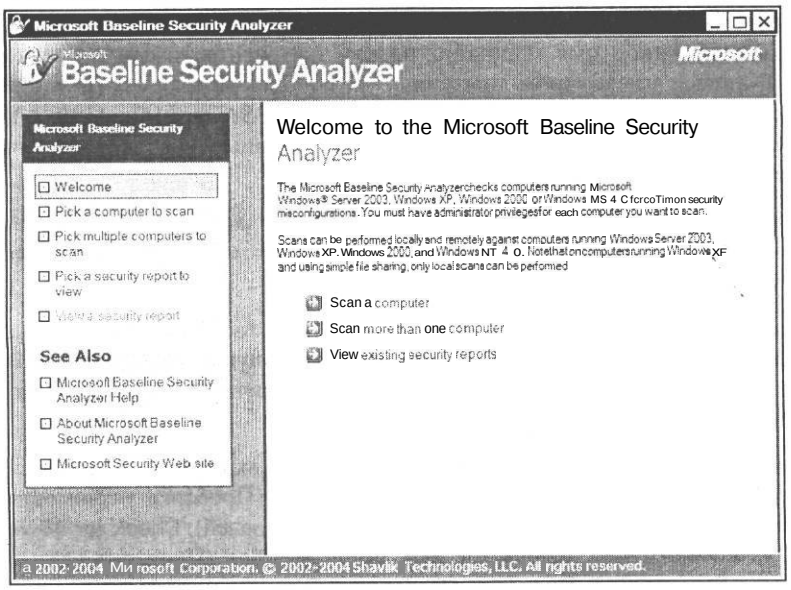



*Рис. 5.5. Рабочее окно программы* ***Microsoft Baseline Security Analyzer***

> Щелкните мышью на ссылке **Scan a computer** (Сканирование компьютера). В правой части рабочего окна отобразятся элементы управления для выбора компьютера, подлежащего проверке (Рис. 5.6).

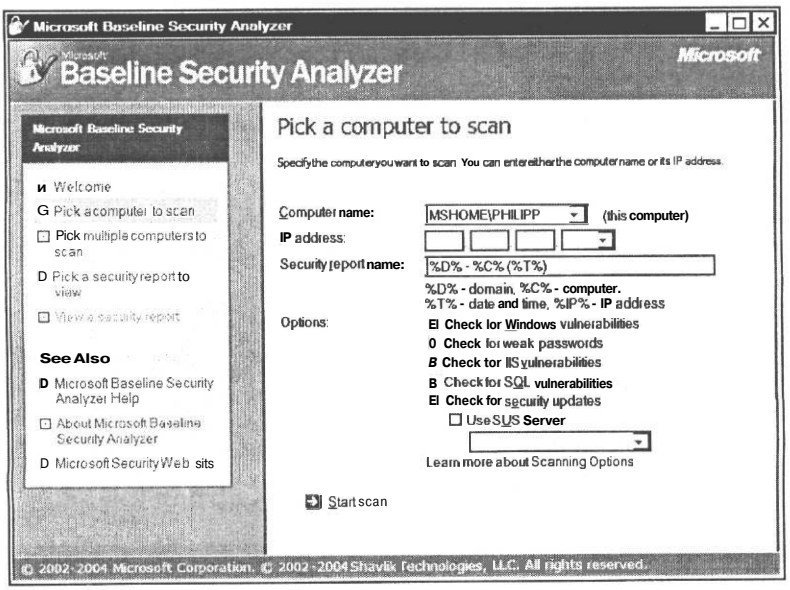



*Рис. 5.6. Выбор компьютера для сканирования*

Вы можете указать либо имя компьютера **(Computer name),** либо его IP-адрес **(IP-address).** По умолчанию выбирается компьютер, с которого запускается программа MBSA.

При сканировании более одного компьютера вы получаете возможность проверить весь домен, указав доменное имя **(Domaine name),** или протестировать все компьютеры, имеющие IP-адреса в некотором диапазоне, указав блок IP-адресов (IP **address range).** В случае тестирования домена или блока IP-адресов MBSA запрашивает все компьютеры группы и сканирует только ответившие машины. Компьютеры, которые не ответили, указываются в отдельном списке.

В поле ввода **Security report name** (Имя файла отчета) задается имя файла отчета, которое по умолчанию включает имя домена (**%D%**), имя компьютера (**%C%**), дату и время (**%T%**) и может включать IP-адрес (**%IP%**).

Для каждой проверенной машины генерируется собственный отчет по безопасности, который сохраняется на компьютере, с которого была запущена программа MBSA. Отчеты сохраняются в XML-формате в папке **SecurityScan** личной директории пользователя, находящейся в папке Мои документы (My Documents).

Установленные флажки группы Options (Параметры) включают тестирование следующих компонентов: **Check for Windows vulnerabilities** (Проверка уязвимости Windows), **Check for weak passwords** (Проверка несовершенства паролей), **Check for IIS vulnerabilities** (Проверка уязвимости IIS), **Check for SQL vulnerabilities** (Проверка уязвимости SQL), **Check for security updates** (Проверка обновления безопасности).

➤ Щелкните мышью на кнопке или ссылке **Start scan** (Начать сканирование). Программа начнет проверку системы. Ход этого процесса будет отображаться в рабочем окне (Рис. 5.7).

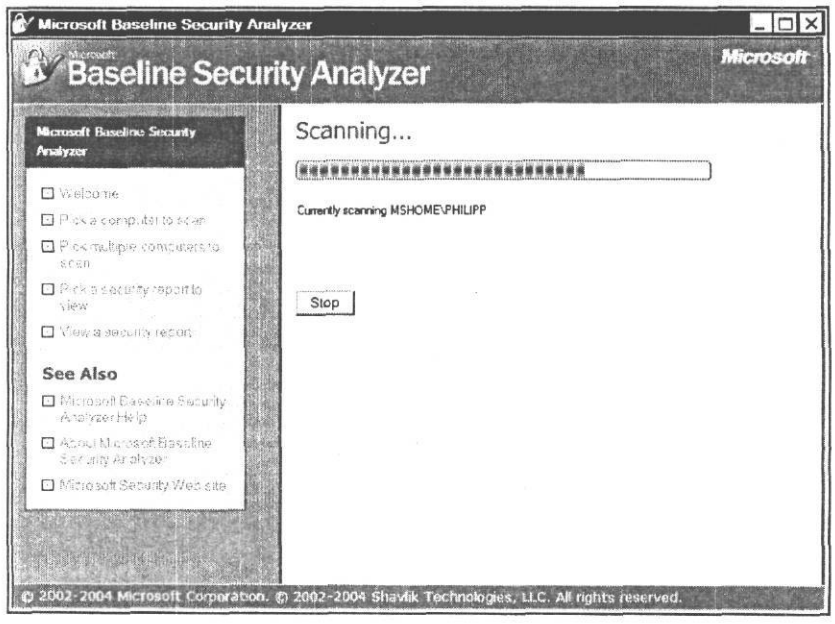



*Рис. 5.7. Сканирование системы*

➤ После окончания проверки в правой части рабочего окна вы увидите ее результаты (Рис. 5.8).

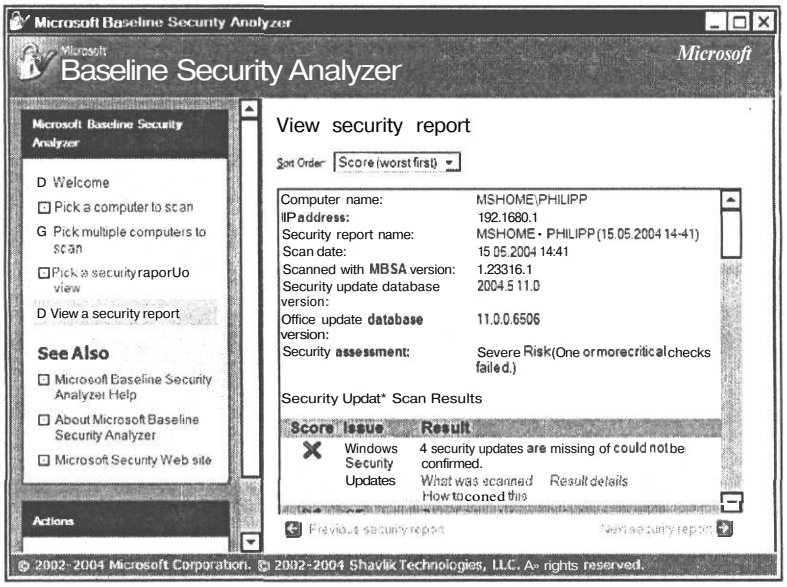



*Рис. 5.8. Результаты сканирования компьютера*

Программа выдает отчет в виде следующих одна за другой таблиц **Security Update Scan Results** (Результаты сканирования обновлений безопасности), **Windows Scan Results** (Результаты сканирования Windows), **Internet Information Services (IIS) Scan Results** (Результаты сканирования службы Internet Information Services (IIS)), **SQL Server Scan Results** (Результаты сканирования сервера SQL), **Desktop Application Scan Results** (Результаты сканирования приложений).

В таблице **Security Update Scan Results** (Результаты сканирования обновлений безопасности) приводится информация о том, каких обновлений не хватает в системе со ссылками на описание этих обновлений и их местонахождение. Причем по умолчанию в начале перечисляются самые опасные дыры, а далее менее опасные. Порядок отображения результатов задается в открывающемся списке **Sort Order** (Порядок сортировки).

Программа выполняет довольно много тестов на предмет обнаружения изъянов безопасности системы. Подробное описание основных из них приведено в этой главе, в разделе «Основные тесты уязвимости Windows». В таблицах отчета о проверке компьютера названия выполненных тестов отображаются в колонке **Issue** (Проверка), а в колонке Results (Результаты) - результат теста.

> Щелкните на ссылке **Result details** (Подробные результаты) в строке **Windows Security Updates** (Обновления безопасности Windows) таблицы. Откроется окно с подробной информацией (Рис. 5.9).

Каждому дефекту в системе безопасности, обнаруженному MBSA, ставится в соответствие выпуск бюллетеня по безопасности Microsoft, в котором содержится развернутая информация о данном обновлении. В результате проверки выявляются недостающие обновления, для которых выдаются ссылки на соответствующие бюллетени по безопасности Microsoft.

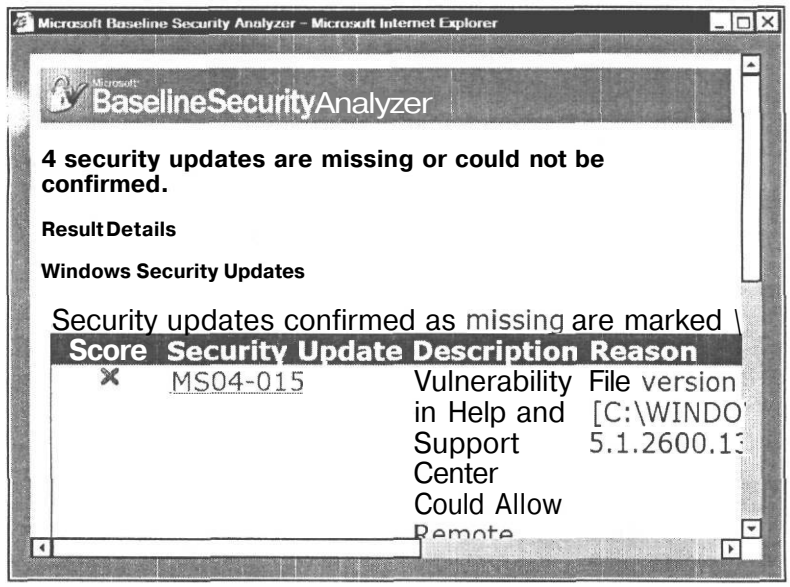



*Рис. 5.9. Окно с подробной информацией*

> Щелкните мышью на выделенной голубым цветом и подчеркнутой ссылке с кодом проблемы (например, **MS04-015**) в колонке **Security Update** (Обновление безопасности). Будет загружена Web-страница **Microsoft Security Bulletin** (Бюллетень безопасности Microsoft) на английском языке с описанием данной проблемы, рекомендациями по ее устранению и ссылкой на файл обновления для англоязычной версии операционной системы (Рис. 5.10).

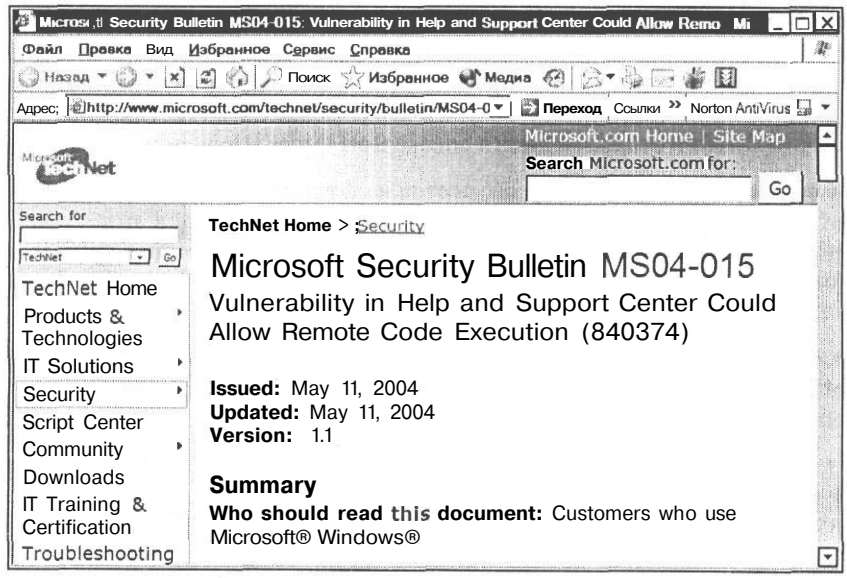



*Рис. 5.10. Бюллетень безопасности Microsoft*

> Найдите на этой странице ссылку **Download the update** (Загрузить обновление) для вашей версии Windows и щелкните на ней мышью. В окне браузера появится страница загрузки обновления для англоязычной версии Windows (Рис. 5.11).

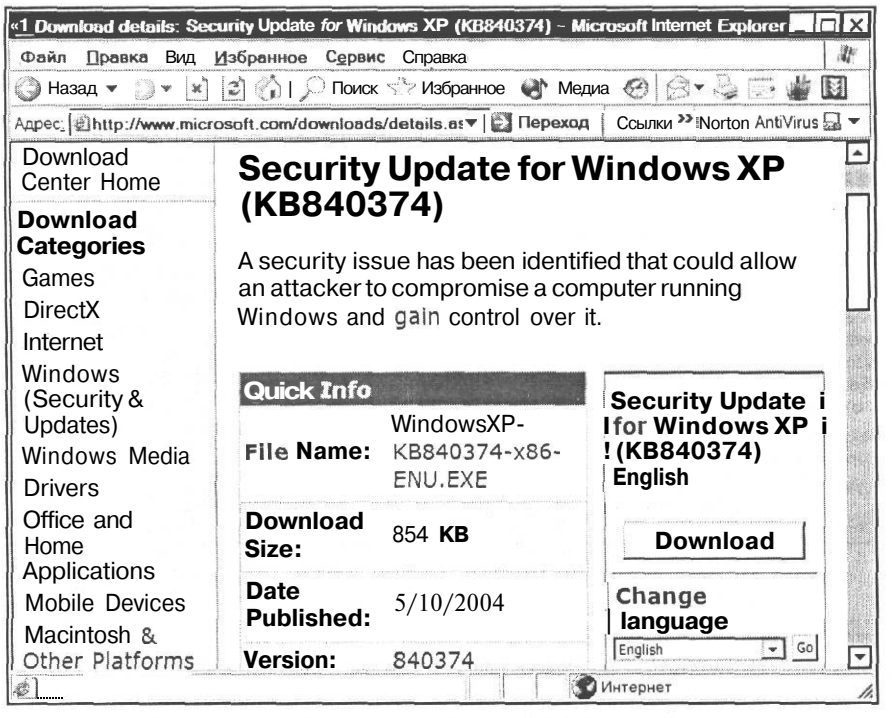



*Рис. 5.11. Web-страница Download Center (Центр загрузки Microsoft) на английском языке*

Если у вас русская версия операционной системы, то для нее необходимо найти такую же страницу на русском языке. Страница на русском языке будет также полезна, если вы работаете с английской версией операционной системы, но испытываете трудности с английским языком. Загрузить русскоязычную страницу бюллетеня можно следующим образом.

➤ В правой части Web-страницы **Download Center** (Центр загрузки Microsoft) найдите открывающийся список **Change language** (Изменить язык), выберите в нем язык **Russian** (Русский) и нажмите кнопку **Go** (Перейти). Откроется аналогичная Web-страница **Центр загрузки Microsoft** на русском языке (Рис. 5.12).

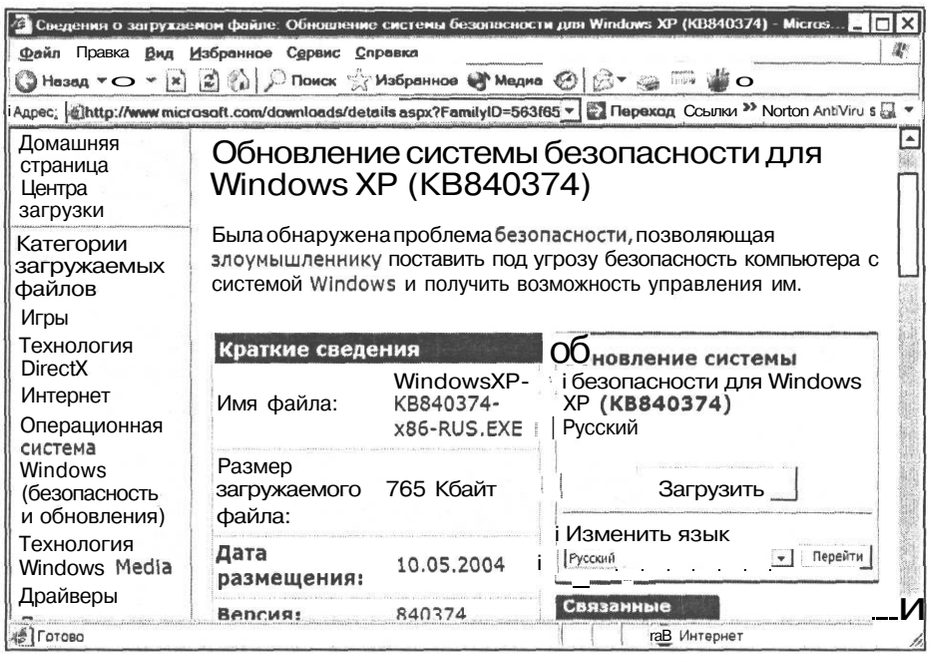



*Рис. 5.12. Web-страница* ***Центр загрузки Microsoft*** *на русском языке*

> На этой странице нажмите кнопку **Загрузить** (Download). Появится диалог **Загрузка файла** (File Download) (Рис. 5.13).

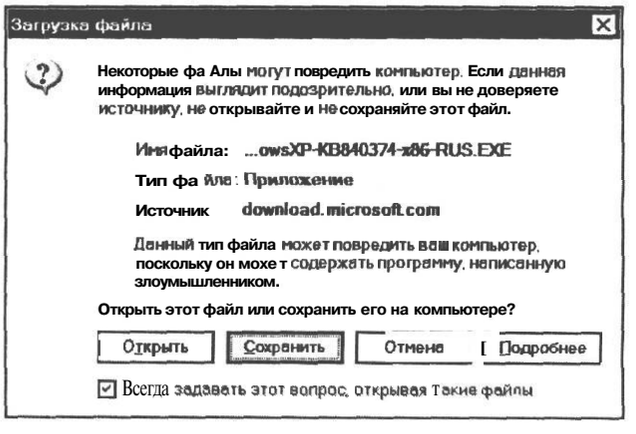



*Рис. 5.13. Диалог* ***Загрузка файла*** *(File Download)*

> Нажмите кнопку **Сохранить** (Save) в этом диалоге. Откроется диалог **Сохранить как** (Save As) (Рис. 5.14) для указания места сохранения файла.

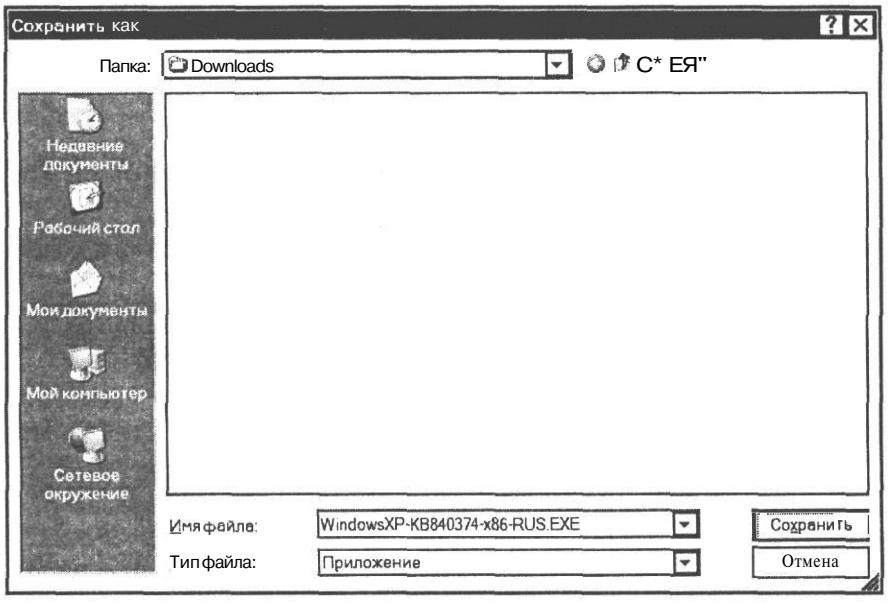



*Рис. 5.14. Диалог* ***Сохранить*** *как (Save As)*

> Выберите папку, в которой вы хотите сохранить файл, и нажмите кнопку **Сохранить** (Save). Программа загрузит выбранный файл и сохранит его в указанной папке. После окончания загрузки в диалоге **Загрузка завершена** (Download complete) (Рис. 5.15) вы увидите сообщение об этом.

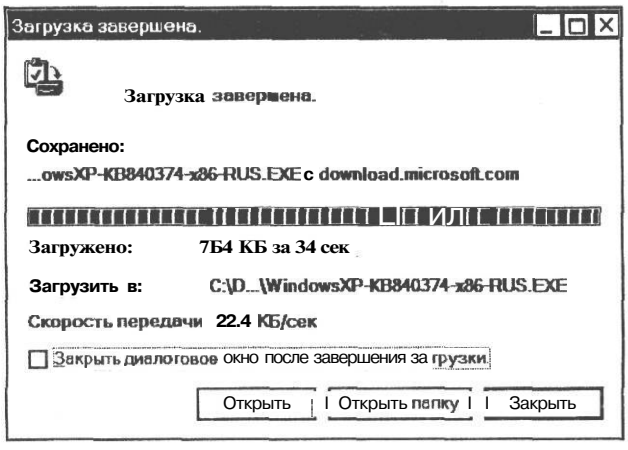



*Рис. 5.75. Загрузка завершена*

- Нажмите кнопку **Открыть папку** (Open Folder) в диалоге **Загрузка завершена** (Download complete). Этот диалог закроется, и появится окно папки, в которой сохранен файл обновления.

После того как обновление загружено, его следует установить.

- Дважды щелкните мышью на значке загруженного файла. Запустится программа установки и выполнит обновление системы.

Подобным же образом следует загрузить и установить все остальные обновления. После установки каждой заплаты необходимо перезагружать компьютер.

Преимущество обновлений по частям состоит в том, что, если вы решите переустановить операционную систему, загружать обновления заново уже не придется.

Следует иметь в виду, что обновления необходимо устанавливать все и в той последовательности, в которой они выходят, иначе может случиться так, что у вас окажутся установленные не самые последние версии файлов и некоторые заплаты придется установить снова. Впрочем, Microsoft Baseline Security Analyzer отследит эту проблему.

## Основные тесты уязвимости Windows

Напомним, что в таблицах отчета о проверке компьютера названия выполненных тестов отображаются в колонке **Issue** (Проверка), а в колонке **Results** (Результаты) — результат теста. Ниже описываются основные проверки.

### Guest Account (Гостевой доступ)

Этот тест определяет, включен ли на сканируемом компьютере режим гостевого доступа. Гостевой доступ в операционных системах Windows 2000 или Windows NT служит для входа пользователей в систему в случае, если пользователь не имеет собственной учетной записи на компьютере, домене или в доменах, из которых разрешен доступ к данному компьютеру. На компьютерах, работающих под управлением Windows XP и использующих простой общий доступ к файлам, все подсоединения пользователей через локальную сеть отражаются в гостевом доступе согласно используемой модели безопасности. Если гостевой доступ включен на компьютерах с операционной системой Windows NT, Windows 2000 и Windows XP, не использующих простой общий доступ к файлам, он будет отмечен как брешь в защите. Если гостевой доступ имеется на компьютерах с Windows XP, которые используют функцию простого общего доступа к файлам, он не будет отмечен как уязвимость

### Local Account Password Test (Тест паролей локальных учетных записей)

Эта проверка определяет учетные записи локальных пользователей, которые используют пустые или простые пароли. Данный тест не выполняется на компьютерах, выступающих в роли контроллеров домена.

В качестве обязательной меры безопасности операционные системы Windows XP, Windows 2000 и Windows NT требуют от пользователей авторизации путем ввода паролей. Однако безопасность любой системы зависит не только от технологии, но и от способа, которым управляется и настраивается система. Данный тест сканирует все учетные записи пользователей данного компьютера и проверяет их на предмет использования следующих паролей:

- пароль пустой;
- пароль совпадает с именем учетной записи пользователя;
- пароль совпадает с именем компьютера;
- паролем служит слово «password»;
- паролем служат слова «admin» или «administrator»;

Кроме того, тест выводит сообщения о заблокированных учетных записях и о тех пользователях, которым впредь закрыт доступ в систему.

### File System (Файловая система)

Этот тест проверяет файловую систему, установленную на каждом жестком диске, чтобы удостовериться, что на компьютере используется система NTFS. Файловая система NTFS обладает высоким уровнем безопасности, который позволяет вам контролировать и ограничивать доступ к файлам и директориям. К примеру, сделав необходимые записи в листах контроля доступа (Access Control Lists, ACL), вы можете позволить своим коллегам видеть файлы на вашем компьютере, но не изменять их.

### Restrict Anonymous (Ограничение анонимных пользователей)

Этот тест определяет, используется ли ключ реестра RestrictAnonymous для ограничения анонимных подключений к сканируемому компьютеру.

Анонимные пользователи могут просматривать определенный набор системной информации, включая имена и описания существующих пользователей, политики доступа и общие имена. Для повышения безопасности системы рекомендуется ограничить данную функцию и закрыть анонимным пользователям доступ к существенной информации. О том, как это сделать, написано в разделе «Запрещение подключения анонимных пользователей» знакомства «Несколько простых шагов
по настройке безопасности Windows XP» этой главы.

### Administrators (Члены группы администраторов)

Эта проверка определяет и выводит на экран список пользователей, принадлежащих к группе администраторов компьютера. В случае если выявляется более двух индивидуальных пользователей, входящих в данную группу, программа указывает их и отмечает данный факт как потенциальную уязвимость в системе защиты. Вообще рекомендуется свести число пользователей с правами администратора системы к минимуму, так как администратор по умолчанию обладает полный контролем над компьютером.

### Autologon (Автоматический вход в систему)

Эта проверка определяет, включен ли на сканируемом компьютере режим автоматического входа в систему и хранится ли при этом пароль доступа в незашифрованном виде или же он зашифрован в реестре. В случае если режим автоматического входа в систему включен и пароль сохранен в незашифрованном виде, данный факт отражается в отчете по безопасности как крайне высокая уязвимость системы защиты. Если режим автома-

тического входа в систему включен и пароль зашифрован в реестре, отчет по безопасности отмечает это как потенциальную брешь в защите.

Режим автоматического входа в систему сохраняет имя пользователя и пароль в реестре и позволяет вам автоматически входить в операционную систему Windows 2000 или Windows NT, не вводя имени и пароля. Такой режим входа в систему дает также и другим пользователям возможность доступа к вашим файлам и совершения злонамеренных действий с системой. Например, любой человек, имеющий физический доступ к вашему компьютеру, может перезагрузить его и автоматически войти в систему. Поэтому, если у вас включен данный режим и вы не хотите от него отказываться, удостоверьтесь, что на компьютере нет никакой важной информации. Так как любой, имеющий возможность физического доступа к вашему компьютеру, может воспользоваться режимом автоматического входа в систему, желательно использовать эту функцию исключительно в надежной и безопасной среде. Вы можете хранить пароль, который используется для автоматического входа в систему, в реестре в незашифрованном виде или же зашифровать его при помощи сервиса локальной авторизации безопасности (Local Security Authority, LSA).

### Password Expiration (Сроки действия паролей)

Этот тест определяет наличие в системе учетных записей пользователей, которые имеют пароли без ограничения срока действия. В целях повышения безопасности системы рекомендуется регулярно изменять имеющиеся пароли. По этой причине в отчете по безопасности MBSA отражается каждая учетная запись с паролем без ограничения срока действия.

### Auditing (Аудит)

Этот тест определяет, запущена ли на сканируемом компьютере система аудита. Операционные системы Microsoft Windows обладают возможностью аудита, которая позволяет отслеживать и записывать ключевые события, происходящие с компьютером, такие как удачные и неудачные попытки входа в систему. Мониторинг журнала событий системы поможет в обнаружении потенциальных уязвимостей и попыток проникновения.

### Services (Сервисы)

Этот тест проверяет наличие на компьютере запущенных сервисных программ, перечисленных в файле **services.txt**. В этом файле содержится список программ, которые не должны быть запущены на сканируемом компьютере. Файл **services.txt** инсталлируется MBSA и сохраняется в инсталляционной папке программы. Пользователь программы может самостоятельно добавить в список **services.txt** дополнительные программы для сканирования. По умолчанию файл содержит следующие сервисные программы: MSFTPSVC (FTP), TlntSvr (Telnet), RasMan (Remote Access Service Manager), W3SVC (WWW), SMTPSVC (SMTP).

В Windows XP, Windows 2000 и Windows NT 4.0 сервисной программой называется программа, которая исполняется на компьютере с работающей операционной системой без необходимости запуска ее пользователем (в ряде случаев пользователю даже не нужно входить в систему). Эти программы предназначены для выполнения не зависящих

от пользователя программ, например, программы приема факсов, находящейся в режиме ожидания входящих сообщений.

### Sharing (Совместно используемые ресурсы)

Этот тест определяет наличие на сканируемом компьютере любых папок, открытых для общего доступа. Тест выдает список всех общих ресурсов, которые имеются на компьютере, в соответствии с разрешениями по уровню пользования общими ресурсами и разрешениями, указанными для файловой системы NTFS. Вы можете отключить возможность совместного доступа к лишним ресурсам или же обезопасить их, ограничив, при помощи соответствующих разрешений, круг пользователей.

### Windows Version (Версия Windows)

Эта проверка определяет версию операционной системы, которая используется на сканируемом компьютере. По сравнению с предыдущими версиями операционные системы Windows XP и Windows 2000 имеют более высокие возможности по обеспечению безопасности и более качественное управление доступом к данным.

### IE Zones (Зоны безопасности в Internet Explorer)

Этот тест перечисляет существующие установки по безопасности для зон обозревателя Internet Explorer и вносит рекомендации по их изменению на сканируемом компьютере для каждого пользователя.

Пользователь может выставить вручную гораздо более безопасные установки для зон, нежели рекомендованные MBSA. В случае если программа сообщает об обнаруженных пользовательских настройках, она не может определить, являются ли они более или менее безопасными, нежели рекомендуемые.

Функция зон Интернета браузера Internet Explorer разделяет Интернет и Интранет на зоны с разным уровнем безопасности. Это дает вам возможность, используя общие установки обозревателя, получать всю информацию с доверенных Web-сайтов или же запретить исполнение ряда приложений, например Java-апплетов или ActiveX-элементов, с непроверенных сайтов.

Обозреватель Internet Explorer по умолчанию имеет четыре зоны: **Интернет** (Internet), **Местная интрасеть** (Local Intranet), **Надежные узлы** (Trusted sites) и **Ограниченные узлы** (Restricted sites). В диалоге **Свойства обозревателя** (Internet Options) вы можете сделать настройки для каждой зоны и, в зависимости от уровня доверия, добавить и удалить сайты в каждую из зон, за исключением зоны **Интернет** (Internet).

Установки для зон также могут выполнить администраторы системы. Кроме того, администраторы могут добавить или удалить сертификаты издателей программного обеспечения, которым они доверяют (или не доверяют) и освободить пользователей в их повседневной жизни от необходимости принятия решений по информационной безопасности.

Для каждой зоны вы можете выбрать «высокий», «средний» и «низкий» уровень безопасности или же сделать собственные пользовательские установки. Microsoft рекомендует установить «высокий» уровень безопасности для сайтов в зоне с неопределенной надежностью.

Пользовательские настройки дают опытным пользователям и администраторам больший контроль над такими функциями безопасности, как доступ к файлам, элементам и скриптам ActiveX, уровнем производительности Java-апплетов, использованием для идентификации протокола Secure Socket Layer (SSL), авторизацией при помощи NTLM (в зависимости от зоны, к которой относится сервер, Internet Explorer может отсылать пароль автоматически, запрашивать пользователя о вводе имени и пароля или же просто запретить запросы на авторизацию, поступающие с сервера).

### Macro Security (Безопасность макросов)

Этот тест определяет уровень безопасности, используемый для защиты от макросов в Microsoft Office XP, Office 2000 и Office 97. MBSA проверяет такие составные компоненты Microsoft Office, как PowerPoint, Word, Excel и Outlook.

Макросы являются автоматически повторяющимися задачами, которые экономят время пользователя при работе. Однако макросы также могут использоваться для переноса вирусов в случае, если пользователь открыл документ, содержащий макрос, созданный злоумышленником. Работа и обмен зараженными документами могут позволить макросу-вредителю распространиться как в другие документы на компьютере пользователя, так и на все компьютеры локальной сети.

## Несколько простых шагов по настройке безопасности Windows XP

Чтобы обеспечить безопасность сети, кроме обновлений операционной системы каждого компьютера, на узловой машине, подключенной к Интернету, следует выполнить минимум обязательных настроек, которые предотвратят многие сетевые атаки и обеспечат безопасное соединение с глобальной сетью. Эти настройки включают запрещение опасных служб, удаление некоторых программ и ограничение установки новых программ, преобразование файловой системы в NTFS, ограничение доступа к общим ресурсам, запрещение гостевого доступа и доступа анонимных пользователей и другие меры неизбежно приведут к потере функциональности компьютера, но обеспечат относительную безопасность.

При создании локальной сети рекомендуется переустановить операционную систему Windows XP на том компьютере, который будет подключен к Интернету, заново, переформатировав жесткий диск и выбрав файловую систему NTFS. Это обеспечит стабильную работу системы, повышенный уровень безопасности и позволит избежать возможных проблем, связанных с вирусами и другими вредителями.

На компьютере, который подключается к провайдеру, лучше не использовать программы, работающие с Интернетом. Во всяком случае, крайне нежелательно использование на этом компьютере таких популярных программ, как Internet Explorer и Outlook Express. Бреши в системе безопасности этих программ используются хакерами наиболее часто.

## Отключение автоматического обновления Windows

Хотя корпорация Microsoft настоятельно рекомендует использовать автоматическое обновление Windows по расписанию, мы не советуем этого делать и предлагаем вообще не использовать никаких автоматических функций, работающих с системными файлами без вашего участия. Хакеры владеют достаточными возможностями, чтобы автоматически «обновить» вашу систему до нужного им уровня. Поэтому рекомендуем отключить автоматическое обновление системы. Для этого следует сбросить флажок Выполнять обновление системы (Keep my computer up to date) на вкладке Автоматическое обновление (Automatic Updates) диалога Свойства системы (System Properties) (Рис. 5.16). Напомним, что этот диалог можно вызвать из Панели управления (Control Panel) или нажатием комбинации клавиш [⊞]+[Pause].

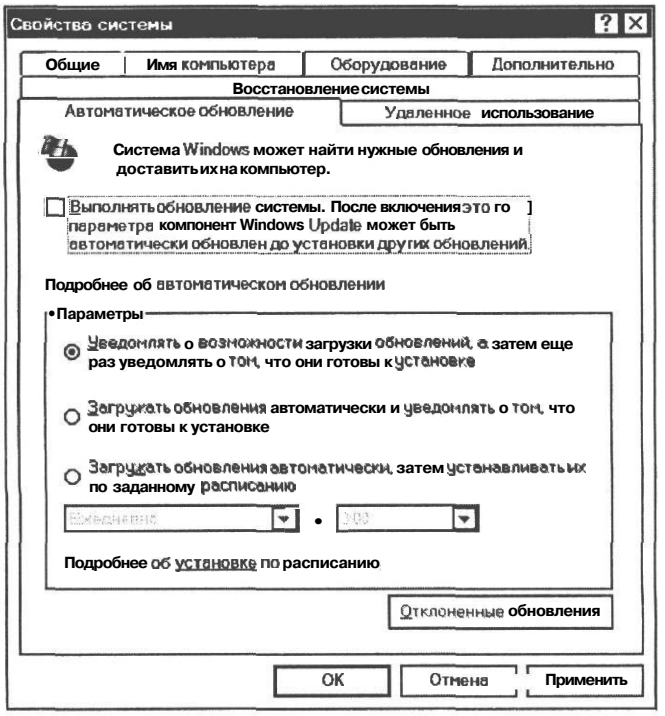



*Рис. 5.16. Вкладка Автоматическое обновление (Automatic Updates) диалога Свойства системы (System Properties)*

## Отключение восстановления Windows

Мы не рекомендуем также использовать автоматическое восстановление системы. Windows XP может корректно восстановить систему далеко не всегда. Выполнять восстановление

лучше другими средствами, например, с помощью Norton Ghost. Чтобы отключить автоматическое восстановление, следует установить флажок **Отключить восстановление системы на всех дисках** (Turn off System Restore) на вкладке **Восстановление системы** (System Restore) диалога **Свойства системы** (System Properties) (Рис. 5.17).

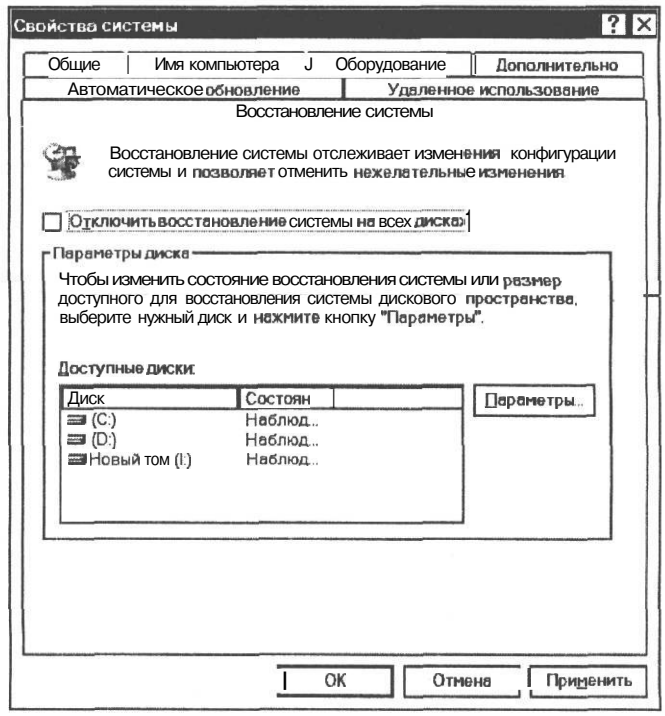



*Рис. 5.17. Вкладка **Восстановление системы** (System Restore) диалога **Свойства системы** (System Properties)*

## Запрещение удаленного доступа к компьютеру

Вредными, с точки зрения безопасности, являются функции использования удаленного помощника и удаленного управления рабочим столом. На компьютере, обеспечивающем общий доступ к Интернету, включение этих режимов просто опасно. Для отключения указанных функций следует сбросить флажки **Разрешить отправку приглашения удаленному помощнику** (Allow Remote Assistance invitations to be sent from this computer) и **Разрешить удаленный доступ к этому компьютеру** (Allow users to connect remotely to this computer) на вкладке **Удаленное использование** (Remote) диалога **Свойства системы** (System Properties) (Рис. 5.18).

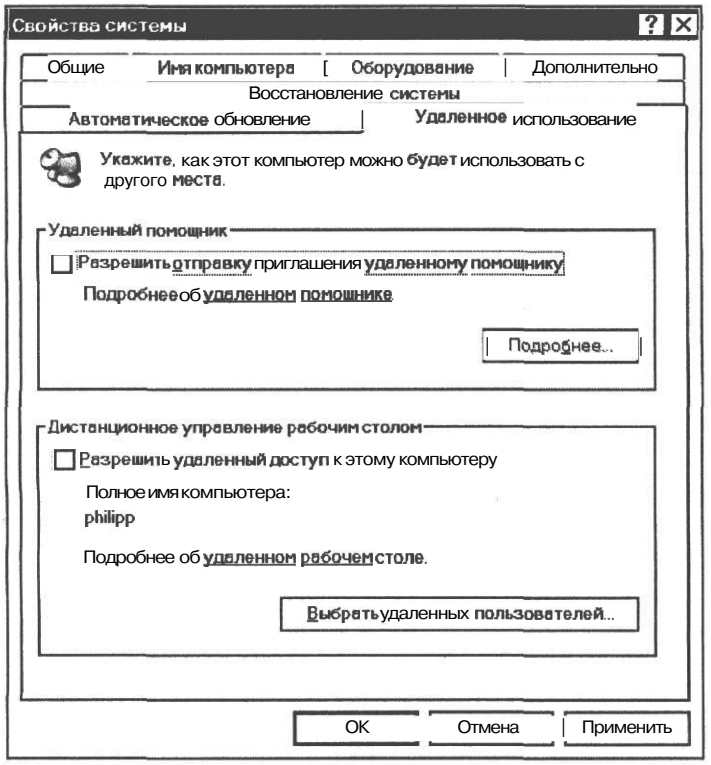



*Рис. 5.18. Вкладка **Удаленное использование (Remote)** диалога **Свойства системы** (System Properties)*

## Запрещение использования DCOM

Среди многочисленных служб, которыми располагает Windows, особое место занимают службы компонентов COM (Component Object Model - Компонентная модель объектов). Из компонентов COM разработчики могут создавать сложные приложения посредством связывания различных объектов. Помимо COM, существует еще модель распределенных объектов - DCOM (Distributed Component Object Model). Она использует различные компоненты, которые могут находиться на разных компьютерах сети и подключаться по мере надобности.

По умолчанию службы компонентов COM включены, но в домашней и малой офисной сети они обычно не используются. В целях безопасности их следует отключить.

➤ В окне **Панель управления** (Control Panel) дважды щелкните мышью на значке **Администрирование** (Administrative Tools). Откроется окно **Администрирование** (Administrative Tools).

➤ Дважды щелкните мышью на значке **Службы компонентов** (Component Services). На экране появится окно консоли MMC **Службы компонентов** (Component Services) (Рис. 5.19).


*Рис. 5.19.* Окно *консоли MMC* ***Службы компонентов*** *(Component Services)*

> Дважды щелкните мышью в левой части окна на ветви **Службы компонентов** (Component Services). Ветвь развернется. В ней содержится папка **Компьютеры** (Computers).

➤ Дважды щелкните мышью на папке **Компьютеры** (Computers). Эта папка откроется, и вы увидите содержащийся в ней элемент **Мой компьютер** (My Computer) (Рис. 5.20).

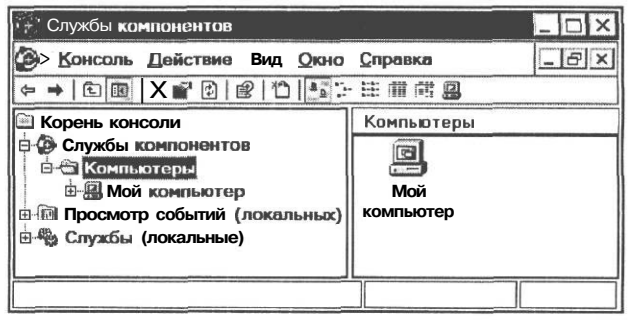



*Рис. 5.20. Содержимое службы компонентов*

> Щелкните правой кнопкой мыши на значке **Мой компьютер** (My Computer) в окне **Службы компонентов** (Component Services) и в появившемся контекстном меню выберите команду Свойства (Properties). На экране появится диалог **Свойства: Мой компьютер** (My Computer Properties).

> Перейдите на вкладку **Свойства по умолчанию** (Default Properties), (Рис. 5.21) щелкнув мышью на этом ярлыке.

➤ Сбросьте флажок **Разрешить использование DCOM на этом компьютере** (Enable Distributed COM on this computer).

➤ Нажмите кнопку **Применить** (Apply).

➤ Закройте диалог **Свойства: Мой компьютер** (My Computer Properties) нажатием кнопки **OK.**

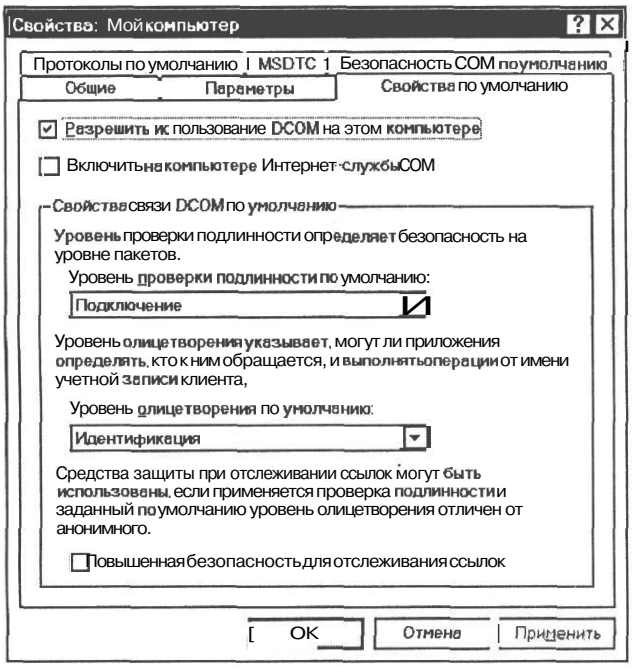



*Рис. 5.21. Вкладка Свойства по умолчанию (Default Properties) диалога Свойства: Мой компьютер (My Computer Properties)*

Такая установка запрещает использование COM и DCOM на компьютере.

## Остановка опасных и бесполезных служб

При загрузке операционной системы запускается множество программ, называемых службами, каждая из которых выполняет определенные функции, обеспечивающие работу системы и прикладных программ. Среди служб есть и такие, которые во многих случаях не используются, а также такие, которые представляют определенную угрозу для безопасности. Кроме того, каждая служба использует часть оперативной памяти, которой всегда не хватает. К опасным и бесполезным службам можно отнести:

Служба обнаружения SSDP (SSDP Discovery Service) - включает обнаружение универсальных PnP-устройств в домашней сети;

Узел универсальных PnP-устройств (Universal Plug and Play Device Host) - обеспечивает поддержку универсальных PnP-устройств узла;

Модуль поддержки NetBIOS через TCP/IP (TCP/IP NetBIOS Helper) - включает поддержку службы NetBIOS через TCP/IP и разрешения имен NetBIOS в адреса. Несмотря на то, что после отключения этой службы компьютер не будет виден в сети по имени (но будет доступен по IP-адресу), очень важно все же отключить ее, так как она открывает возможность несанкционированного доступа к вашему компьютеру.

На компьютере, который подключается к Интернету, работу указанных служб необходимо остановить следующим образом.

➤ В окне **Службы компонентов** (Component Services) (Рис. 5.19) дважды щелкните мышью на ветви **Службы (локальные)** (Services (Local)). В правой части окна отобразится перечень всех служб Windows (Рис. 5.22).

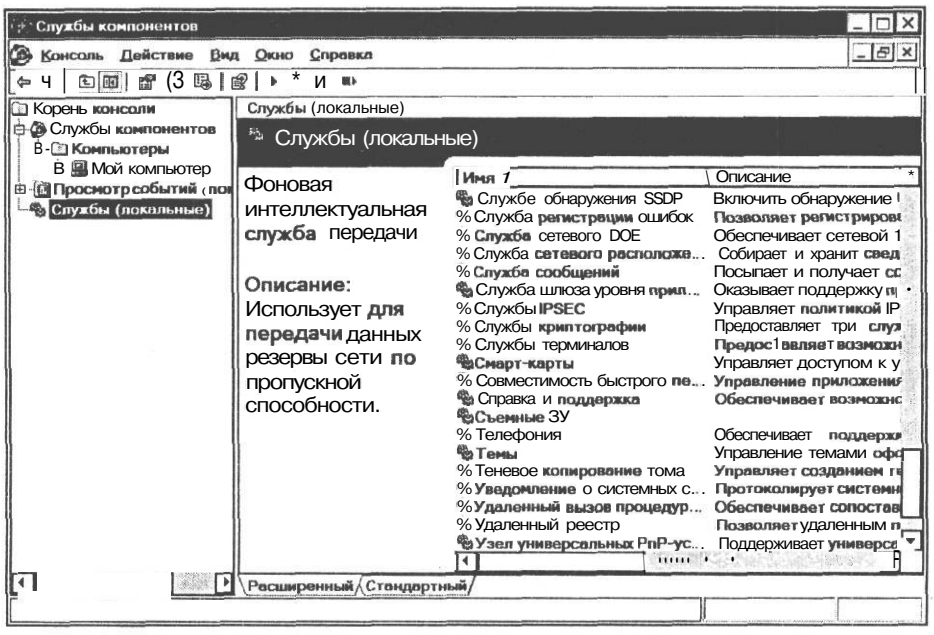



*Рис. 5.22. Службы Windows*

Перечень служб выводится в виде таблицы, где для каждой службы указывается **Имя** (Name), **Описание** (Description), **Состояние** (Status), **Тип запуска** (Startup Type) и другие свойства. Если служба запущена, то в колонке **Состояние** (Status) указано: **Работает** (Started). В противном случае эта колонка для данной службы - пустая.

➤ Щелкните правой кнопкой мыши на строке с названием сервиса **Служба обнаружения SSDP** (SSDP Discovery Service) и в появившемся контекстном меню выберите команду **Свойства** (Proprties). На экране появится диалог **Служба обнаружения SSDP (Локальный компьютер) - свойства** (SSDP Discovery Service Properties (Local Computer)) с открытой вкладкой Общие (General) (Рис. 5.23).

➤ В открывающемся списке **Тип запуска** (Startup Type) выберите **Отключено** (Disabled).

➤ Нажмите кнопку **Применить** (Apply).

> Закройте диалог **Служба обнаружения SSDP (Локальный компьютер) - свойства** (SSDP Discovery Service Properties (Local Computer)) нажатием кнопки **OK.** Вы возвратитесь к окну **Службы компонентов** (Component Services)

Служба будет остановлена. В колонке **Состояние (Status)** строки таблицы с названием выбранного сервиса исчезнет отметка **Работает** (Started).

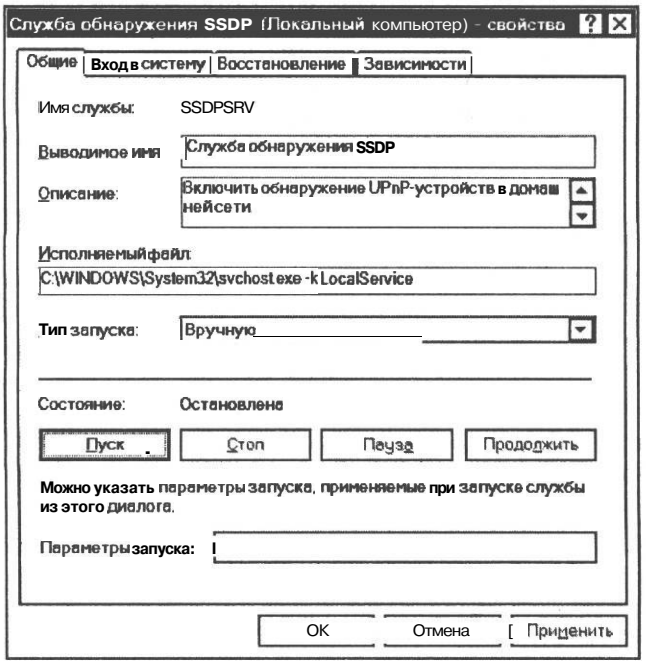



*Рис. 5.23. Вкладка* ***Общие*** *(General) диалога* ***Служба обнаружения SSDP (Локальный компьютер) - свойства*** *(SSDP Discovery Service Properties (Local Computer))*

- Подобным же образом остановите службы Узел универсальных PnP-устройств (Universal Plug and Play Device Host) и Модуль поддержки NetBIOS через TCP/IP (TCP/IP NetBIOS Helper).

➤ Закройте окно Службы компонентов (Component Services), нажав кнопку ☒ в правом верхнем его углу.

Описанным способом можно остановить и другие службы, которые не используются на компьютере. Но следует помнить, что отключать службы надо очень аккуратно. Лучше оставить что-то лишнее, чем удалить необходимый для работы компонент. Лучше устанавливать режим запуска Вручную (Manual), чтобы операционная система при необходимости могла загрузить требуемую службу. В противном случае могут возникнуть ошибки в работе программ вплоть до краха системы, пропадет доступ к некоторым возможностям, да и просто работать станет некомфортно.

## Преобразование файловой системы в NTFS

Как мы уже отмечали ранее, Windows 2000/XP поддерживает три основные файловые системы FAT, FAT32 и NTFS. Наиболее предпочтительной среди них является NTFS, обеспечивающая скоростное выполнение стандартных операций над файлами, включая чтение, запись, поиск, и предоставляющая пользователям дополнительные возможности, такие, например, как восстановление поврежденной файловой системы на больших дисках.

Файловая система NTFS обеспечивает поддержку больших, до 2 терабайт (Тбайт) дисков, контроль доступа к данным и привилегии владельца, играющие исключительно важную роль в обеспечении безопасности и целостности важных конфиденциальных данных. Папки и файлы NTFS могут иметь назначенные им права доступа вне зависимости от того, являются ли они разделяемыми, т. е. доступными для других пользователей сети, или нет.

Выбор файловой системы, которая будет использоваться в Windows 2000/XP, осуществляется пользователем в процессе установки операционной системы и зависит от цели, для которой предполагается использовать компьютер, аппаратной платформы, количества и объема жестких дисков, используемых в системе приложений, требований к безопасности.

Файловая система NTFS является наилучшим выбором для использования на дисках большого объема. Если же к системе предъявляются повышенные требования, которые можно реализовать только в NTFS, например, по эффективному использованию дискового пространства или обеспечению безопасности данных, то данную файловую систему следует использовать и на небольших дисках.

Определить, какая файловая система установлена на ваших дисках, можно на вкладке **Общие** (General) диалога **Свойства** (Properties) (Рис. 5.24) соответствующего диска. Этот диалог открывается щелчком правой кнопкой мыши на значке диска в программе Проводник (Windows Explorer).

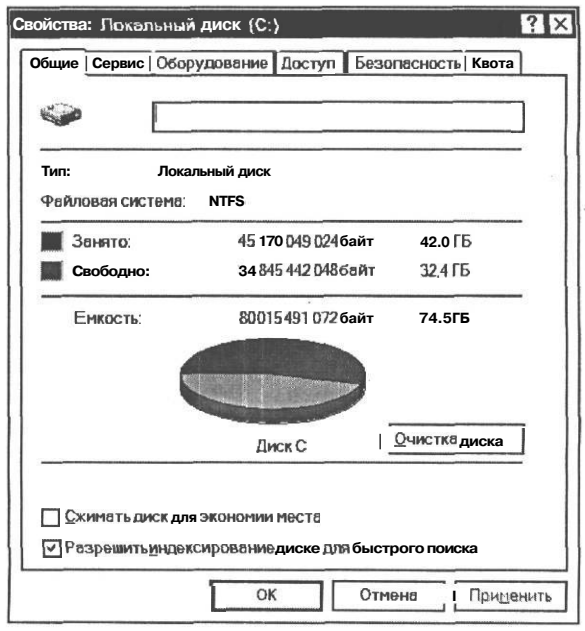



*Рис. 5,24. Вкладка **Общие** (General) диалога **Свойства** (Properties) жесткого диска*

Если у вас установлена файловая система FAT или FAT32, то для обеспечения более эффективного использования дискового пространства и более высокой степени защиты данных следует преобразовать файловую систему в NTFS. Для этого служит команда **CONVERT,** позволяющая преобразовать файловую систему без потери данных.

Примите во внимание, однако, что если вы используете на одном компьютере несколько операционных систем, то не сможете получить доступ к файлам NTFS из другой операционной системы. Кроме того, невозможно преобразовать в NTFS диск, сжатый программой динамического сжатия. Предварительно необходимо выполнить декомпрессию.

Для преобразования файловой системы в NTFS выполните следующие шаги.

➤ Нажмите кнопку Пуск (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Программы ◆ Стандартные • Командная строка** (Programs ◆ Accessories ◆ Command Prompt). На экране появится окно **Командная строка** (Command Prompt) (Рис. 5.25).

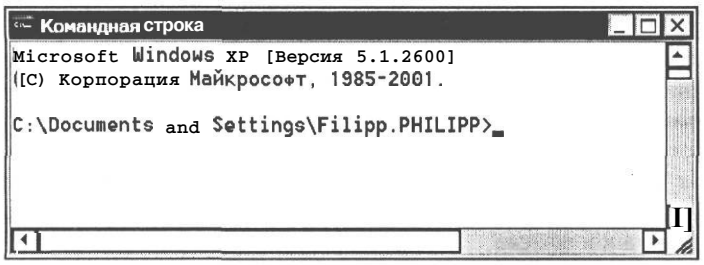



*Рис. 5,25. Окно **Командная строка** (Command Prompt)*

Каждая команда операционной системы состоит из имени, аргументов и параметров. Для выполнения преобразования файловой системы в NTFS следует ввести команду **CONVERT** и **в** качестве ее аргумента указать диск, подлежащий преобразованию, - **C:**, а в качестве параметра - название файловой системы - **NTFS.**

➤ В ответ на приглашение DOS введите с клавиатуры следующую команду:

**CONVERT C: /FS:NTFS /V**

Параметр **/V** предписывает программе отображать на экране сообщения о ходе преобразования. Команда должна заканчиваться нажатием клавиши Enter.

После нажатия клавиши Enter в окне **Командная строка** (Command Prompt) появится сообщение о типе текущей файловой системы на выбранном диске и будет выдан запрос о метке диска. Далее может появиться запрос об отключении тома, на который следует ответить «нет», и после этого, если диск загружаемый, будет предложено отложить процедуру преобразования до следующей перезагрузки операционной системы. С этим предложением следует согласиться, нажав клавиши Y и Enter, после чего появится сообщение: **Преобразование будет выполнено автоматически при следующей перезагрузке операционной системы** (The conversion will be take place automatically the next system restarts).

➤ Закройте окно **Командная строка** (Command Prompt), нажав кнопку ☒ в правом верхнем его углу, и перезагрузите компьютер.

После начальной загрузки Windows автоматически выполнит преобразование файловой системы в NTFS. На экране будут выводиться сообщения с информацией о выполняющихся операциях.

Тома, преобразованные из файловой системы FAT в NTFS, несколько уступают по быстродействию томам, непосредственно отформатированным в NTFS. В преобразованных томах основная таблица файлов (MFT) может оказаться фрагментированной. Кроме того, в преобразованных загрузочных томах разрешения на доступ NTFS недействительны после преобразования тома.

## Выключение режима простого доступа к файлам

По умолчанию в Windows XP включен режим простого общего доступа к файлам. В этом режиме в диалогах свойств файлов и папок отсутствует вкладка **Безопасность** (Security) и исключается возможность задания специальных разрешений доступа к данным.

Чтобы обеспечить возможность настойки специальных разрешений, необходимо выключить указанный режим, бросив флажок **Использовать простой общий доступ к файлам (рекомендуется)** (Use simple file sharing (Recommended)) на вкладке Вид (View) диалога **Свойства папки** (Folder Options). Доступ к этому диалогу осуществляется командой меню **Сервис * Свойства папки** (Tools ◆ Folder Options) в окне программы Проводник (Windows Explorer). Эта операция подробно описана в главе «Создание локальной сети дома и в офисе».

## Ограничение доступа к системному диску

На вкладке **Безопасность** (Security) диалога **Свойства** (Properties) системного диска C: (Рис. 5.26) в список **Группы и пользователи** (Group of user names) по умолчанию включена группа **Все** (Everyone).

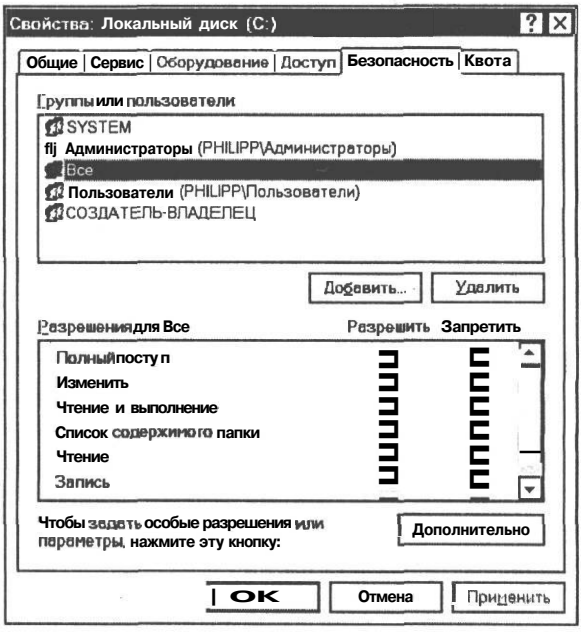



*Рис. 5.26. Вкладка **Безопасность** (Security) диалога **Свойства: Локальный диск (C:)** (Local Disk (C:) Properties)*

- Чтобы открыть указанную вкладку, в окне программы Проводник (Windows Explorer) щелкните правой кнопкой мыши на значке системного диска **Локальный диск (C:)** (Local Disk (C:)) и в появившемся контекстном меню выберите команду Общий доступ и безопасность (Sharing and Security).

Хотя явные разрешения для группы Все (Everyone) в этом диалоге по умолчанию не заданы, все же само присутствие данной группы нежелательно и опасно. Ее следует удалить.

- Щелкните мышью в списке Группы и пользователи (Group of user names) на названии группы Все (Everyone), чтобы выделить ее.
- Нажмите кнопку Удалить (Remove). Выбранная группа будет удалена из списка.
- Нажмите кнопку Применить (Apply).
- Закройте диалог Свойства: Локальный диск **(C:)** (Local Disk (C:) Properties) нажатием кнопки OK.

Удаление группы Все (Everyone) ограничит доступ к системному диску.

## Запрещение общего доступа к дискам и папкам

По умолчанию Windows XP создает ряд скрытых общих дисков и папок, используемых в административных целях, которые не видны в сетевом окружении, но легко доступны с помощью других средств. Увидеть их можно следующим образом.

- Откройте окно Панель управления (Control Panel), нажав кнопку Пуск (Start) и выбрав в главном меню Windows команду Панель управления (Control Panel).
- Откройте окно Администрирование (Administrative Tools), дважды щелкнув мышью на значке Администрирование (Administrative Tools).
- Откройте окно консоли MMC Управление компьютером (Computer Management), дважды щелкнув мышью на значке Управление компьютером (Computer Management).
- Дважды щелкните мышью в левой части окна на ветви Общие папки (Shared Folders), чтобы увидеть ее содержимое.
- Таким же образом откройте папку Общие ресурсы (Shares). В правой части окна Управление компьютером (Computer Management) вы увидите скрытые общие диски и папки, используемые для административных целей (Рис. 5.27).

Значок $ в конце имени каждого ресурса означает, что данный объект скрыт в сетевом окружении.

Наличие таких общих папок представляет определенную угрозу для безопасности сети, так как к ним возможен доступ злоумышленников. Поэтому выделение указанных ресурсов в общее пользование следует запретить. В контекстном меню каждого из этих объектов русской версии Windows XP есть команда Прекратить общий доступ. Однако она действует только в текущем сеансе. После перезагрузки общий доступ к указанным дискам и папкам будет восстановлен. Чтобы все-таки запретить общий доступ, следует отредактировать ключи реестра Windows XP.

На диске CD-ROM, прилагаемом к этой книге, есть файл no share.reg. Достаточно дважды щелкнуть на нем мышью, и необходимые изменения будут внесены в реестр. После этого следует перезапустить компьютер.

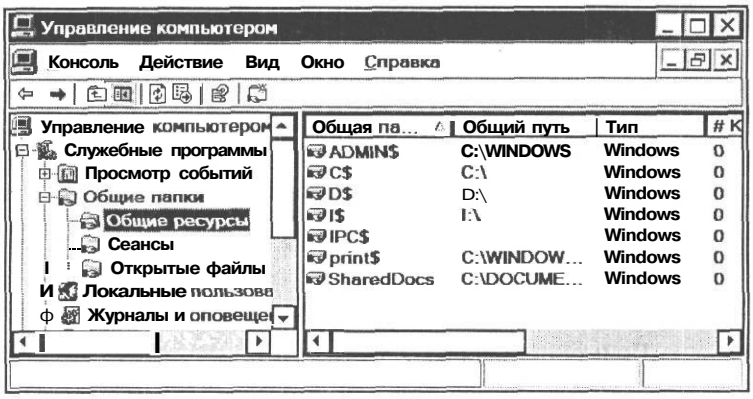



*Рис. 5.27. Скрытые общие ресурсы*

Посмотрим, как отредактировать ключи реестра, не прибегая к использованию файла **по share.reg**. Сначала запустим редактор реестра.

> Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в главном меню Windows выберите команду **Выполнить** (Run). На экране появится диалог **Запуск программы** (Run) (Рис. 5.28).

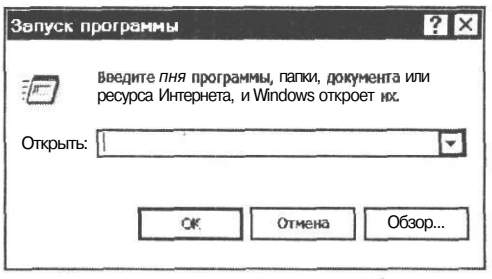



*Рис. 5.28. Диалог **Запуск программы** (Run)*

➤ В поле ввода **Открыть** (Open) этого диалога введите команду **regedit** и нажмите кнопку **OK.** На экране появится окно программы **Редактор реестра** (Registry Editor) (Рис. 5.29).

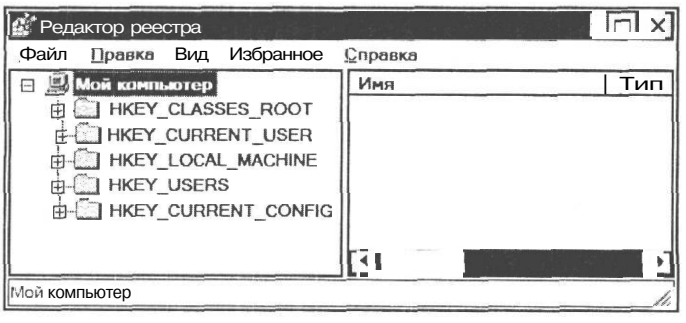



*Рис. 5.29. Окно программы **Редактор реестра** (Registry Editor)*

В левой части этого окна - области навигатора - содержатся папки, каждая из которых представляет собой стандартный раздел на локальном компьютере. В правой части окна - области разделов - отображаются записи выделенного раздела.

Структура реестра содержит пять корневых разделов (ветвей), каждый из них включает подразделы, отображаемые в левой части окна в виде значка папки. Конечным элементом дерева реестра являются ключи или параметры, подразделяющиеся на три типа:

- строковые, например "C:\Windows";
- двоичные, например 10 82 АО 8F. Максимальная длина такого ключа 16 Кбайт;
- DWORD. Этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде, например 0x00000020 (32). В скобках указано десятичное значение ключа.

Отредактируем параметры реестра так, чтобы запретить общий доступ к скрытым пакам.

➤ В правой части окна Редактор реестра (Registry Editor) откройте следующий раздел реестра:

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters**

В этом разделе (Рис. 5.30) следует изменить или добавить ключ типа DWORD с десятичным значением 0 (ноль) и с именем: для сервера - AutoShareServer, для рабочей станции и компьютеров одноранговой сети - AutoShareWKS.

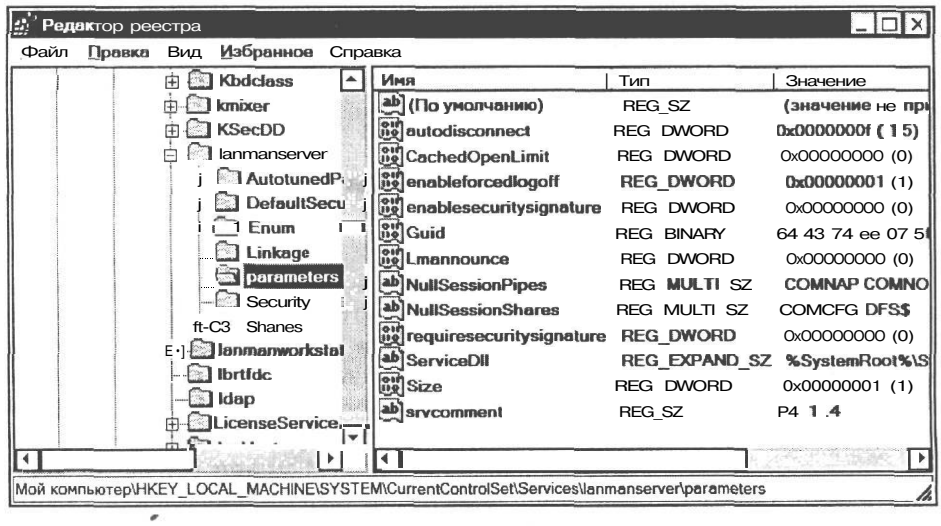



*Рис. 5.30. Редактируемый раздел реестра*

Если такие ключи отсутствуют, добавьте их следующим образом.

> В окне программы Редактор реестра (Registry Editor) выберите команду Правка ◆ Создать * Параметр DWORD (Edit ◆ New ◆ DWORD Value). В правой части этого окна появится новый значок ключа с выделенным названием Новый параметр #1 (New Value #1) и мигающим курсором, приглашающим изменить имя ключа, предлагаемое по умолчанию.

➤ Для сервера введите: **AutoShareServer**. Для рабочей станции и компьютеров одноранговой сети введите: **AutoShareWKS.** Нажмите клавишу Enter. Ключ с указанным именем будет создан, и ему по умолчанию будет присвоено требуемое значение **0x00000000 (0).**

Если один из указанных ключей уже присутствует в реестре и требуется изменить его значение, выделите его и выберите команду меню **Правка * Изменить** (Edit ◆ Change). В появившемся диалоге **Изменение параметра** DWORD (Edit DWORD Value) (Рис. 5.31) отредактируйте значение ключа.

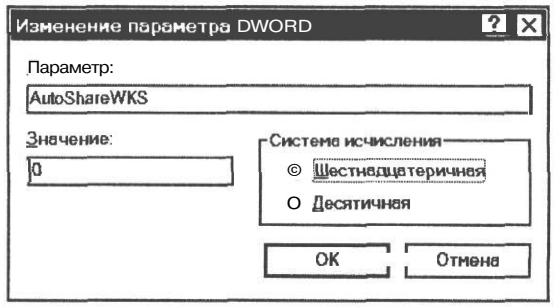



*Рис. 5.31. Диалог* ***Изменение параметра DWORD*** *(Edit DWORD Value)*

> Закройте окно **Редактор реестра** (Registry Editor), выбрав команду меню **Файл * Выход** (File ◆ Exit), и перезагрузите компьютер.

Если после перезагрузки вы откроете папку **Общие ресурсы** (Shares) в окне **Управление компьютером** (Computer Management), то скрытых общих папок и дисков уже не увидите.

## Отключение сетевых компонентов и NetBIOS через TCP/IP

При установке операционной системы Windows XP для всех сетевых подключений, кроме **Протокола Интернета** (TCP/IP) (Internet Protocol (TCP/IP)), по умолчанию устанавливаются еще и другие сетевые компоненты - **Служба доступа к файлам и принтерам сетей Microsoft** (File and Printer sharing for Microsoft Networks) и **Клиент для сетей Microsoft** (Client for Microsoft Networks). На компьютере, подключенном к Интернету, компоненты **Служба доступа к файлам и принтерам сетей Microsoft** (File and Printer sharing for Microsoft Networks) и **Клиент для сетей Microsoft** (Client for Microsoft Networks) являются не обязательными и представляют угрозу безопасности. Поэтому их необходимо отключить, сбросив соответствующие флажки на вкладке **Сеть** (Networking) диалога **Свойства** (Properties) (Рис. 5.32) каждого сетевого подключения и подключения удаленного доступа. Это не отразится на работе данного подключения. Чтобы открыть диалог **Свойства** (Properties), следует щелкнуть правой кнопкой мыши на значке подключения в окне **Сетевые подключения** (Network Connections) и в контекстном меню выбрать команду **Свойства** (Properties). Открыть окно **Сетевые подключения** (Network Connections) можно либо из главного меню Windows командой **Подключение * Отобразить все подключения** (Connect To ◆ Show all connections), либо из **Панели управления** (Control Panel).

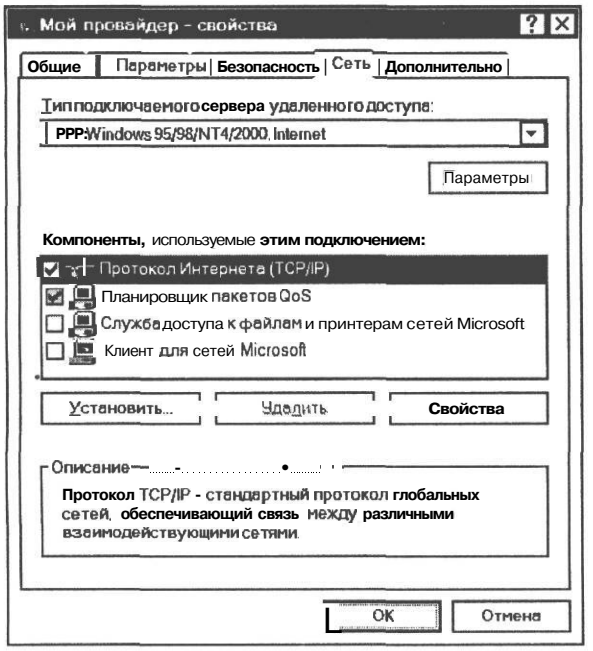



*Рис. 5.32. Вкладка Сеть (Networking) диалога Свойства (Properties) подключения удаленного доступа*

Операционная система по умолчанию устанавливает также Планировщик пакетов QoS (QoS Packet Scheduler), обеспечивающий управление сетевым трафиком. Этот компонент не представляет угрозы для безопасности, но ограничивает пропускную способность канала Интернета. В разделе «Настройка протокола TCP/IP и других свойств сетевого соединения» знакомства «Настройка программного обеспечения в Windows 2000/XP» главы «Создание локальной сети дома и в офисе» было показано, как удалить этот сервис.

Еще одна необходимая для безопасности настройка - запрещение NetBIOS через TCP/IP.

- На вкладке Сеть (Networking) диалога Свойства (Properties) (Рис. 5.32) удаленного или сетевого подключения щелчком мыши выделите Протокол Интернета (TCP/IP) (Internet Protocol (TCP/IP)) и нажмите кнопку Свойства (Properties). Откроется диалог Свойства: Протокол Интернета (TCP/IP) (Internet Protocol (TCP/IP) Properties).
- Нажмите в этом диалоге кнопку Дополнительно (Advanced). Появится диалог Дополнительные параметры **TCP/IP** (Advanced TCP/IP Settings).
- Перейдите на вкладку WINS (Рис. 5.33).

Как уже отмечалось ранее, служба WINS (Windows Internet Naming Service - Служба имен Интернета Windows) обеспечивает преобразование IP-адресов компьютера в понятные логические имена и, кроме того, различает NetBIOS-имена компьютеров, которые они имеют в локальной сети, и преобразовывает эти имена в IP-адреса.

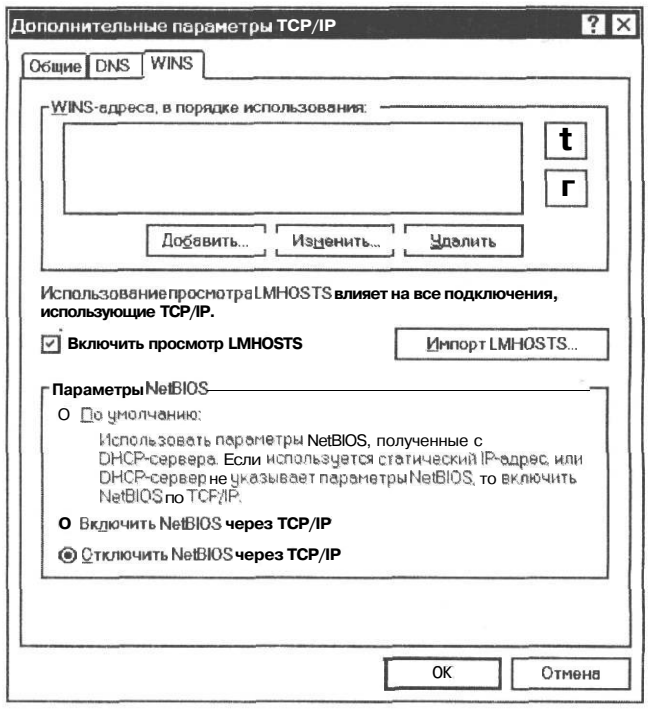



*Рис. 5.33. Вкладка WINS диалога* ***Дополнительные*** *параметры TCP/IP (Advanced TCP/IP Settings)*

Вместе с тем такая функция WINS-сервера является весьма опасной, так как компьютеры локальной сети становятся видны и доступны из Интернета. Поэтому на компьютере, подключенном к Интернету, режим NetBIOS через TCP/IP необходимо запретить.

- Установите переключатель Отключить NetBIOS через TCP/IP (Disable NetBIOS over TCP/IP).
- Закройте диалог Дополнительные параметры TCP/IP (Advanced TCP/IP Settings) и все другие открытые диалоги нажатием кнопки OK.

Сделанная настройка может привести к тому, что компьютер не будет виден в сетевом окружении и к нему нельзя будет обратиться по имени, но к его общим ресурсам можно будет обращаться по IP-адресу: \\192.168.0.1\C$.

## Использование учетных записей и паролей с русскими символами

Многие компьютерные хулиганы используют готовые программы (так называемые «эксплоиты»), которые используют бреши в системе безопасности компьютера для проникновения и причинения ущерба. Большинство таких программ-«эксплоитов» создано англоязычными хакерами, и существует высокая вероятность того, что для их творений русские имена пользователей и пароли составят существенное препятствие.

Исходя из сказанного, имеет смысл для выполнения на компьютере административных функций использовать учетную запись с русским именем и длинным (8-16 символов) паролем, содержащим смесь английских и русских букв, цифр и специальных символов. Все другие учетные записи, в том числе и учетную запись **Администратор** (Administrator), необходимо запретить.

Выполнить указанные действия нужно в следующем порядке.

Если при установке Windows XP не был создан дополнительный пользователь, то создайте нового пользователя с правами администратора. Если пользователь был создан ранее, то его надо переименовать так, чтобы его имя было русским, неброским, например «Иван», и назначить ему пароль.

Пароль должен быть длинным, лучше 16 символов, но не менее 8, и содержать смесь русских и английских букв в верхнем и нижнем регистрах, цифр, а также символов **!@#$%^&*()_+-=?!{}[]`~.,/|\.**

На компакт-диске, прилагаемом к этой книге, в файле **pass_gen.zip** находится архив программы **Генератор паролей** (Рис. 5.34), которую можно использовать для создания паролей, отвечающих указанным требованиям.

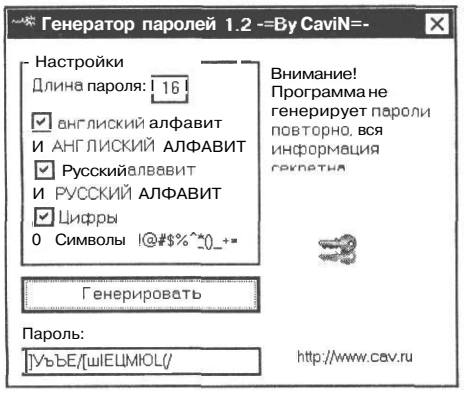



*Рис. 5.34. Программа **Генератор паролей***

Программа не использует некоторые специальные символы, которые можно добавить в пароль вручную. Но и без них **Генератор паролей** значительно облегчает процесс создания учетных записей.

Чтобы отличить похожие русские и английские символы, скопируйте пароль в редактор Microsoft Word или WordPad и выберите шрифт, не содержащий кириллицы. Вы увидите примерно следующее:

```
NbwÊsùÁ0]Pðo#Ì3Ý
```

Запишите пароль на бумаге так, чтобы было понятно, где русские символы, например, подчеркивая те символы пароля, которые выглядят одинаково в русском и английском алфавите:

```
NbwKsшБ0]Pро#М3Э
```

Далее, воспользовавшись оснасткой **Локальные пользователи и группы** (Local Users and Groups) в окне консоли **Управление компьютером** (Computer Management), следует переименовать пользователя **Администратор** (Administrator), присвоив ему неброское русское имя и длинный пароль из 16 символов, содержащих смесь русских и английских символов в обоих регистрах, цифр и специальных символов.

Этот пароль можно не запоминать, так как переименованного администратора лучше запретить совсем, установив флажок **Отключить учетную запись** (Account is Disabled) в диалоге **Свойства** (Properties) данного пользователя (Рис. 5.35), после чего нажать кнопку **Применить** (Apply). Чтобы открыть этот диалог, следует щелкнуть правой кнопкой на папке **Пользователи** (Users) в окне **Управление компьютером** (Computer Management) и выбрать команду контекстного меню **Свойства** (Properties).

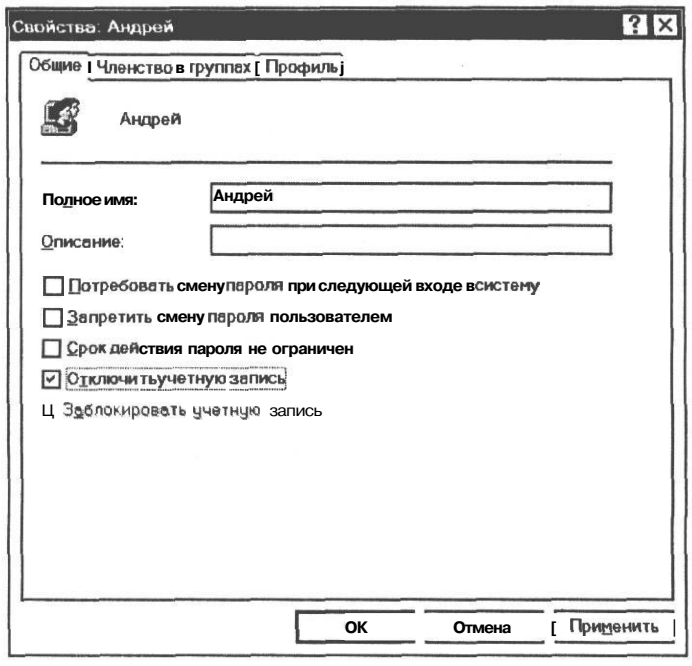



*Рис. 5.35. Диалог **Свойства** (Properties) пользователя*

Подобным же образом запретите все остальные учетные записи, созданные по умолчанию. В окне папки **Пользователи** (Users) запрещенные отключенные учетные записи отмечаются красными кружочками с белыми крестиками.

После переименования учетной записи администратора следует переименовать группу **Администраторы** (Administrators), присвоив ей неброское русское название, например «Дети». Обратите внимание на то, что переименовать группу можно только после переименования учетной записи администратора.

И, наконец, создайте учетную запись простого пользователя, члена группы **Пользователи** (Users), которую будете использовать для входа в систему, только когда компьютер

подключен к Интернету. Когда подключение к Интернету отсутствует и требуется выполнять действия, являющиеся привилегией администратора, используйте учетную запись с правами администратора с русским именем и длинным паролем, содержащим смесь русских и английских символов.

Следование этим правилам позволит свести до минимума возможность несанкционированного проникновения посторонних на ваши компьютеры.

## Запрещение подключения анонимных пользователей

Windows XP дает возможность анонимным пользователям выполнять определенные операции, например, проводить перепись имен учетных записей домена и сетевых ресурсов. Это может быть удобно, например, если администратору требуется предоставить доступ пользователям в доверенном домене, в котором не поддерживается двустороннее отношение доверия. Такая возможность предоставляется параметрами локальной политики безопасности. Но в большинстве случаев доступ анонимных пользователей к сети не требуется и опасен. Его следует запретить.

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Панель управления** (Control Panel).
- В окне **Панель управления** (Control Panel) дважды щелкните мышью на значке **Администрирование** (Administrative Tools), чтобы открыть соответствующее окно.
- В окне **Администрирование** (Administrative Tools) дважды щелкните мышью на значке **Локальная политика безопасности** (Local Security Policy). На экране появится окно **Локальные параметры безопасности** (Local Security Settings) (Рис. 5.36).

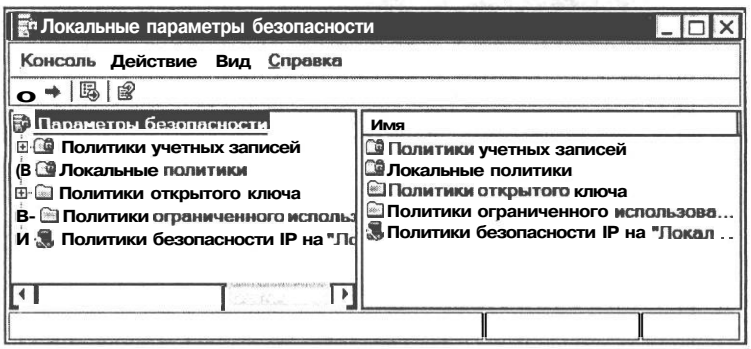



*Рис. 5.36. Окно* ***Локальные параметры безопасности*** *(Local Security Settings)*

- Дважды щелкните мышью на значке **Локальные политики** (Local Policies), чтобы открыть папку соответствующих политик.
- Щелкните мышью на значке папки **Параметры безопасности** (Security Options) в левой части окна **Локальные параметры безопасности** (Local Security Settings). В правой части этого окна вы увидите перечень локальных политик безопасности (Рис. 5.37).

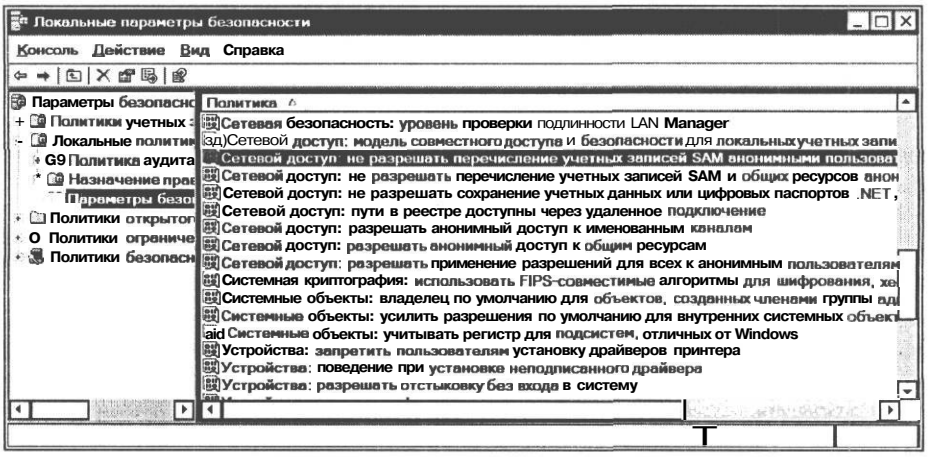



*Рис. 5.37. Перечень локальных политик безопасности*

- Найдите политику **Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts), щелкните правой кнопкой мыши на этой строке и в появившемся контекстном меню выберите команду **Свойства** (Properties). Откроется диалог **Свойства: Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts Properties) (Рис. 5.38).

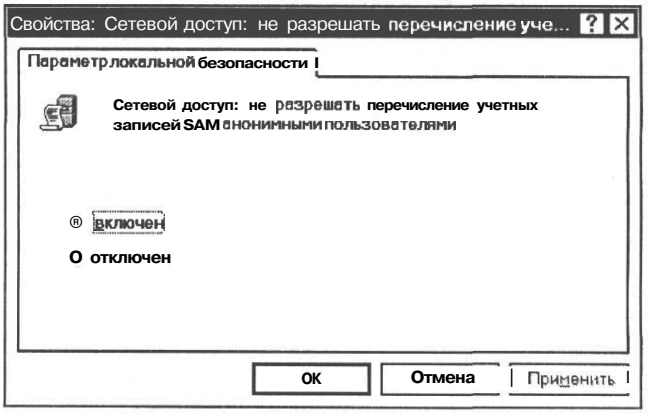



*Рис. 5.38. Диалог Свойства: Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями (Network access: Do not allow anonymous enumeration of SAM accounts Properties)*

- Убедитесь, что установлен переключатель **включен** (Enabled). В противном случае установите его.
- Нажмите кнопку **Применить** (Apply).

➤ Закройте диалог **Свойства: Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts Properties) нажатием кнопки **OK.** Вы возвратитесь к окну **Локальные параметры безопасности** (Local Security Settings) (Рис. 5.36).

Установленному параметру соответствует ключ реестра **RestrictAnonymousSam=1** в разделе **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Ls**.

➤ Щелкните правой кнопкой мыши в окне **Локальные параметры безопасности** (Local Security Settings) на строке **Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts and shares) и в появившемся контекстном меню выберите команду **Свойства** (Properties). На экране появится диалог **Свойства: Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts and shares Properties) (Рис. 5.39).

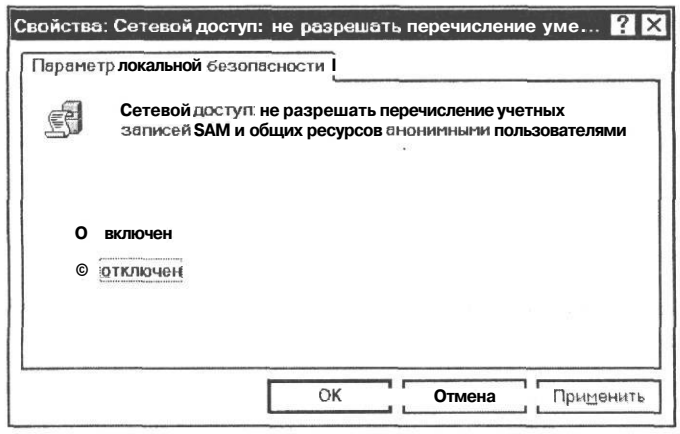



***Рис. 5.39. Диалог Свойства: Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями*** *(Network access: Do not allow anonymous enumeration of SAM accounts and shares Properties)*

> Установите переключатель **включен** (Enabled), нажмите кнопку **Применить** (Apply) и кнопку **OK,** чтобы закрыть диалог.

Установленному параметру соответствует ключ реестра **RestrictAnonymous=1** в разделе **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Ls**. Вместо включения режима можно было бы отредактировать этот ключ реестра.

После включения указанных политик доступ в сеть анонимных пользователей будет запрещен.

Мы перечислили, разумеется, не все возможные настройки безопасности, а только необходимый минимум, который оградит вашу сеть от несанкционированного доступа извне.

# Антивирус Norton Antivirus

Прошли те времена, когда самым большим источником опасности для ваших данных были дискеты, зараженные «классическими» вирусами. Сегодня и работа, и отдых немыслимы без Интернета, и этим активно пользуются авторы вирусов, хакеры и спамеры - часто в одном лице. Хакеры создают новые вирусы и другие вредоносные программы, чтобы незаконно проникать на наши компьютеры, подчинять их себе и затем рассылать с них спам. Угрозы информационной безопасности становятся все более комплексными.

Количество известных вредоносных программ уже приближается к сотне тысяч, появились десятки новых их типов и разновидностей - все чаще смешанных, объединяющих все последние достижения «черной» компьютерной индустрии. Сама эта индустрия набирает обороты, уже начались «гангстерские войны» между кланами компьютерных преступников.

Слово «вирусы» хорошо знакомо пользователям компьютеров. Оно давно переросло свое первоначальное значение и теперь часто употребляется для обозначения любых вредоносных программ, способных размножаться, распространяясь с компьютера на компьютер и заражая подчас целые компьютерные сети, вплоть до глобальных эпидемий в Интернете. Это - «классические» вирусы, сетевые и почтовые черви, «троянские кони», их разновидности - программы скрытого администрирования (backdoor) и другие.

Черви (worm) - это вирусы, которые распространяются в компьютерной сети, но, в отличие от «классических» вирусов, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Backdoor-программы по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске «троянец» устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях «троянца» в системе. Более того, ссылка на троянца может отсутствовать в списке активных приложений. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Будучи установленными на компьютер, программы скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать и отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. В результате эти «троянцы» могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п. Пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

Результатом действия вируса может быть:

- относительно безвредное вмешательство в работу компьютера, например, злая шутка, когда экран гаснет и выдается сообщение, что ваш жесткий диск отформатирован;
- нанесение реального вреда, когда винчестер действительно форматируется или стираются важные файлы;
- настоящее преступление - когда с помощью троянских программ злоумышленники крадут номера ваших кредитных карточек, пароли доступа, другую конфиденциальную информацию.

Борьба с вирусами, червями, «троянцами» и другими вредоносными программами ведется при помощи специализированного программного обеспечения, такого как Norton AntiVirus, DrWeb, Panda, Kaspersky Anti-Virus. Причем грамотно построенная защита обеспечивает двойной контроль: на уровне конкретного компьютера и на уровне локальной сети. Современные средства борьбы с вредоносным кодом достаточно эффективны, и практика показывает, что регулярно вспыхивающие глобальные эпидемии компьютерных вирусов происходят во многом благодаря «человеческому фактору» - большинство пользователей и многие системные администраторы попросту ленятся регулярно обновлять базы данных антивирусных программ и проверять на вирусы входящую электронную почту перед ее прочтением (хотя сейчас это все чаще делают сами провайдеры услуг Интернета).

Мы рассмотрим наиболее популярную антивирусную программу - Norton AntiVirus 2004 Professional компании Symantec, обеспечивающую всестороннюю вирусную защиту и восстановление зараженного программного обеспечения вашего компьютера. Программа автоматически определяет и обезвреживает известные ей вирусы и другие потенциальные угрозы, такие, как spyware, в файлах на дисках вашего компьютера, в архивных файлах, во вложениях Instant Messenger, сообщениях электронной почты и файлах, загружаемых из Интернета.

Norton AntiVirus Professional запускается из главного меню Windows командой Программы * **Norton AntiVirus • Norton AntiVirus 2004 Professional** (Programs ◆ Norton AntiVirus ◆ Norton AntiVirus 2004 Professional).

## Рабочее окно Norton AntiVirus Professional

В рабочем окне **Norton AntiVirus Professional** (Рис. 5.40) в верхней части, под строкой заголовка располагаются три кнопки LiveUpdate (Обновление), **Options** (Параметры), **Help & Support** (Помощь и поддержка). С помощью кнопки **LiveUpdate** (Обновление) запускается средство обновления программы и вирусных баз, а с помощью кнопки **Options** (Параметры) - средство настройки программы. Кнопка **Help & Support** (Помощь и поддержка) открывает меню, с помощью которого можно перейти к справочной системе программы или обратиться за технической поддержкой.

Рабочее окно **Norton AntiVirus Professional** состоит из двух панелей. Слева расположена панель **Norton AntiVirus** с меню, включающим четыре команды:

**Status** (Состояние) - отображает информацию о состоянии системы антивирусной защиты компьютера;

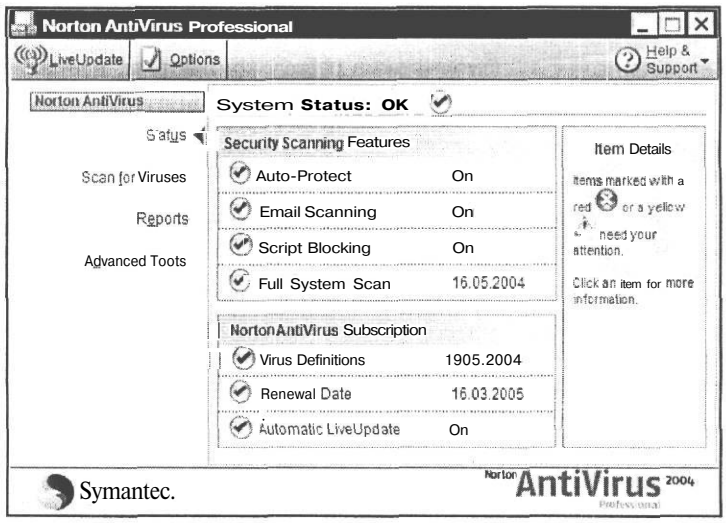



*Рис.* ***5.40. Рабочее окно Norton AntiVirus Professional***

**Scan for Viruses** (Антивирусное сканирование) - выполняет антивирусную проверку системы в целом, отдельных дисков, папок и файлов;

**Reports** (Отчеты) - отображает отчеты о выполненных антивирусных проверках;

**Advanced Tools** (Дополнительные инструменты) - открывает меню с командами для запуска программ UnErase Wizard и Wipe Info. UnErase Wizard позволяет восстановить удаленные по ошибке файлы, а Wipe Info удаляет данные таким образом, что восстановить их уже становится невозможно.

На правой панели рабочего окна отображается информация или элементы управления, соответствующие выбранной на левой панели команде.

Сразу после запуска программы Norton AntiVirus Professional на левой панели по умолчанию выбрана команда **Status** (Состояние) (она отмечена красным значком 4), а на правой панели отображается состояние системы антивирусной защиты вашего компьютера:

**Auto-Protect** (Автозащита) - автоматическая защита компьютера от вирусов (On - включена, Off - выключена);

**Email Scanning** (Сканирование электронной почты) - функция антивирусной проверки входящих и исходящих сообщений электронной почты (On - включена, Off - выключена);

**Script Blocking** (Блокировка скриптов) - функция отслеживания вирусоподобной активности в скриптах - профаммах, написанных на скриптовых языках, таких как Visual Basic Script и JavaScript, и блокирования таких скриптов, представляющих потенциальную угрозу безопасности (On - включена, Off - выключена);

**Full System Scan** (Полное сканирование системы) — дата последнего антивирусного сканирования всей системы;

**Virus Definitions** (Вирусные базы) - дата последнего обновления вирусных баз;

**Renewal Date** (Дата продления) - срок окончания подписки. Обычно зарегистрированным пользователям предоставляется возможность использовать программу и обновлять вирусные базы в течение года. По окончании этого срока подписку следует возобновить;

**Automatic LiveUpdate** (Автоматическое обновление) - функция автоматического обновления программы и вирусных баз (On - включена, Off - выключена).

## Обновление программы и вирусной базы

Сразу после установки Norton AntiVirus Professional следует обновить ее и вирусные базы, чтобы программа в своей работе могла использовать самые последние данные обо всех новых вирусах и прочих угрозах. Обновление выполняется с помощью программы LiveUpdate, которая отыскивает и устанавливает обновления для всех продуктов компании Symantec, установленных на вашем компьютере. Эта программа поставляется вместе с Norton AntiVirus Professional.

Выполним обновление программных компонентов и вирусных баз

- Установите связь с провайдером Интернета.
- В верхней части рабочего окна **Norton AntiVirus Professional** нажмите кнопку **LiveUpdate** (Обновление). Появится первый диалог Мастера **LiveUpdate** (Обновление) (Рис. 5.41) с перечнем всех продуктов Symantec, установленных в системе.

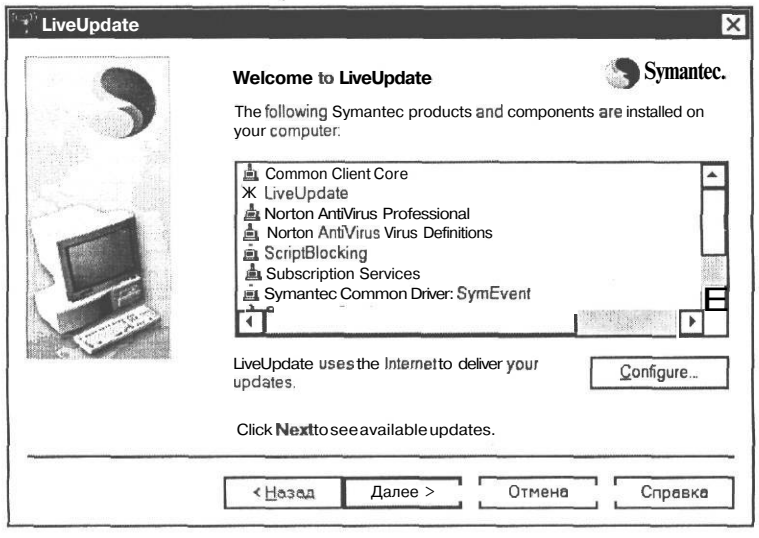



*Рис. 5.41. Первый диалог Мастера **LiveUpdate** (Обновление) с перечнем продуктов Symantec, установленных в системе*

- Нажмите кнопку Далее (Next). Программа подключится к серверу Symantec (Рис. 5.42) и получит список доступных обновлений, после чего предложит, установив или сбросив флажки, выбрать те продукты, которые вы хотите обновить (Рис. 5.43).

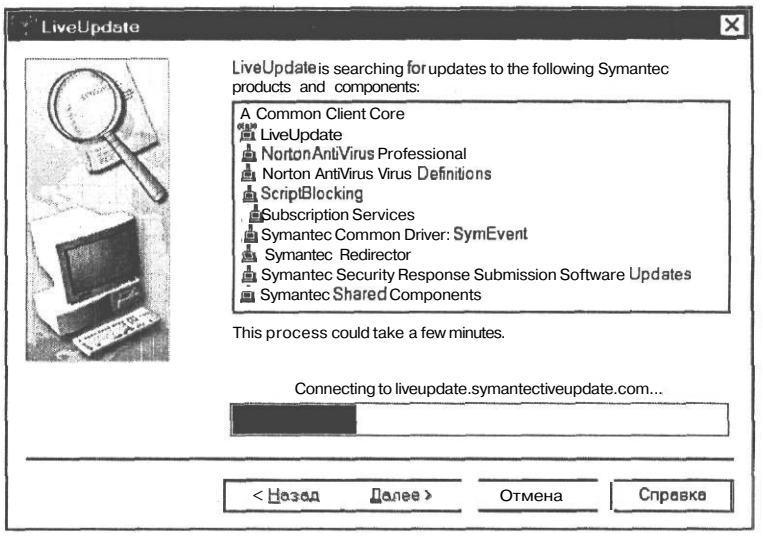



*Рис. 5.42. Подключение к серверу Symantec*

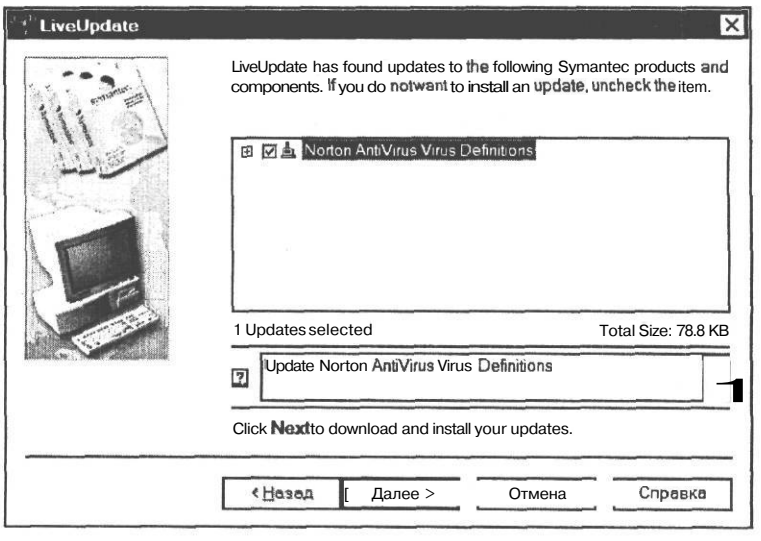



*Рис. 5.43. Список доступных обновлений*

Рекомендуется установить все доступные обновления, а вирусные базы **(Norton AntiVirus Virus Definitions)** - обязательно.

> Нажмите кнопку **Далее** (Next), чтобы начать загрузку и обновление. Этот процесс будет отображаться на линейном индикаторе (Рис. 5.44).

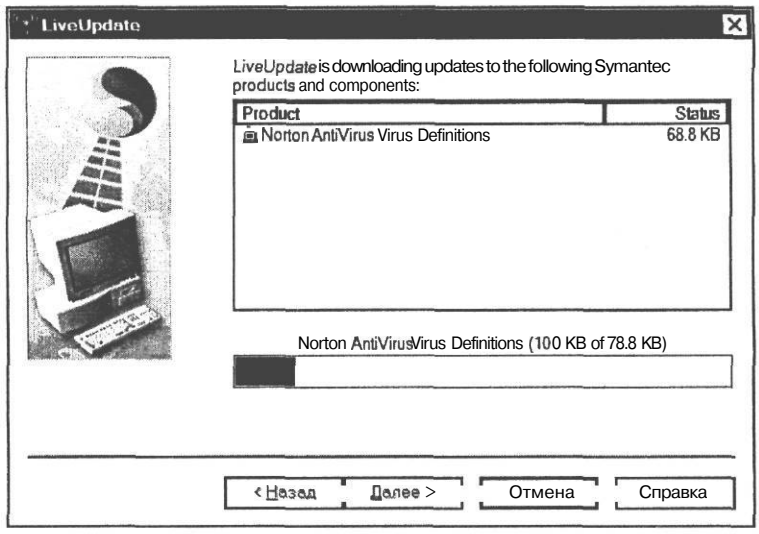



*Рис. 5.44. Загрузка вирусной базы*

Когда загрузка и установка закончится, программа сообщит вам о том, что все выбранные компоненты обновлены (Рис. 5.45). После нажатия кнопки **Готово** (Finish) вы возвратитесь к рабочему окну **Norton AntiVirus Professional.**

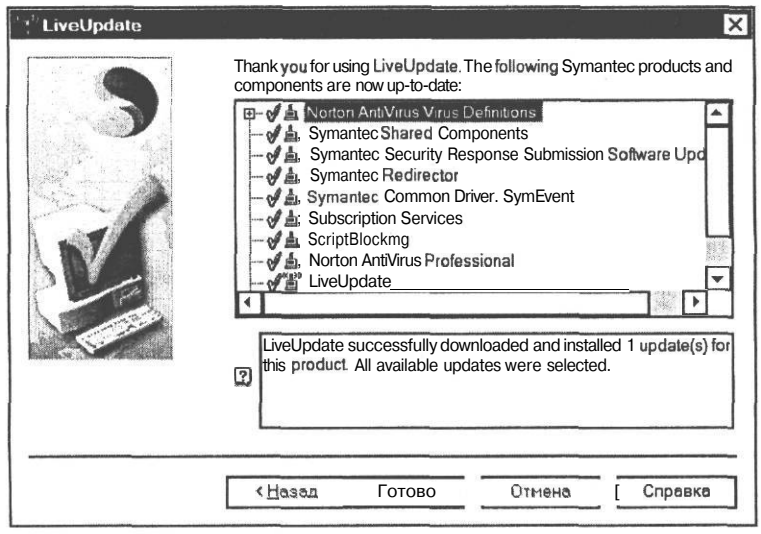



*Рис. 5.45. Загрузка и установка обновлений завершена*

Если же доступные обновления отсутствуют, то сообщение будет таким, как на Рис. 5.46.

В дальнейшем процедуру обновления вирусных баз следует выполнять регулярно, по меньшей мере, раз в неделю или при появлении информации о новых вирусах. Рекомендуется использовать режим автоматического обновления, который настраивается в диалоге **Options** (Параметры).

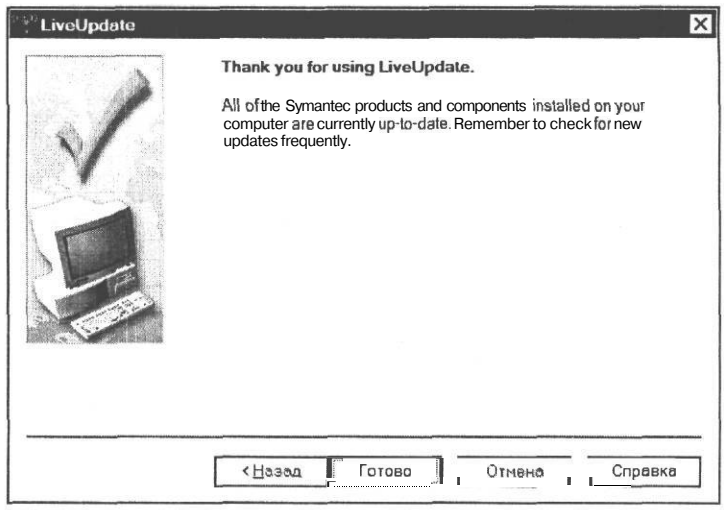



*Рис. 5.46. Сообщение об отсутствии обновлений*

## Антивирусная проверка системы, дисков, папок и файлов

После того как компоненты и вирусные базы обновлены, программа Norton AntiVirus Professional готова к выполнению своих функций. Она будет автоматически загружаться вместе с операционной системой и, постоянно находясь в оперативной памяти, отслеживать все вирусоподобные действия, проверять все открываемые файлы, сообщения электронной почты, вложения Instant Messenger и файлы, загружаемые из Интернета. При обнаружении вируса программа автоматически обезвредит его и сообщит об этом.

Но, кроме использования автоматической защиты, следует регулярно, «вручную» выполнять антивирусное сканирование всей системы, отдельных дисков, папок и файлов вашего компьютера. Это особенно необходимо, когда поведение компьютера становится необычным.

- На левой панели рабочего окна Norton AntiVirus Professional выберите команду **Scan for Viruses** (Антивирусное сканирование). На правой панели вы увидите список задач **(Task),** содержащий команды для выполнения следующих операций сканирования:

**Scan my computer** (Сканирование компьютера) - проверка всей системы;

**Scan all removable drives** (Сканирование всех съемных дисков);

**Scan all floppy disks** (Сканирование всех гибких дисков);

**Scan drives** (Сканирование дисков) - при выборе этого варианта будет предложено указать, какие диски следует проверить (Рис. 5.47), установив флажки;

**Scan folders** (Сканирование папок) - при выборе этого варианта будет предложено указать, какие папки следует сканировать (Рис. 5.48), установив флажки;

**Scan files** (Сканирование файлов) - при выборе этого варианта будет предложено указать, какие файлы должны быть проверены (Рис. 5.49).

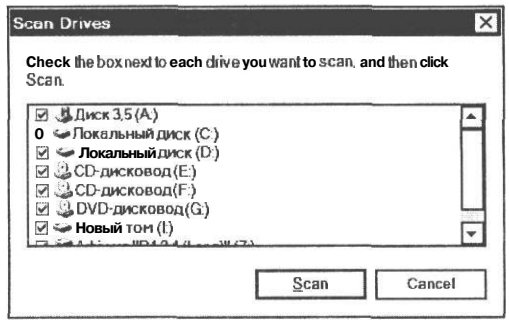



*Рис. 5.47. Диалог* ***Scan Drives*** *(Сканирование дисков) для выбора сканируемых дисков*

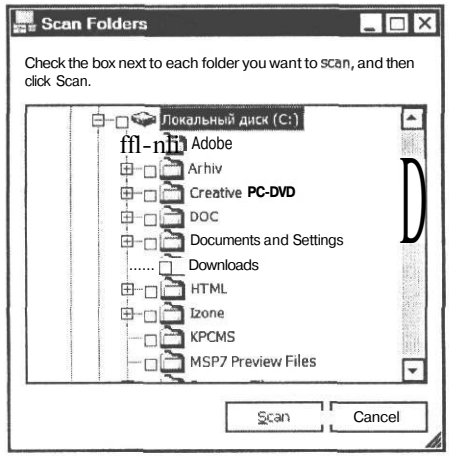



*Рис. 5.48. Диалог* ***Scan Folders*** *(Сканирование папок) для выбора сканируемых папок*

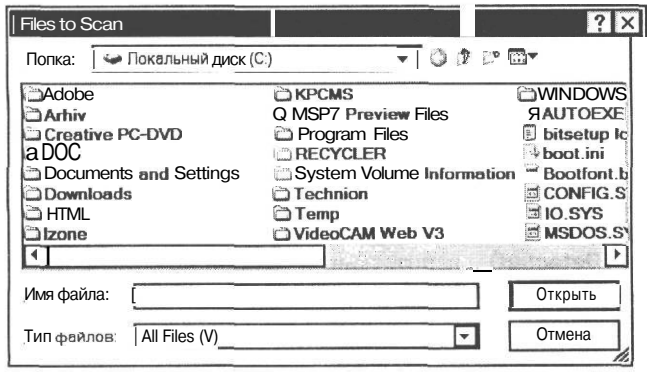



*Рис. 5.49. Диалог* ***Files to Scan*** *(Файлы для сканирования) для выбора сканируемых файлов*

Для выбора объектов сканирования достаточно щелчком мыши выделить соответствующую задачу и щелкнуть мышью на синей ссылке **Scan** (Сканировать) в нижней части правой панели. Можно также щелкнуть мышью на значке слева от названия задачи.

Вы можете поместить в список задач отдельные файлы и папки, например, с файлами, загружаемыми из Интернета, чтобы в дальнейшем выполнять их проверку одним щелчком мыши. Для этого следует щелкнуть мышью на синей ссылке **New** (Новая) и следовать указаниям Мастера сканирования **(Norton AntiVirus Scan Wizard).** Добавленные вами задачи могут быть отредактированы с помощью ссылки **Edit** (Правка) и удалены с помощью ссылки **Delete** (Удалить).

Для сканирования всей системы **(Scan my computer),** а также для сканирования папок и файлов, добавленных вами в список задач, можно установить расписание, и Norton AntiVirus Professional будет выполнять указанную задачу в назначенное вами время. Для установки расписания следует щелкнуть мышью на значке, справа от задачи, в колонке **Task** Shedule (Планирование задач).

После выбора задачи и запуска процесса сканирования щелчком мыши на синей ссылке **Scan** (Сканировать) появится диалог **Norton AntiVirus** (Рис. 5.50). В правой его части будет отображаться процесс сканирования с указанием проверяемого в данный момент файла **(Current Item),** общего числа проверенных файлов **(Scanned),** количества зараженных вирусами файлов **(Detected),** количества обезвреженных файлов **(Fixed),** количества удаленных файлов **(Deleted).**

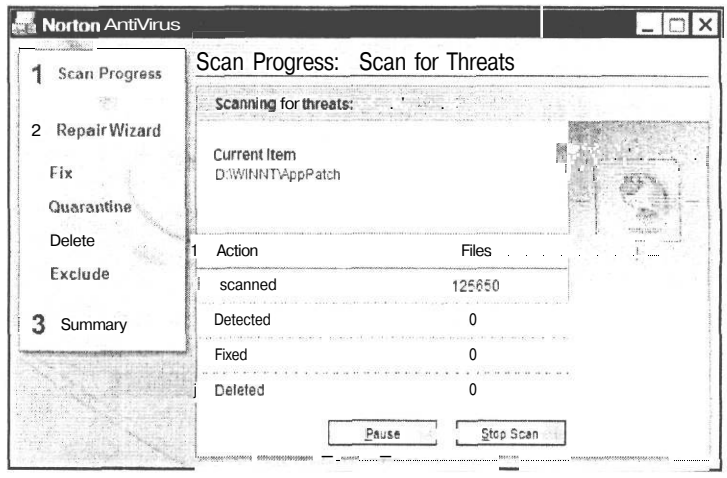



*Рис. 5.50. Процесс сканирования*

После окончания сканирования в этом же диалоге отобразится информация о результатах сканирования (Рис. 5.51). Здесь указывается количество проверенных **(Scanned),** инфицированных **(Detected),** исправленных **(Repaired),** перемещенных в карантин **(Quarantined),** удаленных **(Deleted)** и исключенных из дальнейшего сканирования **(Excluded)** файлов **(Files),** главных загрузочных записей **(Master Boot Record)** и загрузочных записей **(Boot Record).** Если инфицированный файл не может быть обезврежен, то профамма предлагает поместить его в специальную карантинную папку **(Quarantined),** удалив из исходной.

Чтобы увидеть подробные результаты проверки, нажмите кнопку **More Details** (Подробности). После нажатия кнопки **Finished** (Готово) профамма возвратит вас к главному окну Norton AntiVirus Professional.

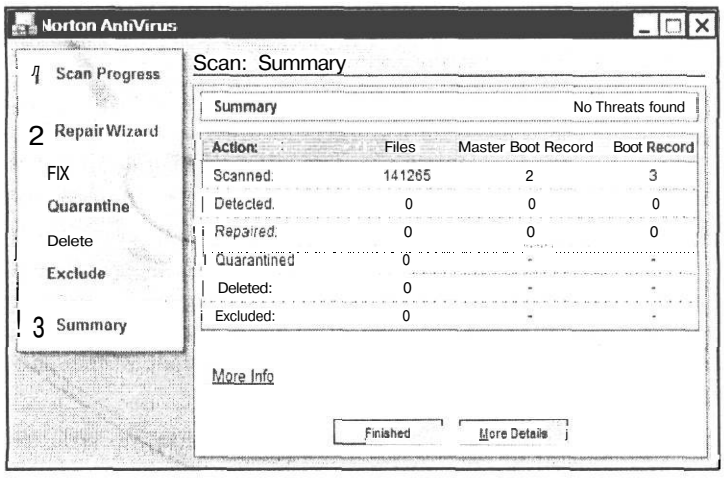



*Рис. 5.51. Информация о результатах антивирусного сканирования*

## Основные настройки Norton AntiVirus Professional

По умолчанию Norton AntiVirus Professional настроен разработчиками таким образом, чтобы обеспечить полную антивирусную защиту компьютера. Однако пользователь может по своему усмотрению корректировать установки с целью достижения оптимальной производительности системы. Можно также выключать те режимы, которые не используются. Параметры Norton AntiVirus Professional настраиваются с помощью диалога **Norton AntiVirus Options** (Параметры Norton AntiVirus) (Рис. 5.52). Чтобы открыть его, достаточно нажать кнопку **Options** (Параметры) в верхней части рабочего окна.

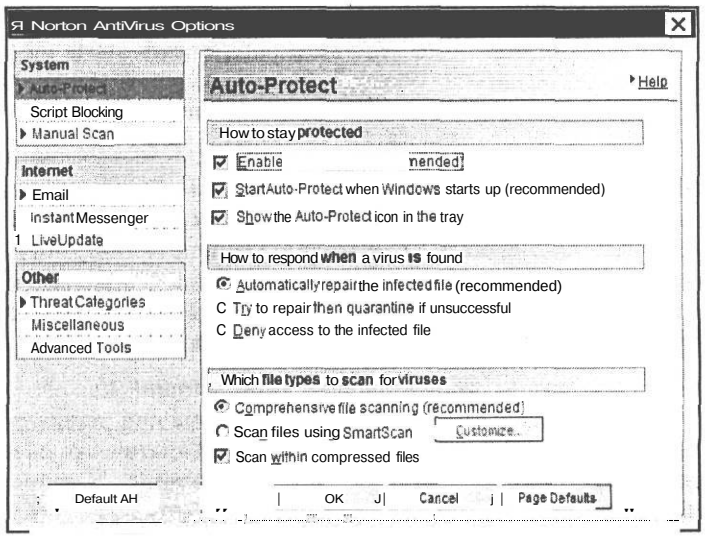



*Рис.* 5.52. *Раздел* ***Auto-Protect*** *(Автозащита) диалога* ***Norton AntiVirus Options*** *(Параметры Norton AntiVirus)*

Все настраиваемые параметры объединены в три категории, перечень которых отображается в левой части диалога:

**System** (Система). Параметры этой группы управляют сканированием и мониторингом вашего компьютера. Они используются для указания того, какие объекты должны сканироваться, что следует искать и как реагировать на обнаружение вируса. Данная категория включает функции автозащиты **(Auto-Protect),** блокирования скриптов **(Script Blocking)** и ручного сканирования **(Manual Scan);**

**Internet** (Интернет). Эта категория включает группы параметров **Email** (Электронная почта), **Instant Messenger и LiveUpdate** (Обновление). Названные параметры определяют действия программы при подключении компьютера к Интернету и используются для включения сканирования электронной почты, вложений Instant Messenger, блокирования червей и определения способа обновления программы;

**Other** (Другие). Содержит группы параметров, позволяющих указать, какие категории угроз должны детектироваться **(Threat Categories),** настроить особенности защиты - **Miscallaneous** (Смешанные), а также модифицировать функции Корзины (Recycle Bin) - **Advanced Tools** (Дополнительные инструменты).

При выделении щелчком мыши одного из разделов каждой категории в правой части диалога отображаются элементы управления для настройки соответствующих параметров.

## Автозащита (Auto-Protect)

Установка флажка **Enable Auto-Protect (recommended)** (Включить автозащиту (рекомендуется)) (Рис. 5.52) включает автоматическую защиту системы. Данный флажок должен быть установлен, чтобы программа могла автоматически отслеживать и блокировать вирусоподобные действия. Заметьте: этот и все другие рекомендуемые **(recommended)** разработчиками режимы должны быть включены для обеспечения максимальной степени защиты.

При установленном флажке **Start Auto-Protect when Windows starts up (recommended)** (Запустить автозащиту при запуске Windows (рекомендуется)) Norton AntiVirus Professional будет автоматически включать антивирусную защиту при каждом запуске операционной системы.

Если установлен флажок **Show the Auto-Protect icon in the tray** (Показать значок в правой части Панели задач), то в правой части Панели задач (Taskbar) отображается значок - **Norton AntiVirus Auto-Protect Enabled** (Автозащита Norton AntiVirus включена). Щелчок правой кнопкой мыши на этом значке откроет меню, с помощью которого можно открыть рабочее окно **(Open Norton AntiVirus),** выключить защиту **(Disable Auto-Protect)** и настроить параметры программы **(Configure Norton AntiVirus).**

Группа переключателей **How to respond when a virus is found** (Как реагировать при обнаружении вируса) позволяет указать действия программы при детектировании вируса: **Automatically repair the infected file (recommended)** (Автоматически обезвредить инфицированный файл (рекомендуется)), **Try to repair then quarantine if unsuccessful** (Попытаться обезвредить, при неудаче поместить в карантин), **Deny access to the infected file** (Отказать в доступе к инфицированному файлу).

Установка одного из переключателей **Which file types to scan for virus** (Какие типы файлов сканировать) дает возможность выбрать либо всестороннее сканирование

**(Comprehensive file scanning (recommended))**, при котором проверяются все программы и файлы всех типов, либо интеллектуальное сканирование (Scan **files using SmartScan**) с проверкой файлов только определенных типов, список которых задается после нажатия кнопки **Customize** (Настроить). При установленном флажке **Scan within compressed files** (Сканировать сжатые файлы) программа будет автоматически проверять также все архивные файлы.

## Ручное сканирование (Manual Scan)

Флажки группы **What items to scan in addition to files** (Какие элементы, кроме файлов, сканировать) (Рис. 5.53) включают сканирование загрузочной записи **(Boot records)** и главной загрузочной записи **(Master boot records).**

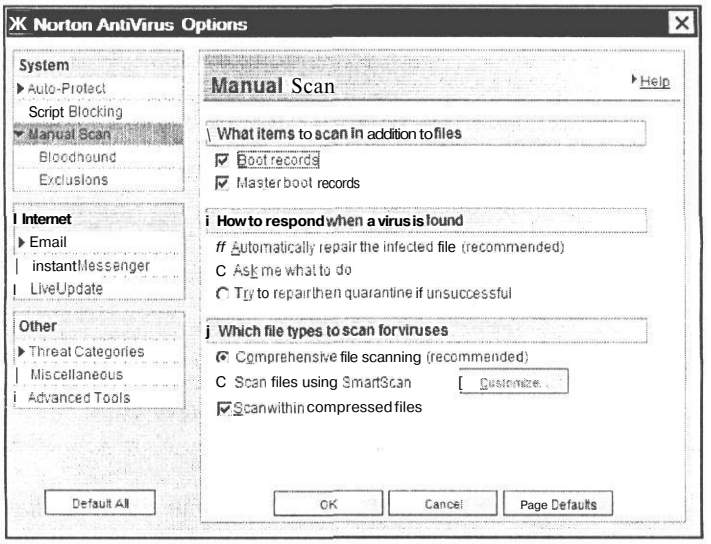



*Рис. 5.53. Раздел **Manual Scan** (Ручное сканирование) диалога **Norton AntiVirus Options** (Параметры Norton AntiVirus)*

С помощью переключателей **How to respond when a virus is found** (Как реагировать при обнаружении вируса) определяются действия программы при детектировании вируса: **Automatically repair the infected file (recommended)** (Автоматически обезвредить инфицированный файл (рекомендуется)), **Ask me what to do** (Запросить), **Try to repair then quarantine if unsuccessful** (Попытаться обезвредить, при неудаче поместить в карантин).

Переключатели **Which file types to scan for virus** (Какие типы файлов сканировать) позволяют выбрать между всесторонним сканированием **(Comprehensive file scanning (recommended))**, при котором проверяются все программы и файлы всех типов, и интеллектуальным сканированием **(Scan files using SmartScan)** с проверкой файлов только определенных типов, список которых задается после нажатия кнопки **Customize** (Настроить). Установка флажка **Scan within compressed files** (Сканировать сжатые файлы) указывает программе на необходимость проверять также все архивные файлы.

## Электронная почта (Email)

Установка флажков группы **What to scan** (Что сканировать) (Рис. 5.54) включает автоматическую проверку входящих **(Scan incoming Email (recommended))** и исходящих сообщений **(Scan outgoing Email (recommended))**. Norton AntiVirus Professional поддерживает все почтовые программы, использующие коммуникационные протоколы POP3 и SMTP.

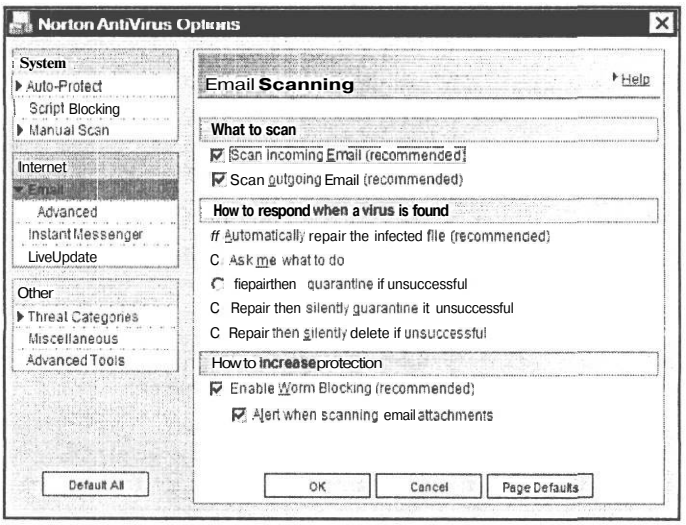



*Рис. 5.54. Раздел Email (Электронная почта) диалога **Norton AntiVirus Options** (Параметры Norton AntiVirus)*

Установка одного из переключателей **How to respond when a virus is found** (Как реагировать при обнаружении вируса) позволяет определить действия программы при детектировании вируса: **Automatically repair the infected file (recommended)** (Автоматически обезвредить инфицированный файл (рекомендуется)), **Ask me what to do** (Запросить), **Repair then quarantine if unsuccessful** (Обезвредить, при неудаче поместить в карантин), **Repair then silently quarantine if unsuccessful** (Обезвредить, при неудаче поместить в карантин без предупреждения), **Repair then silently delete if unsuccessful** (Обезвредить, при неудаче удалить без предупреждения).

При установленном флажке **Enable Worm Blocking (recommended)** (Включить блокирование червей (рекомендуется)) программа сканирует все исходящие почтовые сообщения и сообщает об обнаружении вредителей. Если установлен флажок **Alert when scanning email attachment** (Предупреждение при сканировании почтовых вложений), программа сообщит о сканировании вложений.

## Обновление (LiveUpdate)

Если установлен переключатель **Enable automatic LiveUpdate (recommended)** (Включить автоматическое обновление (рекомендуется)) (Рис. 5.55) программа будет автоматически обновлять компоненты и вирусные базы при подключении к Интернету.

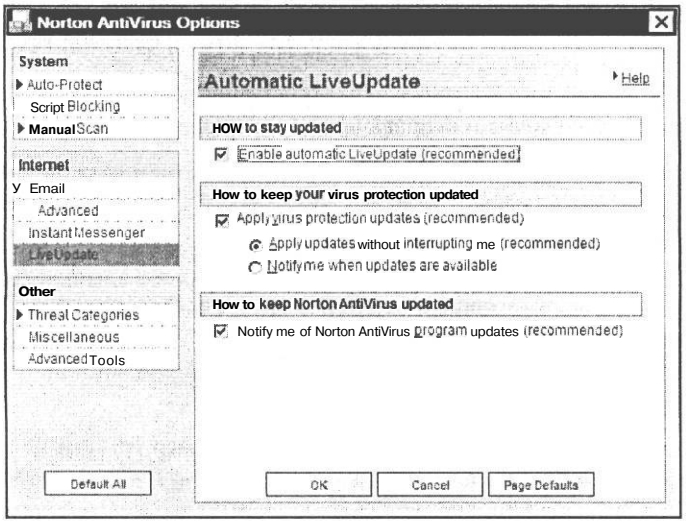



*Рис. 5.55. Раздел **LiveUpdate** (Обновление) диалога **Norton AntiVirus Options** (Параметры Norton AntiVirus)*

При установленном флажке **Apply virus protection updates (recommended)** (Применить обновления вирусной защиты (рекомендуется)) Norton AntiVirus Professional установит полученные обновления. Причем при установленном переключателе **Apply updates without interrupting me (recommended)** (Применить обновления, не отвлекая меня) эти обновления будут установлены автоматически. Если же установлен переключатель **Notify me when updates are available** (Предупредить, когда обновления доступны), программа будет сообщать о каждом доступном обновлении и вы сможете загрузить и установить их вручную.

Если установлен переключатель **Notify me of Norton AntiVirus program updates (recommended)** (Сообщить о доступности обновления программных компонентов Norton AntiVirus (рекомендуется)), программа сообщит также, если обнаружит доступные обновления.

## Правила антивирусной безопасности

Чтобы избежать заражения вирусами, следуйте простейшим правилам:

- используйте защиту от записи на съемных дисках и дискетах;
- следите за информацией о появлении новых вирусов. Такая информация доступна, например, на сайте **http://securityresponse.symantec.com;**
- используйте программу LiveUpdate для регулярного обновления вирусных баз;
- используйте функцию автозащиты **(Auto-Protect)** для предотвращения вирусного инфицирования вашего компьютера;
- если автозащита **(Auto-Protect)** выключена, обязательно проверяйте съемные диски перед использованием;

- будьте осторожны, получая сообщения электронной почты от неизвестных вам адресатов. Ни в коем случае не открывайте вложения, а сразу же удалите их;
- не выключайте режим автоматического сканирования входящей и исходящей почты. Это предотвратит получение и отправку инфицированных вложений;
- сохраняйте включенными все режимы защиты, рекомендованные (recommended) разработчиками.

В случае обнаружения файлового вируса на компьютере, подключенном к сети, необходимо отключить его от сети и проинформировать системного администратора. Если вирус еще не проник в сеть, это защитит сервер и другие рабочие станции. Если же вирус уже поразил сервер, то отключение от сети не позволит ему вновь проникнуть на компьютер после его обезвреживания. Подключение к сети возможно лишь после того, как будут обезврежены все серверы и рабочие станции.

При обнаружении загрузочного вируса отключать компьютер от сети не следует: вирусы этого типа по сети не распространяются (естественно, кроме файлово-загрузочных вирусов).

Если произошло заражение макро-вирусом, то вместо отключения от сети достаточно на период лечения закрыть соответствующий редактор - Word или Excel - на всех компьютерах сети.

Еще раз напомним о необходимости следить за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий, а вирусные базы - новейшими.

## Брандмауэр Agnitum Outpost Firewall Pro

В начале этой главы мы уже говорили об опасностях, которым подвергаются компьютеры и локальные сети, подключенные к Интернету, в частности о хакерских вторжениях. Предотвратить хакерские атаки – кражу конфиденциальной информации, использование вашего компьютера для рассылки спама, атак на другие компьютеры и т. п. - может специализированная программа - брандмауэр или межсетевой экран (Firewall), которая способна не только «спрятать» ваш компьютер от хакеров, но и проконтролировать все входящие и исходящие потоки данных, и пресечь любые враждебные действия до того, как они нанесут реальный вред. Брандмауэр помогает предотвратить доступ посторонних из Интернета к вашим компьютерам и пресекает все попытки программ-шпионов, попавших на ваши компьютеры, установить связь с Интернетом.

Сетевой экран играет роль фильтра, ограждающего локальный компьютер или локальную сеть от несанкционированного доступа из Интернета. Попутно он может обеспечивать блокировку рекламы и активного содержимого Web-страниц.

Как работает брандмауэр? Если на компьютере появился, например, «троянский конь», собирающий пароли и другую конфиденциальную информацию, то при попытке передать эту информацию через сеть сетевой экран сообщит вам, что некая программа пытается соединиться с Интернетом. Вам останется только запретить этой программе доступ в сеть и ликвидировать программу-«троянца».

В операционной системе Windows XP уже встроен персональный Брандмауэр Интернета (Internet Connection Firewall (ICF)), но он контролирует только входящий трафик. А как мы уже знаем, этого явно недостаточно: «троянцы» и spyware передают информацию с вашего компьютера своим хозяевам, т.е. используют исходящее соединение. К тому же этот брандмауэр предоставляет пользователю минимум настроек. Впрочем, если у вас установлена операционная система Windows XP, то Брандмауэр Интернета (Internet Connection Firewall (ICF)) запускается автоматически по умолчанию. Это помогает в некоторой степени защитить ваши данные от различных сетевых неприятностей.

Одним из наиболее популярных брандмауэров является система Agnitum Outpost Firewall Pro. Это - сетевой экран, оптимизированный для использования на домашнем компьютере или в локальной сети организации. На основании выбранного уровня безопасности Agnitum Outpost Firewall Pro блокирует или разрешает определенные соединения с локальной сетью или Интернетом, предупреждает о попытках установить несанкционированные соединения и блокирует их.

## Установка, настройка и интерфейс Agnitum Outpost Firewall Pro

Установочный файл программы Agnitum Outpost Firewall Pro - **OutpostProInstall.exe** - находится в папке **Soft** компакт-диска, прилагаемого к этой книге. Свежую версию программы можно загрузить с Web-страницы разработчика по адресу: **http://www.agnitum.com/download/outpostpro.html.**

Если у вас уже установлена данная программа, то перед установкой новой версии предыдущую следует удалить.

Процесс установки программы достаточно прост и не отличается от установки других программ, работающих в среде Windows. Agnitum Outpost Firewall Pro поддерживает несколько языков, и во время установки вы можете выбрать русский язык интерфейса. Для этого в открывающемся списке диалога **Languages** (Языки) (Рис. 5.56) следует выбрать язык **Russian** (Русский).

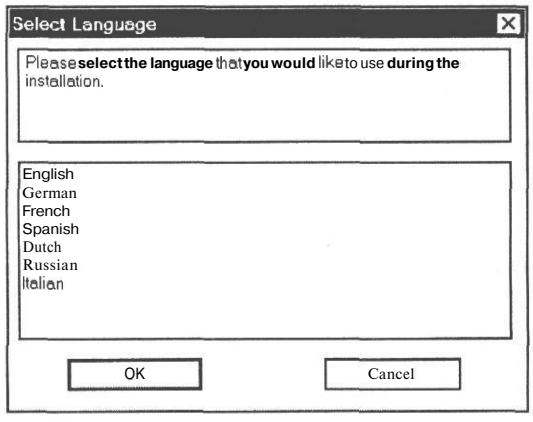



*Рис. 5.56. Диалог* ***Select Language*** *(Выбор языка)*

Сразу после окончания установки на экране появится диалог **Автоконфигурация** (Auto-configuration) (Рис. 5.57) с предложением автоматически создать правила брандмауэра для приложений и сетевых интерфейсов. Однако чтобы быстрее и лучше понять принцип работы брандмауэра, мы рекомендуем создать такие правила, не используя автоматическую конфигурацию, «вручную», как это будет описано далее.

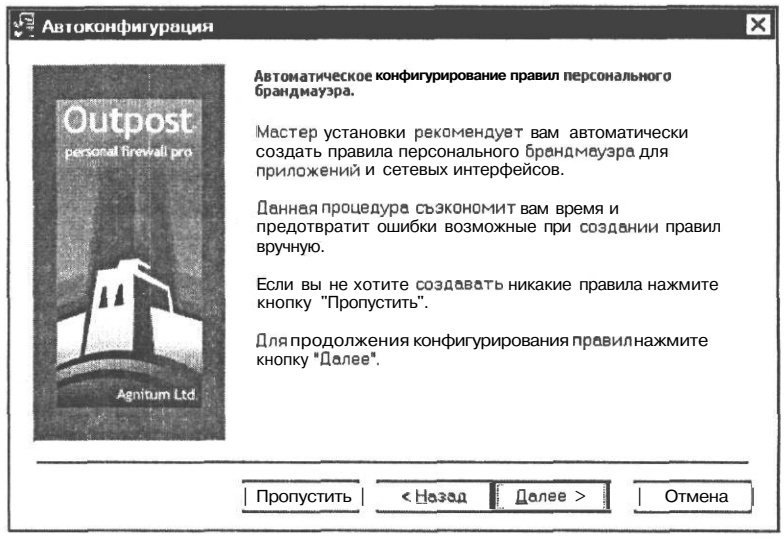



*Рис. 5.57. Диалог **Автоконфигурация** (Auto-configuration)*

> Нажмите кнопку Пропустить (Skip), чтобы автоматически не создавать правила брандмауэра, и в появившемся диалоге **Установка завершена** (Installation Complete) (Рис. 5.58) нажмите кнопку **Завершить** (Finish).

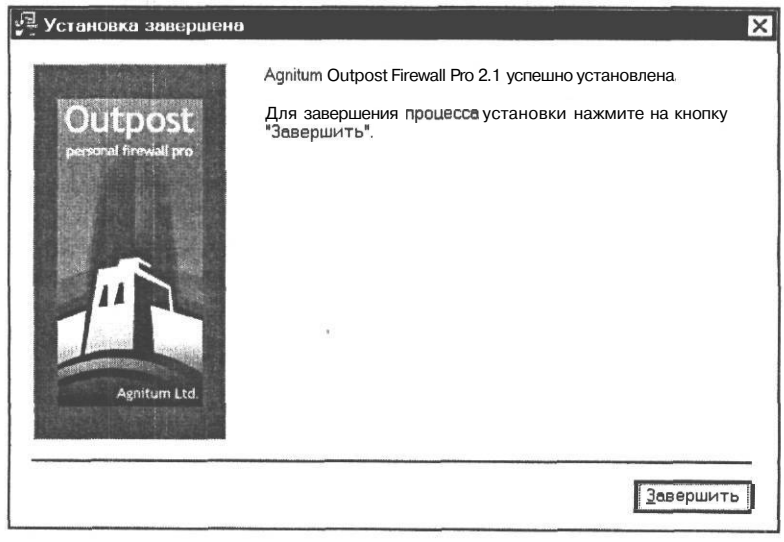



*Рис. 5.58. Диалог **Установка завершена** (Installation Complete)*

После перезагрузки компьютера защитный экран готов к работе.

При установке Agnitum Outpost Firewall Pro автоматически задаются следующие основные настройки:

- брандмауэр запускается при начальной загрузке Windows;
- значок режима работы брандмауэра (?) помещается в правой части Панели задач (Taskbar) Windows;
- при закрытии главного окна брандмауэра его значок (?) остается в правой части Панели задач (Taskbar) Windows.

В дальнейшем пользователь может изменить эти настройки.

После завершения установки и перезагрузки компьютера система Agnitum Outpost Firewall Pro автоматически будет запущена. На экране появится ее главное окно (Рис. 5.59), а в правой части Панели задач (Taskbar) - значок (?) - Outpost Firewall. Если главное окно не появилось, дважды щелкните мышью на значке (?) в правой части Панели задач (Taskbar).

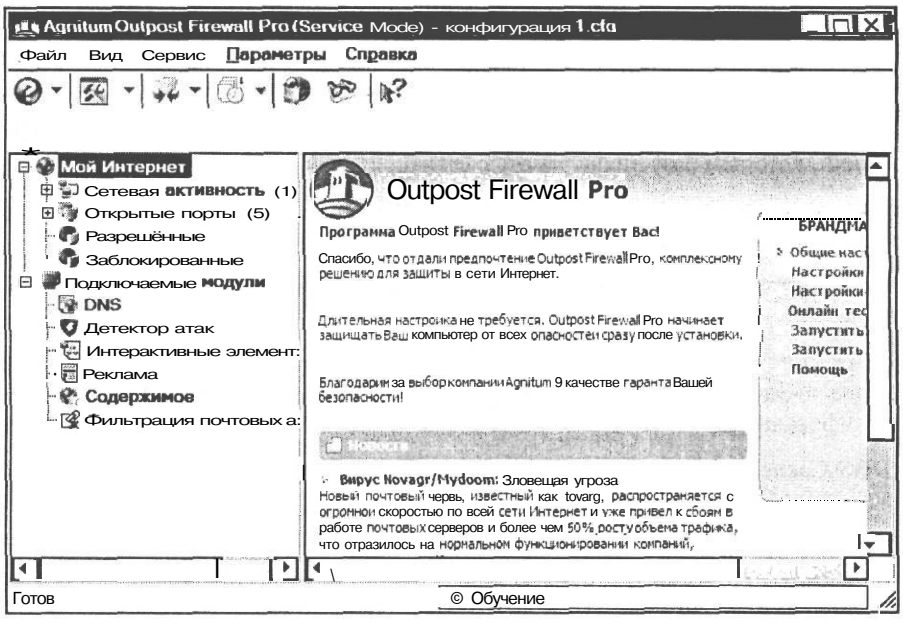



*Рис. 5.59. Главное окно системы Agnitum Outpost Firewall Pro*

Главное окно системы Agnitum Outpost Firewall Pro предназначено для визуального контроля работы компьютера в сети, а также для изменения настроек системы. В этом окне под полосой меню располагается панель инструментов, кнопки которой позволяют осуществлять быстрый доступ к основным режимам и настройкам. У нижнего края главного окна находится строка состояния, в которой отображается информация о назначении элементов управления, текущем состоянии и режиме работы системы. Большую часть главного окна занимают две панели: панель представлений - слева и информационная панель - справа.

Панель представлений отображает перечень компонентов, а информационная панель представляет специальные данные о каждом компоненте, выделенном на панели представлений.

Панель представлений содержит иерархический список объектов, протокол работы системы для которых может отображаться на информационной панели. Этот список поддерживает три уровня иерархии. На первом уровне имеется два объекта:

**Мой Интернет** (My Internet), содержащий двухуровневый иерархический список всех объектов, определяющих работу с сетью;

**Подключаемые модули** (Plug-Ins), содержащий список всех имеющихся в системе подключаемых модулей.

Объект **Мой Интернет** (My Internet) по умолчанию состоит из следующих элементов, относящихся ко второму уровню иерархии:

**Сетевая активность** (Network Activity) - список всех объектов, имеющих соединение с сетью;

**Открытые порты** (Open Ports) - список всех объектов, имеющих открытые порты для сетевого соединения. Порт - это не физический разъем или гнездо, а элемент программной среды, представляющий собой логический номер, соответствующий различным типам данных. Порт необходим для передачи данных в приложения;

**Разрешенные** (Allowed) - список всех работавших со времени начала ведения протокола приложений, которым разрешена работа с сетью;

**Заблокированные** (Blocked) - список всех приложений, для которых была блокирована попытка работы с сетью со времени начала ведения протокола.

Количество и вид элементов в списке **Мой Интернет** (My Internet) определяется пользователем.

Иерархический список **Подключаемые модули** (Plug-Ins) по умолчанию содержит следующие элементы, каждый из которых соответствует определенному типу отображаемой информации:

**DNS** (DNS Cache) - предназначен для кэширования и отображения протокола процесса преобразования DNS-адресов;

**Детектор атак** (Attack Detection) - предназначен для уведомления пользователя о предполагаемой атаке на его компьютер из сети и принятии действий по недопущению нанесения ущерба вашему компьютеру.

**Интерактивные элементы** (Active Content) - предназначен для вывода протокола о запрете выполнения программ на языках VB и JavaScript, а также Java-апплетов, элементов ActiveX и т.п.;

**Реклама** (Ads) - предназначен для вывода протокола о блокировании рекламы;

**Содержимое** (Content) - предназначен для вывода протокола о запрете отображения Web-сайтов или Web-страниц, имеющих определенный Интернет-адрес (DNS-адрес) либо содержащих определенные текстовые строки;

**Фильтрация почтовых вложений** (Attachments Filter) - предназначен для проверки файлов, поступающих на ваш компьютер по электронной почте;

Любая строка панели представлений, в начале которой стоит значок га, может открыть ряд подкатегорий. Значок в в начале строки указывает, что подкатегория уже открыта. Если вы щелкнете мышью на значке в, то все подкатегории объекта будут скрыты и будет показан только тип объекта.

## Настройка политики работы с сетью

Одной из наиболее важных характеристик системы Agnitum Outpost Firewall Pro является политика или режим работы с сетью. Меню для выбора политики вы увидите, если щелкнете правой кнопкой мыши на значке в правой части **Панели задач** (Taskbar) и в появившемся контекстном меню выберете команду **Политики** (Policy) (Рис. 5.60).

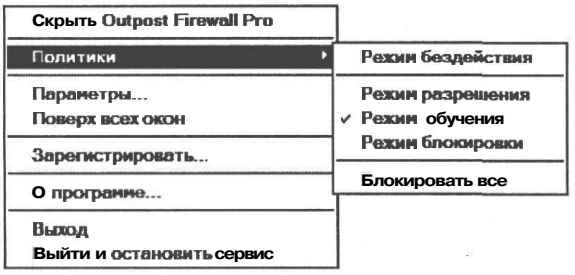



*Рис. 5.60. Меню политик (режимов)*

Выбрать политику брандмауэра можно также, нажав первую слева кнопку на панели инструментов главного окна программы или открыв вкладку **Политики** (Policy) диалога **Параметры** (Options) (Рис. 5.61) командой меню **Параметры** ◆ **Политики** (Options ◆ Policy).

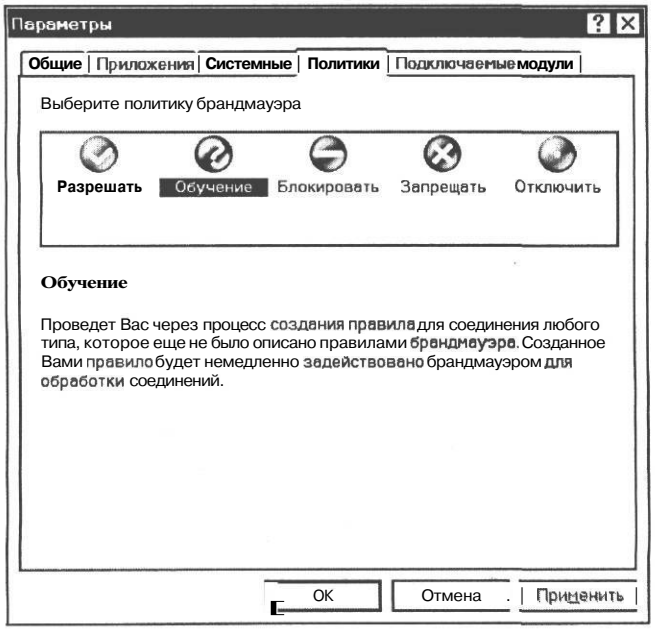



*Рис. 5.61. Вкладка **Политики** (Policy) диалога **Параметры** (Options)*

Существует пять режимов или политик работы с сетью. Название политики, использующееся на вкладке Политики (Policy) диалога Параметры (Options), приведено в скобках:

Режим бездействия (Отключить) (Disable mode) - разрешены все сетевые взаимодействия; брандмауэр отключен. В данном режиме значок в правой части Панели задач (Taskbar) имеет вид  ;

Режим разрешения (Разрешать) (Allow most mode) - разрешены все сетевые взаимодействия, которые явно не заблокированы; значок в правой части Панели задач (Taskbar) имеет вид  ;

Режим обучения (Обучение) (Rules Wizard) - первое сетевое взаимодействие каждого приложения сопровождается предупреждением и дает вам возможность создать правило для работы этого приложения с сетью. Созданное правило будет немедленно задействовано брандмауэром для обработки соединений. В данном режиме значок в правой части Панели задач (Taskbar) имеет вид ;

Режим блокировки (Блокировать) (Block most mode) - запрещены все сетевые взаимодействия, за исключением явно разрешенных. Для каждого приложения, которому необходим доступ в Интернет, потребуется создать правило брандмауэра. Значок в правой части Панели задач (Taskbar) имеет вид ;

Блокировать все (Запрещать) (Stop all) - запрещены все сетевые взаимодействия; значок в правой части Панели задач (Taskbar) имеет вид  .

Сразу после установки на ваш компьютер система Agnitum Outpost Firewall Pro готова к выполнению своих функций и работает в режиме обучения. Этот режим позволяет выявить все приложения, взаимодействующие с сетью, и помогает вам принять решение о допустимости сетевых взаимодействий для каждого приложения. Если приложению позволено общаться с сетью, то работа в этом режиме облегчит вам задание правил, определяющих конкретные параметры сетевых соединений для данного приложения (протоколы, порты и т.д.).

Чтобы изменить политику работы с сетью, следует выбрать нужный режим в контекстном меню значка (?) либо в меню, которое откроется, если нажать кнопку © - на панели инструментов.

## Создаем правила фильтрации для просмотра Web-страниц, почты, новостей, загрузки файлов и обновления вирусных баз

В начале использования брандмауэра рекомендуется оставить систему Agnitum Outpost Firewall Pro работать в режиме обучения и принимать конкретное решение отдельно для каждого сетевого соединения. При первой же попытке любой программы получить или передать информацию через сеть на экране появится диалог с предупреждением о сетевом взаимодействии, в котором вы сможете разрешить или запретить запрашиваемое подключение. После работы в режиме обучения в течение некоторого времени (30 минут - 1 час) система выявит большинство приложений, регулярно обращающихся к сети, и поможет вам определить правила сетевых обращений со стороны этих приложений.

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

Мы рассмотрим общий порядок создания правил на примере использования браузера **Internet Explorer** и программы для работы с почтой и новостями **Outlook Express**, так как это - наиболее распространенные программы для работы в Интернете. Однако мы не рекомендуем пользоваться указанными программами, поскольку они, как и все продукты Microsoft, содержат ошибки в плане безопасности. Кроме того, учитывая их широкую распространенность, именно на эти программы в первую очередь ориентированы деструктивные действия хакеров.

## Правила для просмотра Web-страниц

После подключения к Интернету, при первой же попытке вашего браузера установить связь с каким-либо сервером, защитный экран Agnitum Outpost Firewall Pro, работающий в режиме обучения, выдаст на экран диалог с предупреждением (Рис. 5.62).

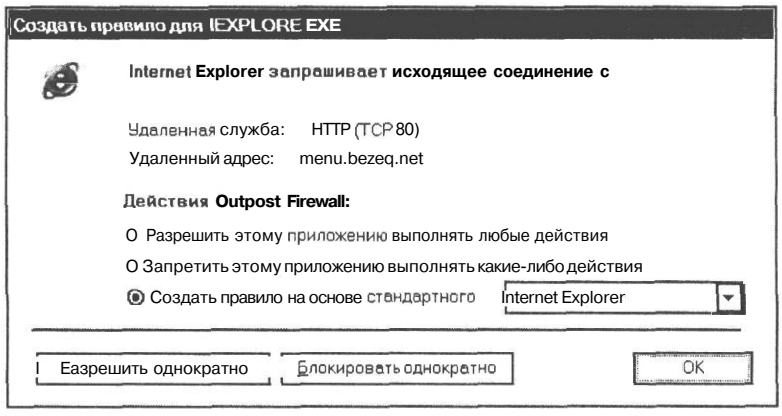



***Рис. 5.62. Диалог Создать правило для IEXPLORE.EXE***
*(Create rule for IEXPLORE.EXE)*

В этом диалоге вам сообщается о том, какое приложение (в данном примере - **Internet Explorer), в** каком направлении запрашивает соединение (в данном примере - **исходящее** (outgoing)), через какой именно порт (в данном примере - 80, зарезервированный за **TCP),** по какому протоколу (HTTP) и по какому сетевому адресу (в данном примере - **menu.bezeq.net).** После появления этого диалога вы можете, установив один из переключателей или нажав кнопку, определить правила выхода в сеть для данного приложения:

**Разрешить этому приложению выполнять любые действия** (Allow all activities for this application). Установка данного переключателя для тех приложений, которым вы доверяете, разрешит им все виды сетевых действий. Программа попадет в список **Доверенные приложения** (Trusted applications), расположенный на вкладке **Приложения** (Application) диалога **Параметры** (Options);

**Запретить этому приложению выполнять какие-либо действия** (Stop all activities for this application). Данный переключатель следует установить для приложений, которые не должны получать выхода в сеть. При этом все виды сетевых действий для этого приложения будут запрещены. Программа попадет в список **Запрещенные приложения** (Blocked applications), находящийся на вкладке **Приложения** (Application) диалога **Параметры** (Options);

**Создать правило на основе стандартного** (Create rules using preset). Для приложений, которые могут выходить в сеть по определенным протоколам, через определенные порты и т.д., следует установить данный переключатель и в открывающемся списке справа выбрать тип приложения, для которого должно быть сформировано правило выхода в сеть. Обычно в открывающемся списке по умолчанию предлагается именно то приложение, которое запрашивает выход в сеть. Программа попадет в список **Пользовательский уровень безопасности** (Partially allowed applications) на вкладке **Приложения** (Application) диалога **Параметры** (Options) (Рис. 5.63);

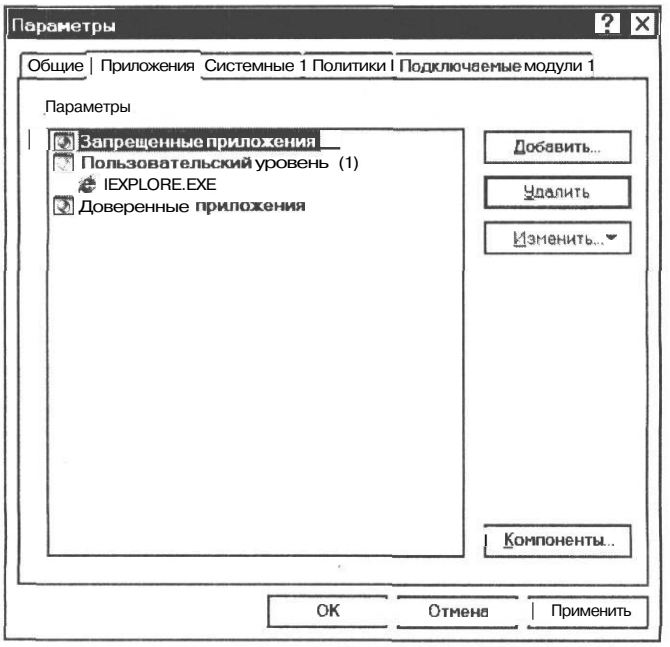



*Рис. 5.63. Вкладка **Приложения** (Application) диалога **Параметры** (Options)*

**Разрешить однократно** (Allow Once). Если вы еще не приняли окончательного решения о возможностях работы в сети данного приложения, то нажатие этой кнопки разрешит одноразовое соединение. При следующей попытке данного приложения создать сетевое соединение вновь появится соответствующее предупреждение. Никакого правила для данного приложения не создается;

**Блокировать однократно** (Block Once). Если для приложения в данный момент выход в сеть нежелателен, то нажатие данной кнопки запретит сетевое соединение. При следующей

попытке этого приложения создать сетевое соединение на экране снова появится диалог с предупреждением о сетевом соединении. Никакого правила для данного приложения не создается.

По умолчанию в диалоге с предупреждением (Рис. 5.62) установлен переключатель Создать правило на основе стандартного (Create rules using preset), а в открывающемся списке указано имя приложения, запрашивающего исходящее соединение. Рекомендуется согласиться с действиями, предлагаемыми системой Agnitum Outpost Firewall Pro по умолчанию, нажав в диалоге кнопку OK. Браузер будет включен в список Пользовательский уровень (Partially allowed applications) на вкладке Приложения (Application) диалога Параметры (Options), и в дальнейшем для него всегда будут применяться правила выхода в сеть, определенные системой Agnitum Outpost Firewall Pro для данного типа приложений.

Если для просмотра Web-страниц вы используете не Internet Explorer, а другой браузер, то настройка правил выхода в сеть для него будет выполняться аналогично.

## Правила для почтовой программы

При первой же попытке отправить или получить почту, брандмауэр Agnitum Outpost Firewall Pro выдаст диалог, примерно такой, как на Рис. 5.64.


*Рис. 5.64. Диалог Создать правило для CCAPP.EXE (Create rulefor CCAPP.EXE)*

Данный диалог предупреждает о том, что некое приложение (CCAPP.EXE - компонент Norton AntiVirus, выполняющий функции почтового клиента) запрашивает исходящее (outgoing) соединение с сервером исходящей почты (smtp.mail.ru) по почтовому протоколу (POP3) через указанный порт (**TCP:110**).

По умолчанию в диалоге установлен переключатель Создать правило на основе стандартного (Create rules using preset), а в открывающемся списке справа от него указывается тип правила - E-mail Client (Почтовый клиент).

Наилучший вариант реакции на это сообщение - нажать кнопку OK, чтобы разрешить почтовой программе выполнять свои функции. Приложение будет включено в список

**Пользовательский уровень** (Partially allowed applications) вкладки **Приложения** (Application) диалога **Параметры** (Options). В дальнейшем доступ этой программы в сеть будет определяться правилами, предусмотренными системой Agnitum Outpost Firewall Pro для почтовых клиентов.

## Правила для чтения новостей

Когда вам потребуется обратиться к серверу новостей, на экране появится предупреждение, подобное тому, которое показано на Рис. 5.65.

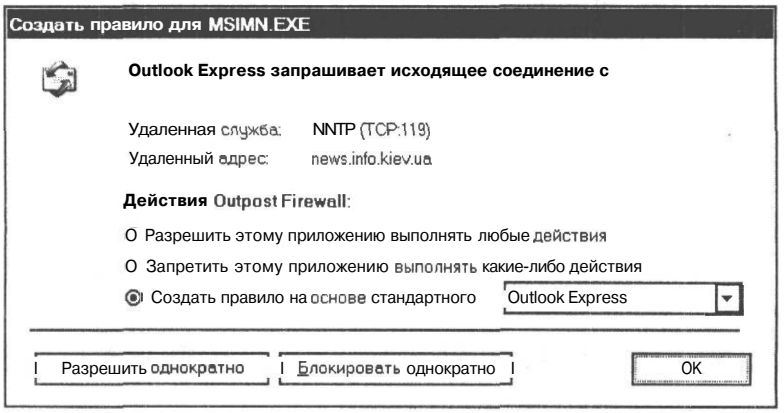



*Рис. 5.65. Диалог* ***Создать правило для*** *MSIMN.EXE (Create rule for MSIMN.EXE)*

В этом диалоге содержится сообщение о том, что приложение **(Outlook Express)** запрашивает **исходящее** (outgoing) соединение с сервером новостей **(news.info.kiev.ua)** по соответствующему протоколу (NNTP) через указанный порт (**TCP:119**). Система Agnitum Outpost Firewall Pro предлагает создать правило для выхода этой программы в сеть на основе стандартных правил, предусмотренных для программы Outlook Express.

После закрытия этого диалога нажатием кнопки **OK** программа Outlook Express будет включена в список **Пользовательский уровень** (Partially allowed applications) вкладки **Приложения** (Application) диалога **Параметры** (Options). В дальнейшем доступ этой программы в сеть будет определяться предусмотренными для нее правилами.

## Правила для менеджера загрузки

Если вы для загрузки файлов используете специализированный менеджер, например GetRight, то при первой же попытке этого приложения подключиться к какому-либо серверу на экране появится предупреждение об этом (Рис. 5.66). До вашего сведения будет доведено, что приложение **(GETRIGHT.EXE)** запрашивает **исходящее** (outgoing) соединение с Web-узлом **(www.3st.ru)** по Web-протоколу (HTTP) через указанный порт (TCP:80).

Рекомендуется закрыть диалог нажатием кнопки OK и создать таким образом правило для работы менеджера загрузки в сети. Менеджер загрузки будет включен в список **Пользовательский уровень** (Partially allowed applications) вкладки **Приложения** (Application) диалога **Параметры** (Options).


***Рис. 5.66. Диалог Создать правило для GETRIGHT.EXE***
*(Create rule for GETRIGHT.EXE)*

## Правила для компонента LiveUpdate программы Norton AntiVirus

При первой попытке обновить вирусные базы программы Norton AntiVirus Professional с помощью компонента LiveUpdate на экране появится диалог **Создать правило для lucomserver.exe** (Create rule for lucomserver.exe) (Рис. 5.67) с сообщением о том, что модуль LiveUpdate запрашивает **исходящее** (outgoing) соединение с Web-узлом **212.199.29.8** по протоколу **HTTP** через порт **TCP:80.**

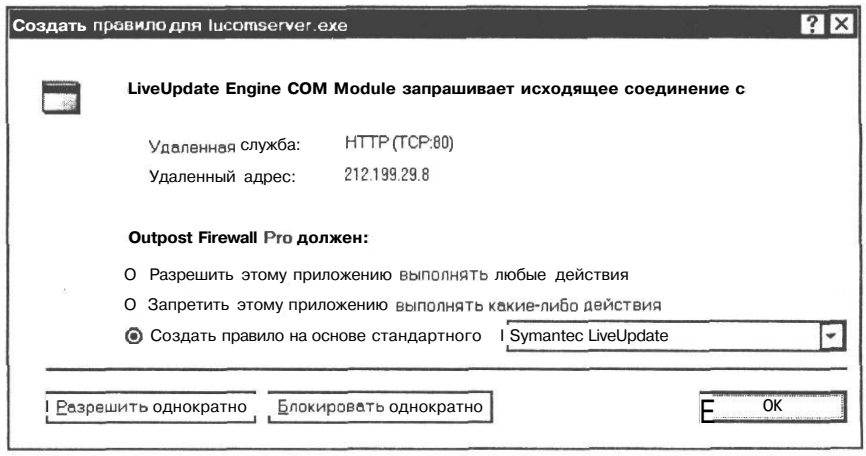



*Рис. 5.67. Диалог* ***Создать правило для lucomserver.exe***
*(Create rule for lucomserver.exe)*

После закрытия этого диалога нажатием кнопки **OK** будет создано правило для работы в сети программы LiveUpdate. Эта программа будет включена в список **Пользовательский уровень** (Partially allowed applications) вкладки **Приложения** (Application) диалога **Параметры** (Options).

Для всех остальных приложений, в корректной работе которых вы уверены, правила выхода в Интернет задаются подобным же образом.

## Что делать, если на экране появился вопрос?

В процессе работы в сети в режиме обучения система Agnitum Outpost Firewall Pro будет выводить на экран запрос всякий раз, когда новая, не знакомая брандмауэру программа, будет запрашивать соединение с сетью. Реагируя на такие запросы, следует руководствоваться следующими соображениями.

Если приложение не должно выходить в Интернет, например, программа Microsoft Word, то следует однозначно запретить этому приложению любое соединение. Многие программы, не имеющие отношения к Интернету, например офисные, могут проверять в Интернете наличие новых версий или просто сообщать авторам о своем местонахождении. В большинстве случаев такая активность является излишней, и ее следует пресекать.

Если вы вообще ничего не знаете о программе, запрашивающей соединение, попробуйте сначала однократно запретить ее. Если такой шаг не повлияет на работу в Интернете других программ - браузера, почтового клиента, то запретите работу неизвестной программы в Интернете навсегда. Вместе с тем, в Windows 2000/XP есть программы, без которых невозможна работа в сети, например **svchost.exe.** Если вы запретите ее соединение с сетью, то браузер не будет работать.

При конфигурации сети с общим доступом к подключению Интернета в Windows XP необходимо также разрешить все сетевые взаимодействия программе **Alg.exe,** обеспечивающей поддержку общего доступа в Интернет средствами Windows XP.

Если соединение запрашивается по какому-либо адресу, который вы не знаете или который вам не нужен, то попробуйте сначала блокировать однократно, после чего вы сможете принять окончательное решение о подключении по данному адресу.

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 брандмауэра, вы сможете изменить те или иные настройки.

## Группирование приложений

Одной из самых важных функций Agnitum Outpost Firewall Pro является фильтрация приложений. Она позволяет пользователю решать, какие из приложений получают возможность соединения.

С точки зрения системы Agnitum Outpost Firewall Pro, все приложения делятся на три группы. В состав первой группы входят те приложения, которым запрещены все сетевые соединения. Рекомендуется относить к этой группе приложения, которым не требуется соединение с Интернет: текстовые редакторы, калькуляторы и т.д.

Ко второй группе относятся приложения, для которых явно, в виде специальных правил, указаны те протоколы, порты и направления, с которыми сетевые соединения разрешены.

К третьей группе относятся программы, которым разрешены все сетевые соединения. Рекомендуется включать в нее только те приложения, которым вы полностью доверяете.

Управление распределением приложений по группам, а также формирование правил для приложений осуществляется на вкладке **Приложения** (Application) диалога **Параметры** (Options) (Рис. 5.68). Доступ к этой вкладке осуществляется посредством команды меню **Параметры** ◆ **Приложения** (Options ◆ Application).

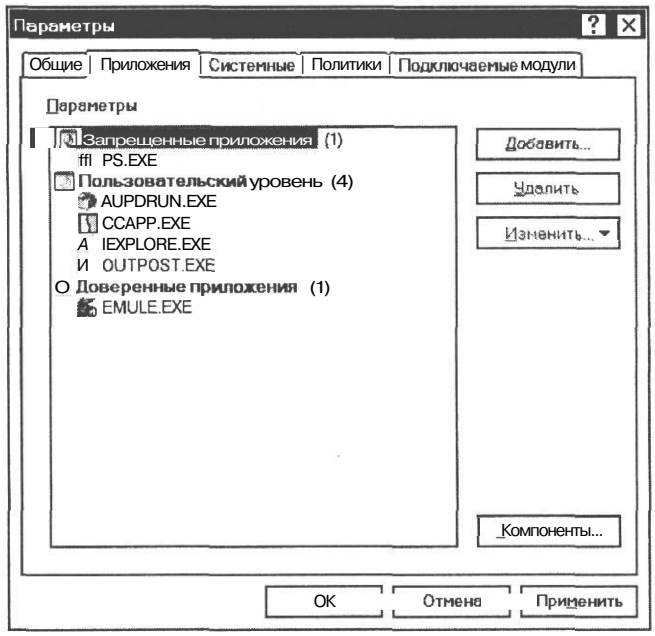



*Рис. 5.68. Приложения распределены по группам*

В поле **Параметры** (Settings) этой вкладки находится иерархический список приложений, распределенных по трем группам:

**Запрещенные приложения** (Blocked applications) - приложения, которым запрещена работа в сети;

**Пользовательский уровень** (Partially allowed applications) - приложения, которым работа в сети разрешена в соответствии с правилами, заданными для этих приложений;

**Доверенные приложения** (Trusted applications) - приложения, которым разрешена работа в сети.

Каждая из этих групп содержит список принадлежащих ей приложений. Это - те приложения, которые уже обращались к сети и которым вы разрешили или запретили сетевую активность.

Вы можете сами добавить приложение в одну из этих групп. Для этого следует щелчком мыши выделить название соответствующей группы и нажать кнопку **Добавить** (Add). В появившемся диалоге открытия файла необходимо указать имя исполняемого файла приложения и нажать кнопку **Открыть** (Open), после чего указанное приложение будет включено в выбранную группу. Вы можете также внести приложение в одну из групп, перетащив значок этого приложения с **Рабочего стола** (Desktop) или из главного меню Windows. Если приложение, которое вы внесли в один из трех списков, уже находилось в другом списке, то из последнего оно будет удалено.

В процессе дальнейшей работы с брандмауэром вам, несомненно, может потребоваться разрешить заблокированному приложению подключаться к сети или же запретить подозрительной программе выход в сеть. Для этого нужно переместить приложение из одной группы в другую. Для перемещения следует щелчком мыши выделить имя приложения и нажать кнопку **Изменить** (Edit). В появившемся меню (Рис. 5.69) следует выбрать одну из следующих команд:

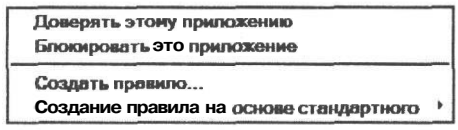



*Рис. 5.69. Меню для перемещения приложений между группами*

**Доверять этому приложению** (Always Trust This App), если вы хотите перенести данное приложение в группу **Доверенные приложения** (Trusted applications);

**Блокировать это приложение** (Always Block This App), если вы хотите перенести данное приложение в группу **Запрещенные приложения** (Blocked applications);

**Создать правило** (Modify Rules), если вы хотите перенести данное приложение в группу **Пользовательский уровень** (Partially allowed applications) и задать собственное правило для данного приложения. В этом случае на экране появится диалог формирования правил для приложения;

**Создание правила на основе стандартного** (Create rules using preset), если вы хотите перенести данное приложение в группу **Пользовательский уровень** (Partially allowed applications) и использовать одно из предопределенных в системе Agnitum Outpost Firewall Pro правил. В этом случае на экране появится меню стандартных правил (Рис. 5.70).

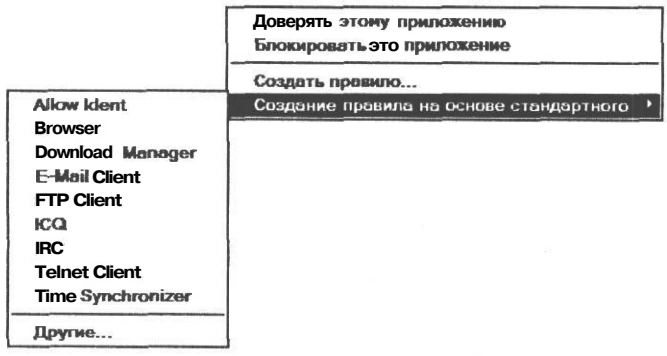



*Рис. 5.70. Меню стандартных правил*

Если выбрать один из пунктов этого меню, содержащий имя программы, для которой задаются предопределенные правила, то соответствующие правила будут внесены в список правил для данного приложения. При выборе пункта меню **Другие** (Custom) на экране появится диалог формирования правил для приложения.

Если приложение находится в группе **Доверенные приложения** (Trusted applications), то пункта **Доверять этому приложению** (Always Trust This App) в меню не будет. Аналогично, если приложение находится в группе **Запрещенные приложения** (Blocked applications), то в меню не будет пункта **Блокировать это приложение** (Always Block This App).

Если приложение находится в группе **Пользовательский уровень** (Partially allowed applications) и выбран пункт **Создать правило** (Modify rules) или **Создание правила на основе стандартного** (Create rules using preset), то приложение в другую группу не переносится, а для него формируется новое правило.

Вы можете также перенести приложение из одной группы в другую, перетащив мышью название приложения в соответствующую группу. Если вы перетащили приложение в группу **Пользовательский уровень** (Partially allowed applications), то сначала появится диалог формирования правил. Для всех остальных групп имя приложения вместе с его значком окажется в списке приложений соответствующей группы.

Напомним, что система Agnitum Outpost Firewall Pro включает в себя большое количество готовых правил обращения к сети, которые разбиты по типам приложений. В системе содержатся правила для просмотра Web-страниц, работы с FTP-сервисом, электронной почтой, сетевой службой новостей, системой удаленной загрузки программ, синхронизации времени и другие.

Если вы формируете одно или несколько правил для приложения, выполняющего любую из вышеперечисленных сетевых операций, то рекомендуется пользоваться предопределенными правилами, имеющимися в системе Agnitum Outpost Firewall Pro и выбираемыми из меню стандартных правил (Рис. 5.70), которое появляется при выборе команды **Создание правила на основе стандартного** (Create rules using preset). В таком случае вам не придется разбираться, как те или иные программы используют порты и протоколы для выполнения сетевых операций.

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

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

## Настройки для локальных сетей

С точки зрения Agnitum Outpost Firewall Pro принципиальная разница между локальной сетью и Интернетом состоит в уровне доверия, которое пользователь им оказывает. Локальная сеть создается дома или в офисе и охватывает обычно «дружественные» компьютеры, которые используются членами семьи или коллегами. Компьютеры, объединенные в локальную сеть, можно условно назвать доверенной зоной. В доверенной зоне Agnitum Outpost Firewall Pro не осуществляет контроль сетевых взаимодействий. Посмотрим, как включить вашу локальную сеть в доверенную зону.

> Выберите команду меню **Параметры * Системные** (Options ◆ System). На экране появится диалог **Параметры** (Options) с открытой вкладкой **Системные** (System) (Рис. 5.71).

➤ В группе **Настройка сети** (LAN Settings) нажмите кнопку **Параметры** (Settings). Откроется диалог **Настройка локальной сети** (LAN Settings) (Рис. 5.72).

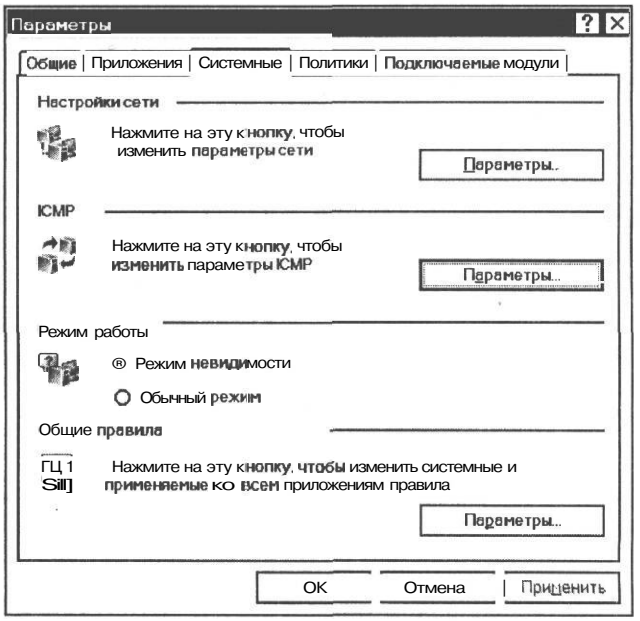



*Рис. 5.71. Вкладка **Системные** (System) диалога **Параметры** (Options)*

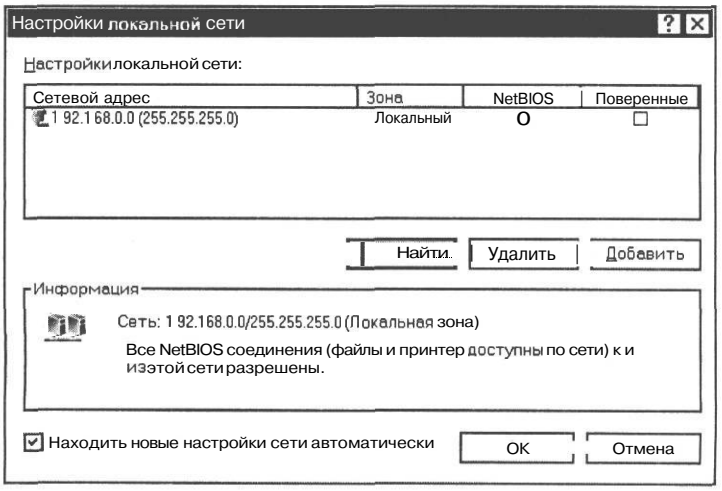



*Рис. 5.72.Диалог **Настройка локальной сети** (LAN Settings)*

В поле **Сетевой адрес** (Network Address) этого диалога обычно уже содержится IP-адрес вашей локальной сети - **192.168.0.0 (255.255.255.0).** Но если этот адрес был удален или не выполнялась автоматическая конфигурация после установки профаммы, то адрес может отсутствовать. В таком случае нажмите кнопку **Найти** (Detect), чтобы обнаружить сеть.

При установленном флажке **Находить новые настройки сети автоматически** (Auto-detect new network settings) программа будет самостоятельно обнаруживать новые сети, и вам не придется добавлять их вручную.

> Чтобы разрешить все соединения данной локальной сети, установите флажок **Доверенные** (Trusted).

Если же нужно удалить сетевой адрес из доверенных, то данный флажок следует сбросить.

➤ Чтобы разрешить входящие и исходящие соединения NetBIOS (доступ к файлам и принтерам) для данного сетевого адреса, убедитесь, что установлен флажок **NetBIOS.**

Протокол NetBIOS применяется операционной системой Windows в качестве протокола для доступа к удаленным файлам и принтерам. Брандмауэр Agnitum Outpost Firewall Pro позволяет либо запретить, либо разрешить использование данного протокола при сетевом соединении с определенными узлами, задаваемыми IP-адресами или DNS-адресами. Целесообразно разрешить использование протокола NetBIOS только при сетевом соединении с компьютерами вашей локальной сети. По умолчанию флажок **NetBIOS** установлен.

Для блокировки соединения с данной сетью следует сбросить флажки **NetBIOS и Доверенные** (Trusted).

При использовании брандмауэра, кроме локальной сети, вы можете указать также зону сетевых адресов, для которых контроль сетевых взаимодействий выполняться не будет. Эта зона представляет собой список узлов или подсетей, задаваемых своими IP-адресами или DNS-адресами, для которых брандмауэр 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.

Для формирования списка доверенных адресов следует нажать кнопку **Добавить** (Add). В появившемся диалоге **Сетевой адрес** (Network Address) (Рис. 5.73) установите переключатель, соответствующий типу адреса, введите адрес или диапазон адресов и нажмите кнопку **Добавить** (Add). После закрытия диалога **Сетевой адрес** (Network Address) нажатием кнопки **OK** новый адрес появится в диалоге **Настройка локальной сети** (LAN Settings), где, установив флажок **Доверенные** (Trusted), вы сможете включить данный адрес в доверенную зону.

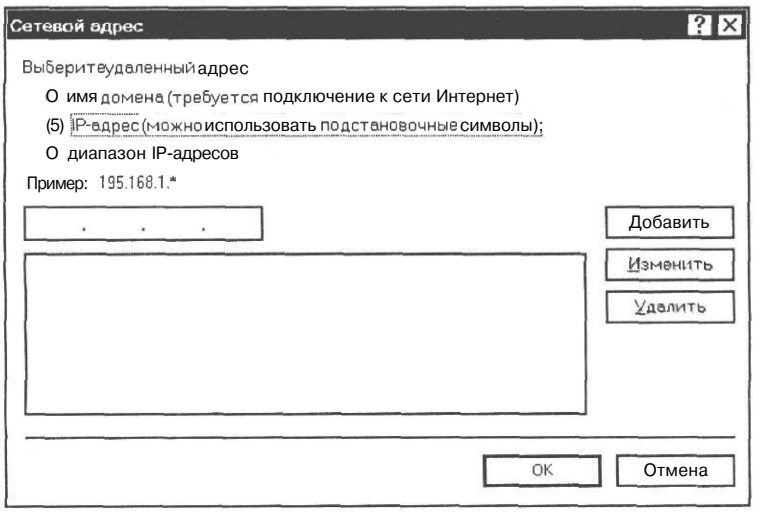



*Рис. 5.73. Диалог* ***Сетевой адрес*** *(Network Address)*

Выделив сетевой адрес и нажав кнопку Удалить (Remove), вы удалите его из списка. Удаление адреса из списка оказывает тот же эффект, что и сброс флажков **NetBIOS и Доверенные** (Trusted). Отсутствие удаленного адреса в списке означает, что соединения **NetBIOS** будут блокированы для этого адреса.

➤ Закройте диалог **Настройка локальной сети** (LAN Settings) нажатием кнопки **OK.**

Важно помнить, что компьютеры в доверенной зоне имеют право приоритетного соединения. Даже блокированные приложения могут взаимодействовать с сетями и узлами, включенными в доверенную зону. Целесообразно назначать данный уровень исключительно проверенным компьютерам. Если используются лишь совместные файлы и печать, рекомендуется выбрать уровень доступа **NetBIOS.**

## Смотрим информацию обо всех подключениях в процессе работы в Интернете

Система Agnitum Outpost Firewall Pro дает возможность визуально контролировать сетевые взаимодействия вашего компьютера с другими узлами сети. Вы можете адаптировать параметры этого контроля к своим задачам, изменив соответствующие настройки отображения информации.

Во время работы в Интернете рекомендуется регулярно просматривать в главном окне брандмауэра Agnitum Outpost Firewall Pro информацию, соответствующую элементам списков **Разрешенные** (Allowed) и **Заблокированные** (Blocked), входящих в состав объекта **Мой Интернет** (My Internet). Чтобы увидеть информацию о разрешенных соединениях, следует щелкнуть мышью в левой части информационной панели на названии элемента **Разрешенные** (Allowed). В правой части этой панели отобразится общая статистика соединений, разрешенных Outpost Firewall (Рис. 5.74).

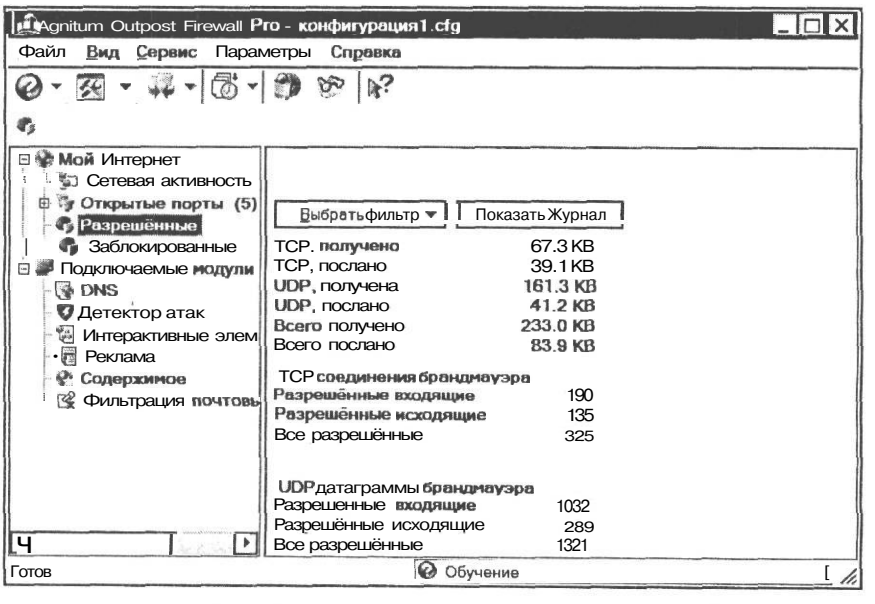



*Рис. 5.74. Статистика разрешенных соединений*

После нажатия кнопки **Показать журнал** (Show Detailed Log) откроется окно **Журнал Outpost Firewall Pro** (Outpost Firewall Pro Viewer) (Рис. 5.75), показывающий историю каждой операции, выполненной программой. Окно журнала состоит из двух панелей: слева - панель дерева консоли, справа - информационная панель. Дерево консоли представляет собой перечень фильтров и соответствующих настроек. Информационная панель построена в виде таблицы с записями журналов и настроек, которые выделены в дереве консоли.

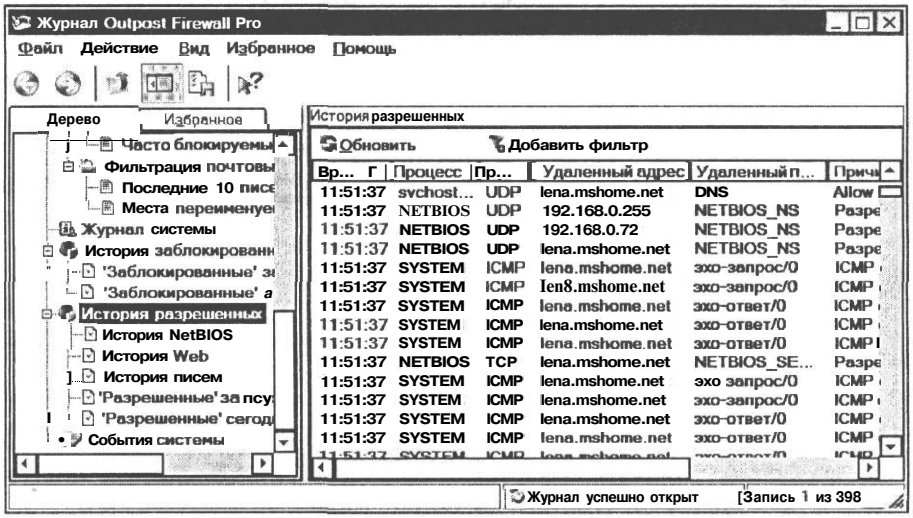



*Рис. 5.75. История разрешенных соединений*

История разрешенных соединений, представлена в виде таблицы (Рис. 5.75). Каждая строка таблицы связана с одним сетевым взаимодействием. При этом одно и то же приложение может упоминаться более одного раза в том случае, если его обмен с сетью осуществляется через несколько портов. Для каждого соединения указывается:

**Время** (Start Time) - дата и время установки соединения;

**Процесс** (Application) - имя приложения, установившего связь;

**Протокол** (Protocol), по которому установлена связь;

**Удаленный адрес** (Remote Address), по которому установлена связь;

**Удаленный порт** (Remote Port), через который установлена связь;

**Причина** (Reason), по которой данный обмен с сетью был разрешен. Ею может быть имя соответствующего правила для приложения, описание служебного обмена, например, для преобразования DNS-адреса в IP-адрес. Если система работает в режиме бездействия, то для элемента **Разрешенные** (Allowed Connections) никакая причина не указывается.

Основное назначение информации списка **Разрешенные** (Allowed Connections) - формирование истории сетевых обращений. При работе с этим списком следует убедиться в том, что приложения, которым действительно разрешено работать с сетью, взаимодействуют с ней по корректным протоколам, поддерживают связь с корректными удаленными портами и т.д. В случае если информация о каком-либо приложении вызывает у вас сомнение, рекомендуется изменить для него правила контроля сетевых взаимодействий или переместить в другую группу, как это описано в разделе «Группирование приложений».

Чтобы увидеть список заблокированных соединений, следует щелкнуть мышью в левой части окна журнала на названии элемента История заблокированных (Blocked Connections). Список заблокированных соединений, который появится в правой части этой панели, представлен в виде таблицы с теми же полями, что и у списка История разрешенных (Allowed Connections) (Рис. 5.76).

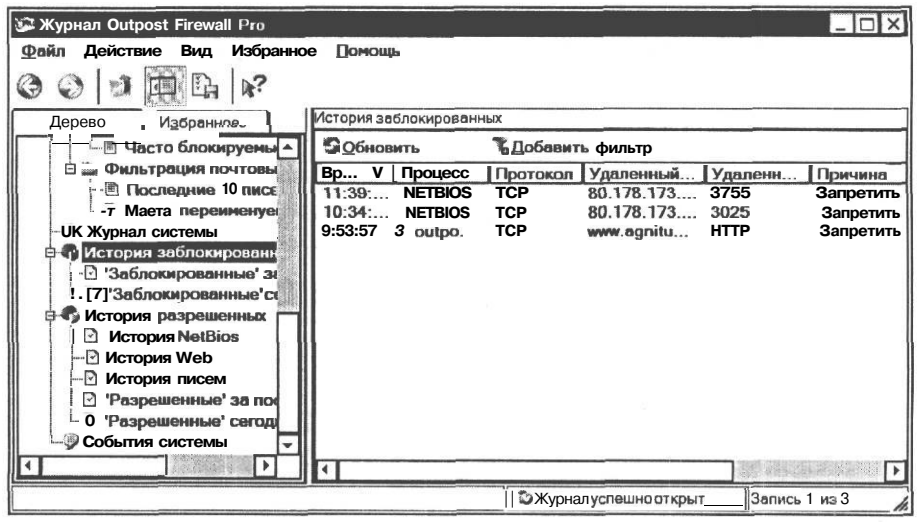



*Рис. 5.76. История заблокированных соединений*

Основное назначение информации списка Заблокированные (Blocked Connections) - обнаружить ошибочно заблокированные сетевые соединения, а также приложения, обращающиеся к портам или протоколам, к которым им обращаться запрещено. Если в протоколе для элемента История заблокированных (Blocked Connections) появились приложения, которые должны осуществлять сетевое взаимодействие, и при этом информация о протоколе, удаленном узле, портах и других параметрах, с вашей точки зрения, является корректной, — это свидетельствует о том, что для данных приложений вы задали слишком жесткие правила работы. Может также оказаться, что вы вообще не задали никаких правил для этих приложений и выбрали политику работы Режим блокировки (Block most mode). В таком случае, если подобная политика является целесообразной с точки зрения безопасности, необходимо сформировать для данного приложения правила, обеспечивающие его нормальную работу в сети, как описано в разделе «Группирование приложений».

Если же приложение обращается в сеть по протоколам или портам, которые этому приложению действительно должны быть запрещены, то вы можете предположить, что данное приложение выполняет нерегламентированные операции, например, собирает и передает разработчикам приложения данные о пользователях и т.п.

## Подключаемые модули

Система Agnitum Outpost Firewall Pro построена по модульному принципу: часть возможностей брандмауэра реализована в виде отдельных библиотек, каждая из которых представляет собой отдельный файл с расширением **.ofp,** способный динамически подключаться к системе. Эти файлы находятся в папке Plugins, вложенной в ту папку, в которой установлена программа. Каждый из модулей имеет свои независимые настройки.

При установке системы Agnitum Outpost Firewall Pro инсталлируются все поставляемые вместе с брандмауэром подключаемые модули. Эти модули интегрированы в Agnitum Outpost Firewall Pro так, что информация об их работе отображается в главном окне системы, где они являются элементами списка **Подключаемые модули** (Plug-Ins). В ходе дальнейшей работы пользователь может подключать вновь разработанные модули и удалять модули, уже подключенные к системе, но устаревшие.

Для управления составом включенных в систему Agnitum Outpost Firewall Pro подключаемых модулей предназначена вкладка **Подключаемые модули** (Plug-Ins) диалога **Параметры** (Options) (Рис. 5.77). Доступ к ней осуществляется командой меню **Параметры * Подключаемые модули** (Options ◆ Plug-Ins Setup).

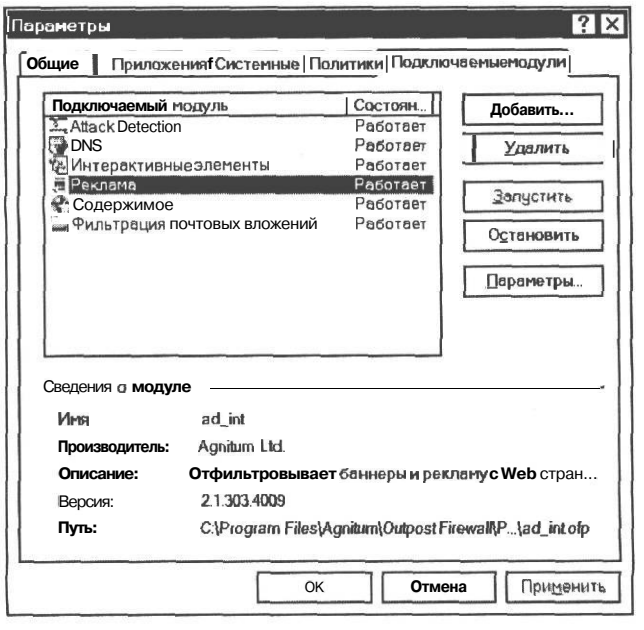



*Рис. 5.77. Вкладка **Подключаемые модули** (Plug-Ins) диалога **Параметры** (Options)*

На этой вкладке содержится список подключаемых модулей, входящих в систему. В каждой строке этого списка отображаются значок модуля, его название и текущее состояние, т.е. работает он в настоящий момент времени или остановлен. Подключаемые модули имеют следующее назначение:

**Детектор атак** (Attack Detection) (файл **prot_int.ofp**) - уведомление пользователя об атаке на его компьютер из сети.

**DNS** (Domain Name Cache) (файл **dns_int. ofp)** - ускорение работы в сети посредством кэширования DNS-адресов, которые затем используются для преобразования в IP-адреса;

**Интерактивные элементы** (Active Content Filtering) (файл **web_int. ofp)** - запрет использования активных элементов Web-страниц, а также файлов cookie, всплывающих окон и т.п.;

**Реклама** (Advertisement Blocking) (файл **add_int. ofp)** - ограничение отображения Web-страниц по содержащимся в них HTML-строкам или размеру графического изображения;

**Содержимое** (Content Filtering) (файл **cnt_int. ofp)** - запрет отображения Web-страниц по их DNS-адресу либо по содержащимся в них текстовым строкам;

**Фильтрация почтовых вложений** (Attachments Filter) (файл **file_int. ofp)** - проверка файлов, поступающих по электронной почте.

Вы можете, щелчком мыши выделив любой модуль и нажав кнопку **Остановить** (Stop), остановить его работу. Для запуска ранее остановленного модуля следует нажать кнопку **Запустить** (Start). С помощью кнопки Добавить (Add) можно подключить к системе новый модуль, а нажатием кнопки **Удалить** (Remove) - удалить выделенный модуль.

## Блокировка рекламы

С помощью подключаемого модуля Реклама (Advertisement Blocking) осуществляется ограничение отображения рекламы на просматриваемых Web-страницах. Хотя реклама и не представляет потенциальной опасности для вашего компьютера, ее ограничение значительно (на 20%-30%) ускоряет процесс загрузки Web-страниц и облегчает работу с Web-документами.

Ограничение отображения рекламы достигается посредством указания HTML-строк и размеров графических изображений, которые не должны показываться браузером. На месте не показываемых изображений будут выводиться строки: AD и AD-SIZE. Список HTML-строк и размеров изображений задается в диалоге настроек модуля. Вызвать этот диалог можно, выделив на вкладке Подключаемые модули (Plug-Ins) диалога Параметры (Options) модуль Реклама (Ads) и нажав кнопку Параметры (Settings). Можно также выбрать команду Параметры (Properties) в контекстном меню модуля Реклама (Ads) в главном окне программы Agnitum Outpost Firewall Pro. Контекстное меню появится, если щелкнуть правой кнопкой мыши на названии элемента Реклама (Ads).

Данный диалог содержит две вкладки. На вкладке Строки HTML (Content Blocking) (Рис. 5.78) указывается список HTML-строк, которые не должны показываться браузером. При установленном флажке Блокировать HTML-строки (Block Ad content containing specific keywords) элементы Web-страниц, определяемые HTML-строками из расположенного ниже списка, отображаться не будут. Так как по умолчанию флажок установлен, и список HTML-строк содержит большое количество элементов, то сразу после начала использования система Agnitum Outpost Firewall Pro оградит вас от ненужной рекламы без дополнительных настроек.

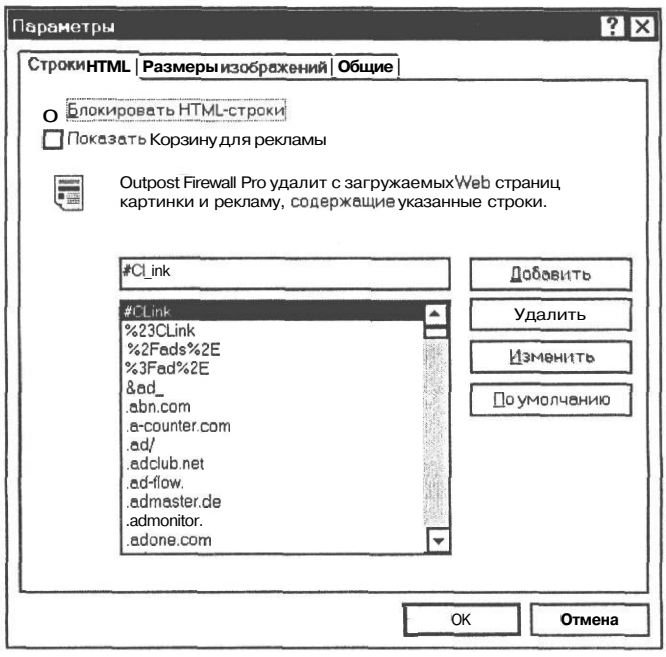



*Рис. 5.78. Вкладка **Строки HTML** (Content Blocking) диалога **Параметры** (Options)*

Для внесения новых HTML-строк в список, задающий ограничение отображения информации Web-страниц, в системе Agnitum Outpost Firewall Pro существует два основных способа. Первый из них предусматривает непосредственный ввод HTML-строки в поле ввода над списком и нажатие кнопки Добавить (Add).

Второй способ связан с использованием объекта, называемого корзиной для рекламы (**Trashcan**). Корзина для рекламы представляет собой окно (Рис. 5.79), которое постоянно находится на **Рабочем столе** (Desktop) Windows. Чтобы отобразить это окно, следует на вкладке **Строки** HTML (Content Blocking) диалога **Параметры** (Options) (Рис. 5.78) установить флажок **Показать Корзину для рекламы** (Show Ad Trashcan on your desktop).

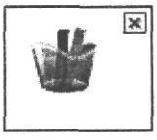


*Рис. 5.79. Корзина для рекламы*

Для того чтобы добавить HTML-строку в список, задающий ограничение отображения Web-страниц, следует выделить на текущей Web-странице тот из ее элементов, вывод которого вы хотите запретить, и перетащить его мышью в окно корзины для рекламы.

Весьма полезной является функция удаления изображений определенного размера. Как известно, рекламные баннеры имеют строго фиксированные размеры, и это дает возможность вырезать их из общего трафика. Размеры удаляемых изображений задаются на вкладке **Размеры изображений** (Image Blocking) (Рис. 5.80).

При установленном по умолчанию флажке **Блокировать изображения по размеру** (Block images of specific size) все изображения, размер которых соответствует перечисленному в поле списка, не будут выводиться на Web-странице.

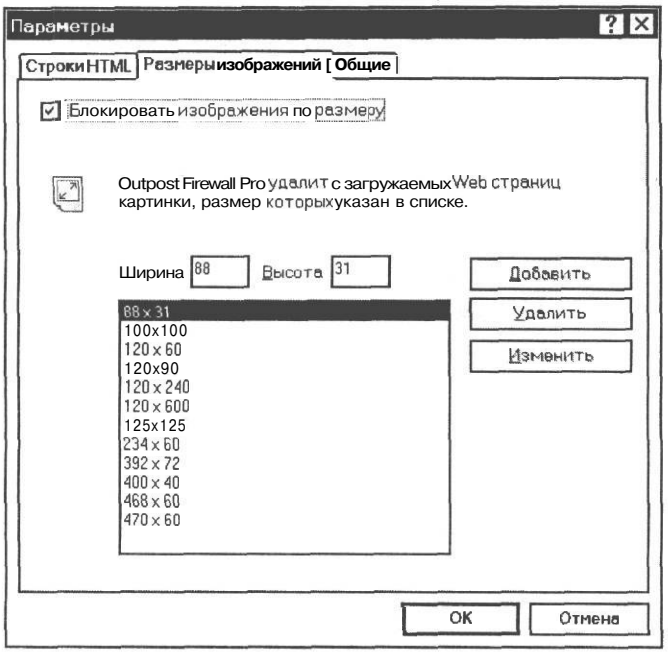



*Рис. 5.80. Вкладка **Размеры изображений** (Image Blocking) диалога **Параметры** (Options)*

Вы можете дополнить список новыми размерами, указав нужные значения в полях ввода Ширина (Width) и **Высота** (Height) и нажав кнопку **Добавить** (Add). Для удаления элемента из списка следует выделить его и нажать кнопку **Удалить** (Remove). Можно также изменить размеры любого элемента, выделив его в списке, откорректировав размеры в полях ввода и нажав кнопку **Изменить** (Modify).

В настоящее время в российских сетях используются следующие основные размеры баннеров: 468x60, 120x80, 100x100, 88x31 пикселов. Встречаются также и баннеры других размеров: 125x125, 234x60, которые весьма распространены в Интернете. Кроме того, постепенно становятся популярными такие форматы, как 470x60, 470x70, 400x40, 120x240, 60x60. Сразу после установки брандмауэр Agnitum Outpost Firewall Pro настроен таким образом, чтобы не отображались графические изображения размером 88x31, 100x100, 120x60, 120x90, 120x240, 120x600, 125x125, 234x60, 392x72, 400x40, 468x60 и 470x60 пикселов.

## Фильтрация почтовых вложений

Как известно, в большинстве случаев вирусы попадают в компьютер вместе с файлами, вложенными в сообщения электронной почты. Для организации проверки поступающих по электронной почте присоединенных файлов предназначен модуль **Защита файлов** (Attachments Filter). Режимы проверки задаются по типам поступающих файлов на вкладке **Фильтрация почтовых вложений** (E-mail Attachments Filter) диалога **Параметры** (Options) (Рис. 5.81). Этот диалог открывается после выбора в контекстном меню подключаемого модуля **Фильтрация почтовых вложений** (Attachments Filter) команды **Параметры** (Properties).

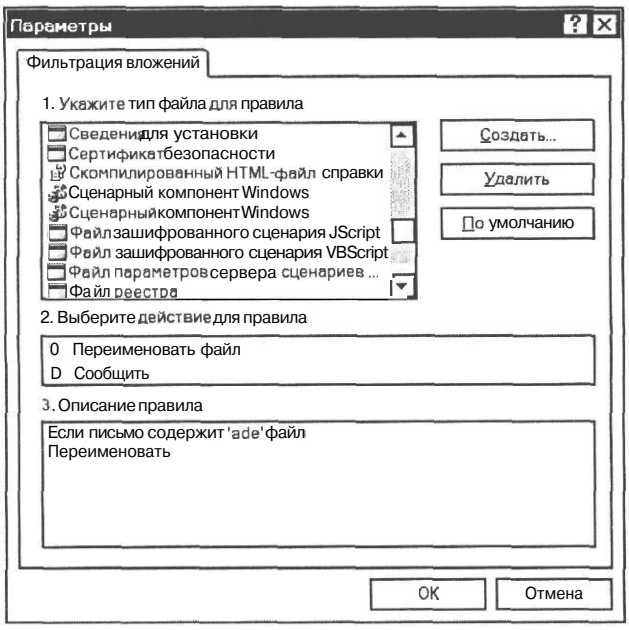



*Рис. 5.81. Вкладка **Фильтрация почтовых вложений** (E-mail Attachments Filter) диалога **Параметры** (Options)*

В верхней части диалога, в поле списка **Укажите тип файла для правила** (Specify the File type for your rule) приведен обширный перечень типов файлов. Если щелчком мыши выделить один из типов, то установленные флажки в поле **Выберите действие для правила** (Select the Action for your rule) покажут, какие действия должны выполняться с файлами данного типа, а в поле **Описание правила** (Rule Description) вы увидите словесное описание действий. Эти действия сводятся либо к переименованию файла, либо к предупреждению пользователя перед загрузкой. Чтобы изменить правила, следует, выделив нужный тип файла, установить или сбросить соответствующий флажок.

Можно также добавлять новые типы файлов и правила для них. Для этого следует нажать кнопку **Создать** (New) и в поле ввода **Тип файла** (Specify file type) появившегося диалога **Тип файла** (File Type) (Рис. 5.82) ввести расширение имени файла, например, doc. В поле ввода **Описание** (Description) автоматически отобразится название приложения - **Документ Microsoft Word** (Document Microsoft Word). После закрытия диалога **Тип файла** (File Type) нажатием кнопки **OK** созданный тип появится в поле списка **Укажите тип файла для правила** (Specify the File type for your rule). Теперь, выделив его и установив нужные флажки, вы укажете правила для действий с файлами данного типа, поступившими по электронной почте.

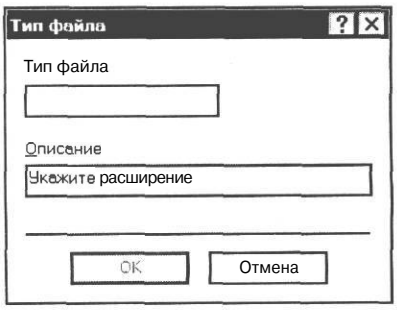



*Рис. 5.82. Диалог **Тип файла** (File Type)*

Следует отметить, однако, что блокировка файлов, осуществляемая данным модулем, является весьма слабой защитой.

## Детектор атак

Данный модуль предназначен для уведомления пользователя об атаке на его компьютер из сети и принятия мер по недопущению причинения ущерба вашему компьютеру. Модуль **Детектор атак** (Attack Detection) позволяет задать условия, при которых выдается предупреждение, и имеет настройки для указания реакции в случае, если заданный уровень безопасности превышен. Определение условий и характера реагирования выполняется на вкладке Защита (Protection) диалога **Параметры** (Options) (Рис. 5.83). Чтобы открыть эту вкладку, следует в контекстном меню модуля **Детектор атак** (Attack Detection) выбрать команду **Параметры** (Properties).

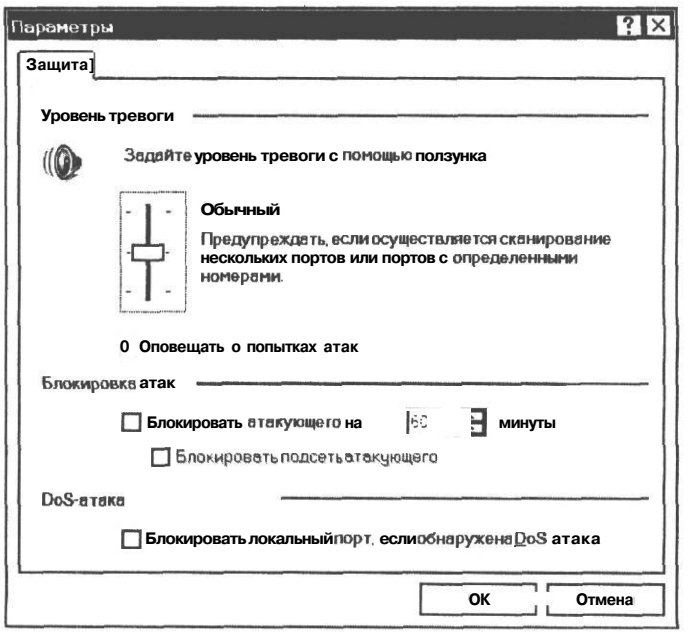



*Рис. 5.83. Вкладка **Защита** (Protect) диалога **Параметры** (Options)*

В верхней части этой вкладки, в области **Уровень тревоги** (Alert level) с помощью ползункового регулятора вы можете задать уровень безопасности. Чем выше уровень, тем меньше условий требуется для выдачи предупреждения. Ползунковый регулятор может находиться в трех положениях:

- верхнее - **Максимальный** (Maximum) уровень тревоги - предупреждение выдается в случае, если обнаружено даже единичное сканирование порта;
- среднее - **Обычный** (Normal) уровень тревоги - предупреждение выдается в случае, если осуществляется сканирование нескольких портов или портов с определенными в системе номерами, т.е. в тех ситуациях, которые брандмауэр распознает как атаку на компьютер;
- нижнее - **Безразличный** (Minimum) уровень тревоги - предупреждение выдается в случае однозначной множественной атаки.

При установленном флажке **Оповещать о попытках атак** (Report detected attacks) вы получите сообщение в случае атаки.

В нижней части диалога, в области **Блокировка атак** (Block intruders) вы можете задать действия, которые система выполнит при обнаружении атаки на ваш компьютер:

- блокировку всех сетевых обменов того компьютера, с которого осуществляется атака на ваш компьютер, - при установке флажка **Блокировать атакующего на ... минуты** (Block intruder's IP for ... minutes). В этом случае в поле ввода со счетчиком справа от этого флажка вы можете задать время, на которое будут заблокированы сетевые обмены атакующего (по умолчанию - на 60 минут);
- блокировку всех сетевых обменов всей подсети, к которой принадлежит атакующий компьютер, - при установке флажка **Блокировать подсеть атакующего** (Also block intruder subnet). Если атакующий находится с вами в одной подсети, например, подключается к Интернету через вашего же провайдера, то установкой флажка вы можете заблокировать и себя;
- блокировку локального порта, если обнаружена DoS-атака, т.е. атака типа «Denial of Service - Отказ в обслуживании», при установке флажка **Блокировать локальный порт, если обнаружена DOS-атака** (Block local port if DoS attack is detected).

Для отображения процесса сканирования портов вашего компьютера и удаленных атак предназначен элемент **Детектор атак** (Attack Detection) иерархического списка **Подключаемые модули** (Plug-Ins). Если щелчком мыши выделить в левой части панели представления элемент **Детектор атак** (Attack Detection), то в правой части отобразится статистика атак (Рис. 5.84).

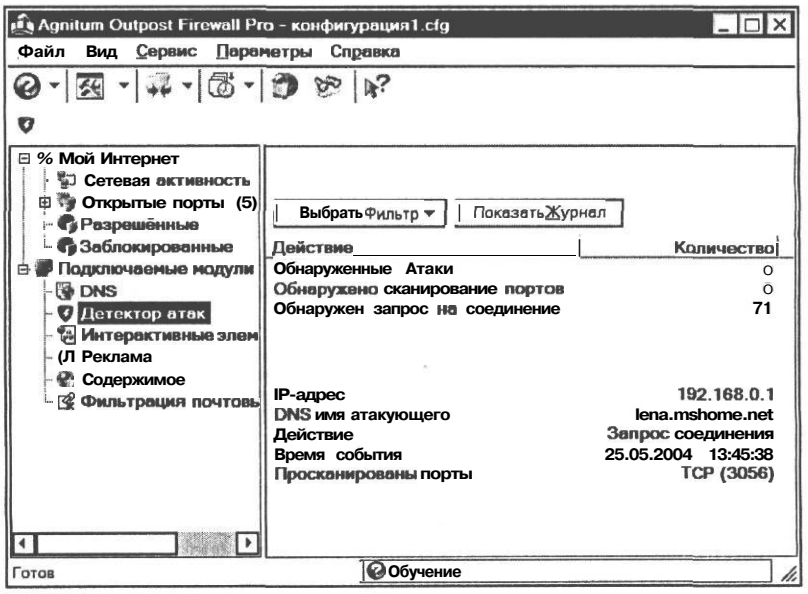



*Рис. 5.84. Статистика атак*

Если теперь нажать кнопку **Показать журнал** (Show Detailed Log), вы увидите таблицу с информацией об имевших место атаках из сети (Рис. 5.85). В таблице указываются: **Дата/время** (Date/Time), **Действие** (Attack Type), **IP-адрес** (IP Address), **Просканированы порты** (Scan Port Details).

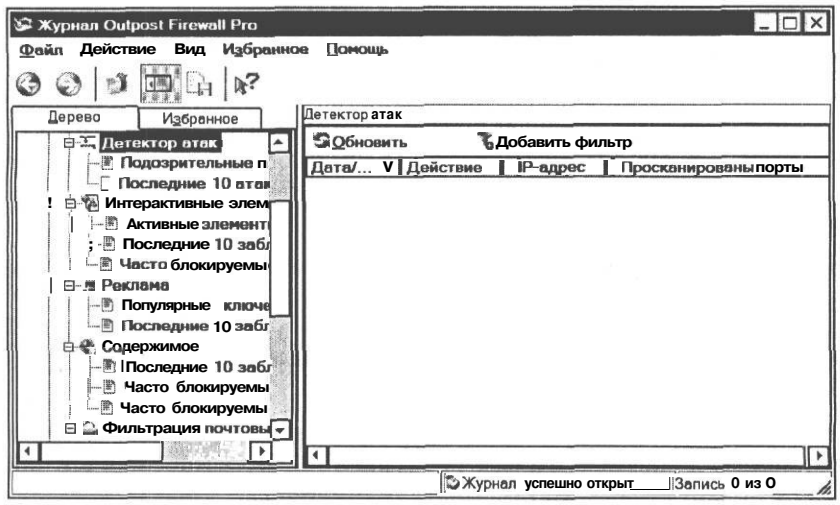



*Рис. 5.85. Информация об атаках*

Повторим, что для блокирования атаки используются описанные выше элементы управления вкладки **Защита** (Protect) диалога **Параметры** (Options).

## Стратегия защиты компьютера

Теперь, когда мы познакомились с основными функциями системы Agnitum Outpost Firewall Pro, рассмотрим общие принципы организации защиты вашей локальной сети с помощью этого брандмауэра от наиболее распространенных опасностей, возникающих при работе в Интернете.

Наиболее оптимальной стратегией защиты сети является следующая. На компьютере, обеспечивающем общий доступ к Интернету, устанавливается Agnitum Outpost Firewall Pro и используется политика обучения, которая включается по умолчанию. Поработав в режиме обучения 1-2 дня, программа зарегистрирует большинство приложений, которым регулярно нужен сетевой доступ. Как только регистрация закончится, следует назначить брандмауэру политику блокирования, т.е. запрещения всего, что не разрешено. Для этого достаточно щелкнуть правой кнопкой мыши на значке (?) в правой части **Панели задач** (Taskbar) и в появившемся контекстном меню выбрать команду **Политики ◆ Режим блокировки** (Policy ◆ Block most mode) (Рис. 5.60).

Если в дальнейшем возникнет необходимость настроить правила для новых программ, то нужно будет снова включить режим обучения, щелкнув правой кнопкой мыши на значке (?) в правой части **Панели задач** (Taskbar) и выбрав в контекстном меню команду **Политики * Режим обучения** (Policy ◆ Rules Wizard) (Рис. 5.60). После того как брандмауэр «научится», нужно будет повторно запретить все, что не разрешено, включив **Режим блокировки** (Block most mode).

Главное правило при работе с Agnitum Outpost Firewall Pro - это следовать настройкам программы при отсутствии у вас особых причин изменять эти настройки.

Теперь напомним о некоторых возможностях системы и кратко познакомимся с теми функциями, о которых еще не говорили.

Как было сказано в начале главы, основными опасностями при работе с сетью являются:

- проникновение на ваш компьютер посторонних программ;
- попытка получения доступа к информации на вашем компьютере или информации о работе вашего компьютера;
- поступление на ваш компьютер ненужной информации (рекламы, баннеров).

## Защита от проникновения посторонних программ

Для защиты от проникновения на ваш компьютер посторонних программ брандмауэр позволяет запретить создание сетевых взаимодействий для всех программ, кроме тех, которым вы явно даете разрешение. В этом случае брандмауэр должен работать в **Режиме блокировки** (Block most mode) или в **Режиме обучения** (Rules Wizard) с соответствующим образом настроенными правилами сетевого взаимодействия. Кроме того, вы можете контролировать сетевые соединения с помощью информации, отображаемой в главном окне. Режимы работы системы Agnitum Outpost Firewall Pro описаны в разделе «Настройка политики работы с сетью».

Обязательно следует запретить использование на просматриваемых Web-страницах таких ресурсов, как ActiveX, Java-апплеты, программы на языках VB и JavaScript. При этом не все Web-страницы будут отображаться правильно, но безопасность важнее. Если для некоторых Web-страниц использование таких средств необходимо, то следует воспользоваться возможностью Agnitum Outpost Firewall Pro, позволяющей запретить использование этих программных средств по умолчанию, но разрешить их использование на известных и проверенных вами Web-страницах, список которых вы составляете сами. Эти настройки выполняются на вкладке **Web Страницы** (Web Pages) диалога **Параметры Интерактивных элементов** (Active Content Properties) (Рис. 5.86), которую можно открыть, выбрав в меню кнопки на панели инструментов команду **Интерактивные элементы** (Active Content).

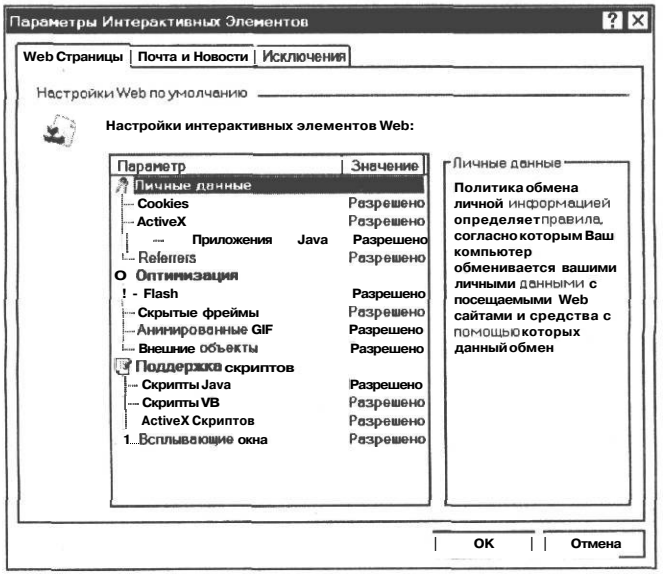



*Рис. 5.86. Вкладка **Web Страницы** (Web Pages) диалога **Параметры Интерактивных Элементов** (Active Content Properties)*

## Блокировка доступа к информации на компьютере

Для предотвращения попыток получения доступа к информации на вашем компьютере или информации о работе вашего компьютера можно запретить создание на вашем компьютере файлов Cookies. Такая настройка выполняется на вкладке **Web Страницы** (Web Pages) диалога **Параметры Интерактивных Элементов** (Active Content Properties) (Рис. 5.86). В частности, вы можете, как и в случае с ActiveX, Java-апплетами, программами на VB и JavaScript, ограничивать или разрешать создание файлов **Cookies** для всех Web-страниц или только для Web-страниц из заданного вами списка.

## Защита от «троянских коней»

Для защиты от «троянских коней» вы можете оставить систему работать в Режиме обучения (Rules Wizard), и тогда при попытке обращения «троянца» к сети система проинформирует вас об этом и поможет заблокировать выход в сеть этого приложения. Можно также запретить создание сетевых взаимодействий для всех программ, кроме тех, разрешение для которых вы даете явно, и работать в Режиме блокировки (Block most mode).

При обнаружении подозрительного соединения вы можете, благодаря информации, выдаваемой брандмауэром, определить DNS-адрес или IP-адрес узла, с которым находящаяся на вашем компьютере подозрительная программа пытается установить соединение, после чего принять соответствующие меры.

## Ограничение поступления ненужной информации

Для предотвращения поступления на компьютер ненужной информации вы можете запретить отображение на экране рекламы и баннеров. Поскольку имена большинства баннерных служб известны, можно выключить отображение тех Web-страниц, в которых есть HTML-строки, указывающие на имена баннерных служб.

Сразу после установки система содержит большой список рекламных HTML-строк. Чтобы добавить в этот список какую-либо HTML-строку из Web-страницы, отображающейся в данный момент времени на экране, вы можете воспользоваться корзиной для рекламы. Вы также можете отменить запрет на отображение тех или иных частей Web-страницы либо вовсе отказаться от использования корзины для рекламы. Порядок работы с HTML-строками и корзиной для рекламы описан в разделе «Блокировка рекламы».

Учитывая тот факт, что подавляющее большинство баннеров - это графическое изображение одного из стандартных размеров, вы можете запретить вывод на экран изображений определенного размера.

Система Agnitum Outpost Firewall Pro позволяет также запретить отображение на экране тех или иных Web-сайтов и Web-страниц. Этот запрет реализуется с учетом списков запрещенных словосочетаний и имен доменов, которые по умолчанию содержатся в брандмауэре. Данные списки формируются при настройке системы на вкладках Блокировка по содержимому (Blocked Words) (Рис. 5.87) и Блокировка по адресу (Blocked Sites) (Рис. 5.88) диалога Параметры (Options). Для доступа к этим вкладкам следует в меню кнопки  на панели инструментов выбрать команду Содержимое (Content).

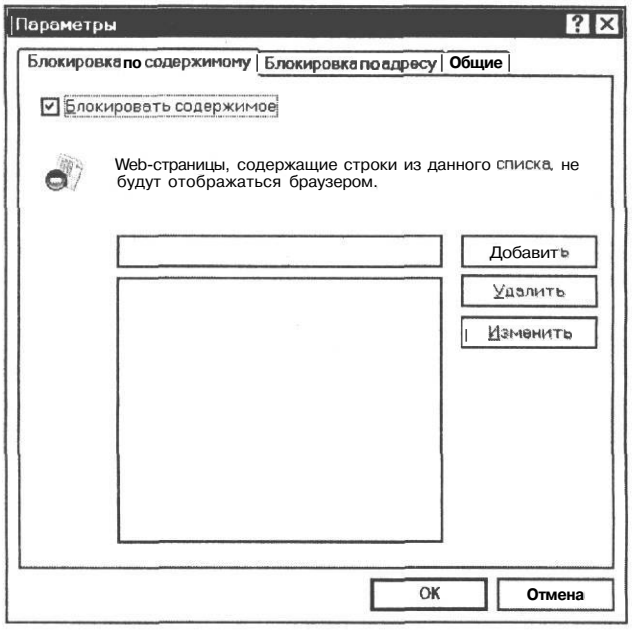



*Рис. 5.87. Вкладка **Блокировка по содержимому (Blocked** Words) диалога **Параметры** (Options)*

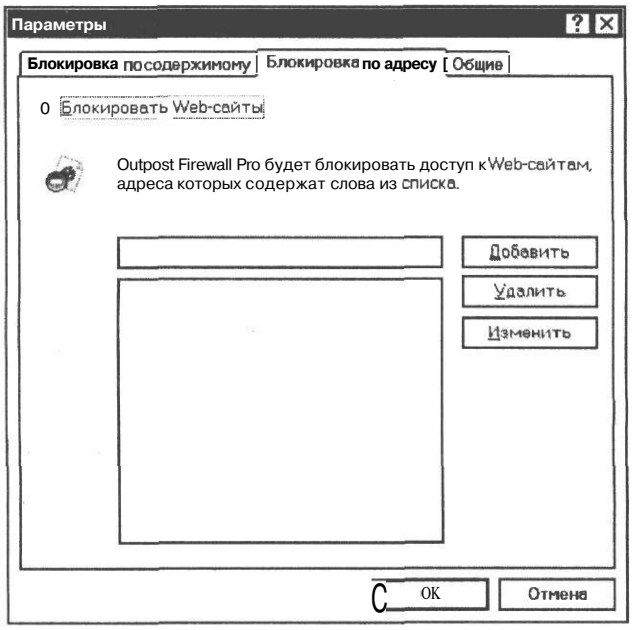



*Рис. 5.88. Вкладка **Блокировка по** адресу (Blocked Sites) диалога **Параметры** (Options)*

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 присутствует слово «порнография». Сразу после установки системы оба эти списка пусты, и вам следует сформировать их самостоятельно. Для этого в поля ввода обеих вкладок следует вводить словосочетания и адреса Web-сайтов и нажимать кнопку **Добавить** (Add).

Если затем защитить настройки брандмауэра паролем, то вы воспрепятствуете изменению этих данных. Таким способом вы можете, например, заблокировать на домашнем компьютере доступ к определенной информации для детей. Защита паролем осуществляется на вкладке **Общие** (General) диалога **Параметры** (Options) (Рис. 5.89). Чтобы открыть эту вкладку, следует выбрать команду меню **Параметры** * **Общие** (Options ◆ General).

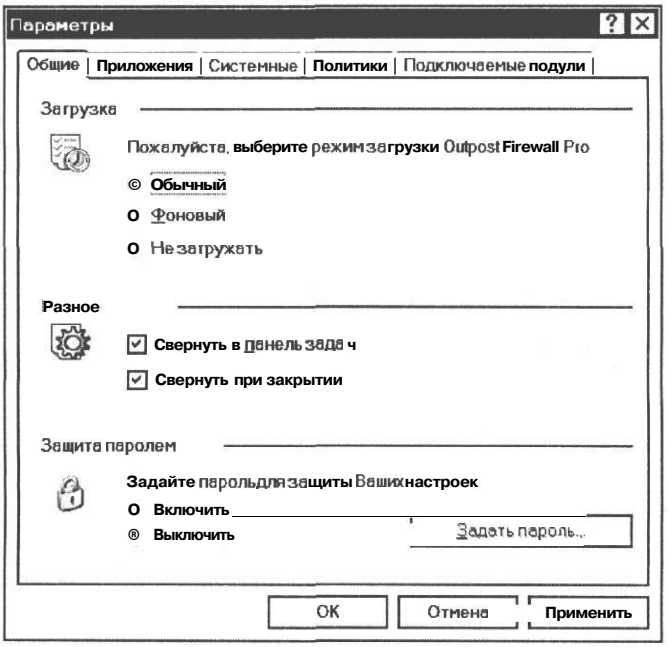



*Рис. 5.89. Вкладка **Общие** (General) диалога **Параметры** (Options)*

## Настройка системных протоколов

Важной особенностью брандмауэра является возможность настройки системных протоколов, поскольку многие попытки нарушения работоспособности локальных компьютеров связаны с использованием злоумышленниками данных протоколов. Эти настройки выполняются на вкладке **Системные** (System) диалога **Параметры** (Options) (Рис. 5.71), которая открывается командой меню **Параметры * Системные** (Options ◆ System).

Для предотвращения попыток нарушения работоспособности вашего компьютера с использованием злоумышленниками служебного протокола **ICMP** система Agnitum Outpost Firewall Pro позволяет разрешить или запретить использование ICMP-сообщений того или иного типа.

Протокол ICMP (Протокол управляющих сообщений сети) позволяет Интернет-узлам предоставлять информацию об ошибках или сообщать о нетипичных условиях в сети. ICMP-сообщения передаются через Интернет в поле данных IP-датаграмм. Конечной целью ICMP-сообщений является не приложение или целевой компьютер, а программное обеспечение IP в системе пользователя. Любой компьютер может послать ICMP-сообщение на другой компьютер.

Рекомендуется использовать настройки протокола **ICMP,** заданные в брандмауэре по умолчанию. В случае если вы меняете настройки, необходимо четко представлять себе, почему вы это делаете, а также быть уверенными в том, что это не приведет к ухудшению работоспособности системы в целом. Брандмауэр позволяет восстановить те настройки протокола ICMP, которые были заданы по умолчанию.

Сканирование портов вашего компьютера со стороны злоумышленника заключается в посылке запроса на установку соединения. Когда установлен переключатель **Обычный режим** (Normal), компьютер посылает либо подтверждение соединения (данный порт на вашем компьютере открыт), либо уведомление, что порт закрыт. Если установлен переключатель **Режим Невидимости** (Stealth), ваш компьютер не будет высылать уведомления о том, что порт закрыт, что поставит компьютер-злоумышленник в сложное положение - ему неизвестно, открыт или закрыт порт (может быть, пакет утерян, либо узел отсутствует). Таким образом, в **Режиме Невидимости** (Stealth) другие компьютеры сети не могут обнаружить ваш компьютер.

В заключение напомним еще раз, что использование только одного защитного экрана на компьютере, предоставляющем общий доступ к Интернету, не гарантирует стопроцентной безопасности вашей сети. Для обеспечения полной безопасности необходимо «залатать» все «дыры» в системе безопасности Windows и постоянно поддерживать ее в обновленном состоянии, правильно настроить операционную систему, установив режимы максимальной безопасности, и использовать антивирусную защиту с самыми свежими вирусными базами.

# ГЛАВА 6.
# Электронная почта внутри и снаружи локальной сети

Имея несколько компьютеров, объединенных в локальную сеть, можно организовать внутреннюю офисную почтовую службу, объединив ее с Интернет-почтой так, чтобы каждый пользователь сети на своем компьютере, имея свой индивидуальный адрес E-mail, мог получать и отправлять не только внутреннюю сетевую, но также и внешнюю Интернет-почту. Эту задачу успешно решает программа Eserv (http://www.eserv.ru), разработанная компанией Etype (Калининград).

Программа Eserv позволяет организовать внутри локальной сети обмен почтой и новостями, используя для этого стандартные почтовые программы MS Internet Mail, MS Internet News, MS Outlook Express, Netscape Messenger, The Bat и другие. Для работы с почтой, новостями и Интернетом можно использовать любую операционную систему - Windows 3.1/95/98/NT/2000/XP, Unix, Mac OS, OS/2, а также программное обеспечение, работающее на IP-стеках в DOS.

Почта в Интернете, как правило, передается по протоколу SMTP (Simple Mail Transfer Protocol - Протокол простой передачи почты). В каждом сеансе передачи одна программа выступает отправителем почты, другая - приемником. В роли отправителя обычно выступает одна из пользовательских программ, перечисленных выше, либо промежуточный почтовый сервер. В роли приемника всегда выступает почтовый сервер. Программа-отправитель работает в режиме «клиент» (как противоположность режиму «сервер»). Клиент инициирует сессию, соединяясь с почтовым сервером, сервер принимает соединение и выполняет команды, выдаваемые клиентом. В начале сессии клиент посылает команду «приветствие», в которой сообщает свое доменное имя. Затем для каждого передаваемого письма сообщает адрес отправителя, адрес получателя и, наконец, само письмо. В конце сессии клиент передает команду «выход» и завершает сеанс связи. Администратором SMTP-сервера задаются правила, по которым происходит прием и дальнейшая обработка принятой почты.

Полученная для пользователей SMTP-сервера почта попадает в пользовательские ящики и хранится в них до тех пор, пока почтовые программы-клиенты не заберут ее. Для получения пользователями своей почты из личных почтовых ящиков предназначен сервер POP3 (Post Office Protocol v3 - Почтовый протокол, версия 3), встроенный в Eserv.

Чтобы получить почту из заданных ящиков, называемых учетными записями (Mail accounts), почтовая программа пользователя соединяется с сервером POP3, сообщает серверу имя ящика и пароль для доступа к нему, которые вы указываете в настройке, получает список имеющихся сообщений, затем получает все сообщения и дает команды удаления прочитанных писем с сервера. Реальное удаление сообщений в ящике производится сервером не сразу при получении команды «удалить», а в момент завершения POP3-сеанса. Таково требование протокола POP3. Пока сервер выдает содержимое конкретного ящика, этот ящик заблокирован. Таким образом, одновременно две программы не могут читать почту из одного и того же ящика. Обычно это и не требуется.

Программа Eserv дает возможность отправки Интернет-почты и новостей из внутреннего сервера локальной сети на внешний и в обратном направлении и позволяет работать в Интернете всем пользователям локальной сети через одно модемное или иное соединение с провайдером без необходимости каждому компьютеру локальной сети иметь внешний IP-адрес. Эти функции выполняет встроенный почтовый сервер.

Большинство почтовых серверов для локальных сетей при своей настройке требуют указать имя локального домена. При этом возможны три случая:

- у фирмы нет своего доменного имени. В этом случае приходится указывать вымышленный домен, например **domen.ru;**
- у фирмы есть доменное имя, например **firma.ru,** и все пользователи почты находятся в одной локальной сети;
- у фирмы есть доменное имя, например **firma.ru,** но пользователи почты работают в разных локальных сетях в разных офисах.

Во всех этих случаях невозможно будет отправить почту на адрес вида **info@domen.ru** или **info@firma.ru** за пределы локальной сети, если только в почтовом сервере не предусмотрена возможность маршрутизации. Другими словами, если получатели почты с доменом **firma.ru** сидят в разных локальных сетях в разных офисах, то многие почтовые серверы для локальных сетей не позволят им обмениваться письмами. Программа Eserv легко решает эту и многие другие проблемы.

Eserv может работать так же, как Интранет- и Интернет-сервер, по протоколам HTTP (Web-сервер) и FTP (файловый сервер), а также в качестве почтового сервера не только для локальной сети, но и в Интернете. При этом каждый пользователь может использовать популярное программное обеспечение - любой браузер (MS Internet Explorer, Netscape Navigator, Ariadna, Arena, Opera, Lynx и т.п.), FTP-клиенты (CuteFTP, FAR, ReGet, GetRight и др.), программы ICQ типа VypressMessenger, AOL Instant Messenger и практически любое другое программное обеспечение.

Далее мы рассмотрим, как с помощью программы Eserv обеспечить доставку внутренней и внешней почты в локальной сети. Предполагается, что компьютеры локальной сети имеют общий доступ к Интернету через модемное соединение и на компьютере, к которому подключен модем, установлена операционная система Windows XP. При этом локальная сеть имеет IP-адрес 192.168.0.0, а компьютер с модемным соединением - IP-адрес 192.168.0.1. Остальные компьютеры сети получают IP-адрес динамически: 192.168.0.*. Для этого на клиентских компьютерах должен быть установлен режим автоматического назначения IP-адреса.

Каждый клиентский компьютер должен получить адрес. Поэтому важно, чтобы узловой компьютер все время оставался включенным или запускался раньше всех остальных компьютеров сети. В противном случае клиентские компьютеры не смогут получить IP-адрес.

В этой главе мы на конкретном примере покажем, как в локальной сети из трех компьютеров установить почтовый сервер Eserv и настроить почтовый оборот. При настройке программы Eserv мы назначим локальной сети вымышленный домен **local.ru,** а пользователям присвоим вымышленные имена - **user1, user2 и user3.** Таким образом, их внутренние почтовые адреса будут такими: **userl @local.ru, user2@local.ru и user3@local.ru.**

У пользователя **user1** будет также внешний почтовый ящик - **user1@mail.ru**, а у пользователя **user3 - user3@yandex.ru.** И почта с этих внешних адресов будет автоматически доставляться во внутренние почтовые ящики **user1@local.ru и user3@local.ru.** Но когда пользователь **user2** будет отправлять сообщение пользователю **userl** на адрес **user1@mail.ru**, почта будет попадать адресату в почтовый ящик **user1@local.ru**, не выходя за пределы локальной сети. Пользователь **user2** в нашей конфигурации не сможет посылать, почту «наружу», за пределы локальной сети, и получать «снаружи», а только внутри локальной сети, так как у него отсутствует внешний почтовый ящик. У пользователей **userl и user3** не будет никаких ограничений по работе с почтой. Они смогут и посылать и получать сообщения, благодаря наличию внешних почтовых ящиков. Так как мы будем использовать вымышленные имена, то в каждом случае будем обсуждать возможности выбора реальных имен.

## Конфигурирование Eserv с помощью Мастера

Программа Eserv должна быть установлена на компьютере сети, к которому подключен модем. После установки автоматически запускается **Мастер конфигурирования Eserv** (Рис. 6.1). Этот Мастер можно вызвать также, запустив файл **EservWzd.exe** из папки **Program Files\Eserv2.**

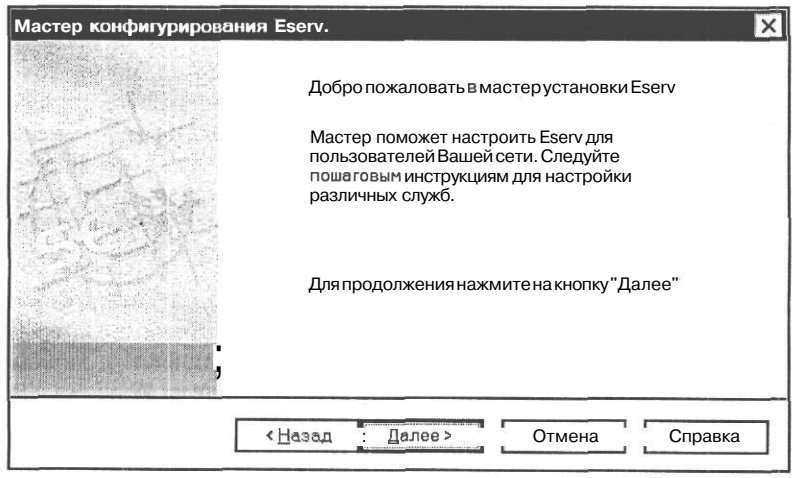



*Рис. 6.1. Первый диалог **Мастер конфигурирования Eserv***

## Выбор устанавливаемых служб

После нажатия кнопки Далее (Next) в первом диалоге Мастера откроется второй диалог **Мастер конфигурирования Eserv. Список служб** (Рис. 6.2).

В этом диалоге предлагается выбрать сервисы, которые необходимо установить. Мы установим только **Почтовый сервер,** а о других возможностях поговорим позднее.

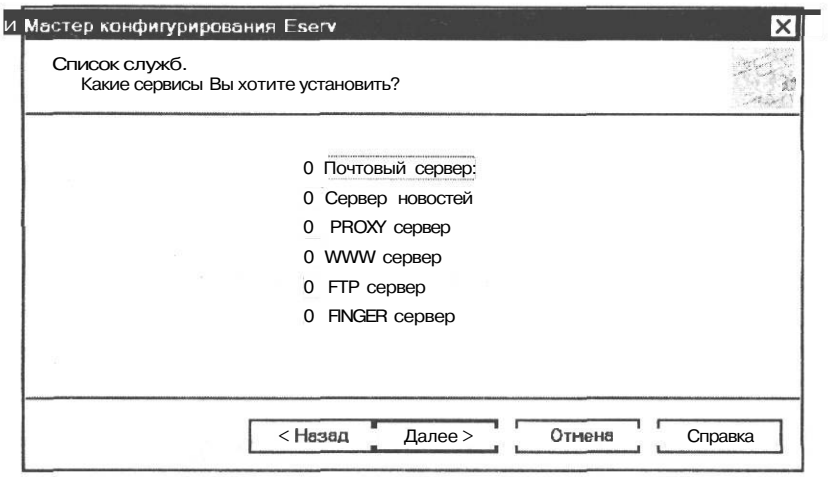



*Рис. 6.2. Второй диалог **Мастер конфигурирования Eserv. Список служб***

> Сбросьте флажки **Сервер новостей, PROXY сервер, WWW сервер, FTP сервер, FINGER сервер.**

Оставьте установленным только флажок **Почтовый сервер.**

## Настройка соединения с Интернетом

Когда вы нажмете кнопку **Далее** (Next), появится следующий диалог **Мастер конфигурирования Eserv. Настройка соединения с Интернет** (Рис. 6.3).

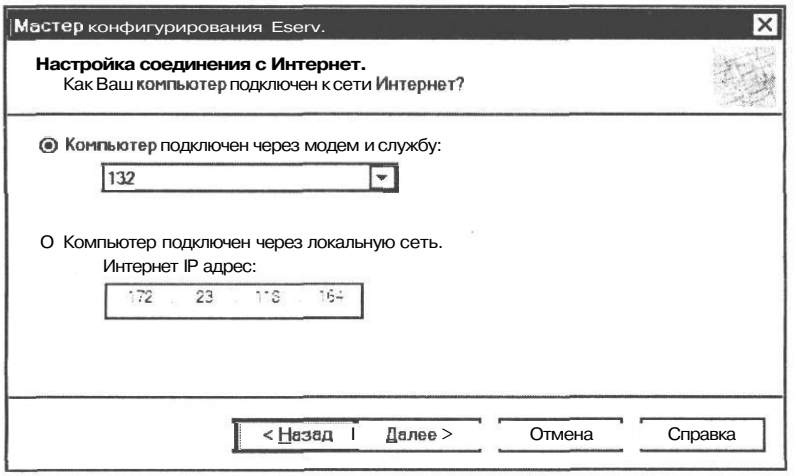



*Рис. 6.3. Третий диалог **Мастер конфигурирования Eserv. Настройка соединения с Интернет***

Здесь следует, установив переключатель, указать программе, каким образом компьютер подключен к Интернету - через модем или через локальную сеть.

➤ Так как мы рассматриваем вариант подключения через модем, установите переключатель Компьютер подключен через модем и службу.

➤ В открывающемся списке под этим переключателем выберите подключение к провайдеру, если их несколько.

## Настройка телефонного доступа к Интернету

В следующем, четвертом диалоге **Мастер конфигурирования Eserv. Настройка телефонного доступа к Интернет** (Рис. 6.4) вы должны указать **Телефонные номера провайдера,** а также **Имя** и **Пароль** для доступа.

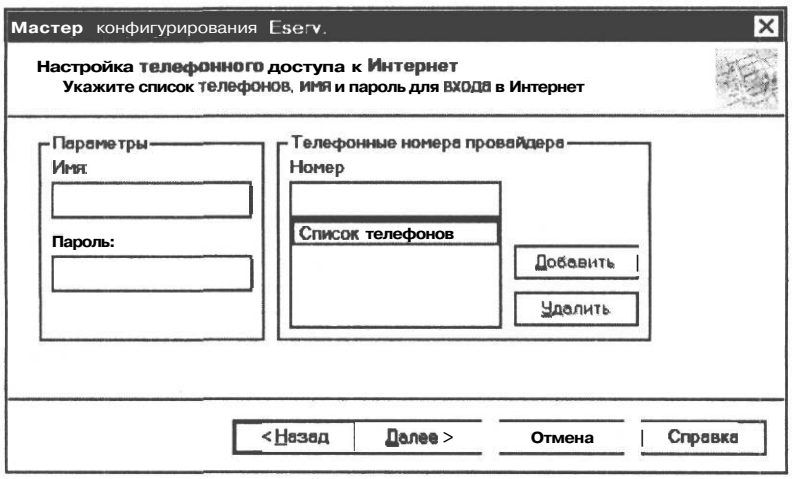



***Рис. 6.4. Четвертый диалог Мастер конфигурирования Eserv. Настройка телефонного доступа к Интернет***

> В поле ввода Номер введите номер телефона, используемый для соединения с сервером провайдера.

По умолчанию операционная система использует тоновый набор номера. Чтобы в Windows XP использовать импульсный набор, как это принято в российских телефонных сетях, следует перед номером обязательно поставить английский символ p, например, **p957-13-00**.

➤ Нажмите кнопку Добавить. Этот номер появится в перечне Список телефонов.

Подобным же образом добавьте другие номера, если провайдер предоставляет несколько номеров для соединения. Если какой-то номер указан неправильно, то его можно удалить из списка, выделив и нажав кнопку Удалить.

➤ В поле ввода Имя введите имя (Login), используемое для доступа.

> В поле ввода Пароль укажите пароль доступа к серверу провайдера.

## Настройка доступа к Eserv

После нажатия кнопки **Далее** (Next) откроется следующий диалог **Мастер конфигурирования Eserv. Настройка доступа к Eserv** (Рис. 6.5).

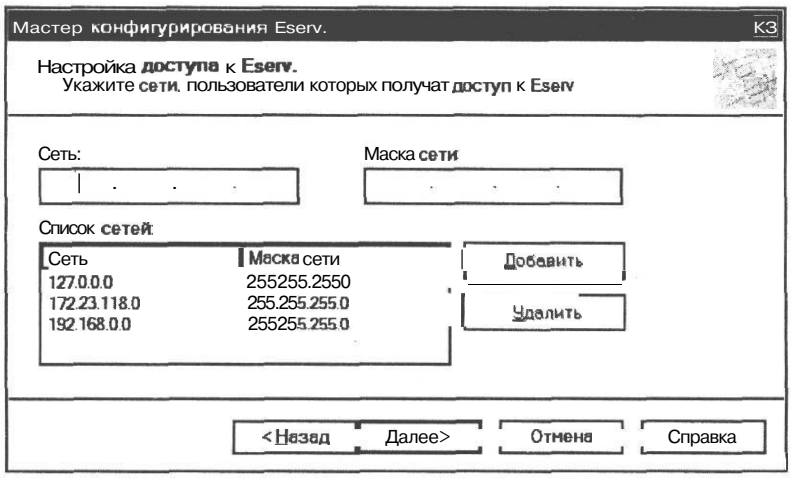
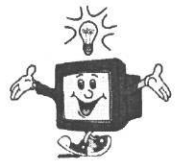



*Рис. 6.5. Пятый диалог **Мастер конфигурирования Eserv. Настройка доступа к Eserv***

В этом диалоге необходимо указать адреса сетей, которые должны получить доступ к Eserv.

*Адрес сети здесь - это IP-адрес, заканчивающийся на 0, например 192.168.0.0. Это означает диапазон адресов от 192.168.0.1 до 192.168.0.255. Все компьютеры с адресами из этого диапазона смогут работать с Eserv.*

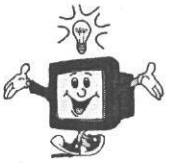


Самый популярный из используемых в настоящее время сетевых протоколов TCP/IP требует наличия у каждого компьютера сети уникального номера - IP-адреса. Если на компьютере установлено два сетевых адаптера, они должны иметь разные IP-адреса. Например, при подключении к Интернету с помощью кабельного модема, подсоединяемого к сетевой плате, эта сетевая плата будет иметь IP-адрес, отличный от IP-адреса сетевого адаптера, подключенного к локальной сети.

В сочетании с IP-адресом используется номер, называемый маской подсети, который позволяет разбить сеть на более мелкие сегменты. Важно помнить конкретный набор номеров, используемый в локальной сети.

Существуют группы IP-адресов, специально зарезервированных для небольших сетей. Одна из таких групп используется средством общего доступа к подключению Интернета (Internet Connection Sharing, ICS) - это адреса **192.168.0.***, где * означает число в диапазоне от 0 до 255. Эти номера используются в сочетании с маской подсети 255.255.255.0. Данная маска подсети определяет подсеть класса С.

*Выбирайте именно этот диапазон адресов для вашей локальной сети - **192.168.0.***, если вы не пользуетесь встроенными средствами Windows XP для общего доступа к Интернету - в противном случае может возникнуть ситуация когда доступ к вашему серверу будет открыт из сети Интернет.*



Весьма вероятно, что в поле **Список сетей** уже присутствует IP-адрес локальной сети **192.168.0.0 и** маска подсети **255.255.255.0.** В противном случае их следует ввести.

- В поле ввода **Сеть** введите IP-адрес сети: **192.168.0.0**.
- В поле ввода **Маска сети** введите: **255.255.255.0.**

> Нажмите кнопку **Добавить.** Указанные значения отобразятся в поле **Список сетей.**

Чтобы удалить сеть из списка сетей, следует выделить ее и нажать кнопку **Удалить.**

## Настройка почтового сервера

**В следующем диалоге Мастер конфигурирования Eserv. Настройка почтового сервера** (Рис. 6.6) вводятся локальный почтовый домен и параметры почтовых серверов провайдера.

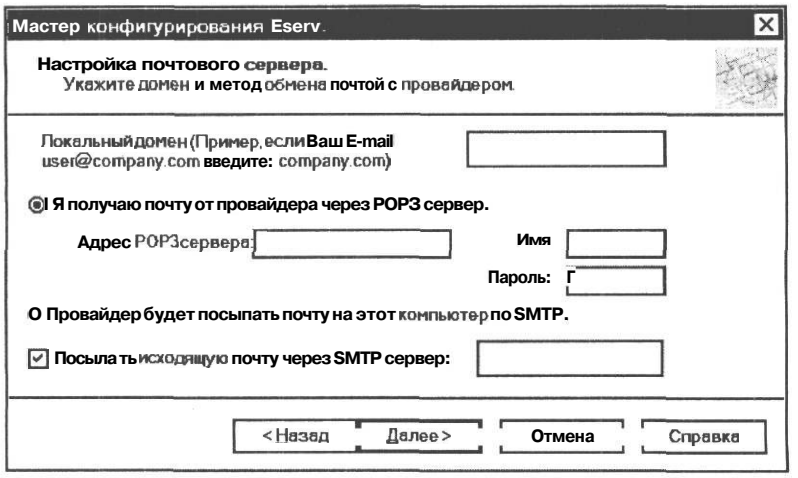



***Рис. 6.6. Шестой диалог Мастер конфигурирования Eserv. Настройка почтового сервера***

В поле вода **Локальный домен** необходимо указать имя вашего почтового домена. Локальный почтовый домен - это часть адреса электронной почты справа от символа @. Например, если адрес вашего электронного почтового ящика **service@firma.ru,** то локальный домен - **firma.ru.**

Если у вас или в вашей организации нет своего доменного имени, т.е. интернет-адреса вида **ваша_фирма@провайдер**, то не следует добавлять в список локальных доменов домен провайдера, лучше ввести «фиктивный» домен, иначе письма, адресованные из вашей сети другим клиентам провайдера, не будут отправляться наружу без специальных настроек.

Если у вас имеется зарегистрированный домен Интернета и почтовый ящик этого домена находится на сервере провайдера, вне локальной сети, то внутри сети также лучше пользоваться вымышленным доменом. Поэтому используем для нашего примера «фиктивный» домен **local.ru.**

➤ В поле ввода **Локальный домен** введите название локального домена: **local.ru.**

Программу Eserv можно настроить так, что она будет забирать почту для всех пользователей сети с одного внешнего почтового ящика у провайдера и посылать почту за пределы локальной сети также через один ящик. А можно получать и отправлять почту через разные ящики.

Мы настроим получение почты с разных внешних ящиков, принадлежащих пользователям нашей локальной сети, а отправление почты - через один почтовый ящик. К сожалению, это не всегда возможно по следующим причинам. Если вы используете в адресах домен, полученный от провайдера, то отсылка всей почты на SMTP-сервер провайдера не вызовет проблем, но, возможно, вам придется вводить имя и пароль для доступа к SMTP-серверу. Но если для каких-либо пользователей в почтовых адресах используется домен другого провайдера или службы бесплатной почты, то ваш провайдер может отказаться посылать такую почту через свой SMTP-сервер.

Укажем имена почтовых серверов провайдера.

> Установите переключатель **Я получаю почту от провайдера через POP3 сервер.**

➤ В поле вода **Адрес POP3 сервера** введите соответствующий адрес, полученный от провайдера. В нашем примере это - **pop.mail.ru** - адрес POP3-сервера бесплатной почтовой службы mail.ru, в которой зарегистрирован почтовый ящик **user1@mail.ru** пользователя **user1**.

> В поле ввода **Имя** введите имя (Login) пользователя: **user1**.

> В поле ввода **Пароль** введите пароль для доступа к почтовому серверу.

Если в сети отсутствует пользователь, которому соответствует указанный почтовый ящик на сервере провайдера, то почта будет попадать на адрес **postmaster@local.ru.** О том, как связать внешний ящик с внутренним пользователем, будет рассказано далее

➤ Установите флажок **Посылать исходящую почту через SMPT сервер** и в поле ввода справа от него введите имя SMPT-сервера провайдера. В нашем примере - **smtp.mail.ru** - адрес SMTP-сервера бесплатной почтовой службы mail.ru, в которой зарегистрирован почтовый ящик **user1@mail.ru** пользователя **user1**.

Заметьте, в этом диалоге указывается только один почтовый ящик на сервере провайдера. Внешние почтовые ящики других пользователей сети мы добавим при последующей детальной настройке.

## Список пользователей и пароли

После нажатия кнопки Далее (Next) вы перейдете к седьмому диалогу **Мастер конфигурирования Eserv. Список пользователей и пароли** (Рис. 6.7).

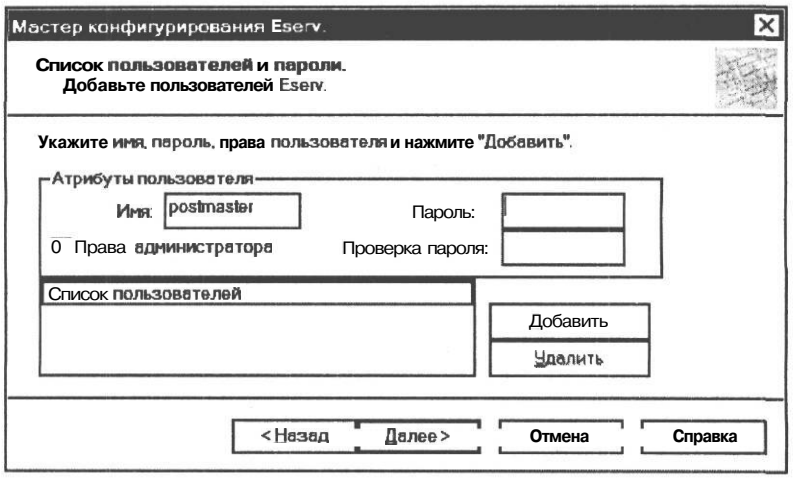



***Рис. 6.7.*** *Седьмой* ***диалог Мастер конфигурирования Eserv. Список пользователей и пароли***

Здесь следует указать имена всех пользователей вашей локальной сети, которые имеют право на подключение к почтовому серверу. Эти имена являются частью адресов электронной почты слева от символа @.

> В поле ввода **Имя** введите имя первого пользователя: **user1**.

➤ В поле вода **Пароль** укажите пароль, который будет использовать этот пользователь для доступа к Eserv.

➤ В поле ввода **Проверка пароля** подтвердите указанный пароль.

При установленном флажке **Права администратора** данному пользователю будут присвоены права администратора.

➤ Нажмите кнопку **Добавить.** Указанное имя появится в поле **Список пользователей.** Установленный флажок слева от имени указывает на то, что пользователь располагает правами администратора.

➤ Подобным же образом добавьте имя второго пользователя - user2 - и его пароль.

Помните, что при настройке Eserv вы должны добавлять не вымышленные имена, а реальных пользователей, которые будут получать и отправлять почту.

## Настройка планировщика (POP3 сервер)

В следующем, восьмом диалоге **Мастер конфигурирования Eserv. Настройка планировщика (POP3 сервер)** (Рис. 6.8) следует определить периодичность проверки и получения входящей почты на сервере провайдера.

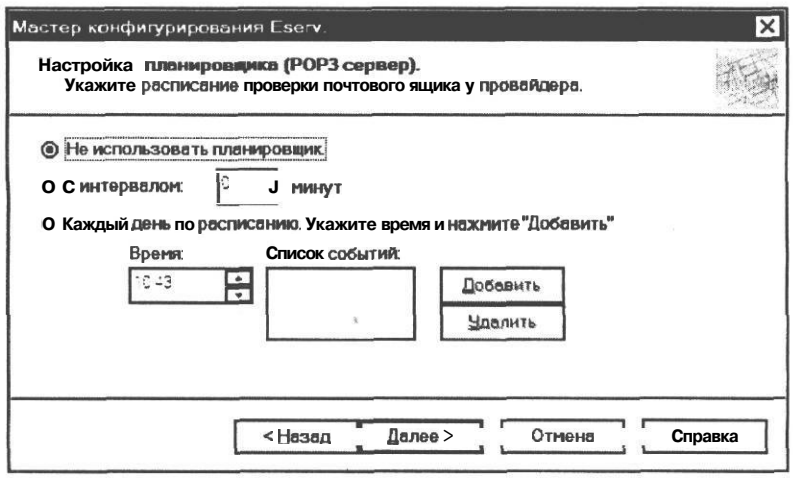



***Рис. 6.8. Восьмой диалог Мастер конфигурирования Eserv. Настройка планировщика (POP3 сервер)***

Если установить переключатель **Не использовать планировщик,** то входящая почта не будет доставляться автоматически. Для ее получения нужно будет «вручную» подключится к почтовому серверу.

Чтобы регулярно проверять наличие входящей почты, следует установить переключатель **С интервалом ... минут** и в поле ввода указать временной промежуток. Для целей отладки программы можно установить интервал, равный одной минуте.

Если требуется получать почту ежедневно в определенное время, то следует установить переключатель **Каждый день по расписанию** и в поле ввода со счетчиком **Время** указать время доставки почты, после чего нажать кнопку **Добавить,** чтобы поместить выбранное время в поле **Список событий.** Добавив описанным способом новые значения, вы составите расписание проверки почты на сервере провайдера.

Когда вы установите в соответствии с вашими требованиями расписание получения входящей почты, нажмите кнопку **Далее** (Next).

## Настройка планировщика (SMPT сервер)

В следующем диалоге **Мастер конфигурирования Eserv. Настройка планировщика (SMPT сервер)** (Рис. 6.9) с помощью переключателей задается расписание отправки исходящей почты.

Первые три переключателя аналогичны таким же переключателям в диалоге **Мастер конфигурирования Eserv. Настройка планировщика (POP3 сервер)** (Рис. 6.8).

При установленном переключателе **Отправлять почту сразу после поступления** программа отправит новое почтовое сообщение немедленно. Это - оптимальный вариант, если подключение к Интернету непрерывное.

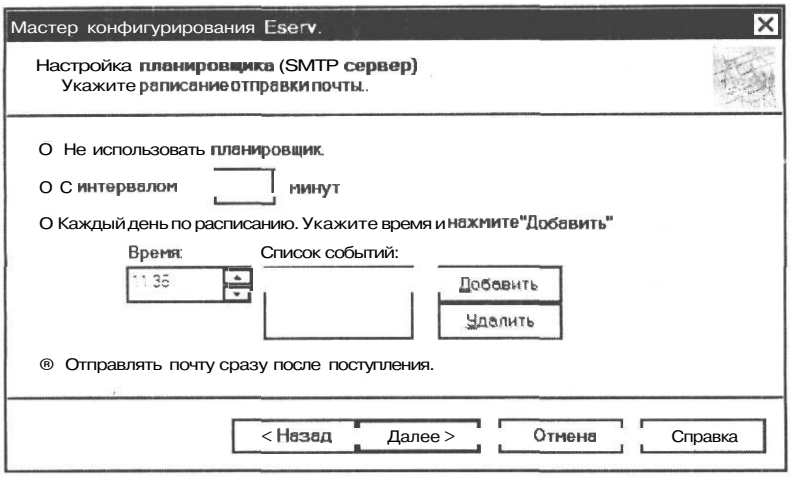



*Рис. 6.9. Девятый диалог Мастер конфигурирования Eserv. Настройка планировщика (SMPT сервер)*

## Настройка планировщика (Удаление временных файлов)

После нажатия кнопки **Далее** (Next) вы перейдете к очередному диалогу **Мастер конфигурирования Eserv. Настройка планировщика (Удаление временных файлов)** (Рис. 6.10).

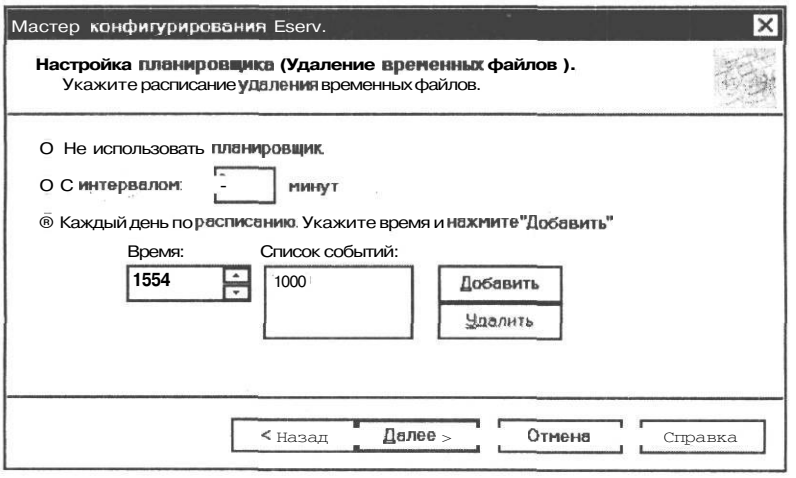



*Рис. 6.10. Десятый диалог Мастер конфигурирования Eserv. Настройка планировщика (Удаление временных файлов)*

В этом диалоге задается расписание удаления временных файлов, создаваемых программой в процессе своей работы. Настройка выполняется точно так же, как и в двух предыдущих диалогах.

➤ После настройки расписания удаления временных файлов нажмите кнопку **Далее** (Next). Откроется последний диалог **Мастер конфигурирования Eserv. Настройка конфигурации Eserv закончена** (Рис. 6.11) с сообщением о завершении настройки конфигурации программы.

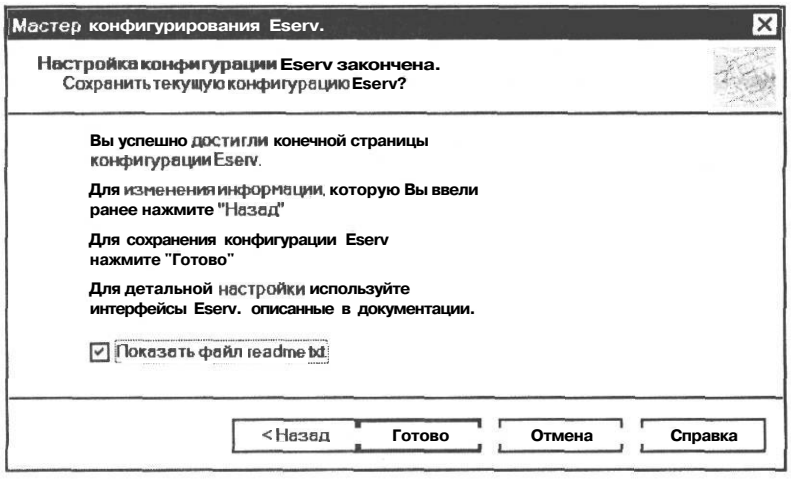



*Рис. 6.11. Последний диалог* ***Мастер конфигурирования Eserv. Настройка конфигурации Eserv закончена***

> Сбросьте флажок **Показать файл readme.txt** и нажмите кнопку **Готово,** чтобы сохранить созданную конфигурацию. Диалог **Мастер конфигурирования Eserv. Настройка конфигурации Eserv закончена** закроется.

Мастер конфигурирования Eserv, завершая свою работу, создает файл настроек **Eserv.ini**, который сохраняется в папке **Eserv\CONF** и используется при последующих запусках Eserv.

# Детальная настройка конфигурации Eserv

Дальнейшую, детальную настройку следует выполнять в рабочем окне программы Eserv/2.99. Запуск профаммы осуществляется из главного меню Windows командой Все программы ◆ Eserv2 ◆ Запустить **ESERV2-server** (All * Eserv2 ◆ Запустить ESERV2-server). После первого запуска программы на экране появится диалог Редактор реестра (Registry Editor) (Рис. 6.12), запрашивающий подтверждение ввода новой информации в реестр Windows.

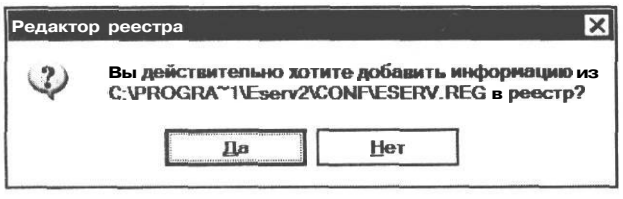



*Рис. 6.12. Диалог Редактор реестра (Registry Editor)*

> Нажмите кнопку Да (Yes), подтверждая таким образом необходимость добавления информации в реестр.

После этого откроется главное окно Eserv/2.99 (Рис. 6.13). Это окно разделено на три части. Слева находится тематическое дерево разделов настройки, принцип работы с которым такой же, как и с иерархией каталогов в Проводнике (Windows Explorer). Справа вверху отображаются параметры настройки, а справа внизу - контекстные подсказки о настройках выбранного раздела и поля диалога для изменения значений конкретных параметров и добавления элементов в списки.

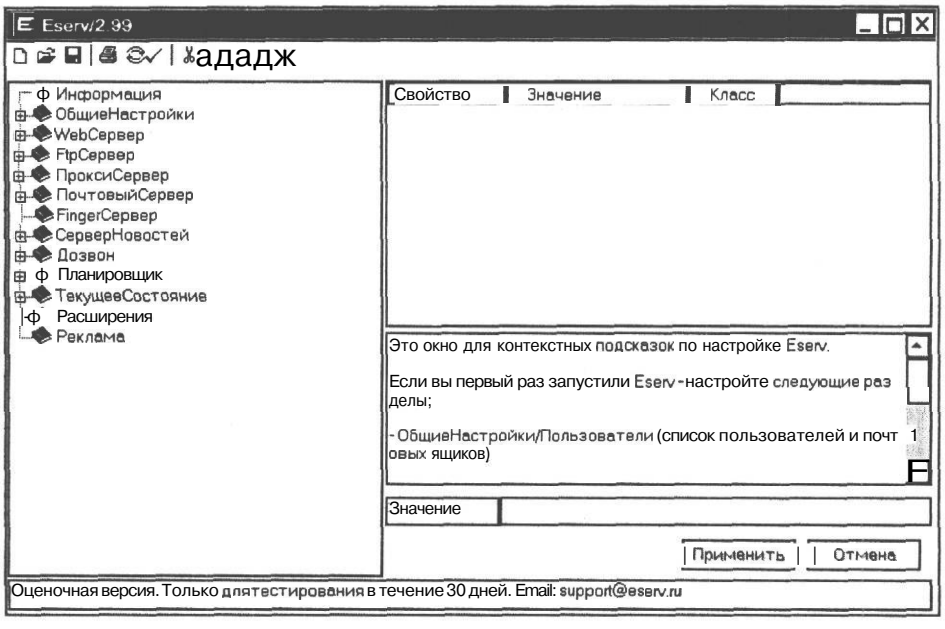



*Рис. 6.13. Главное окно программы* ***Eserv/2.99***

Общий принцип работы по настройке следующий. Открывается раздел в левом окне. Справа при этом появляется список параметров и подсказка по разделу. Следуя подсказке, изменяются параметры и нажимается кнопка **Применить** (в английской версии - кнопка OK). Для изменения текущего значения параметра дважды щелкните мышкой по имени этого параметра в списке параметров. При этом элементы управления изменятся в соответствии с типом меняемого параметра (текстовое поле ввода, либо открывающийся список, либо диалог для выбора каталога или файла и т.д.). Для того чтобы указанный набор параметров действовал не только в текущем сеансе работы сервера, но и при последующих запусках, конфигурацию нужно сохранить с помощью кнопки - **Сохранить конфигурацию** (Save Configuration) на панели инструментов.

При первом запуске программы Eserv/2.99, если **Мастер конфигурирования Eserv** не использовался, для настройки почтового сервера следует отредактировать следующие разделы:

**ОбщиеНастройки/Пользователи** (CommonSettings/Users) - список пользователей и почтовых ящиков;

**ПочтовыйСервер/SMTPсервер/ЛокальныеДомены** (MailServer/SMTPserver / LocalDomains) - список ваших почтовых доменов;

Дозвон/Соединения (Dialer/Connections) - способ соединения с провайдером, если подключение осуществляется через модем;

**Планировщик/Задания/POP3RECV** и SMTPSEND (Scheduler/Tasks/POP3RECV SMTPSEND) - управление доставкой внешней почты.

После внесения изменений в разделы следует нажать кнопку - Сохранить конфигурацию (Save Configuration) на панели инструментов.

Но, поскольку для настройки почтового сервера мы использовали Мастер конфигурирования **Eserv**, все перечисленные разделы уже настроены. Вы можете убедиться в этом, просмотрев их. Вы можете также редактировать все параметры. Как выполнять реальные настройки, мы покажем в следующих разделах.

# Подключение нового пользователя сети

Предположим теперь, что к нашей локальной сети подключился новый пользователь с **user3** с внешним почтовым ящиком user3@yandex.ru. Теперь почтовый сервер Eserv должен получать почту также и с этого почтового адреса и класть ее в ящик пользователя user3@local.ru в локальной сети. А отправляться почта пользователя **user3** будет через сервер провайдера или, в нашем случае, почтовую службу mail.ru, как и почта всех прочих пользователей локальной сети.

Чтобы сделать необходимые настройки для нового пользователя необходимо добавить пользователя, присвоить ему алиас и добавить новое задание на получение почты.

## Добавление пользователя

Прежде всего, нового пользователя следует добавить в раздел дерева настроек ОбщиеНастройки/Пользователи.

➤ На дереве разделов настроек откройте раздел ОбщиеНастройки/Пользователи (CommonSettings/Users).

Вы увидите, что в данном разделе перечислены все пользователи нашей локальной сети - **user1** и **user2**, которых вы добавили на стадии конфигурирования Eserv с помощью Мастера (Рис. 6.14).

➤ В поле ввода Значение (Value) в правой нижней части рабочего окна введите имя нового пользователя, в нашем примере - **user3**, и нажмите кнопку Добавить (Add). Это имя появится на дереве разделов в папке ОбщиеНастройки/Пользователи (CommonSettings/Users), а в колонке Свойство (Property) таблицы в правой верхней части рабочего окна появится свойство Пароль (Password) для данного пользователя.

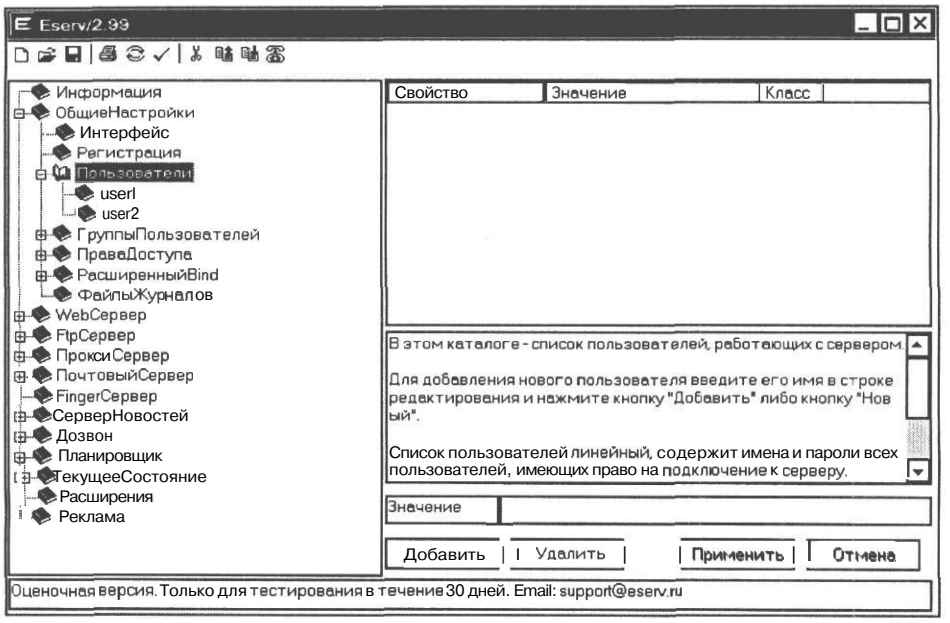



*Рис. 6.14. Раздел **ОбщиеНастройки/Пользователи**(CommonSettings/Users)*

> Дважды щелкните мышью на свойстве Пароль (Password) и в поле ввода Password (Пароль) ведите пароль данного пользователя, который он будет использовать при обращении к почтовому серверу. Нажмите кнопку Применить (OK), чтобы закрепить этот пароль за пользователем.

Для удаления пользователя его имя следует выделить на дереве и нажать кнопку Удалить (Delete).

Заметьте, что список пользователей содержит имена и пароли всех пользователей, имеющих право на подключение к почтовому серверу.

## Настройка алиасов

Наша следующая задача - указать внешние Интернет-адреса электронной почты всех пользователей сети, чтобы программа Eserv могла автоматически получать для них почту и складывать ее в локальные почтовые ящики. Для этого используются так называемые алиасы.

Алиасы - это почтовые адреса внутри локальной сети, которые являются псевдонимами внешних адресов. Во всех случаях, когда Eserv разбирает адреса получателей письма, он прежде всего сверяет адрес со списком алиасов в разделе **Почтовый сервер/SMTPсервер/Алиасы** (MailServer/SMTPserver/Aliases) и подставляет взамен обнаруженных псевдонимов те адреса, на которые они ссылаются. Изменения текста и заголовков писем при этом не происходит - алиасы применяются только для того, чтобы изменить обработку некоторых адресов внутри Eserv. Например, если из локальной

сети отправить письмо на внешний адрес **user1@mail.ru**, которому присвоен алиас **user1@**local.ru, то оно не будет отправлено через Интернет, а сразу попадет в локальный почтовый ящик **user1@local.ru**. Таким образом мы устанавливаем соответствие между локальным адресом и внешним почтовым ящиком.

При конфигурировании Eserv с помощью Мастера мы указали адреса серверов POP3 и SMTP для адреса userl @ mail.ru. Но пока этому адресу не будет присвоен алиас, пользователь userl не будет получать входящую почту. Все письма, поступающие на этот адрес, будут перенаправляться на адрес postmaster@local.ru. Точно так же без алиаса невозможно будет отправить письма с адреса userl **@mail.ru**.

Посмотрим, как присвоить алиас почтовому адресу userl **@mail.ru**.

➤ На дереве разделов в левой части рабочего окна **Eserv/2.99** откройте раздел Почтовый **сервер/SMTPсервер/Алиасы** (MailServer/SMTPserver/Aliases) (Рис. 6.15).

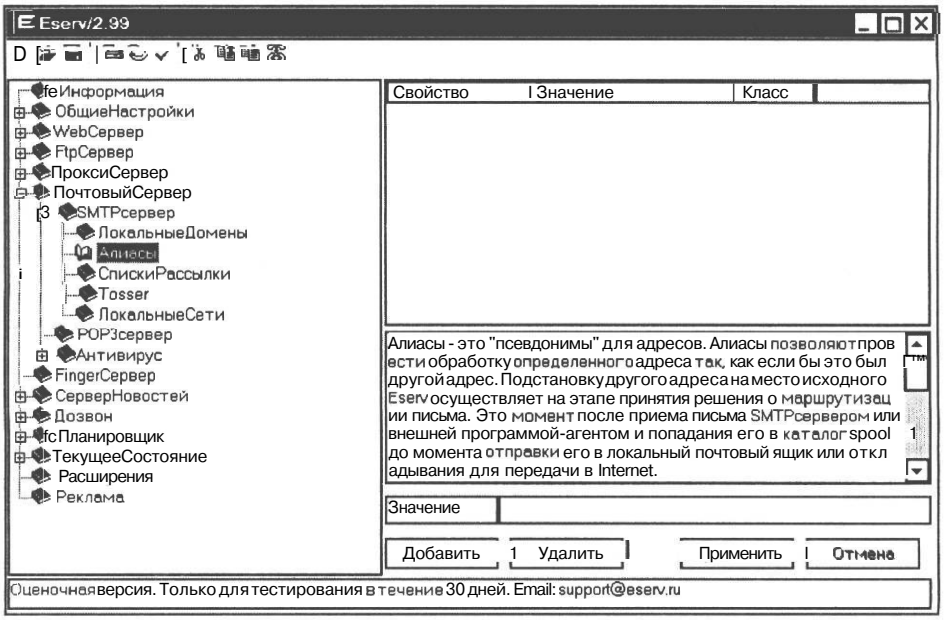



*Рис. 6.15. Раздел Почтовый **сервер/SMTPсервер/Алиасы** (MailServer/SMTPserver/Aliases)*

> Щелкните мышью в поле ввода Значение (Value) в правой нижней части рабочего окна, введите адрес внешней электронной почты **user1@mail.ru** пользователя userl и нажмите кнопку Добавить (Add). Указанный адрес отобразится в колонке Свойства (Property) таблицы параметров текущего раздела в правой верхней части рабочего окна.

Теперь присвоим этому адресу алиас (псевдоним).

➤ Дважды щелкните мышью в колонке Свойство (Property) на введенном адресе. Данный адрес будет помещен в поле у нижнего края рабочего окна.

➤ Щелкните мышью в поле ввода справа от этого адреса в правой нижней части рабочего окна, введите алиас - **user1@local.ru** и нажмите кнопку Применить (OK). Указанный алиас появится в колонке Значение (Value), справа от адреса электронной почты (Рис. 6.16).

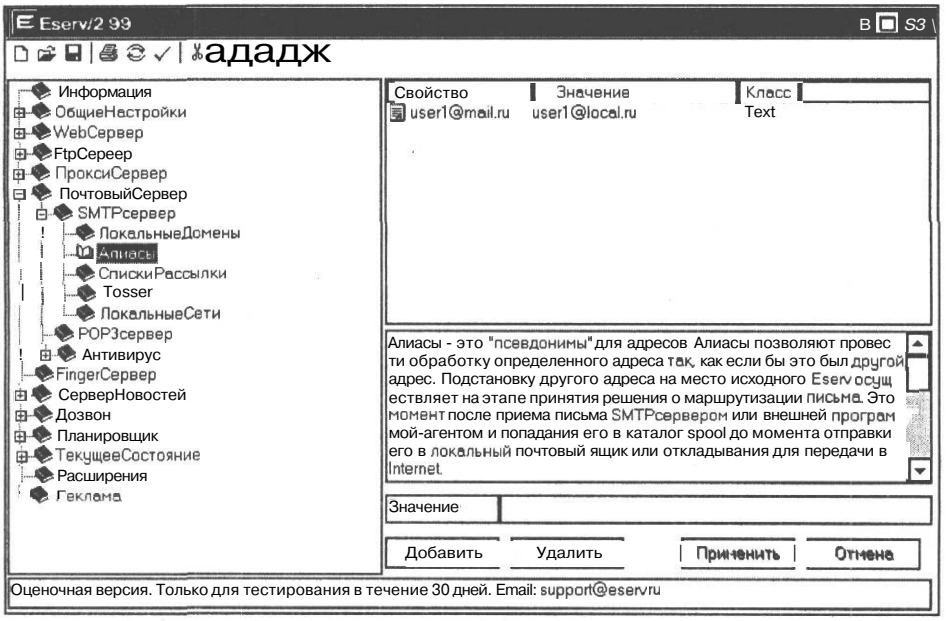



*Рис. 6.16. Почтовому адресу присвоен алиас*

Обратите внимание: для ввода адреса следует напечатать его и нажать кнопку Добавить (Add); для ввода алиаса следует дважды щелкнуть мышью на адресе в столбце Свойства (Property), ввести алиас и нажать кнопку Применить (OK). Можно также сразу ввести в строке два адреса, разделив их пробелом, и нажать кнопку Добавить (Add).

Подобным же образом присвоим алиас почтовому адресу user3@yandex.ru добавленного нами нового пользователя user3.

➤ В поле ввода Значение (Value) в правой нижней части рабочего окна введите адрес электронной почты нового пользователя user3@yandex.ru и нажмите кнопку Добавить (Add). Этот адрес появится в колонке Свойство (Property) таблицы параметров текущего раздела.

> Дважды щелкните мышью в колонке Свойство (Property) на адресе user3@yandex.ru, в поле ввода справа от этого адреса в правой нижней части рабочего окна, введите алиас - user3@local.ru и нажмите кнопку Применить (OK). Этот алиас появится в колонке Значение (Value), справа от адреса электронной почты.

Для удаления адреса и его алиаса из таблицы следует щелчком мыши выделить адрес и нажать кнопку Удалить (Delete).

➤ Сохраните созданную конфигурацию, нажав кнопку [] - **Сохранить конфигурацию** (Save Configuration) на панели инструментов.

Почтовый сервер осуществляет подстановку другого адреса на место исходного на этапе принятия решения о маршрутизации письма. Это - момент после приема письма SMTP-сервером и попадания его в каталог Eserv2\mail\spool до момента отправки его в локальный почтовый ящик или откладывания для передачи через Интернет. Подстановка адресов осуществляется на основе заданной таблицы **алиасов**. Вместо адресов из столбца Свойство (Property) подставляются соответствующие адреса из столбца Значение (Value), и дальнейшая обработка происходит так, как будто исходного адреса не было. Так можно осуществлять перенаправление сообщений из одного ящика в другой, локальной почты - наружу, преобразовывать краткий адрес в полный и т.д. Причем в тексте письма и в заголовке адреса не меняются. Замена действует только внутри **Eserv** и в программе маршрутизации.

Обратите внимание на то, что внутри сети почта циркулирует без подключения к Интернету: программа по **алиасам** определяет локального пользователя и сразу же кладет письмо в его ящик.

# Добавление задания на доставку почты

Теперь следует настроить встроенный планировщик заданий на получение внешней почты, поступающей на адрес user3@yandex.ru. Задание на получение почты, поступающей на адрес **user1@mail.ru**, было настроено при конфигурировании почтового сервера с помощью Мастера.

➤ Откройте раздел настроек **Планировщик/Задания** (Scheduler/Tasks).

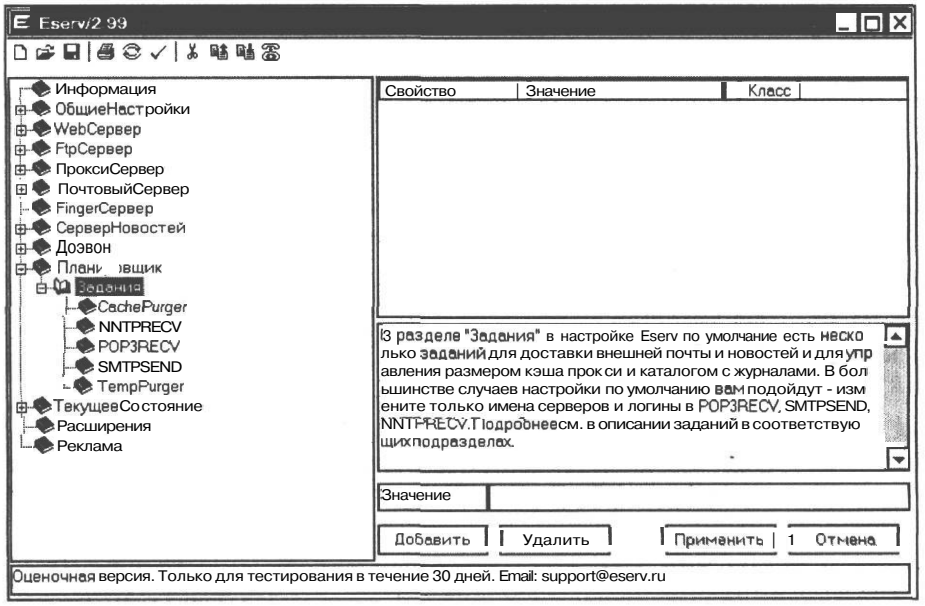



*Рис. 6.17. Раздел **Планировщик/Задания** (Scheduler/Tasks)*

В этом разделе на дереве вы увидите несколько заданий (Рис. 6.17). В частности, для получения почты с внешнего сервера используется задание POP3RECV, для отправки

почты предназначено задание SMTPSEND, для доставки новостей - задание NNTPRECV, для управления размером кэша прокси - задание CachePurger, для очистки временного каталога с журналами - задание TempPurger. В большинстве случаев настройки каждого задания, установленные по умолчанию, являются оптимальными. Необходимо изменить только имена почтовых серверов, а также имена и пароли пользователей.

В разделе **Планировщик/Задания/POP3RECV** (Scheduler/Tasks/POP3RECV) уже определено задание на получение почты, поступающей на адрес **user1@mail.ru** (Рис. 6.18).

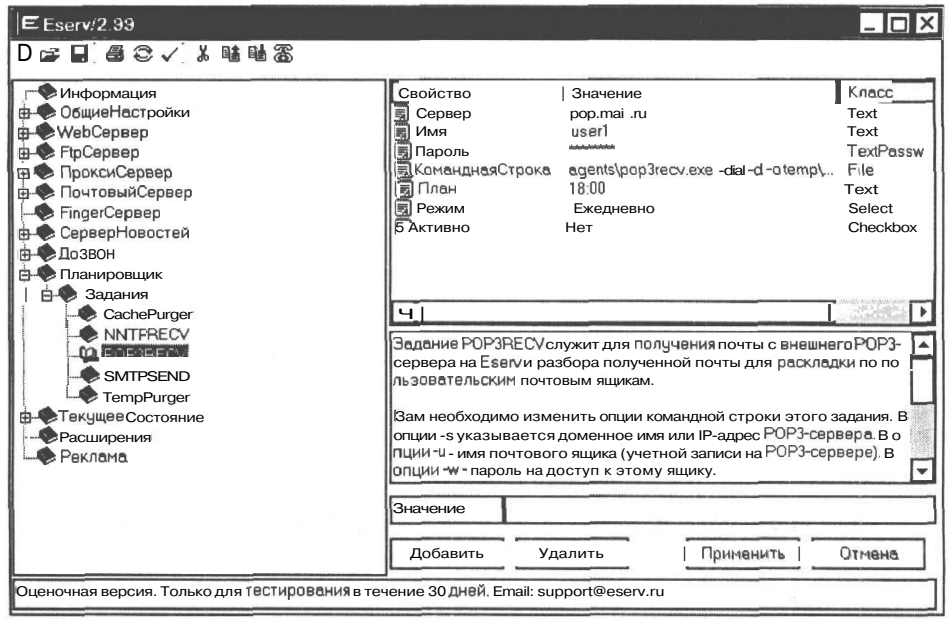



*Рис. 6.18. Задание на получение почты с сервера провайдера*

Теперь необходимо создать такое же задание на получение почты, поступающей на адрес user3@yandex.ru.

- Убедитесь, что выделен раздел **Планировщик/Задания** (Scheduler/Tasks). В противном случае - выделите его.
- В поле ввода Значение (Value) у нижнего края рабочего окна введите: POP3RECV и нажмите кнопку Добавить (Add).

Новый раздел в папке **Планировщик/Задания** (Scheduler/Tasks) не появится, но в задание POP3RECV будут добавлены новые строки: Сервер (Server), Имя (Login), Пароль (Password), **КомандныяСтрока** (CommandLine), План (Schedule), Режим (Mode), Активно (Active). Эти поля теперь необходимо заполнить.

- Щелчком мыши выделите раздел **Планировщик/Задания/POP3RECV** (Scheduler/Tasks/POP3RECV), чтобы увидеть их настройки раздела (Рис. 6.19).

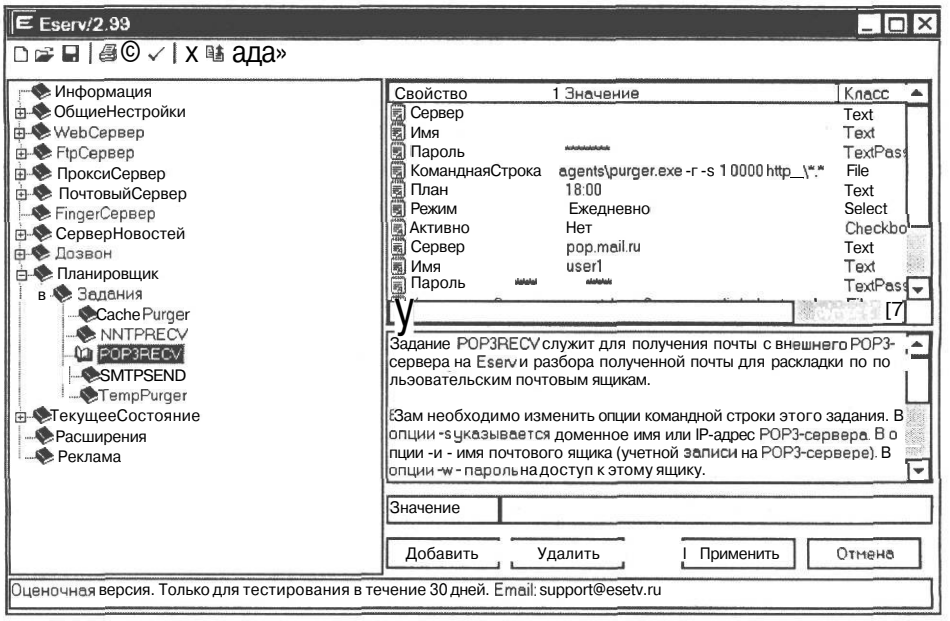



*Рис. 6.19. Новые строки в задании* ***POP3RECV***

Заполним сведения, необходимые для доставки почты, поступающей на адрес - **user3@yandex.ru.**

> Дважды щелкните мышью в столбце **Свойство** (Property) на первой строке **Сервер** (Server).

➤ В поле ввода **Server** (Server) в правой нижней части рабочего окна введите имя почтового сервера, с которого нужно забирать почту, - **pop.yandex.ru.**

➤ Нажмите кнопку **Применить** (OK). Это имя будет помещено в поле **Значение** (Value) свойства **Сервер** (Server).

➤ Подобным же образом введите **Имя** (Login) пользователя - **user3 - и Пароль** (Password) для доступа к почтовому ящику **user3@yandex.ru.**

Командную строку следует скопировать из уже настроенного задания. Сделайте это следующим образом.

➤ Дважды щелкните в столбце **Свойство** (Property) таблицы на второй строке **КомандноеСтрока** (CommandLine), имеющей следующее значение:

**agents\pop3recv.exe -d -o temp\%TempFile%.eml -s %Server% -u %Login% -w %Password% &agents\Erobot.exe -c agents\pop3toss.cfg -o temp\%TempFile%.toss -i temp\%PrevTempFile%.eml.**

Эта командная строка будет помещена в поле ввода в нижней части рабочего окна **Eserv/2.99**.

- Протащив мышь при нажатой левой кнопке от левого края поля ввода до его правого края, выделите все содержимое этого поля. Выделение можно выполнить также, щелкнув мышью в начале строки и нажав комбинацию клавиш Shift+End. Убедитесь, что выделена вся командная строка, так как она довольно длинная.
- Нажмите комбинацию клавиш Ctrl+C, чтобы скопировать выделенную командную строку в буфер обмена.
- Дважды щелкните в столбце Свойство (Property) таблицы на первой строке КомандНаяСтрока (CommandLine), имеющей значение **agents\purger.exe** -r -s 10000 **http__*.***, чтобы поместить ее в поле ввода.
- Выделите все содержимое поля ввода.
- Нажмите комбинацию клавиш Ctrl+V, чтобы вставить содержимое буфера обмена в поле ввода.
- Нажмите кнопку Применить (OK). Новое значение для первого свойства **КомандНаяСтрока** (CommandLine) появится в таблице.

Основные параметры командной строки имеют следующий смысл:

-s - доменное имя или IP-адрес сервера POP3;

-и - имя почтового ящика (учетной записи) на сервере POP3;

-w — пароль для доступа к этому ящику.

Другие параметры изменять не рекомендуется. Полный список параметров можно получить, запустив программу POP3RECV.exe из командной строки с параметром /?: POP3RECV.exe /?. По умолчанию POP3RECV.exe находится в папке Program **Files\agents**. Это - консольная программа, которая запускается Eserv и работает незаметно для пользователя.

В командной строке запускается также программа Erobot.exe, перемещающая принятую почту в папку mail\spool, расположенную в папке Eserv, для последующей обработки. В ее параметрах ничего менять не надо.

Чтобы закончить настройку задания, укажите требуемые значения для свойств План (Schedule), Режим (Mode) и Активно (Active) и сохраните измененную конфигурацию, нажав кнопку - Сохранить конфигурацию (Save Configuration) на панели инструментов.

## Настройка почтовых клиентов

На почтовом сервере Eserv заводятся учетные записи всех пользователей или, другими словами, их почтовые ящики. Эти ящики создаются автоматически при добавлении пользователей в раздел **ОбщиеНастройки/Пользователи** (CommonSettings/Users).

Почтовые программы-клиенты каждого пользователя сети, такие как Outlook Express, могут забирать почту из почтовых ящиков, а также отправлять почту другим пользователям этого сервера или «наружу». Чтобы выполнять эти действия, почтовому клиенту нужно знать, где находится почтовый сервер Eserv и из какого ящика получать почту. Для этого в почтовом клиенте каждого пользователя необходимо создать учетную запись для доступа к Eserv.

В Outlook Express 6 для создания новой учетной записи следует выбрать команду меню Сервис * Учетные записи (Tools ◆ Accounts). В появившемся диалоге Учетные записи в Интернете (Internet Accounts) нужно нажать кнопку Добавить (Add) и в открывшемся меню выбрать Почта (Mail). Будет запущен Мастер подключения к Интернету (Internet Connection Wizard), в диалогах которого следует указать необходимые параметры.

Если у пользователя есть внешний почтовый ящик, что в качестве имени пользователя и адреса электронной почты следует указать соответственно имя пользователя и адрес внешнего почтового ящика, которые указаны в разделе Почтовый **сервер/SMTPсервер/Алиасы** (MailServer/SMTPserver/Aliases), а в качестве обратного адреса - адрес этого же внешнего почтового ящика. Если же внешний почтовый ящик отсутствует - то указываются локальное имя и адрес. На вкладке Общие (General) диалога Свойства (Properties) учетной записи это должно выглядеть примерно так, как на Рис. 6.20.

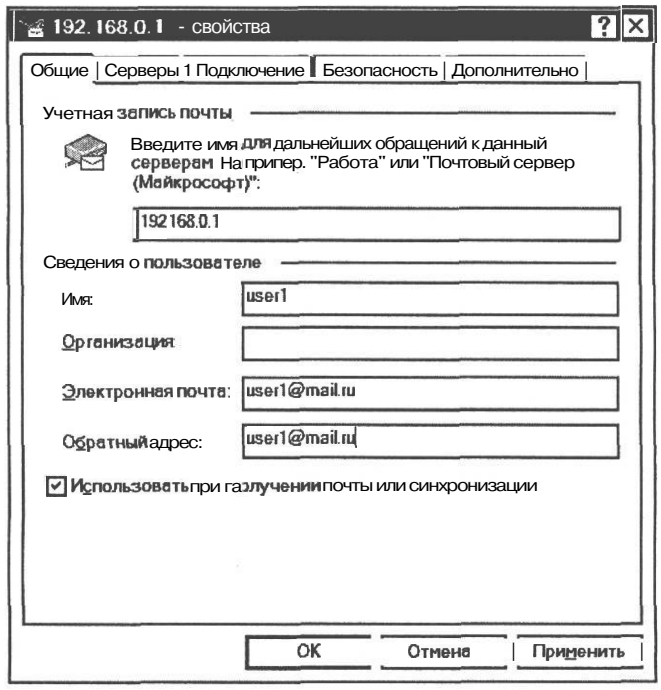



*Рис. 6.20. Указание адресов электронной почты в учетной записи*

На вкладке **Серверы** (Servers) (Рис. 6.21) диалога **Свойства** (Properties) учетной записи в качестве серверов входящей (POP3) и исходящей (SMTP) почты следует указать реальное сетевое имя или локальный IP-адрес того компьютера, на котором запущен Eserv. В нашем примере это - **192.168.0.1**, так как мы рассматриваем только общее подключение через модем в Windows XP.

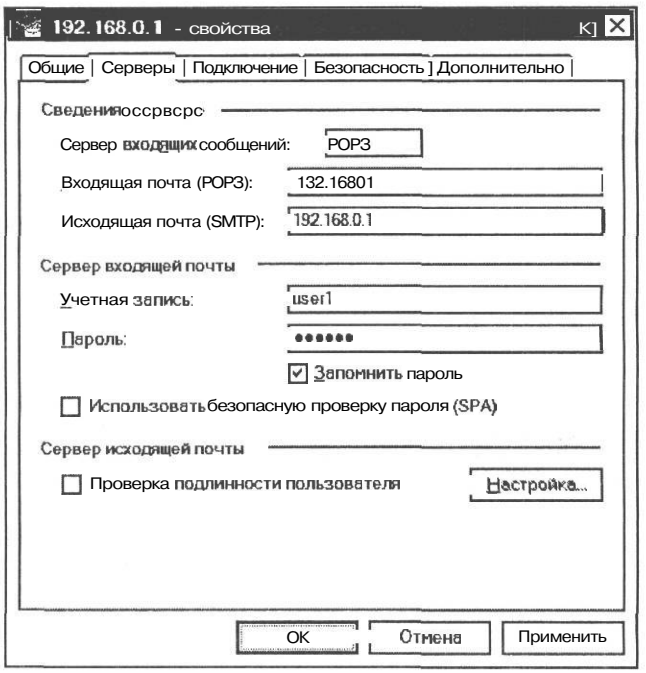



*Рис. 6.21. Указание серверов входящей (POP3) и исходящей (SMTP) почты в учетной записи*

## Тестирование почтового сервера

После того как Eserv и почтовые клиенты настроены, можно проверить их работоспособность, написав письма другим пользователям сети. Нажмите в почтовом клиенте кнопку **Создать сообщение** (Create message), в поле Кому (To) введите адрес электронной почты получателя и отправьте его.

Если отправить не удалось и почтовая программа при этом сообщает о невозможности найти сервер, то нужно проверить, запущен ли на серверном компьютере Eserv, работает ли сетевое оборудование и TCP/IP-связь с этим компьютером.

Сетевое оборудование должно обеспечивать сетевой интерфейс с Интернетом и сетевой интерфейс с локальной сетью - логически два интерфейса, но физически это может быть и одно устройство.

Функционирование протокола TCP/IP в обоих сетевых интерфейсах можно проверить двумя утилитами, входящими в комплект Windows, – ping.exe и telnet.exe. Эти программы устанавливаются автоматически при установке протокола TCP/IP.

Для проверки функционирования протокола TCP/IP в сетевом интерфейсе с Интернетом установите соединение с Интернетом, запустите программу Командная строка (Command Prompt) и выполните команду вида:

**ping.exe имя_почтового_сервера_провайдера (или любого другого), например:**

**ping.exe pop.mail.ru**

Для проверки функционирования протокола TCP/IP в локальной сети подключение к Интернету не требуется. Достаточно в командной строке ввести команду вида:

**ping.exe имя_клиентского_компьютера_в_локальной_сети, например:**

**ping.exe 192.168.0.1**

Обе эти команды должны отработать без сообщений об ошибках и выдать информацию о времени прохождения пакетов.

Если после ввода команды ping.exe появляются сообщения об ошибках: Timeout (Превышен интервал ожидания для запроса), Bad IP (Неправильный IP), Network unreachable (Сеть недоступна) или подобные, то у вас неверно настроен протокол TCP/IP в сетевом интерфейсе либо проблемы с сетевыми адаптерами или соединительными кабелями.

Если команда ping.exe работает нормально и выдает время прохождения пакетов, то на следующем шаге проверьте работу TCP-связи с Eserv с помощью утилиты telnet.exe, которая использует протокол Telnet, входящий в набор протоколов TCP/IP, для подключения к удаленному компьютеру в сети. Программное обеспечение клиента Telnet позволяет компьютеру подключаться к удаленному серверу Telnet и запускать приложения на этом сервере.

> Запустите программу Eserv, откройте окно Командная строка (Command Prompt) и введите команду:

**telnet.exe 192.168.0.1 25**

Здесь **192.168.0.1** - IP-адрес компьютера, на котором запущен Eserv, 25 - номер порта.

Вы должны получить ответ:

**220 Eserv/2.99 ESMTP server ready.**

Если с помощью программы telnet.exe вы добились такого результата, то TCP/IP в вашей сети работает правильно. В этом случае невозможность отправки сообщения из почтового клиента говорит о неправильной настройке именно этой программы, а не сети или Eserv.

Для выхода из программы telnet.exe следует в командной строке ввести команду quit или q и нажать клавишу Enter.

Когда вы устраните все неполадки, если они имели место, Eserv будет автоматически, по заданному расписанию отправлять и получать почту для всех пользователей сети и раскладывать ее в локальные почтовые ящики. Если при настройке почтового сервера вы не задали расписания доставки почты, то для получения почты следует нажать кнопку - POP3RECV, а для отправки почты - кнопку - SMTPSEND на панели инструментов Eserv. Каждый пользователь сети сможет без проблем отправлять и получать почту как внутри локальной сети, так и за ее пределами с помощью своей почтовой программы.

# Возможности других сервисов Eserv

Кроме почтового сервера, программа Eserv позволяет создать в локальной сети серверы новостей, WWW, FTP, PROXY.

## Сервер новостей

При работе с сервером новостей программа-клиент, служащая для чтения новостей, например Outlook Express, соединяется по протоколу TCP с сервером новостей. По команде пользователя программа обычно может получить список групп новостей, доступных для получения на этом сервере, и список сообщений в любой группе. При этом запрашиваются обычно не все имеющиеся сообщения, а только за указанный период времени, указанное количество последних сообщений или все сообщения после сообщения с заданным номером. Сервер не знает и не помнит, какое сообщение пользователь получал последним. Эту информацию хранит пользовательская программа. В полученном списке сообщений есть адреса и имена отправителей сообщений, даты отправки, темы сообщений и размеры сообщений. Сами сообщения в этой операции не загружаются. После того как пользователь выберет сообщения, какие он хочет прочесть, программа чтения новостей получает их с сервера полностью.

Такой способ работы с новостями сильно отличается от работы с почтой, которую пользователь получает в «пакетном режиме» - все сообщения сразу. Сеансы связи с сервером POP3 обычно коротки. С новостями все наоборот - пользователь выбирает сообщения для загрузки вручную и читает их, не отсоединяясь от сервера. Если соединение происходит через модем, все это время модем должен быть на линии. Таким образом, довольно много онлайнового времени тратится впустую. А если несколько пользователей в локальной сети читают одни и те же сообщения с сервера новостей, то каждое из этих сообщений фактически передается через модем несколько раз.

Eserv позволяет получать сообщения из внешних групп новостей в пакетном режиме, проводя на линии минимум времени. Затем эти сообщения сохраняются на диске в каталогах локального NNTP-сервера. Программы чтения новостей локальных пользователей соединяются с этим локальным сервером, передача новостей происходит быстрее, время сеансов в локальной сети не ограничено. Администратор сервера выбирает группы новостей, которые будут загружаться Eserv, а также указывает, с каких внешних NNTP-серверов получать эти группы.

Сообщения, которые пользователи пишут в группы новостей, также будут сначала попадать на локальный сервер и сразу становиться видимыми другим пользователям локальной сети, после чего будут передаваться Eserv в Интернет.

Кроме описанной оптимизации работы пользователей с внешними группами новостей, NNTP-сервер Eserv позволяет иметь локальные группы новостей, сообщения в которых доступны только пользователям локальной сети и не передаются в Интернет. Это удобно для организации локальных дискуссий и как средство, помогающее автоматизировать внутренний документооборот организации. Имеется возможность также ограничивать доступ пользователей к отдельным группам новостей.

Настройка сервера новостей производится в разделе **СерверНовостей** (NewsServer) дерева разделов. В списке **ЛокальныеГруппыНовостей** (LocalNewsGroups) задаются имена локальных групп новостей и их описание. Права доступа пользователей к тем или иным группам определяются по тем же общим правилам, что и для всех объектов Eserv, в разделе **ОбщиеНастройки/ПраваДоступа/Объекты** (CommonSettings / AccessRights / Objects). В качестве объекта доступа указывается имя группы.

В списке **ВнешниеСерверыНовостей** (RemoteNewsServers) задается список доменных имен либо IP-адресов других серверов новостей, с которыми Eserv будет обмениваться новостями. В разделе, создаваемом для каждого из этих серверов, задается список групп, которые Eserv должен получать с этих серверов, и атрибуты конкретных групп.

Чтобы добавить сервер или группу, нужно войти в соответствующий раздел СерверНовостей (NewsServer), ввести в строке редактирования наименование и нажать кнопку Добавить (Add). Для удаления - выделить наименование сервера или группы и нажать кнопку Удалить (Delete). Атрибуты групп становятся доступными для изменения при двойном щелчке мышью по наименованию атрибута. После изменения атрибута следует нажать кнопку **Применить** (OK). Для сохранения всех выполненных настроек следует нажать кнопку  - Сохранить конфигурацию (Save Configuration) на панели инструментов.

## Сервер WWW

Основная задача WWW-сервера, входящего в Eserv, - обеспечение работы Web-интерфейса. Тем не менее, он может с успехом использоваться в качестве обычного Web-сервера как для Интранета в локальной сети, так и для Интернета.

Web-интерфейс Eserv выполняет ту же роль, что и графический интерфейс управления Eserv, однако имеет некоторые преимущества. Администратор может управлять Eserv удаленно, т.е. не обязательно на том же самом компьютере, на котором запущен Eserv. К Web-интерфейсу можно обратиться из браузера с любого компьютера в локальной сети и даже из Интернета. Полномочия администратора проверяются при этом обычным способом через запрос имени и пароля, т.е. несанкционированный доступ исключен. Web-интерфейс, в отличие от графического, может настраиваться администратором, так как он основан на использовании HTML-шаблонов, поддающихся редактированию.

Web-сервер, основная задача которого - обработка запросов клиентских браузеров, работает по протоколу HTTP/1.1, по умолчанию, на порту 3128. Настройка номера порта и других параметров производится в разделе **WebСервер** (Webserver) дерева настроек Eserv. После изменения номера порта следует сохранить конфигурацию и перезапустить Eserv.

Eserv может передавать браузеру по протоколу HTTP любые файлы, расположенные в корневом каталоге Web-сервера и в виртуальных каталогах. Виртуальные каталоги - это каталоги с файлами для WWW, расположенные не обязательно в каталогах, подчиненных корневому. Но для браузеров они будут выглядеть как вложенные подчиненные каталоги.

По умолчанию корневым каталогом Web-сервера будет каталог wwwroot, находящийся в папке Eserv. Файл index.html из этого каталога будет выдаваться по адресу URL **http://имя_сервера:порт/index.html** или просто **http://имя_сервера:порт/**, так как index.html является файлом по умолчанию для любого каталога сервера.

Подкаталоги папки **wwwroot** будут выдаваться сервером как вложенные каталоги. Например, в папке **wwwroot** есть каталог **admin,** который содержит файлы Web-интерфейса. Для браузера адрес этого каталога будет выглядеть так: **http://имя_сервера:порт/admin/**. Виртуальные каталоги будут также выглядеть как подкаталоги: **http://имя_сервера:порт/подкаталог/**, но при этом не обязаны находиться в папке **wwwroot.** При настройке виртуальных каталогов задается два основных параметра: строка, которая будет подставлена вместо строки «подкаталог» в URL, приведенном выше, и папка, в которой хранятся файлы для этого виртуального каталога.

Виртуальные каталоги настраиваются в разделе **WebСервер/ВиртуальныеКаталоги** (WebServer\VirtualFolders). При обработке HTTP-запросов Web-сервер Eserv сверяется со списком виртуальных каталогов и при совпадении берет файлы из заданных там реальных каталогов.

## Сервер FTP

Для пересылки файлов через Интернет с одного компьютера на другой используется протокол FTP, входящий в семейство протоколов TCP/IP. При этом оба компьютера должны поддерживать соответствующие роли FTP: один должен быть клиентом FTP, а другой - сервером FTP. Программа Eserv может работать в роли сервера FTP.

Если HTTP - основной протокол, применяемый для передачи гипертекстов, изображений и других файлов в WWW, и, соответственно, основной протокол браузеров, то FTP - более старый протокол передачи файлов, используемый в основном в файловых архивах. Браузеры работают с обоими этими протоколами.

Настраивается FTP-сервер в разделе **FTPсервер** (FtpServer) дерева настроек. Его параметры во многом аналогичны параметрам Web-сервера. Каталогом по умолчанию является папка **ftproot**. Могут создаваться также виртуальные каталоги.

## Сервер PROXY

Прокси-сервер действует как защитный барьер между внутренней сетью (интрасетью) и Интернетом, закрывая доступ других пользователей Интернета к секретным сведениям во внутренней сети или на локальном компьютере.

Прокси-серверы HTTP и FTP в Eserv предназначены для выполнения запросов браузеров клиентских компьютеров на получение информации из Интернета. Прокси запускается на компьютере, имеющем прямой доступ к Интернету, а браузеры на всех остальных компьютерах локальной сети настраиваются так, чтобы получать информацию через него.

Eserv может сохранять копии уже полученных файлов на диске и при повторных запросах того же файла выдавать его браузеру клиента уже без загрузки из Интернета. Эта возможность обеспечивается кэшированием.

Прокси-сервер работает по протоколу HTTP, но обслуживает HTTP- и FTP-запросы браузеров. Он настраивается в разделе **ПроксиСервер** (ProxyServer). Там можно выбрать режим кэширования, параметры режимов, каталог, где будет находиться кэш прокси. Как менять эти параметры, описано в контекстной подсказке программы настройки.

Раздел **ПроксиСервер/ЧерныйСписокURL** (ProxyServer/URLBlackList) предназначен для задания списка внешних Web-серверов, доступ к которым должен ограничиваться прокси-сервером. При обращении пользовательских браузеров к этим страницам будет выдаваться запрос имени и пароля пользователя, и доступ будет разрешен только пользователям из привилегированной группы.

Можно также ограничивать доступ только к отдельным каталогам или файлам на Web-серверах. Для добавления серверов в «черный список» перейдите в раздел **ЧерныйСписокURL** (URLBlackList), введите фрагмент URL и нажмите кнопку **Добавить** (Add). Если прокси-сервер обнаружит в запросе одну из перечисленных в этом списке строк, он ограничит доступ. Кроме того, можно указывать фрагменты URL в качестве объектов доступа в разделе **ПраваДоступа/Объекты** (AccessRights/Objects) и определять права доступа пользовательских групп к ним.

По умолчанию прокси-сервер работает на порту с номером 3128. Причем на том же порту работает встроенный HTTP-сервер (Web-сервер). Он автоматически отличает прокси-запросы от обычных обращений к локальному серверу. Номер порта задается в разделе **WebСервер** (Webserver).

Eserv можно настроить на выполнение автодозвона. Если используется подключение к Интернету через модем и в момент обращения браузера к прокси-серверу модемное соединение не установлено, Eserv может автоматически дозвониться и выполнить запрос прозрачно для пользователя, как будто связь уже была установлена. Если прокси-сервер работает в режиме «минимальный трафик», то дозвон будет производиться не по любому запросу, а только в том случае, если в текущем режиме работы невозможно выполнить запрос передачей файлов из кэша. Автодозвон может производиться по запросу любого из пользователей Eserv.

# ГЛАВА 7.
# Жизнь внутри сети: игры, чат, видеотелефон

Соединение компьютеров в сеть значительно увеличивает их возможности, позволяя при этом сэкономить деньги. Создав домашнюю сеть или сеть небольшой организации, вы сможете эффективно задействовать все ресурсы своих компьютеров, используя их и для работы, и для развлечений. Домашняя или малая офисная сеть позволяет пользователю обращаться к ресурсам других компьютеров или устройств, на самом деле не работая непосредственно на этих компьютерах. Пользователь может совместно с другими членами своей семьи или коллегами по работе просматривать содержимое Интернета, играть в сетевые игры, использовать чат, голосовую и видеосвязь для общения с другими пользователями локальной сети и работать совместно над общими документами.

## Сетевые многопользовательские игры

Любителей компьютерных игр особенно привлекает возможность использования сетевого многопользовательского режима. Несомненно, в аркадных играх типа 3D Action (Сражение в 3-х измерениях) значительно интереснее сражаться не с запрограммированными чудовищами, а с персонажами, управляемыми другими людьми, которые, например, вполне могут устроить засаду, подложить мину и использовать множество других неожиданных приемов. Когда сражение в разгаре, невероятно трудно оторваться от экрана...

Чтобы играть в сети, необходимо установить игру, которая поддерживает сетевой многопользовательский режим, на компьютеры всех игроков. Если игра базируется на клиент-серверной технологии (а таких игр сейчас большинство), то она сначала должна быть запущена на одном из компьютеров в качестве игрового сервера. Остальные компьютеры могут присоединиться к игре, подключившись к игровому серверу.

Посмотрим, как настроить такие сетевые игры для использования в локальной сети на примере игры Unreal Tournament 2004 (Фантастическое сражение).

Прежде всего установите игру на все компьютеры сети, которые будут играть. После запуска Unreal Tournament 2004 (Фантастическое сражение) на экране появляется главное меню (Рис. 7.1).

Как уже отмечалось, один из компьютеров сети должен быть запущен в режиме игрового сервера. Остальные компьютеры работают в режиме клиентов, которые могут включиться в игру. Рассмотрим настройки сервера и клиента.


*Рис. 7.1. Главное меню Unreal Tournament2004*

## Настройка игрового сервера

Для настройки игрового сервера следует в главном меню Unreal Tournament 2004 (Фантастическое сражение) (Рис. 7.1) выбрать команду Host Game (Игровой сервер). Появится диалог Host Game (Игровой сервер), содержащий четыре вкладки.

На левой панели открытой по умолчанию вкладки Game Type (Тип игры) (Рис. 7.2) следует щелчком мыши выбрать вариант игры, руководствуясь пояснениями, которые вы видите на правой панели.

После выбора варианта игры вы автоматически перейдете на вкладку Select Map (Выбор сценария) (Рис. 7.3).

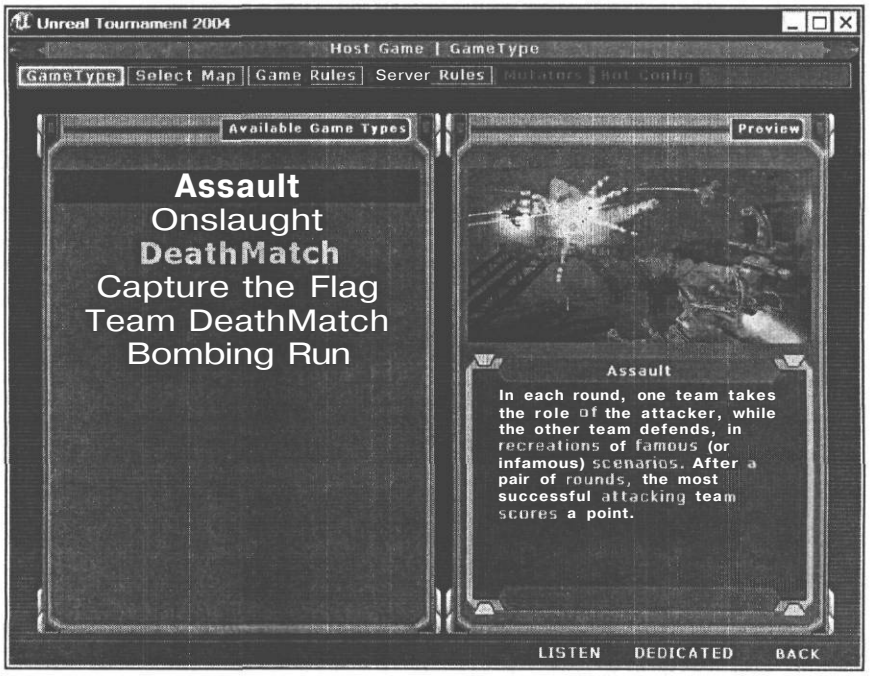



*Рис. 7.2. Вкладка **Game Type** (Тип игры) диалога **Host Game** (Игровой сервер)*

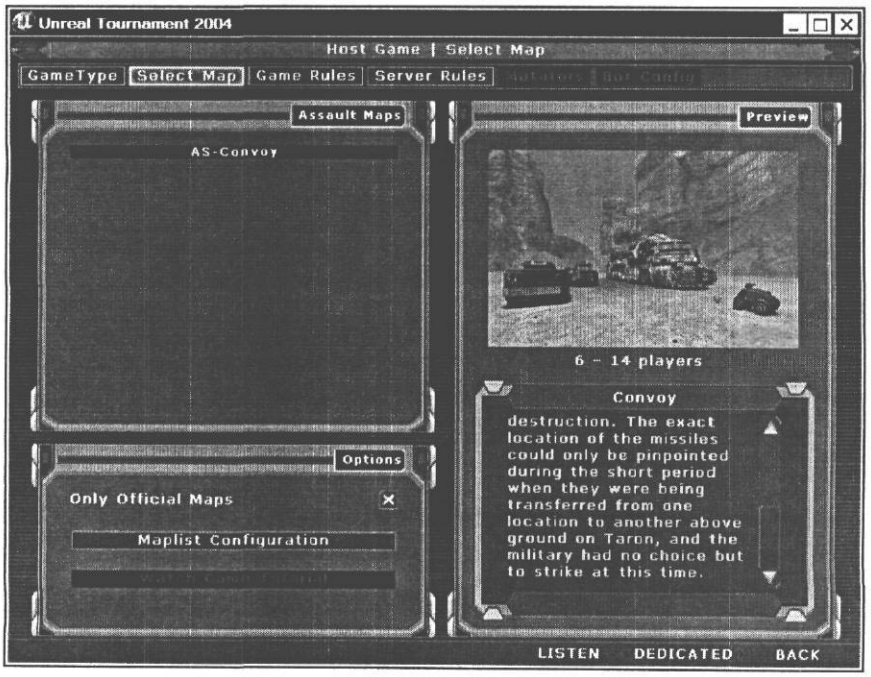



*Рис. 7.3. Вкладка **Select Map** (Выбор сценария)*

Если для выбранного варианта игры имеется набор сценариев, то в левой части диалога следует выбрать один из них. После этого на вкладках Game Rules (Правила игры) и Server Rules (Правила сервера) следует задать соответственно правила игры и правила сервера. Если их не изменять, то будут использованы правила, заданные по умолчанию. С помощью кнопки Back (Назад) осуществляется возврат к предыдущей вкладке.

Когда все параметры настроены, можно запустить игровой сервер. При этом нажатие кнопки Listen (Участие) запускает сервер в режиме участия, т.е. пользователь данного компьютера может участвовать в игре. Если же нажать кнопку Dedicate (Консольный режим), то игровой сервер будет запущен в консольном режиме, в котором пользователь данного компьютера играть не сможет; только другие компьютеры сети смогут, подключившись к игровому серверу, принимать участие в игре.

## Настройка клиентов

После запуска Unreal Tournament 2004 на компьютере-клиенте следует в главном меню (Рис.43) выбрать команду Join Game (Присоединиться к игре). В верхней части окна программы появятся шесть вкладок. Для игры в локальной сети следует перейти на вкладку LAN (Локальная сеть), после чего появится и будет выделено имя игрового сервера (Рис. 7.4), в нашем случае - UT2004 Server. Для выбранного сервера указывается текущий сценарий игры (Map), количество игроков (Players) и время прохождения сигнала (Ping).

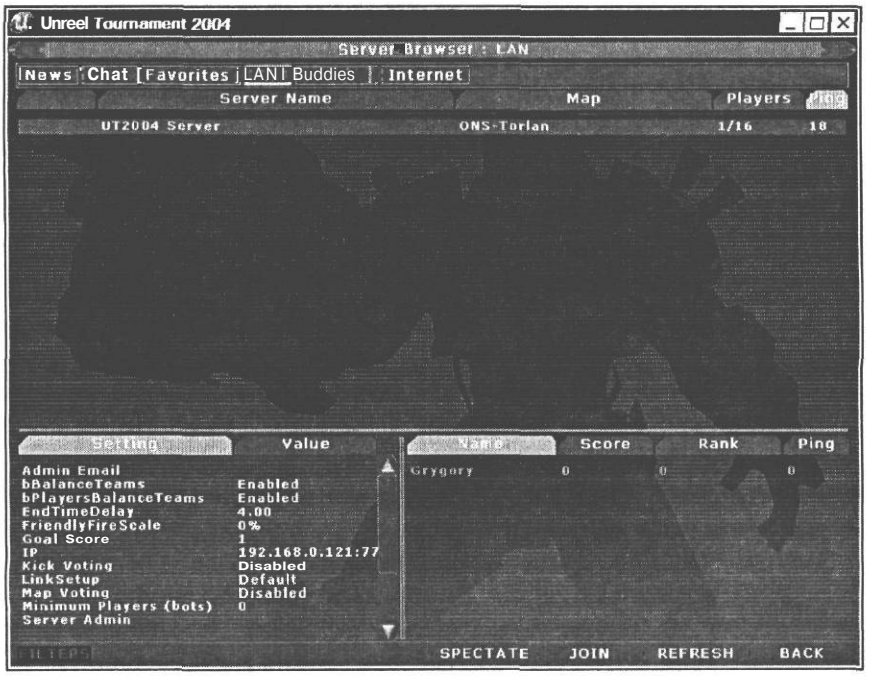



*Рис. 7.4. Вкладка LAN (Локальная сеть) для выбора игрового сервера в локальной сети*

В нижней части рабочего окна программы приводятся параметры сервера (Settings) и их значения (Value), а также имена уже присоединившихся игроков и их результаты (Score). Теперь, чтобы вступить в игру, достаточно нажать кнопку Join (Присоединиться).

# Windows NetMeeting

Для организации чата (общения с помощью клавиатуры), голосовой и видеосвязи между компьютерами локальной сети наилучшим образом подходит программа Windows NetMeeting. Впрочем эта программа позволит общаться не только внутри сети, но также и со всеми другими пользователями, компьютеры которых подключены к Интернету.

NetMeeting позволяет связываться и разговаривать с собеседником, видеть его изображение на экране своего компьютера, в реальном времени обмениваться текстовыми сообщениями, печатая их на клавиатуре, пересылать файлы, совместно работать с прикладными программами.

Для обеспечения звуковой связи компьютер должен быть оснащен звуковой картой, акустическими системами или наушниками и микрофоном. Для передачи видеоизображений компьютер должен быть оборудован платой видеосъемки с камерой либо видеокамерой, подключенной к параллельному порту (порту принтера) или к порту USB. На некоторых компьютерах с процессором менее мощным, чем Pentium, видеоизображение может не передаваться.

Камеры с платами для видеосъемки менее требовательны к вычислительным ресурсам по сравнению с камерами, которые подключаются непосредственно к параллельному порту компьютера. Цветной камерой, которая подключается к параллельному порту, желательно оборудовать компьютеры с процессорами Pentium 133 или более мощными.

В звуковой и видеосвязи одновременно могут участвовать только два пользователя. Компьютер должен быть достаточно быстрым. Аналогичным требованиям должен соответствовать компьютер вашего собеседника. Если требуется осуществлять связь с пользователем за пределами локальной сети, то подключение к Интернету должно быть на высокой скорости. Наилучшая работа NetMeeting обеспечивается на быстрых соединениях Интернета (модем со скоростью передачи данных 56 килобайт в секунду или выше, либо в локальной сети).

Программа NetMeeting включена во все версии операционной системы Windows и устанавливается по умолчанию при стандартной установке Windows.

В Windows 98 программа NetMeeting запускается из главного меню командой Программы * **Internet Explorer + Microsoft NetMeeting** (Programs ◆ Internet Explorer • Microsoft NetMeeting) или командой **Программы ◆ Microsoft NetMeeting** (Programs ◆ Microsoft NetMeeting).

В Windows 2000 запуск Microsoft NetMeeting осуществляется командой Программы * **Стандартные ◆ Связь ◆ NetMeeting** (Programs ◆ Accessories * Communications ◆ NetMeeting).

Если команда для запуска NetMeeting отсутствует в меню, то следует установить программу с помощью **Мастера установки компонентов Windows** (Windows Components Wizard), который запускается кнопкой **Установка и удаление компонентов Window** (Add/Remove Windows Components) диалога **Установка и удаление программ** (Add/Remove Programs). Этот диалог запускается из **Панели управления** (Control Panel).

В Windows XP, хотя NetMeeting и устанавливается по умолчанию, команда его запуска в главном меню отсутствует. Отсутствует также возможность удаления программы и повторной установки в диалоге **Установка и удаление программ** (Add/Remove Program). Для запуска NetMeeting в Windows XP следует использовать файл **conf.exe** из папки **Program Files\NetMeeting**.

Здесь мы рассмотрим версию Windows NetMeeting 3.01, которая входит в состав операционной системы Windows 2000/XP.

Обновленную версию программы Windows NetMeeting можно загрузить с сайта Microsoft по адресу: **http://www.microsoft.com/windows/netmeeting/**.

## Первый запуск и настройка Microsoft NetMeeting

При первом запуске NetMeeting на экране появляется Мастер начальной настройки **NetMeeting** (Рис. 7.5), который позволяет быстро собрать всю необходимую для работы программы информацию и настроить имеющееся оборудование.

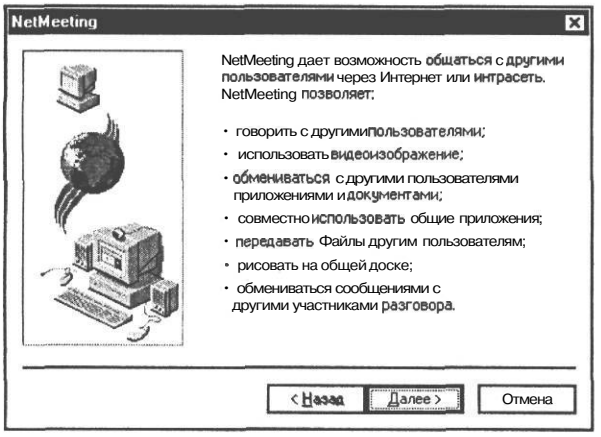



*Рис. 7.5. Первый диалог Мастера начальной настройки NetMeeting*

При последующих запусках программы этот Мастер появляться не будет, но вы сможете изменить все настройки в самой программе.

После нажатия кнопки Далее (Next) откроется следующий диалог Мастера настройки (Рис. 7.6).


*Рис. 7.6. Второй диалог Мастера начальной настройки **NetMeeting***

Здесь необходимо ввести личную информацию: Имя (First name), **Фамилию** (Last name), адрес **Электронной почты** (E-mail address), **Размещение** (Locations), **Комментарий** (Comments). Эти сведения необходимы для регистрации на сервере каталогов в Интернете, чтобы другие пользователи могли найти вас. Заполнение первых трех полей является обязательным. Если предполагается общение с иностранными пользователями, то информацию следует ввести на английском языке.

Для работы только в локальной сети эти сведения не требуются. Однако программа не будет работать, если вы не заполните первые три поля.

➤ Введите в первые три поля ввода информацию о себе.

> Нажмите кнопку **Далее** (Next), чтобы перейти к следующему диалогу Мастера настройки (Рис. 7.7).


*Рис. 7.7. Третий диалог Мастера начальной настройки* ***NetMeeting***

В этом диалоге можно включить режим автоматического подключения к серверу каталогов при запуске NetMeeting. В этом случае вы сможете связаться с любым пользователем, подключенным к этому серверу и зарегистрированным на нем. Данный режим необходим только в том случае, если вы планируете связываться с другими пользователями за пределами локальной сети.

> Сбросьте флажок **Подключаться к серверу каталогов при запуске** (Log on to a directory server when NetMeeting starts).

При установленном флажке Не **регистрироваться на сервере каталога** (Do not list my name in the directory) программа не зарегистрирует вас на сервере, и другие пользователи не смогут вас вызвать. Чтобы другие пользователи сервера каталога видели вас в списке, этот флажок следует сбросить.

➤ Нажмите кнопку **Далее** (Next). Появится следующий диалог Мастера настройки (Рис. 7.8), в котором следует выбрать скорость передачи данных для вызовов NetMeeting.

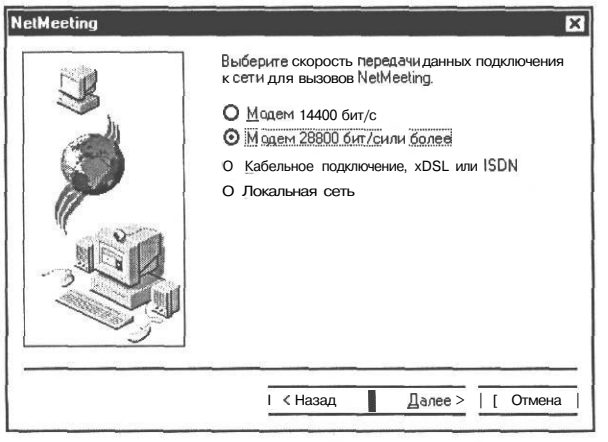



*Рис. 7.8. Четвертый диалог Мастера начальной настройки* ***NetMeeting***

В зависимости от используемого вида связи скорость передачи данных будет различной. Для обеспечения оптимального режима работы следует указать способ соединения.

> Установите переключатель **Локальная сеть** (Local Area Network), так как мы предполагаем осуществлять связь в локальной сети.

➤ Нажмите кнопку **Далее** (Next). Откроется пятый диалог Мастера настройки (Рис. 7.9).

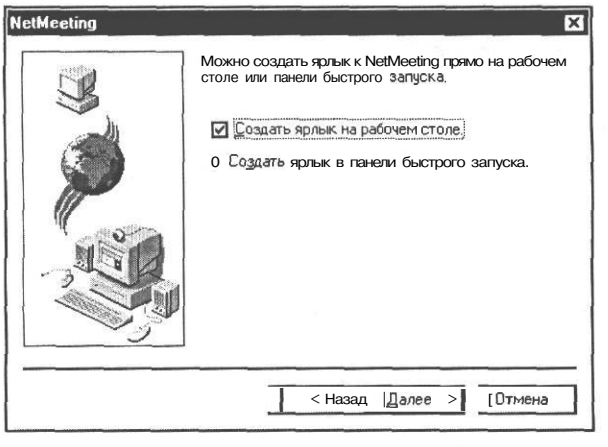



*Рис. 7.9. Пятый диалог Мастера начальной настройки* ***NetMeeting***

В этом диалоге Мастер настройки предлагает создать ярлыки для запуска программы на рабочем столе (Put a shortcut to NetMeeting on my desktop) и на панели быстрого запуска (Put a shortcut to NetMeeting on my Quick Launch bar). Это особенно актуально в Windows XP, в главном меню которого команда запуска NetMeeting отсутствует.

> Убедитесь, что установлены флажки **Создать ярлык на рабочем столе** (Put a shortcut to NetMeeting on my desktop) и **Создать ярлык в панели быстрого запуска** (Put a shortcut to NetMeeting on my Quick Launch bar) и нажмите кнопку **Далее** (Next). Появится диалог **Мастер настройки звука** (Audio Tuning Wizard) (Рис. 7.10).


*Рис. 7.10. Первый диалог* ***Мастер настройки звука*** *(Audio Tuning Wizard)*

Данный диалог сообщает о предстоящем тестировании звукового оборудования и необходимости закрыть все звуковоспроизводящие и записывающие программы. Если на компьютере не установлена звуковая карта, то проверка аудиосистемы будет пропущена.

> Нажмите кнопку **Далее** (Next), чтобы перейти к следующему диалогу **Мастер настройки звука** (Audio Tuning Wizard) (Рис. 7.11), в котором осуществляется тестирование воспроизведения звука.

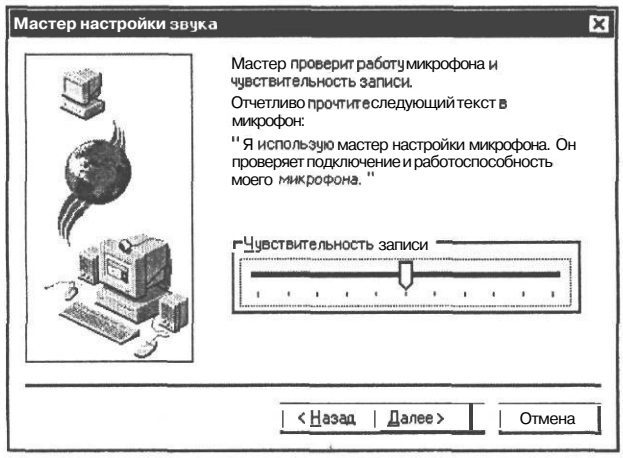

*Рис. 7.11. Диалог* ***Мастер настройки звука*** *(Audio Tuning Wizard) для регулировки уровня воспроизведения*

Перед проверкой необходимо включить громкоговорители или наушники и с помощью аппаратных регуляторов установить оптимальную громкость.

> Нажмите кнопку **Проверка** (Test). Вы услышите звуковой сигнал. С помощью ползункового регулятора **Громкость** (Volume) установите требуемую громкость воспроизведения. Чтобы закончить тестирование, нажмите кнопку **Остановить** (Stop).

Если звук отсутствует вообще, то проверьте, включены ли акустические системы и установлены ли драйверы звуковой карты.

> Нажмите кнопку Далее (Next). Откроется следующий диалог Мастер настройки звука (Audio Tuning Wizard) (Рис. 7.12) для настройки чувствительности микрофона.




*Рис, 7.12. Диалог Мастер настройки звука (Audio Tuning Wizard) для регулировки чувствительности микрофона*

Если микрофон не подключен, этот диалог будет пропущен.

> Убедитесь, что микрофон включен, и произнесите несколько фраз в микрофон. Можно использовать тот текст, который вы видите в диалоге. Мастер попытается автоматически настроить уровень сигнала.

> Нажмите кнопку Далее (Next). Если микрофон не был включен, появится диалог с сообщением о неудавшейся настройке (Рис. 7.13). В этом случае следует проверить подключение микрофона, после чего повторить попытку.


*Рис. 7.13. Диалог Мастер настройки звука (Audio Tuning Wizard) с сообщением о неудачной настройке*

Если же настройка прошла успешно, то появится последний диалог **Мастер настройки звука** (Audio Tuning Wizard) (Рис. 7.14) с сообщением об успешном завершении настройки.

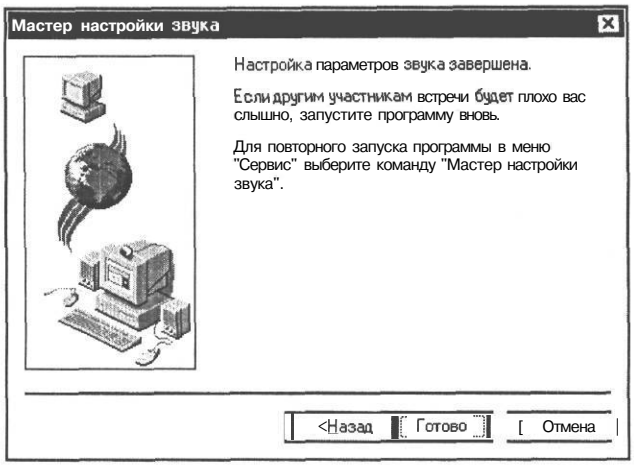



*Рис. 7.14. Диалог **Мастер настройки звука** (Audio Tuning Wizard) с сообщением о завершении настроек*

> Закройте этот диалог нажатием кнопки **Готово** (Finish).

Работа Мастера настройки завершится, и на экране появится рабочее окно программы **NetMeeting** (Рис. 7.15).

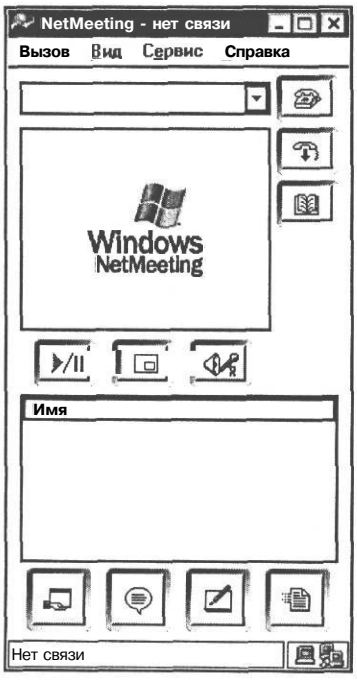



*Рис. 7.15. Рабочее окно программы **NetMeeting***

## Рабочее окно NetMeeting

В верхней части рабочего окна находится меню, включающее команды **Вызов** (Call), Вид (View), **Сервис** (Tools), **Справка** (Help). Под меню располагается открывающийся список для ввода или выбора адреса вызываемого пользователя. Справа от открывающегося списка вы видите три кнопки:

- **Вызвать** (Place Call) - для отправки вызова абонентам;
- **Конец вызова** (End Call) - для завершения связи;
- **Поиск пользователя в каталоге** (Find Someone in a Directory) - для поиска контактов в каталоге.

Здесь и далее текст справа от кнопок - это всплывающая подсказка, которая появляется на экране при установке указателя мыши на данном элементе управления.

Под открывающимся списком для выбора адреса расположено окно просмотра видео с логотипом Windows NetMeeting, в котором вы увидите изображение с видеокамеры, подключенной к вашему компьютеру.

> Если видеокамера подключена, нажмите кнопку - **Включить видео** (Start Video), чтобы увидеть изображение.

Повторное нажатие этой кнопки выключит изображение.

Кнопка - **Картинка в картинке** (Picture-in-Picture) предназначена для включения режима, при котором вы будете видеть оба изображения - принимаемое и передаваемое.

С помощью кнопки - **Настройка громкости звука** (Adjust Audio Volume) вы можете настроить чувствительность микрофона и громкость динамиков. При ее нажатии в рабочем окне **NetMeeting** появляются соответствующие элементы управления (Рис. 7.16).

В этом режиме вместо кнопки - **Настройка громкости звука** (Adjust Audio Volume) появляется кнопка Б - **Вывод списка участников** (View Participant List). Когда вы ее нажмете, вы возвратитесь в режим по умолчанию, при котором в нижней части диалога присутствует поле списка Имя (Name) (Рис. 7.15) для отображения перечня участников встречи.

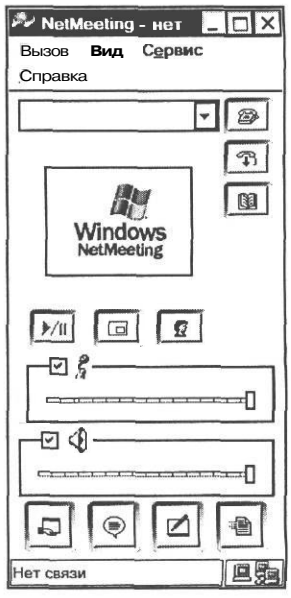



*Рис. 7.16. Элементы управления для настройки звука*

Под полем списка вы видите четыре кнопки, открывающие доступ к специальным функциям программы:

- **Общие приложения** (Share Program) - для совместной работы с программами;
- **Разговор** (Chat) - для передачи и приема сообщений в режиме чата;
- **Доска** (Whiteboard) - специальное окно, в котором участники встречи могут вводить текст и рисовать;

- **Передача файлов** (Transfer Files) - для передачи файлов участникам встречи.

В строке состояния у нижнего края окна **NetMeeting** обычно отображается текстовая информация о назначении команд меню, текущем режиме работы и значки, сообщающие о состоянии вызова. Пока соединение с Интернетом или в локальной сети не устанавливалось, в левой части строки состояния выводится сообщение: Нет **связи** (Not in a call). На это же указывает значок - Нет **связи** (Not in a call) в правой части этой строки. Значок - **Нет регистрации** (Not logged on) сообщает об отсутствии регистрации в каталоге.

## Настройка видео

Прежде чем вызывать абонента, желательно познакомиться с настройками свойств передаваемого и принимаемого изображения. Это выполняется на вкладке Видео (Video) диалога **Параметры** (Options) (Рис. 7.17), который появляется при выборе команды меню **Сервис** ◆ **Параметры** (Tools • Options).

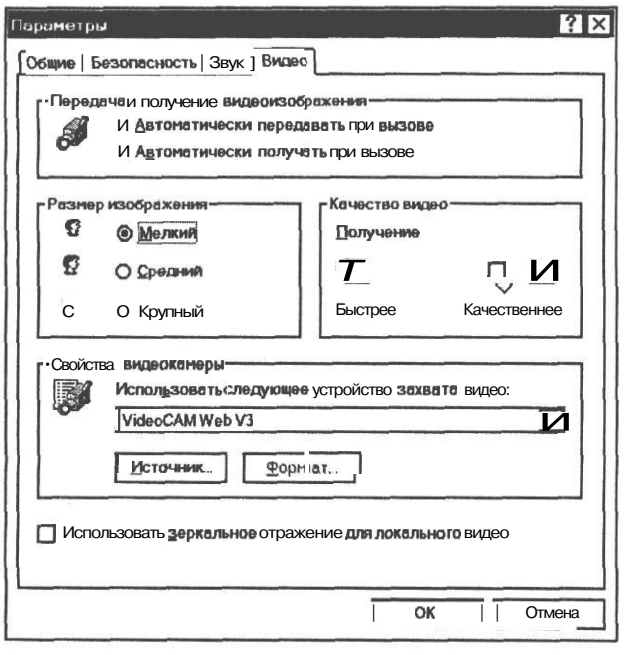



*Рис. 7.17. Вкладка **Видео** (Video) диалога **Параметры** (Options)*

При установленных флажках **Автоматически передавать при вызове** (Automatically send video at the start of each call) и **Автоматически получать при вызове** (Automatically receive video at the start of each call) программа будет соответственно передавать и получать изображение, если в рабочем окне NetMeeting нажата кнопка | М | - **Включить видео** (Start Video).

С помощью переключателей **Размер изображения** (Send image size) можно выбрать один из трех вариантов размера передаваемого видео: Мелкий (Small), **Средний** (Medium), **Крупный** (Large).

Для настройки получаемого изображения воспользуйтесь ползунковым регулятором Качество видео. Получение (Video quality. I prefer to receive). Он регулирует степень сжатия и частоту кадров принимаемого изображения. Перемещение ползункового регулятора влево, в сторону Быстрее (Faster video) повышает степень сжатия и увеличивает число кадров. Скорость движения в изображении увеличится, но качество картинки снизится. Перемещение ползункового регулятора вправо, в сторону Качественнее (Better quality) понизит степень сжатия и уменьшит число кадров. Качество изображения улучшится, но движение будет выглядеть как замедленное (возможна потеря кадров).

В открывающемся списке Использовать следующее устройство захвата видео (The video capture device I want to use is) приводится перечень всех устройств ввода видео, обнаруженных программой. Если у вас несколько устройств, то следует выбрать то, которое будет использоваться. Для настройки параметров камеры следует нажать кнопку Источник (Source). Диалог, который появится, зависит от модели камеры и поставляется вместе с камерой. Обычно в нем можно отрегулировать яркость, контрастность, оттенок, насыщенность, четкость, баланс белого, яркость средних тонов, настроить выдержку, диафрагму, фокус, увеличение и другие параметры. Кнопка Источник (Source) доступна только в режиме приема изображения. Если эта кнопка не доступна, то будет доступна кнопка Формат (Format) для настройки основных свойств изображения.

Установка флажка Использовать зеркальное отражение для локального видео (Show mirror image in preview video window) позволяет отразить получаемое изображение по горизонтали. Если включено отражение, левая и правая стороны меняются местами. Значение этого параметра не влияет на вид изображения на компьютерах других пользователей и на вид получаемых от них изображений.

С помощью команд Сервис ◆ Видео * Размер окна (Tools ◆ Video ◆ Window Size) вы можете установить размер окна с видеоизображением **100%**, 200%, 300% и 400%.

## Вызов собеседника в локальной сети

Чтобы связаться с пользователем локальной сети необходимо знать имя его компьютера.

В Windows 98 узнать имена всех компьютеров локальной сети можно, открыв окно папки Сетевое окружение (Network).

В Windows XP выяснить имена компьютеров в сети можно, открыв окно рабочей группы, доступ к которому осуществляется из окна Сетевое окружение (Network). Подробно об этом описано в главе «Создание локальной сети дома и в офисе».

С помощью программы NetMeeting связаться с любым пользователем локальной сети чрезвычайно просто.

- В поле открывающегося списка адресов в рабочем окне NetMeeting введите имя вызываемого компьютера.
- Нажмите кнопку – Вызвать (Place Call). NetMeeting попытается установить связь с указанным компьютером.

На вашем экране появится окно с сообщением об этом (Рис. 7.18). Вы можете нажать кнопку Отмена (Cancel), чтобы отменить вызов.

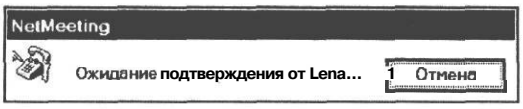



*Рис. 7.18. Окно с сообщением об ожидании подключения*

Если вызываемый абонент отклонит ваш вызов, то вы увидите соответствующее сообщение (Рис. 7.19).

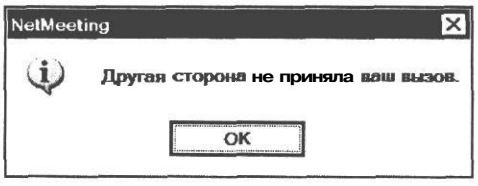



*Рис. 7.19. Сообщение об отклонении вызова*

Пользователь вызываемого компьютера услышит в своих динамиках телефонный звонок вызова, и на его экране появится диалог с сообщением о вызове. Если он примет ваш вызов, то связь будет установлена и вы сможете разговаривать друг с другом. В левой части строки состояния появится сообщение На связи (In a call). Об этом же будет сообщать значок - На связи (In a call) в правой части строки состояния. В поле списка Имя (Name) вы увидите имена пользователей, участвующих во встрече (Рис. 7.20).


*Рис. 7.20. Связь установлена*

Если к компьютеру вызванного пользователя подключена видеокамера, то вы увидите изображение с нее в окне программы, там, где прежде выводилось изображение с вашей

камеры (Рис. 7.20). Чтобы видеть изображение со своей камеры в отдельном окне, следует выбрать команду меню **Вид ◆ Локальное видео (новое окно)** (View ◆ My Video (New Window)) (Рис. 7.21).


*Рис. 7.21. Окно Локальное видео (My Video)*

Можно также, нажав кнопку [ ] - Картинка в картинке (Picture-in-Picture) или выбрав команду меню Вид ◆ Картинка в картинке (View ◆ Picture-in-Picture), включить режим, при котором в рабочем окне NetMeeting вы будете видеть изображения с обеих камер (Рис. 7.22).


*Рис. 7.22. Режим «картинка в картинке»*

Если изображение просматривается до начала вызова, то по умолчанию оно будет автоматически отправлено сразу же после установки соединения. Чтобы выключить автоматическую передачу изображения, выберите команду меню **Сервис ◆ Видео ◆ Передавать** (Tools ◆ Video ◆ Send). Повторный выбор команды снова включит режим передачи.

По умолчанию программа также автоматически принимает изображение. С помощью команды **Сервис * Видео ◆ Получать** (Tools ◆ Video ◆ Receive) вы можете выключить автоматический прием изображения.

Во время разговора вы можете регулировать громкость входного и выходного сигнала с помощью ползунковых регуляторов, которые появятся, если нажать кнопку | | - **Настройка громкости звука** (Adjust Audio Volume) (Рис. 7.16).

Чтобы прервать встречу, нажмите **кнопку** | | - **Конец вызова** (End Call).

## Прием вызова

Когда один из пользователей локальной сети пошлет вам вызов, вы услышите в динамиках телефонный звонок, а на экране появится диалог **NetMeeting - входящий вызов** (NetMeeting) (Рис. 7.23) с сообщением о входящем вызове. Вы можете либо отклонить его, нажав кнопку **Отказать** (Ignore), либо принять, нажав кнопку Принять (Accept). При поступлении безопасного вызова отображается также кнопка **Сведения** (Details). Воспользуйтесь ей для просмотра сведений о типе защиты и о сертификате. О безопасных вызовах читайте ниже.

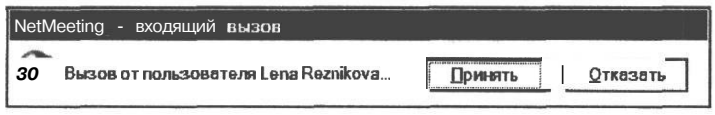



*Рис. 7.23. Диалог **NetMeeting - входящий вызов** (NetMeeting)*

Вы можете также включить режим автоматического приема вызовов, выбрав команду меню **Вызов ◆ Автоматически принимать вызовы** (Call ◆ Automatically Accept Calls). В этом случае все вызывающие вас пользователи будут подключаться к вашему компьютеру автоматически. Для отмены данного режима следует повторно выбрать указанную команду.

Если вы слишком заняты и не можете отвечать на вызовы, выберите команду меню **Вызов * Не беспокоить** (Call ◆ Do Not Disturb). В таком случае программа будет автоматически отклонять все входящие вызовы. Выключить данный режим можно повторным выбором этой команды.

## Способы вызова абонентов за пределами локальной сети

С помощью NetMeeting можно вызывать абонентов не только в локальной сети, но также в Интернете либо непосредственно через модемное подключение. Установка программного обеспечения NetMeeting на компьютере вызываемого абонента не обязательно. Такие вызовы могут принимать многие программы, поддерживающие общепринятые стандарты обмена данными.

Для отправки вызова за пределы локальной сети следует в поле открывающегося списка для ввода или выбора адреса ввести один из следующих адресов:

- IP-адрес компьютера;
- адрес сервера каталога и электронной почты;
- номер телефона.

После ввода адреса необходимо нажать кнопку [ ] - **Вызвать** (Place Call).

Если это возможно, способ вызова определяется автоматически. В противном случае на экран выводится диалог **Вызов** (Place A Call) (Рис. 7.24). Данный диалог можно открыть также, нажав кнопку [ ] - **Вызвать** (Place A Call), когда поле открывающегося списка адресов пустое.

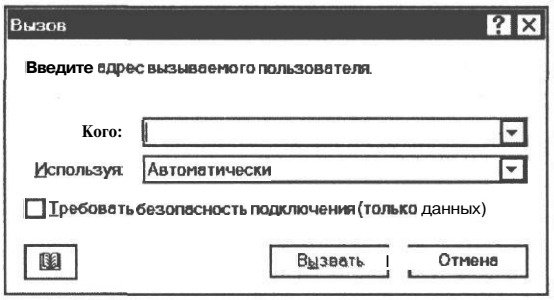



*Рис. 7.24. Диалог **Вызов** (Place A Call)*

В поле ввода **Кого** (To) указывается имя вызываемого компьютера.

В открывающемся списке **Используя** (Using) следует выбрать нужный тип подключения. Набор элементов в нем может изменяться в зависимости от установленных служб.

**Если установить флажок Требовать безопасность подключения (только данных)** (Require security for this call (data only)), то данный вызов будет безопасным. При этом NetMeeting будет шифровать все данные, отправляемые или получаемые с помощью программ Разговор (Chat), Доска (Whiteboard), общих программ или в файлах, которыми обмениваются участники. В безопасных вызовах недоступны средства передачи звука и изображений, поскольку NetMeeting не поддерживает их шифрование. Во время встречи не могут совместно использоваться безопасные и небезопасные вызовы. Все вызовы должны быть одного типа. Если возможность размещения безопасных вызовов отсутствует, данный флажок недоступен.

Если обеспечение безопасности построено на последовательных вызовах, для отправки вызова следует пользоваться кнопкой [ ] – **Вызвать** (Place Call), а не адресной строкой или ярлыком. При вызове через открывающийся список адресов или через ярлык диалог **Вызов** (Place A Call) с флажком **Требовать безопасность подключения (только данных)** (Require security for this call (data only)) не отображается.

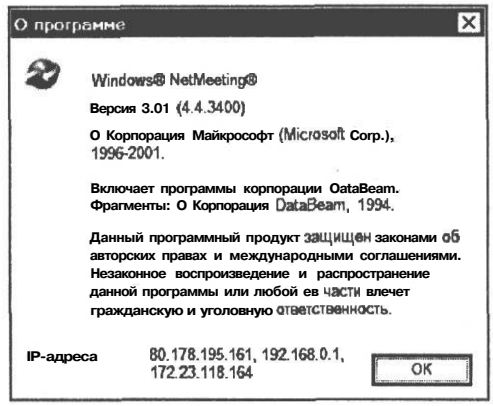



*Рис. 7.26. Диалог О программе (About Windows NetMeeting)*

Если в диалоге указано несколько адресов, то следует использовать первый.

Если на компьютере не установлена программа Winsock 2, IP-адрес в диалоге О программе (About Windows NetMeeting) не отображается. В таком случае он может быть определен следующим способом.

- Нажмите кнопку Пуск (Start) на Панели задач (Taskbar) и в появившемся главном меню Windows выберите команду Программы • Стандартные * Командная строка (Programs ◆ Accessories ◆ Command Prompt). Появится окно Командная строка (Command Prompt).
- В окне Командная строка (Command Prompt) при установленной связи с провайдером Интернета введите команду ipconfig и нажмите клавишу Enter. Вы получите IP-адреса всех сетевых адаптеров (Рис. 7.27).

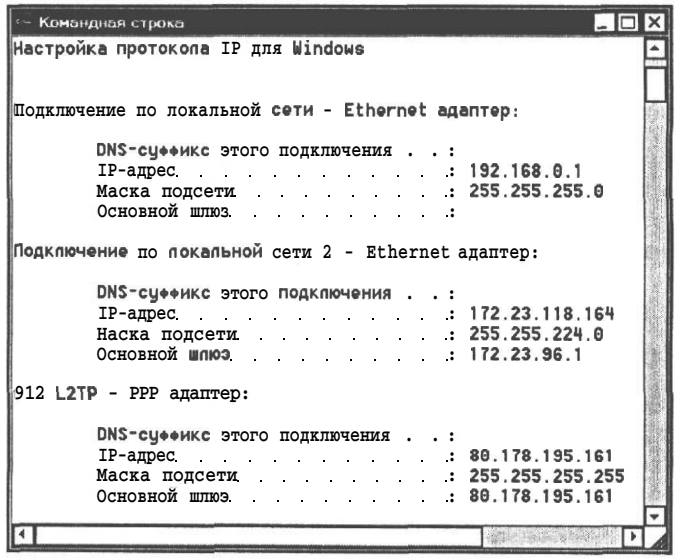



*Рис. 7.27. Определение IP-адреса текущего подключения*

В данном случае нас интересует PPP-адаптер. В этом примере строка **IP-адрес** для PPP-адаптера указывает: **80.178.195.161**.

Полученный таким образом IP-адрес текущего сеанса подключения к Интернету вам следует немедленно сообщить своему абоненту одним из способов быстрой связи и ждать его вызова по NetMeeting, не прерывая текущего сеанса подключения к Интернету.

Описанными способами можно определить IP-адрес компьютера в локальной сети и с его помощью осуществлять вызов. Напомним, что в нашем случае он имеет вид 192.168.0.*.

## Вызов с помощью каталога Интернета Microsoft

Каталог Интернета корпорации Microsoft (Microsoft Internet Directory) предоставляет возможность поддержки программой NetMeeting службы Messenger сети MSN (служба мгновенной доставки сообщений), которая сообщает, когда ваши друзья, коллеги или родственники находятся на связи.

Люди, которых вы добавили в список контактов службы Messenger сети MSN, появляются в качестве контактов в каталоге Интернета Microsoft в программе NetMeeting.

Каталог Интернета Microsoft позволяет увидеть людей, находящихся на связи и доступных для мгновенного подключения, как с помощью службы Messenger сети MSN, так и с помощью NetMeeting. Имеется также возможность выполнить вызов для своих контактов непосредственно из службы Messenger сети MSN.

Каталог Интернета Microsoft открывается нажатием кнопки | \ - **Поиск пользователя в каталоге** (Find Someone in a Directory). В нем содержатся контакты, которые вы добавили в список контактов службы Messenger сети MSN. Контактами называются другие пользователи, у которых имеются учетные записи Hotmail. Вызовы NetMeeting для контактов Hotmail могут отправляться из службы Messenger сети MSN или из каталога Интернета Microsoft.

Если вы еще не создали контакты, то сделайте это следующим образом.

> Нажмите кнопку | \ - **Поиск пользователя в каталоге** (Find Someone in a Directory). Появится диалог **Поиск пользователя** (Find Someone) (Рис. 7.28), в окне которого содержится ссылка **Click here to download MSN Messenger** (Щелкните здесь для загрузки MSN Messenger) для загрузки программы MSN Messenger с сайта **http://messenger.msn.com/**.

> Щелкните мышью на указанной ссылке, чтобы выполнить загрузку.

➤ После загрузки и автоматической установки этой программы вам будет предложено создать учетную запись Hotmail на сайте **http://www.hotmail.com/.** Создайте учетную запись Hotmail, заполнив предложенную анкету.

x Далее будет предложено создать так называемый цифровой паспорт .NET, который необходим для входа в программу MSN Messenger. Создайте цифровой паспорт .NET, указав в анкете требуемые сведения.

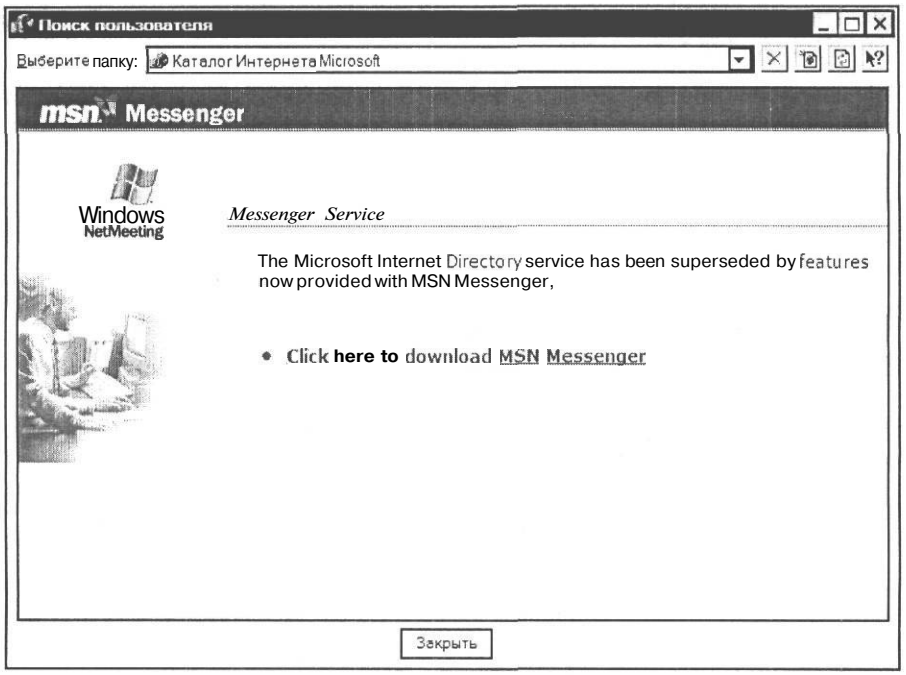



*Рис. 7.28. Диалог* ***Поиск пользователя*** *(Find Someone)*

После этого в программе MSN Messenger вы сможете создать контакты с людьми, имеющими такие же учетные записи Hotmail, воспользовавшись ссылкой **Добавить контакт** (Add Contact). Созданные контакты автоматически появятся в папке **Каталог Интернета Microsoft** (Microsoft Internet Directory) диалог **Поиск пользователя** (Find Someone) программы NetMeeting, и вы сможете отправлять им вызов при условии, что у них также установлена служба Messenger сети MSN. Напомним, что диалог **Поиск пользователя** (Find Someone) в программе NetMeeting открывается кнопкой | | - **Поиск пользователя в каталоге** (Find Someone in a Directory). Можно также выбрать команду меню **Вызов** ◆ **Каталог** (Call ◆ Directory).

## Вызов через шлюз H.323

Windows NetMeeting поддерживает стандарт H.323 для аудио- и видеоконференций, а также стандарт T.120 для конференций с передачей данных. Поэтому с помощью NetMeeting можно отправлять и получать вызовы из приложений, в которых также поддерживаются эти стандарты. Используя соответствующие службы и оборудование независимых производителей, NetMeeting позволяет выполнять телефонные вызовы через шлюз H.323. Кроме того, обеспечивается возможность вызова устройств модулей для проведения конференций с подключением нескольких узлов (MCU), в которых реализован стандарт H.323.

Подключение к автоматической телефонной системе или к системе проведения видеоконференций может выполняться через компьютер со шлюзом H.323. Шлюз H.323 соединяет IP-сеть с коммутируемыми сетями. Правильное имя или IP-адрес шлюза можно узнать у системного администратора телефонии.

Настроить подключение к шлюзу H.323 нужно следующим образом.

x Выберите команду меню **Сервис * Параметры** (Tools ◆ Options).

x В появившемся диалоге **Параметры** (Options) на вкладке **Общие** (General) нажмите кнопку **Расширенный вызов** (Advanced Calling). Откроется диалог **Расширенные параметры вызова** (Advanced Calling Options) (Рис. 7.29).

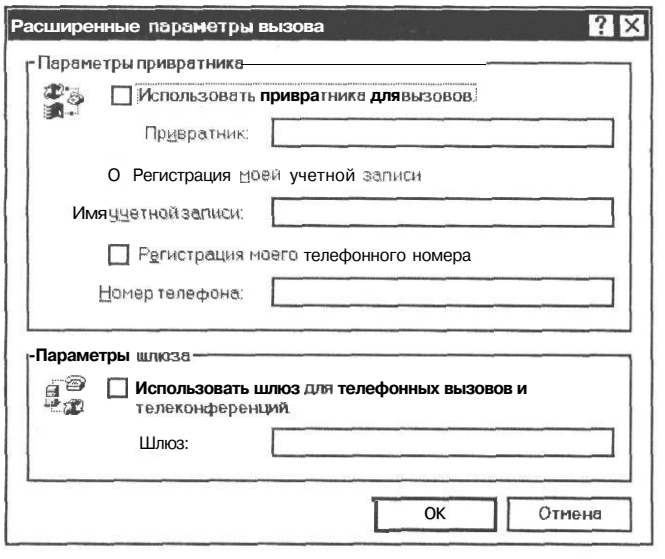



*Рис. 7.29. Диалог **Расширенные параметры вызова** (Advanced Calling Options)*

> В группе элементов управления **Параметры шлюза** (Gateway settings) установите флажок **Использовать шлюз для телефонных вызовов и телеконференций** (Use a gateway to call telephones and videoconferencing system).

x В поле ввода **Шлюз** (Gateway) укажите имя компьютера-шлюза.

x Закройте диалоги **Расширенные параметры вызова** (Advanced Calling Options) и **Параметры** (Options), нажав кнопку OK в каждом из них.

Для вызова через автоматическую телефонную систему выполните следующие действия.

x Выберите команду меню **Вид** ◆ **Номеронабиратель** (View ◆ Dial Pad). В рабочем окне NetMeeting появится цифровая клавиатура для набора номера (Рис. 7.30).

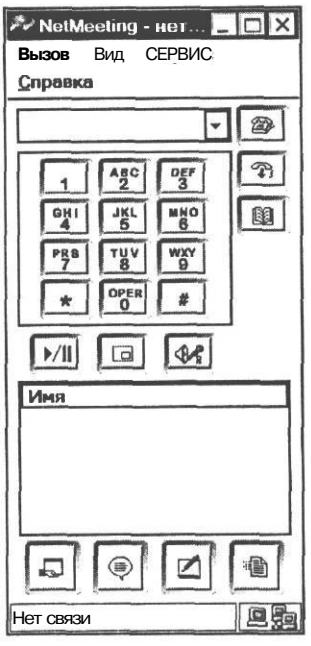



*Рис. 7,30. Номеронабиратель*

> Введите основной номер телефона с помощью кнопок номеронабирателя или с клавиатуры компьютера и нажмите кнопку [☎] – Вызвать (Place Call).

После ответа на вызов автоматической телефонной системы с помощью номеронабирателя можно ввести добавочный номер или выбрать нужный пункт телефонного меню. Добавочный номер и команды меню отправляются на телефонную систему по мере их ввода. После набора номера с помощью номеронабирателя повторно нажимать кнопку [☎] - Вызвать (Place Call) не следует. Буквы через номеронабиратель вводить нельзя.

## Вызов с помощью привратника H.323

Еще одна возможность телефонных вызовов через NetMeeting обеспечивается так называемыми привратниками H.323. Привратник - это сетевой компьютер, облегчающий установку соединения с другими пользователями и компьютерами. Привратник является центром всех звонков в своей зоне управления. Он выполняет следующие задачи: прием и отклонение вызовов, преобразование адресов электронной почты в сетевые адреса, управление допуском, контроль пропускной способности и функции управления зонами. Кроме того, привратник может управлять дозвоном, авторизировать звонки, управлять пропускной способностью и выполнять функции управления звонками.

Для использования привратника H.323 необходимо зарегистрироваться в этом привратнике, указав номер телефона или имя учетной записи. Регистрация в привратнике позволяет получать вызовы на данном компьютере. Если точно неизвестно, какой номер телефона и какую учетную запись необходимо использовать для регистрации в привратнике H.323, свяжитесь с администратором телефонии или поставщиком услуг.

Для настройки привратника следует в диалоге **Расширенные параметры вызова** (Advanced Calling Options) (Рис. 7.29) установить флажок **Использовать привратника для вызовов** (Use a gatekeeper to place calls) и в поле ввода **Привратник** (Gatekeeper) указать имя или IP-адрес компьютера-привратника. При вызове сервера конференций необходимо указать в этом поле имя управляющего модуля для подключений с несколькими узлами (MCU).

Если в подключении к привратнику в офисе или на предприятии используется адрес электронной почты или телефонный номер, установите флажок **Регистрация моей учетной записи** (Log on using my account name) или **Регистрация моего телефонного номера** (Log on using my phone number) и затем введите в соответствующее поле адрес или номер телефона.

## Передача вызовов по телефону

Вызовы по телефону могут передаваться в NetMeeting. При этом доступны только средства передачи звука и изображений. Такие возможности NetMeeting для конференций с передачей данных, как программы Разговор (Chat), Доска (Whiteboard), общий доступ к программам и передача файлов, недоступны. Для передачи вызовов по телефону необходимо использовать NetMeeting 3.1.

Для выполнения видеовызова по телефону обе стороны должны использовать модем V.80 для видеоконференций. При этом в меню **Вызов** (Call) появляется команда **Видеовызов по телефону** (Video Call by Phone). Для успешной передачи вызова необходимо, чтобы обе стороны включили режим **Видеовызов по телефону** (Video Call by Phone).

После начала передачи вызова в NetMeeting связь между сторонами невозможна, пока не завершена передача вызова. После передачи вызова в NetMeeting недоступны программы Разговор (Chat), Доска (Whiteboard), общий доступ к программам и передача файлов. Если используется видеовызов по телефону, в вызов не могут добавляться новые участники.

## Вызов с помощью команды Выполнить (Run)

В Windows имеется системная команда callto:, позволяющая выполнять вызовы NetMeeting, даже когда сама программа не запущена. Для ее использования следует нажать кнопку Пуск (Start) на Панели задач (Taskbar) и в появившемся главном меню Windows выбрать команду Выполнить (Run).

В поле открывающегося списка Открыть (Open) появившегося диалога Запуск программы (Run) (Рис. 7.31) можно ввести один из следующих вариантов вызова:

**callto:имя компьютера, например callto:Jon. Этот вариант используется в локальной сети;**

**callto:IP-адрес, например callto:80.178.151.169;**

**callto:имя сервера/адрес электронной почты,**

**например callto:ils2.microsoft.com/alex@hotmail.com**

**callto:адрес электронной почты, например callto:sono@mail.ru.**

Одного только адреса электронной почты будет достаточно в том случае, если оба абонента - вызывающий и вызываемый - подключены к одному и тому же серверу.

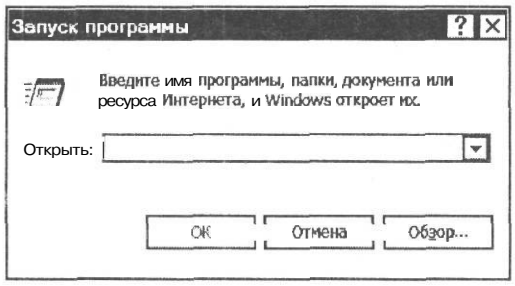



*Рис. 7.31. Диалог* ***Запуск программы*** *(Run)*

После ввода одного из указанных вариантов и нажатия кнопки **OK** будет запущена программа NetMeeting и выполнен вызов абонента.

## Как решить проблему неудачного подключения

Проблемы с подключением к удаленному компьютеру могут возникнуть из-за того, что вы или ваш собеседник используете брандмауэр или устройство трансляции сетевых адресов (NAT), которые не позволяют подключаться к Интернету напрямую. Если ваш поставщик услуг Интернета использует брандмауэр или устройство NAT, попытка подключиться может закончиться неудачей даже тогда, когда никто из вас не использует эти средства.

Если удаленному компьютеру не удается установить прямую связь с вашим компьютером, то, вероятнее всего, это связано с тем, что подключение защищено брандмауэром. Проще всего решить эту проблему можно, отключив брандмауэр на время сеанса связи. В Windows XP сделайте это следующим образом.

Убедитесь, что связь с провайдером Интернета не установлена.

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в главном меню Windows выберите команду **Подключение * Отобразить все подключения** (Connection ◆ Display All Connections). Откроется окно **Сетевые подключения** (Network Connections).
- Щелкните правой кнопкой мыши на значке того подключения, которое используется для установки связи с провайдером Интернета, и в появившемся контекстном меню выберите команду **Свойства** (Properties). Появится диалог **Свойства** (Properties) выбранного подключения.
- Перейдите на вкладку **Дополнительно** (Advanced) (Рис. 7.32).
- Сбросьте флажок **Защитить мое подключение к Интернету** (Protect my computer and network by limiting or preventing access to this computer from the Internet).
- Закройте диалог **Свойства** (Properties) нажав кнопку **OK.**

После этого при очередном сеансе связи с большой степенью вероятности вы сможете принять вызов от удаленного компьютера.

Не забудьте, завершив сеанс связи, снова включить брандмауэр.

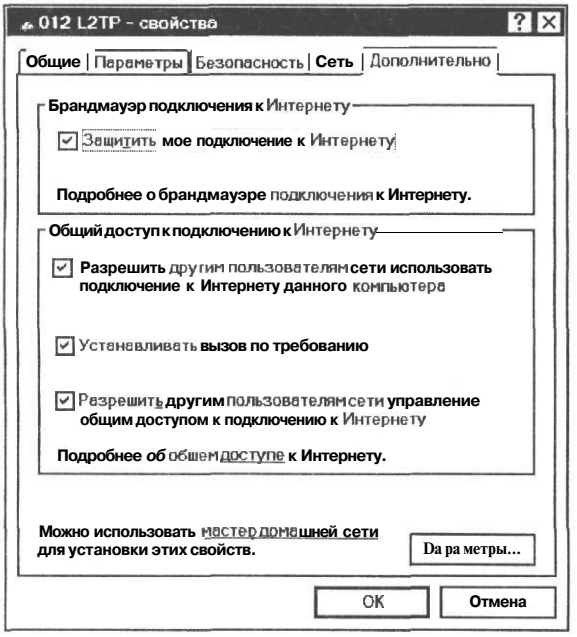



*Рис. 7,32. **Вкладка Дополнительно** (Advanced) диалога **Свойства** (Properties)*

## Создание ярлыков вызова

Чтобы облегчить и ускорить вызов абонентов, целесообразно использовать ярлыки вызова. Ярлык содержит информацию о том, кого и как следует вызвать. Это избавляет вас от необходимости каждый раз искать адрес вызываемого собеседника. Ярлыки вызова создаются следующим образом.

➤ Выберите команду меню **Вызов * Создать ярлык вызова** (Call ◆ Create SpeedDial). На экране появится диалог **Создать ярлык вызова** (Create SpeedDial) (Рис. 7.33).

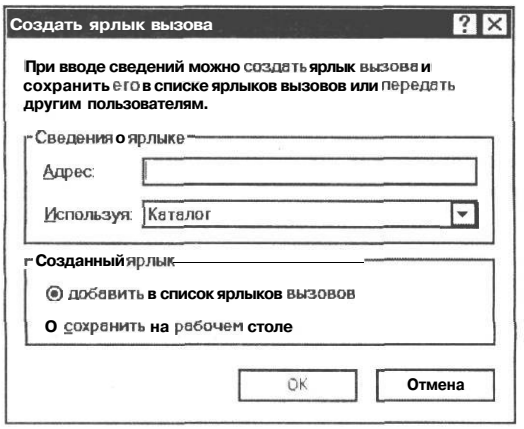



*Рис. 7.33. Диалог **Создать ярлык вызова** (Create SpeedDial)*

➤ В поле ввода Адрес (Address) введите адрес компьютера абонента.

Ярлыки могут создаваться для подключений к серверу каталогов и к сетевому серверу. В этом случае в качестве адреса введите имя сервера каталогов/адрес электронной почты, например **ils.microsoft.com/neofit@hotmail.com**. При добавлении пользователя того же сервера достаточно указать только адрес электронной почты.

Если используется протокол TCP/IP в локальной сети или в Интернете, необходимо указать имя компьютера или IP-адрес.

➤ В открывающемся списке Используя (Call using) укажите необходимый тип подключения.

При установленном переключателе добавить в список ярлыков вызовов (Add to SpeedDial list) ярлык будет помещен в папку Ярлык (Speed Dial) диалога Поиск пользователя (Find Someone). Там вы и сможете его найти. На жестком диске компьютера ярлыки по умолчанию сохраняются в папке **NetMeeting\SpeedDial**.

Если установить переключатель сохранить на рабочем столе (Save on the Desktop), ярлык вызова будет помещен на Рабочий стол (Desktop).

> Закройте диалог Создать ярлык вызова (Create SpeedDial) нажатием кнопки OK. Ярлык будет создан и помещен в папку Ярлык (Speed Dial).

Чтобы выполнить вызов с помощью ярлыка, выполните следующие шаги.

➤ В рабочем окне **NetMeeting** нажмите кнопку | | - Поиск пользователя в каталоге (Find Someone in a Directory).

➤ В открывающемся списке Выберите папку (Select a directory) появившегося диалога Поиск пользователя (Find Someone) откройте папку Ярлык (Speed Dial).

➤ Щелчком мыши выделите нужный ярлык.

> Нажмите кнопку Вызвать (Call). Программа установит связь с абонентом.

Если ярлык помещен на Рабочий стол (Desktop), то достаточно дважды щелкнуть мышью на нем. Откроется программа NetMeeting, если она не была запущена ранее, и абонент будет вызван.

## Организация и проведение встреч

Программа NetMeeting позволяет обмениваться информацией с друзьями и коллегами, совместно работать над проектами, вести обучение в группе, проводить презентации. Это реализуется с помощью встреч. В ходе встречи можно коллективно работать над созданием документов, таблиц и файлов, не устанавливая при этом соответствующие приложения на компьютеры всех ее участников. Кроме того, имеется возможность отправлять файлы одному или всем участникам встречи.

Для проведения встреч может использоваться как компьютер одного из ее участников, так и специальный сервер конференций. Организуя встречу, необходимо указывать ее имя, пароль, сведения о безопасности и возможных участниках. Если для проведения встречи

используется сервер конференций, можно подключиться к серверу и выбрать нужную встречу в списке. Если имя встречи не указано, можно воспользоваться именем, которое задано по умолчанию - Personal Conference (Личная конференция) или выбрать любое другое имя.

Организатор встречи может сделать ее безопасной, ограничить круг ее участников и определить, кто может рассылать приглашения на встречу. Он также выбирает средства, которые будут использоваться во время встречи, например, программы Доска (Whiteboard) и Разговор (Chat).

Безопасные вызовы, как уже отмечалось, поддерживают только передачу данных. В этих вызовах применяется шифрование данных, проверка подлинности и защита паролем. Звук и видеоизображения в NetMeeting не шифруются, однако при работе с этими средствами можно также пользоваться паролями.

Общение участников встречи обеспечивается программой Разговор (Chat), средствами передачи звука и видеоизображений. Для представления рисунков и графиков другим участникам можно пользоваться программой Доска (Whiteboard). Также существует возможность передачи файлов и подключения к удаленным компьютерам с помощью средств общего доступа к рабочему столу.

Для организации встречи выполните следующие действия.

➤ Выберите команду меню Вызов ◆ Начать встречу (Call ◆ Host Meeting). На экране появится диалог Начать встречу (Host a Meeting) (Рис. 7.34).

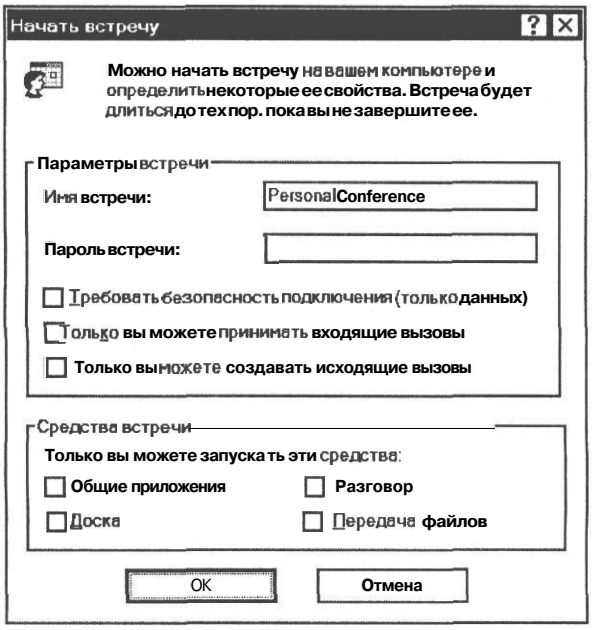



*Рис. 7.34. Диалог Начать встречу (Host a Meeting)*

➤ В поле ввода **Имя встречи** (Meeting Name) введите название встречи или оставьте указанное по умолчанию **Personal Conference** (Личная конференция).

x В поле **Пароль встречи** (Meeting Password) укажите пароль для встречи, если необходимо.

➤ Чтобы встреча была безопасной, установите флажок **Требовать безопасность подключения (только данных)** (Require security for this meeting (data only)). Напомним, что в безопасных встречах поддерживаются только вызовы с передачей данных.

Чтобы контролировать участников, которые будут подключаться к встрече, следует установить флажок **Только вы можете принимать входящие вызовы** (Only you can accept incoming calls).

Если необходимо запретить участникам встречи приглашать на нее посторонних, установите флажок **Только вы можете создавать исходящие вызовы** (Only you can place outgoing calls).

Выбор соответствующего варианта в группе флажков **Средства встречи** (Meeting Tools) позволит указать набор средств, которые могут применяться в ходе встречи. При проведении безопасной встречи средства передачи звука и изображений недоступны. Включение и отключение используемых средств может выполняться непосредственно по ходу встречи.

> Нажмите кнопку **OK,** чтобы начать встречу. Программа переключится в режим связи.

Сообщите участникам встречи о времени ее начала. Передайте им пароль и укажите, будет ли встреча безопасной.

Чтобы подключиться к встрече, участник, который получил приглашение, должен направить вызов в место проведения встречи или ее участнику. Если вызов участника встречи, который не является ее организатором, оказался неудачным, то следует направить вызов в место ее проведения.

По мере подключения участников их имена будут отображаться в поле списка Имя (Name). Обмен видеоизображениями и звуком возможен только с одним участником встречи.

Участие во встрече автоматически завершается после выхода из нее участника, с помощью которого было выполнено подключение к этой встрече. Таким образом, продолжительность участия во встрече в этом случае определяется временем участия в ней другого пользователя.

Организатор встречи может удалить любого ее участника, щелкнув правой кнопкой мыши на его имени в списке и выбрав команду контекстного меню **Удалить со встречи** (Remove from Meeting). Можно также нажать комбинацию клавиш Shift + F10.

Чтобы завершить встречу, достаточно нажать кнопку - **Конец вызова** (End Call).

## Чат

Поскольку передача изображений и звука возможны только между двумя участниками встречи, то при групповом общении особенно полезной оказывается программа Разговор (Chat). С ее помощью участники встречи могут беседовать друг с другом, посылая друг

другу текстовые сообщения. Эти сообщения отображаются в окне профаммы **Разговор** (Chat). Если вызов был передан в NetMeeting по телефону, то программа Разговор (Chat) не доступна.

➤ Чтобы отправлять и получать текстовые сообщения, в режиме связи нажмите кнопку – **Разговор** (Chat). На экране появится окно программы Разговор (Chat) (Рис. 7.35). Такое же окно увидят все участники встречи.


*Рис. 7.35. Окно программы* ***Разговор*** *(Chat)*

> В поле вода **Сообщение** (Message) введите текст для отправки.

➤ Чтобы отправить сообщение всем участникам встречи, в открывающемся списке **Отправить** (Send To) выберите **Всем собеседникам** (Everyone In Chat). Если вы хотите передать сообщение одному получателю, выберите в открывающемся списке **Отправить** (Send To) его имя.

➤ Нажмите кнопку – **Отправка сообщения** (Send Message) в окне программы **Разговор** (Chat). Можно также нажать клавишу Enter.

Передаваемые и получаемые сообщения будут отображаться в поле в верхней части окна **Разговор** (Chat).

С помощью команд меню Правка (Edit) фрагменты сообщений можно **Вырезать** (Cut), **Скопировать** (Copy) и **Вставить** (Paste), а также **Очистить все** (Clear All). Диалог участников встречи можно сохранить в текстовом файле командой меню **Файл * Сохранить** (File ◆ Save) и напечатать командой **Файл * Печать** (File ◆ Print).

Для завершения чата достаточно закрыть программу Разговор (Chat) командой меню **Файл * Выход** (File ◆ Exit).

Вы можете изменить шрифт, вид сообщений и отображаемые сведения. Эти настройки выполняются в диалоге **Параметры** (Options) (Рис. 7.36), который открывается командой **Вид ◆ Параметры** (View ◆ Options) из меню программы **Разговор** (Chat).

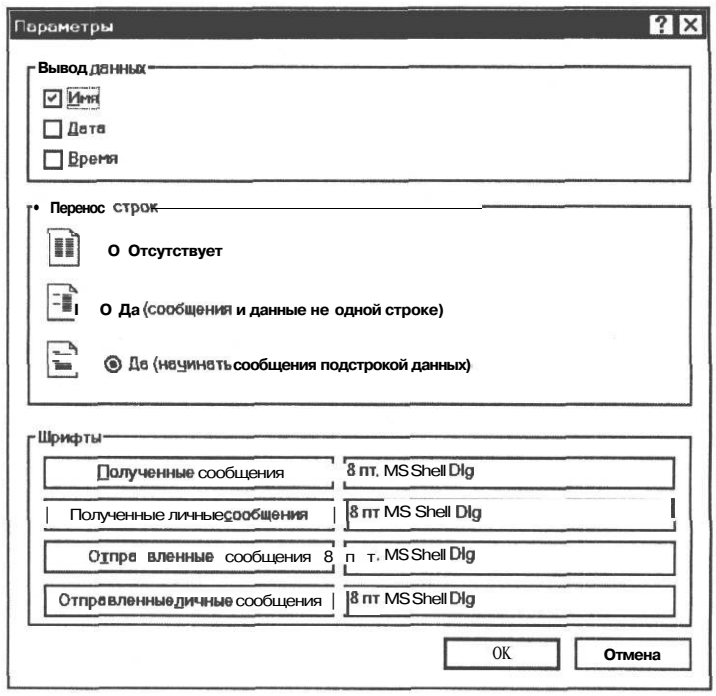



*Рис. 7.36. Диалог Параметры (Options) программы Разговор (Chat).*

Группа флажков Ввод данных (Information display) позволяет указать, какие сведения должны отображаться в месте с сообщениями: Имя (Person's name), Дата (Date), Время (Time).

Переключатели Перенос строк (Message format) определяют, как переносятся строки:

Отсутствует (Entire message is on one line) - сообщение может выводиться за пределами видимой области экрана. Для просмотра всего текста сообщения нужно будет пользоваться горизонтальной полосой прокрутки;

Да (сообщения и данные на одной строке) (Wrap (message appears next to information display));

Да (начинать сообщения под строкой данных) (Wrap (message appears below information display)).

Кнопки группы Шрифты (Fonts) дают возможность задать индивидуальный шрифт для получаемых, получаемых личных, отправляемых и отправляемых личных сообщений. Следует нажать соответствующую кнопку и в появившемся стандартном диалоге Шрифт (Font) сделать необходимые настройки. Название и размер выбранного шрифта отобразятся в поле справа от кнопки.

# Программа Доска

Участники встречи могут вводить текст и рисовать в окне программы Доска (Whiteboard). Эта программа позволяет добавлять и удалять страницы, рисовать фигуры, печатать текст, выделять различные элементы с помощью инструментов выделения.

Чтобы открыть программу Доска (Whiteboard) (Рис. 7.37), в режиме связи нажмите кнопку - **Доска** (Whiteboard) в окне NetMeeting. Программой можно пользоваться также как графическим редактором в автономном режиме, без связи с другими компьютерами.


*Рис. 7.37. Окно программы Доска (Whiteboard)*

Графические и текстовые объекты, созданные в программе Доска (Whiteboard) можно копировать в буфер обмена, а затем вставлять в другие программы. И наоборот, объекты из других приложений, окон, областей рабочего стола могут быть помещены в программу Доска (Whiteboard). Ее инструменты позволяют дополнить эти объекты необходимыми элементами оформления и примечаниями. Результаты проделанной работы будут видны другим участникам встречи, которые не имеют доступа к вашему рабочему столу.

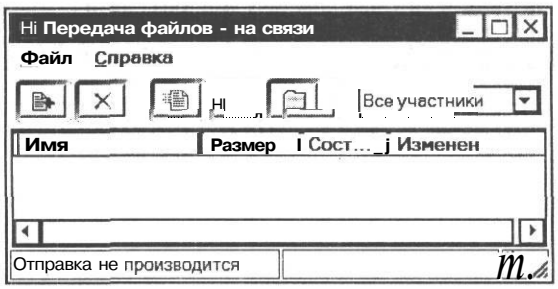
Синхронный режим работы, включенный по умолчанию, обеспечивает автоматическое отображение одинаковых страниц у всех участников встречи. Чтобы работать над страницей индивидуально, режим синхронизации можно отключить командой меню **Вид** * **Синхронизовать** (View ◆ Synchronize). При этом автоматически отображаться на компьютерах остальных участников страница не будет, ее можно будет открыть только вручную. Отмена режима синхронизации не изменяет вид текущей страницы на экранах других участников встречи.

Результат совместной работы с программой Доска (Whiteboard) можно сохранить командой меню **Файл** ◆ **Сохранить** (File ◆ Save). При сохранении используется собственный формат программы. Это значит, что открыть такой файл в других графических редакторах невозможно.

## Передача и прием файлов

Во время встречи вы можете передавать файлы другим участникам, а также получать файлы от них.

> В режиме связи нажмите кнопку | | - **Передача файлов** (Transfer Files) в нижней части окна NetMeeting. Откроется программа **Передача файлов** (File Transfer) (Рис. 7.38).




*Рир. 7.38. Окно программы **Передача файлов** (File Transfer)*

> В окне программы **Передача файлов** (File Transfer) нажмите кнопку | [ - **Добавить файлы** (Add Files) и в появившемся диалоге **Выбор файлов для отправки** (Select Files to Send) укажите файлы, которые хотите послать другим участникам встречи. Выбранные файлы появятся в окне программы **Передача файлов** (File Transfer).

➤ В открывающемся списке, справа от кнопок, укажите получателей - **Все участники** (Everyone) или выберите конкретного адресата.

Чтобы удалить файл из списка отправляемых, нажмите кнопку | X | - **Удалить файлы** (Remove Files).

➤ Нажмите кнопку | | - **Отправить все** (Send All).

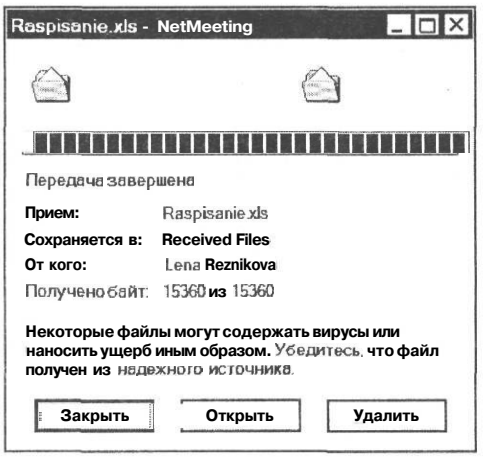
Если отправку файла требуется прервать, нажмите кнопку | **О** | - **Отменить передачу** (Stop Sending). Файл из списка может быть отправлен только один раз. Чтобы повторить отправку, повторно нажмите кнопку | \ - **Добавить файлы** (Add Files) и выберите файл еще раз.

Файл, который был создан при работе с общей программой, может быть отправлен только пользователем, установившим совместный доступ к этой программе.

При удаленном доступе к компьютеру на его рабочем столе, в правой части **Панели задач** (Taskbar) найдите значок - **NetMeeting.** Щелкните на этом значке и на появившейся панели быстрого доступа (Рис. 7.39) нажмите первую справа кнопку | | для отправки файлов. Этим способом можно вызывать и другие программы **NetMeeting.**

*Рис. 7.39. Панель быстрого доступа*

При получении файлов от других участников на экране появляется диалог с указанием имени полученного файла (Рис. 7.40). Прием выполняется автоматически.




*Рис, 7.40. Диалог получения файла*

После нажатия кнопки **Принять** (Open) этот диалог закроется. Если во время передачи файла кнопка **Принять** (Open) нажата не была, то после того, как файл получен, вместо этой кнопки отображается Закрыть (Close), которая закрывает диалог. Чтобы отказаться от получения файла, нажмите кнопку **Удалить** (Delete).

Полученный файл по умолчанию помещается в папку **NetMeeting\Received Files** на жестком диске компьютера. Вы можете просмотреть ее содержимое, нажав кнопку [C] - **Просмотр полученных файлов** (View received files) в окне программы **Передача файлов** (File Transfer).

## Совместная работа с приложениями

NetMeeting позволяет участникам встречи совместно работать с прикладными программами, просматривать файлы и редактировать их. Например, вы можете организовать коллективную работу над общим документом Microsoft Word. Документ можно открыть на компьютере и сделать его общим. Другие пользователи смогут вносить свои изменения непосредственно в сам документ. Причем необходимая для работы с документом программа должна быть установлена только на том компьютере, где был открыт общий документ. Установка этой программы на компьютерах других участников не требуется. Работать с общими приложениями могут все участники встречи, но поочередно. На рабочих столах общие приложения каждого из участников выводятся в отдельных окнах.

Организовать совместную работу с приложением можно следующим образом.

- В режиме связи запустите программу, которая должна использоваться совместно, например Microsoft Word, и откройте в ней нужный документ.

➤ Нажмите кнопку - **Общие приложения** (Share Program) в нижней части окна программы NetMeeting. Появится диалог **Общий доступ** (Sharing) (Рис. 7.41).

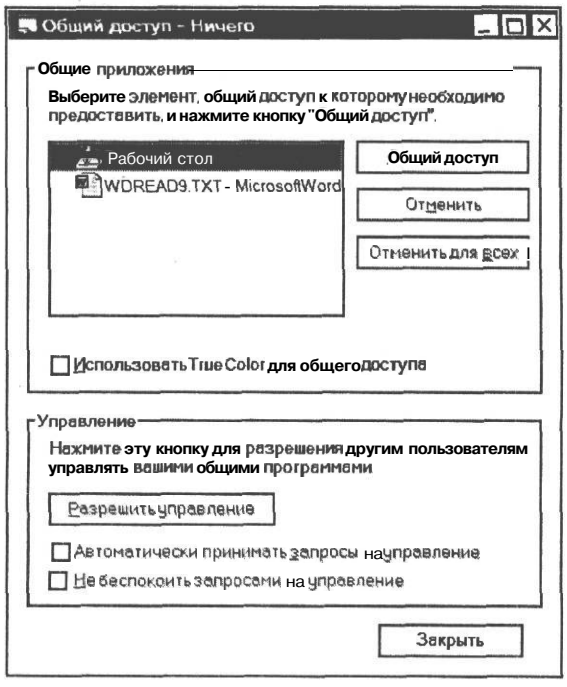



*Рис. 7.41. Диалог **Общий доступ** (Sharing)*

Чтобы вызвать этот диалог, можно также щелкнуть мышью на значке - **NetMeeting** в правой части **Панели задач** (Taskbar), и в появившейся панели быстрого доступа (Рис. 7.39) нажать первую слева кнопку - **Общие приложения** (Sharing).

В поле списка **Общие приложения** (Share Programs) приведен перечень запущенных программ, к которым может быть разрешен общий доступ участников встречи.

➤ Щелчком мыши выделите имя программы, которая должна стать общей.

Общий доступ может быть предоставлен одновременно к нескольким приложениям.

> Нажмите кнопку **Общий доступ** (Share), чтобы сделать программу доступной всем пользователям. В этот момент окно с общей программой появится на экранах всех участников встречи.

Установка флажка **Использовать True Color для общего доступа** (Share in true color) позволит использовать режим полноцветного отображения. Однако это нежелательно. Режим True Color может замедлить совместную работу с приложением, особенно при удаленных подключениях.

➤ Чтобы разрешить участникам встречи управление общей программой, в диалоге **Общий доступ** (Sharing) нажмите кнопку **Разрешить управление** (Allow Control).

➤ В главном окне NetMeeting щелкните правой кнопкой мыши на имени участника встречи, которому необходимо предоставить доступ к программе, и в появившемся контекстном меню выберите команду Предоставить управление (Grant Control).

После этого указанный участник встречи сможет управлять программой. Общая программа (Рис. 7.42) не может управляться сразу несколькими пользователями. Пометка управляемое (controllable) в заголовке окна общей программы на экранах участников встречи означает, что управление осуществляется пользователем, который разрешил общий доступ к программе. Пометка управляемое (**имя_участника**) (controlled by ...) означает, что управление осуществляется пользователем, имя которого указано в заголовке.

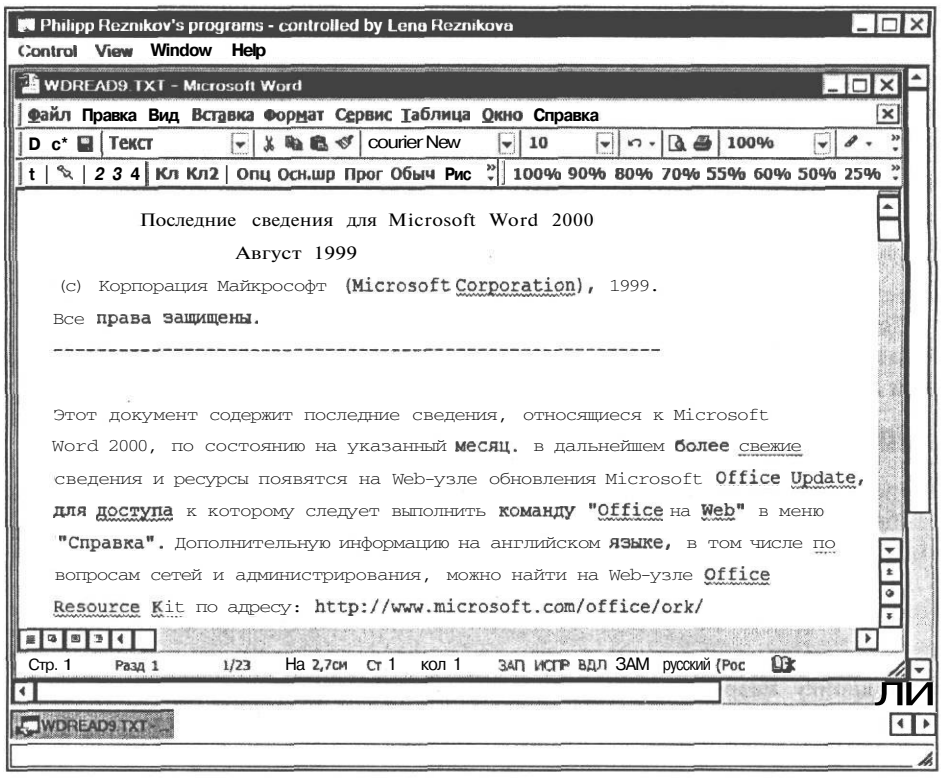



*Рис. 7.42. Общее приложение на экране участника встречи*

Если кнопка Разрешить управление (Allow Control) в диалоге Общий доступ (Sharing) недоступна, это означает, что программа не была сделана общей. Прежде чем предоставить возможность управления программой другому пользователю, эту программу или свой рабочий стол следует сделать общими.

Кнопка Разрешить управление (Allow Control) может быть использована в любое время на протяжении всей встречи. После нажатия этой кнопки ее надпись изменится на Запретить управление (Prevent Control). После команды Запретить управление (Prevent Control) другие участники не смогут работать с общей программой до тех пор, пока снова не будет нажата кнопка Разрешить управление (Allow Control).

Если участнику встречи требуется получить управление, то он в меню окна общей программы выберет команду **Управление * Запросить управление** (Control ◆ Request Control). Эта команда доступна, только если нажата кнопка **Разрешить управление** (Allow Control) в диалоге **Общий доступ** (Sharing). При этом NetMeeting выведет на экран соответствующий запрос на подтверждение. Чтобы разрешить управление, следует нажать кнопку **Принять** (Accept). Чтобы разрешение выдавалось автоматически, в диалоге **Общий доступ** (Sharing) установите флажок **Автоматически принимать запросы на управление** (Automatically accept request for control).

Если в список пользователей, которые могут управлять программой, добавление новых участников не предполагается, установите флажок **Не беспокоить запросами на управление** (Do not disturb with requests for control right now).

Щелчком мыши в любом месте рабочего стола участник, выделивший программу в общее пользование, может в любой момент снова взять управление общей программой на себя. Одновременное управление программой несколькими пользователями невозможно.

Чтобы отменить общий доступ к программе в диалоге **Общий доступ** (Sharing), нажмите кнопку **Отменить** (Unshare) для одного приложения или кнопку **Отменить для всех** (Unshare All) для всех общих приложений.

Если после открытия диалога **Общий доступ** (Sharing) было запущено другое приложение, то для добавления в список совместного доступа нового элемента следует еще раз запустить этот диалог, воспользоваться кнопкой - **Общие приложения** (Share program) в рабочем окне NetMeeting.

## Общий доступ к компьютеру

Если в поле списка **Общие приложения** (Share Programs) диалога **Общий доступ** (Sharing) выбрать **Рабочий стол** (Desktop), то будет предоставлен коллективный доступ к компьютеру. Если элемент **Рабочий стол** (Desktop) недоступен, то, вероятно, был установлен общий доступ к другому приложению. Предоставление совместного доступа к рабочему столу при наличии других общих приложений не допускается.

Чтобы предоставить свой компьютер для совместной работы других участников встречи, нажмите кнопку **Разрешить управление** (Allow Control). Такое управление означает полный доступ к компьютеру других участников встречи, которые используют программу NetMeeting 3.0 или более позднюю версию. Пользователи более ранних версий NetMeeting не имеют возможности управлять компьютером или программой, доступ к которым предоставляет участник с NetMeeting 3.0 или более поздней версией.

Общий доступ к окну Проводника (Windows Explorer) означает возможность такого доступа и ко всем открытым в Проводнике (Windows Explorer) папкам. Кроме того, все запущенные из общего окна программы автоматически становятся общими для остальных участников вплоть до завершения встречи.

Участники встреч использующие NetMeeting 2.1 или более ранней версии не имеют доступа к общим рабочим столам участников, которые используют версию NetMeeting 3.0 или более позднюю.

## Совместная работа с Microsoft Office 2000/2002/2003

Приложения Microsoft Office 2000/2002/2003 позволяют совместно работать над своими документами одновременно нескольким пользователям. Эта возможность доступна в программах Word, Excel, Access и PowerPoint.

Чтобы начать совместную работу в одной из этих программ, следует открыть в ней документ, предназначенный для общего использования.

Далее, в меню **Сервис** ◆ **Совместная работа** (Tools ◆ Online Collaboration) указанных программ можно воспользоваться одним из следующих вариантов действий:

- чтобы немедленно начать встречу, выберите команду **Начать собрание** (Meet Now);
- чтобы присоединиться к встрече позже, выберите команду **Назначить собрание** (Schedule Meeting).

Назначение встречи на определенное время возможно только в том случае, если на компьютере установлено приложение Microsoft Outlook. Если это не так, то команда **Назначить собрание** (Schedule Meeting) будет недоступна.

Если проводящий встречу выбирает команду **Начать собрание** (Meet Now), когда программа NetMeeting не выполняется, то она будет запущена автоматически в фоновом режиме и откроется диалог **Поиск пользователя** (Find Someone). На компьютерах других участников встречи этого не происходит.

В диалоге **Поиск пользователя** (Find Someone) вы можете выбрать ярлыки вызова или контакты и, нажав кнопку **Вызвать** (Call), послать вызовы участникам встречи.

Одновременно на экране появится панель инструментов **Собрание по сети** (Online Meeting) (Рис. 7.43). Кнопки этой панели позволяют:

- **Вызвать участника** (Call Participant); имена участников появляются в открывающемся списке;
- **Удалить участника** (Remove Participants), выбрав его имя в списке;
- **Разрешить совместное редактирование** (Allow other to edit);
- Отобразить **окно разговора** (Display Chat Window);
- **Отобразить доску** (Display Whiteboard);
- **Завершить собрание** (End Meeting).


*Рис. 7.43. Панель инструментов **Собрание по сети** (Online Meeting)*

Чтобы предоставить открытый документ в общее пользование, достаточно нажать кнопку - **Разрешить совместное редактирование** (Allow other to edit). При этом появится

диалог **Собрание по сети** (Online Meeting) (Рис. 7.44), извещающий о совместном использовании файла. Дальнейшие действия аналогичны вышеописанным. Следует в окне программы NetMeeting щелкнуть правой кнопкой мыши на имени участника встречи, которому необходимо предоставить доступ к программе, и в появившемся контекстном меню выбрать команду **Предоставить управление** (Grant Control).

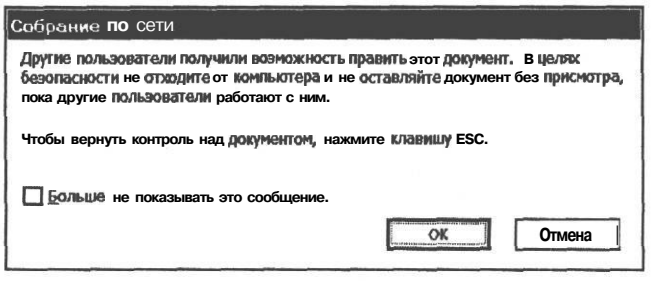



*Рис. 7.44. Диалог* ***Собрание по сети*** *(Online Meeting)*

Чтобы отменить совместное использование документа достаточно щелчком мыши вывести кнопку из нажатого состояния. Появится соответствующее сообщение (Рис. 7.45).

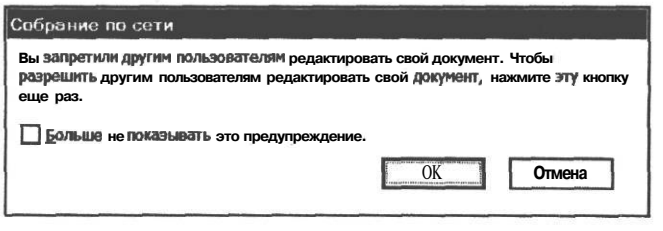



*Рис. 7.45. Сообщение о запрещении редактирования документа*

В ходе собрания по сети можно совместно использовать приложения и документы, участвовать в разговоре, обмениваясь текстовыми сообщениями, передавать файлы и работать на доске. При совместной работе участники могут просматривать и изменять документ. Если режим совместной работы отключен, в каждый момент времени только один человек может изменять документ, но в разговоре и на доске могут одновременно общаться несколько пользователей. Совместно используемый документ и приложение, в котором он создан, должны быть открыты только на компьютере организатора собрания по сети.

Для окончания встречи нажмите кнопку - Завершить **собрание** (End Meeting).

Как видите, приложения Microsoft Office 2000/2002/2003 работают совместно с NetMeeting, который реализует современные технологии связи для работы в сети над общими документами.

# ПРИЛОЖЕНИЕ. **Содержание компакт-диска**

| № | Название файла | Название программы | Назначение | Статус |
|---|---|---|---|---|
| Содержимое папки Soft | | | | |
| 1 | Eserv299r.exe | Eserv 2.99 | Подключение локальной сети к Интернету | Демоверсия |
| 2 | **MBSASetup-en.msi** | Microsoft Baseline Security Analyzer 1.2 | Анализ безопасности компьютера | Бесплатно |
| 3 | mdmcisco.inf | | Файл настроек нуль-модемного соединения | Бесплатно |
| 4 | no share.reg | | Прекращение общего доступа к дискам | Бесплатно |
| 5 | OutpostProInstall.exe | Agnitum Outpost Firewall Pro 2.0 | Межсетевой экран | Демоверсия |
| 6 | **OutpostProInstall-2.1**.x.exe | Agnitum Outpost Firewall Pro 2.1 | Межсетевой экран | Демоверсия |
| 7 | pass_gen.zip | Генератор паролей | Генерирует сложные пароли | Бесплатно |
| 8 | **unreal_tournament_2004_demo.exe** | Unreal Tournament 2004 | Сетевая игра | Демоверсия |
| Содержимое папки **Soft\More** | | | | |
| 9 | AdbeRdr60_enu_full.exe | Acrobat Reader 6 | Чтение файлов в формате PDF | Бесплатно |
| 10 | **aports.zip** | Active Ports 1.4 | Монитор открытых портов | Бесплатно |
| 11 | bpftp243_upgrade.exe | BulletProof FTP 2.43 | FTP-клиент | Демоверсия |
| 12 | **cms200b6.zip** | Courier Mail Server 2.0 | Почтовый сервер | Демоверсия |
| 13 | eprus.exe | EType Internet Phone 1.0 | Компьютерный телефон для сети | Демоверсия |
| 14 | LanScope.exe | LanScope v. 2.5 | Сканер общих ресурсов | Бесплатно |
| 15 | NVinst.exe | NetView 2.8 | Сканер общих ресурсов | Бесплатно |
| 16 | **oms07r.zip** | Office Mail Server 0.7.26 | Почтовый сервер | Бесплатно |
| 17 | **proxyi.exe** | AnalogX Proxy Server | Подключение локальной сети к Интернету | Бесплатно |

| | | | | |
|---|---|---|---|---|
| 18 | psmail.zip | PsMail | Почтовый сервер | Бесплатно |
| 19 | pspf.exe | Sygate Personal Firewall 5.5 | Межсетевой экран | Демоверсия |
| 20 | q2-314-demo-x86.exe | Quake 2 | Сетевая игра | Демоверсия |
| 21 | radmin21.zip | Remote Admin 2.1 | Удаленное администрирование компьютеров в сети | Демоверсия |
| 22 | radminru.zip | Remote Admin 2.1 (Русская версия) | Удаленное администрирование компьютеров в сети | Демоверсия |
| 23 | raidenftpd2.exe | RaidenFTPD 2.4 | FTP-сервер | Демоверсия |
| 24 | remote.zip | COOL! Remote Control 1.12 | Удаленное администрирование компьютеров в сети | Демоверсия |
| 25 | tembria.exe | Tembria Network Monitor 1.2.3 | Мониторинг сети | Демоверсия |
| 26 | tpf-5.5.1332.exe | Tiny Personal Firewall 5.5.132 | Межсетевой экран | Демоверсия |
| 27 | tpf5_manual.pdf | | Руководство по программе Tiny Personal Firewall | Бесплатно |
| 28 | ultrafxp.exe | UltraFXP 1.0 | FTP-клиент | Демоверсия |
| 29 | watznew_1_9_5_eng.zip | WatzNew 1.9.5 | Слежение за обновлениями Web-сайтов | Демоверсия |
| 30 | wgsetup.EXE | WinGate 5.2.3 | Подключение локальной сети к Интернету | Демоверсия |
| 31 | Winproxy.exe | WinProxy 5.1 | Подключение локальной сети к Интернету | Демоверсия |
| 32 | lanmanual.pdf | | Руководство по программе WinProxy (Построение локальной сети) | Бесплатно |
| 33 | QuickStartGuide.pdf | | Руководство по программе WinProxy (Быстрый старт) | Бесплатно |
| 34 | WinProxy_UserManual_en.pdf | | Руководство по программе WinProxy (Что нового) | Бесплатно |
| 35 | WinProxy5-1_UserGuide.pdf | | Руководство по программе WinProxy (Описание работы) | Бесплатно |
| 36 | wswsetup.exe | WebSite-Watcher 3.60 | Слежение за обновлениями Web-сайтов | Демоверсия |
| 37 | xs7demo.zip | Xspider 7.0 | Анализ безопасности компьютера | Демоверсия |

# Содержание

# 100% САМОУЧИТЕЛЬ

# ЛОКАЛЬНАЯ СЕТЬ СВОИМИ РУКАМИ

**Отдел распространения издательской группы «ТРИУМФ»**
(«Издательство Триумф», «Лучшие книги», «Только для взрослых», «Технолоджи - 3000», «25 КАДР»)
**Телефон: (095) 720-07-65, (095) 772-19-56. E-mail: opt@triumph.ru**
**Интернет-магазин: www.3st.ru**
**КНИГА-ПОЧТОЙ: 125438, г.Москва, а/я 18 «Триумф». E-mail: post@triumph.ru**

**ОТВЕТСТВЕННЫЕ ЗА ПЕРЕГОВОРЫ:**
**Региональные магазины – директор по развитию Волошин Юрий**
**Московские магазины - главный менеджер Малкина Елена**
**Оптовые покупатели - коммерческий директор Марукевич Иван**

Идея, план и примеры книги: И.Я. Минаев.

Сборка компакт-диска: И.Ю. Матвиенко.

Корректор: Е.В. Горбачева.

Верстка: Е.О. Русакова.

Дизайн обложки: О.В. Русецкая.

Подписано в печать с оригинал-макета 27.07.2004 г.
Формат 70x100 1/16. Печ. л. 23. Заказ № 3767.
Тираж 4000 экз.

ООО «ТЕХНОЛОДЖИ - 3000».
Россия, 125438, г. Москва, а/я 18.
Лицензия серия ИД № 03452 от 08.12.2000 г.

Отпечатано в полном соответствии с качеством предоставленных
диапозитивов в ОАО «Можайский полиграфический комбинат»
143200, г. Можайск, ул. Мира, 93

Отдел распространения издательской группы

**«ТРИУМФ»**

(«Издательство Триумф», «Лучшие книги»,
«Только для взрослых», «Технолоджи - 3000», «25 КААР»)

**принимает заказы на продажу книг по почте наложенным платежом**

Вы можете заказать наложенным платежом книги по ценам издательства заполнив БЛАНК ЗАКАЗА, расположенный далее, и отправив его нам по адресу:

**125438, г. Москва, а/я 18 «Триумф»**

Принимаются заказы, оформленные на ксерокопии бланка заказа или от руки.

Вы можете также сделать заказ в нашем Интернет-магазине «Три ступеньки®»:

**www.3st.ru**

Или по электронной почте:

**post@triumph.ru**

Получив Вашу заявку, мы оформим и выполним Ваш заказ в кратчайшие сроки.

**ВНИМАНИЕ !!!**

**Указанные иены складываются из оптовых (!) иен издательства и почтовых расходов, за исключением АВИАтарифа.**

## *Лучшие издания*

| | Лот | Книга | Цена |
|---|---|---|---|
| *«100% САМОУЧИТЕЛЬ»* | | | |
| *Перевертыш* | 086 | 200% самоучитель КОМПЬЮТЕРА и ИНТЕРНЕТА. (480 с.) | 171 |
| *НОВИНКА* | 118 | 100% самоучитель КОМПЬЮТЕРА. (288 с.) | 137 |
| *НОВИНКА* | 119 | 100% самоучитель ИНТЕРНЕТА. (208 с.) | 137 |
| *То, что надо!* | 093 | 100% самоучитель Windows. Все версии от 98 до XP. Установка, настройка и успешная работа. — **А.Ю. Гаевский.** (400 с.) | 149 |
| *НОВИНКА* | 111 | 100% Самоучитель бухгалтера. **1С:Бухгалтерия. (384 с.)** | 217 |
| *НОВИНКА* | 115 | Локальная сеть своими руками. 100% самоучитель. + *КОМПАКТ-ДИСК.* (368 с.) | 217 |
| *Серия «КНИГА + ВИДЕОКУРС»* | | | |
| *Рассекреченные методики* | 033 | Компьютер с нуля! *КНИГА + ВИДЕОКУРС.* (384 с.) | 179 |
| | 080 | Windows **98/ME/2000/XP.** *КНИГА + ВИДЕОКУРС.* (400 с.) | 179 |
| | 087 | Интернет с нуля! *КНИГА + ВИДЕОКУРС.* (352 с.) | 189 |
| | 099 | Видеомонтаж с нуля! *КНИГА + ВИДЕОКУРС.* (432 с.) | 299 |
| | 110 | Сборка и апгрейд компьютера с нуля! *КНИГА + ВИДЕОКУРС.* (368 с.) | 217 |
| *Серия «Я ♥»* | | | |
| *Уникальные издания. Это СУПЕР!* | 001 | Я ЛЮБЛЮ ЦИФРОВУЮ ФОТОГРАФИЮ. 20 программ для хранения, обработки, печати и демонстрации цифровых фотографий. + *CD-ROM.* (448 с.) | 299 |
| | 002 | Я ЛЮБЛЮ КОЛЛЕКЦИОНИРОВАТЬ МУЗЫКУ НА ПК. 50 программ для создания, клонирования, копирования и перекодирования музыкальных дисков AudioCD, MP3, DVD-Audio и музыкальных файлов в форматах MP3, WMA, WAV (PCM), OGG, MP3Pro, MPC (MP+), VQF, MIDI, RM, Dolby Digital (AC3) и Dolby Surround. + *CD-ROM.* (416 с.) | 257 |
| | 003 | Я ЛЮБЛЮ КОМПЬЮТЕРНУЮ САМООБОРОНУ. 25 способов и программ для защиты своего компьютера, своей сети, своей информации от хакеров, конкурентов, спецслужб, начальников, сослуживцев и других любопытных чудаков. + *CD-ROM.* (432 с.) | 257 |
| | 092 | Я ЛЮБЛЮ ИНТЕРНЕТ. 25 программ для участия в чатах и видеоконференциях, поиска музыки, Интерет-телефонии, защиты от спама, быстрой загрузки файлов, безопасной работы в сети, чтения Web-страниц только по-русски: ICQ, NetMeeting, The Bat!, WinAmp, Opera, Agnitum Outpost, MP3Locator, GetRight, Promt XT Internet и другие... + *CD-ROM.* (384 с.) | 224 |
| | 084 | Я ЛЮБЛЮ ВИДЕОМОНТАЖ. 15 программ для ввода/вывода видео, видеомонтажа, создания спецэффектов, видеокомпозиций и озвучивания фильмов: ScenalyzerLive, Ulead MediaStudio, Adobe Premiere, Adobe After Effects, Hollywood FX, Boris RED, Canopus XPlode, Morph Man, Ulead COOL 3D, Illusion, Sound Forge, Audiograbber, WinMP3 Locator, Gnucleus, Audio Compositor. + *CD-ROM.* (432 с.) | 299 |
| | 096 | Я ЛЮБЛЮ ДОМАШНИЙ **КИНОТЕАТР.** 11 недорогих вариантов домашнего кинотеатра на базе компьютера и без него. + + *CD-ROM.* (416 с.) | 257 |
| | 114 | Я ЛЮБЛЮ ЗАПИСЫВАТЬ ДИСКИ **CD-R/W** и **DVD±R/W.** 15 программ для записи и копирования музыкальных дисков, фотослайдшоу, дисков для хранения данных, мультизагрузочных дисков восстановления и хранения файлов, а также для создания обложек и печати изображений на самих дисках: Nero Burning Rom, EasyCD, InstantCD+DVD, Ulead DVD PictureShow, WinOnCD, Nero Cover Design и другие... + *CD-ROM.* **( (384** с.) | 257 |
| | 100 | Я ЛЮБЛЮ СОЗДАВАТЬ И КОПИРОВАТЬ ВИДЕОДИСКИ. 25 программ для создания и копирования видеодисков VideoCD, SuperVideoCD, MPEG 4, DVD и нестандартных дисков X(S)VideoCD. + *CD-ROM.* (400 с.) | 257 |

| | Лот | Книга | Цена |
|---|---|---|---|
| *Серия* ***«СОВРЕМЕННЫЙ САМОУЧИТЕЛЬ»*** | | | |
| *Книга-лотерея* | 009 | АСТРОЛОГИЯ с помощью компьютера и без него. Самоучитель. + *КОМПАКТ-ДИСК.* — А.Г. Колесников. **(368 с.)** | 242 |
| *Лидер продаж* | 015 | **1С:Бухгалтерии** 7.7 в вопросах и ответах. Самоучитель. (384 с.) | 299 |
| *Книга-лотерея* | 012 | Компьютер для студентов. Самоучитель. (400 с.) | 169 |
| *Серия «БЫСТРО И ЛЕГКО»* | | | |
| *НОВИНКА* | 103 | Быстро и легко. СЕТЬ для дома и офиса. Создание, настройка, диагностика и зашита. + *КОМПАКТ-ДИСК.* (400 с.) | 257 |
| *То, что надо!* | 082 | Быстро и легко. Сетевые игры: в локальной сети, через модем, через **Интернет.** + ***КОМПАКТ-ДИСК.*** (400 с.) | 217 |
| *Эксклюзив* | 029 | Быстро и легко. Цифровые видеокамеры, видеомонтаж и фабрика видеодисков дома: Ulead **MediaStudio Pro** 7. + *КОМПАКТ-ДИСК.* **(592 с.)** | 299 |
| *То, что надо!* | 098 | Быстро и легко. **ХАКИНГ** и **АНТИХАКИНГ:** защита и нападение. + *КОМПАКТ-ДИСК.* **(400 с.)** | 217 |
| *Серия «ОФИЦИАЛЬНЫЙ УЧЕБНЫЙ КУРС» от разработчиков компании* **Adobe®** | | | |
| *От разработчиков* | 022 | **Adobe®** After **Effects®** 6.0. + *КОМПАКТ-ДИСК. (416* с.) | 299 |
| | 117 | **Adobe® Premiere®** Pro. + *DVD-ДИСК.* (512 с.) | 320 |
| | 104 | **Adobe® Acrobat® 6.0.** + ***КОМПАКТ-ДИСК*** (416 с.) | 299 |
| | 091 | **Adobe® Photoshop®** 7. + *КОМПАКТ-ДИСК.* (496 с.) | 299 |
| | 112 | **Adobe® Photoshop®** CS. + *КОМПАКТ-ДИСК.* **(528** с.) | 320 |
| | 120 | **Adobe® Illustrator®** CS. + *КОМПАКТ-ДИСК.* (496 с.) | 320 |
| | 113 | **Adobe® Encore®** DVD. + *DVD-ДИСК.* (384 с.) | 299 |
| *Серия «25 КАДР»* | | *ВИДЕО & КНИГА* | |
| *ЭКСКЛЮЗИВ* | 105 | Новый способ освоить создание **ВИДЕОДИСКОВ:** VCD, SVCD, DVD, MPEG 4. + ***Видеокурс.*** (400 с.) | 320 |
| *ЭКСКЛЮЗИВ* | 106 | Ulead MediaStudio Pro 7. ВИДЕОМОНТАЖ. + *Видеокурс.* (640 **с.**) | 398 |
| *Серия «ЗНАНИЯ И ОПЫТ ЭКСПЕРТОВ»* | | | |
| *СЛОВАРЬ* | 107 | Англо-русский энциклопедический СЛОВАРЬ по современной электронной технике и программированию. (784 с.) | 237 |
| *Мировой бестселлер* | 019 | Прикладная криптография с исходными текстами программ на языке **Си.** — Б. Шнайер. (816 с.) | 399 |
| *Эксклюзив* | 101 | Эффективный **Web-сайт.** + *КОМПАКТ-ДИСК.* (560 с.) | 320 |
| *НОВИНКА* | 116 | Разработка и сопровождение проектов. Microsoft Project 2003. + *КОМПАКТ-ДИСК.* (352 с.) | 320 |
| *НОВИНКА* | 109 | Администрирование и безопасность баз данных системы программ **1С:ПРЕДПРИЯТИЕ.** + *КОМПАКТ-ДИСК.* (368 с.) | 320 |
| *Серия «В ДЕЙСТВИИ»* | | | |
| *Для программистов* | 095 | Фракталы и **вейвлеты** для сжатия изображений в **действии.** + *КОМПАКТ-ДИСК.* (320 с.) | 242 |
| | 089 | Форматы и алгоритмы сжатия изображений в действии. + *КОМПАКТ-ДИСК.* (336 с.) | 242 |
| | 102 | Криптография на Си и С++ в действии. + *КОМПАКТ-ДИСК.* (464 с.) | 299 |

**Аля получения книг наложенным платежом**
**выберите интересующие Вас книги из предложенного списка**
**и оформите БЛАНК ЗАКАЗА:**
**внимательно заполните соответствующие колонки**
**и внесите свои данные в поля на обороте бланка заказа.**
**Оформленный БЛАНК ЗАКАЗА пришлите нам по адресу:**

**125438, г. Москва, а/я 18 «Триумф»**

***Также принимаются заказы, оформленные на ксерокопии бланка заказа или от руки.***

| Лот книги | Название книги (можно кратко) | Цена книги | Кол-во | Стоимость |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | **Итоговая стоимость заказа:** | | | |

## *БЛАНК ЗАКАЗА*



*Заполняйте поля аккуратно большими отдельными буквами.*

1. Фамилия, имя, отчество

_____

2. Почтовый адрес

индекс_____ **область** _____

_____ **район** _____

населенный пункт (город, поселок) _____

_____

улица, дом, кв. _____

_____

_____

3. Телефон для связи (в том числе код города)

_____

4. Хотели бы Вы получать БЕСПЛАТНЫЙ каталог наших книг?

☐ Да ☐ Нет

5. Пожалуйста, укажите название и адрес магазина, в котором Вы приобрели нашу книгу.

_____

_____

_____ **Заранее** благодарим Вас!

Дата_____ Подпись _____

ГЛАВА 5.

# Защита сети от вирусов и атак через Интернет

Каждый, кто пользуется компьютером, знает, что конфиденциальности, целостности и доступности данных угрожает множество опасностей, начиная с атак хакеров и кончая сетевыми вирусами-червями. Причем нарушение безопасности чревато серьезными потерями. Получая доступ к ресурсам многих миллионов компьютеров в Интернете, вы одновременно, в той или иной степени, открываете другим компьютерам Интернета доступ к ресурсам компьютеров вашей локальной сети. Перечислим основные опасности, которым подвергается ваша сеть:

- вместе с почтой, в виде вложений в компьютеры сети, кроме вирусов, могут проникнуть Интернет-черви. Некоторые почтовые программы, а также неопытные пользователи, не сознавая угрозы, открывают вложения сами. Если такое послание открыть, то выполняющийся «червь» стремительно поражают систему;
- на ваших компьютерах могут исполняться, например, при отображении Web-страниц, содержащих элементы ActiveX или Java-апплеты, поступившие извне программы, которые, в общем случае, могут выполнять любые опасные действия, например, передавать файлы с вашей частной информацией другим компьютерам в сети или просто удалять ваши данные, причем управлять работой этих программ вы не имеете возможности;
- при неправильной настройке системы другие компьютеры Интернета могут получить или попытаться получить доступ к файлам ваших винчестеров, в которых хранится конфиденциальная информация;
- ваш компьютер может использоваться для атаки другого компьютера, так что вы не будете знать об этом;
- многие Web-узлы могут размещать на ваших компьютерах файлы (cookies или referrers), по которым они смогут определять, к какой информации вы обращались и, напротив, кто обращался к вашему компьютеру;
- на ваши машины могут попасть «троянские кони», т.е. программы, которые передают частную информацию (например, пароли доступа в Интернет или номера кредитных карточек) с вашего компьютера на компьютер злоумышленника. Распространенным вариантом вторжения является установка на компьютере различных серверов для удаленного управления (Backdoor). Если подобная программа оказалась в вашей системе, то ее хозяин сможет работать на вашем компьютере почти как на своем собственном. Основным отличием «троянца» от вируса является именно то, что вирус, попавший на ваш компьютер, никак не связан со своим создателем, а «троянский конь» как раз и предназначен для последующего взаимодействия с пославшим его злоумышленником;
- на ваших компьютерах без вашего ведома может быть размещена специальная программа-шпион (spyware), которая передает своему разработчику информацию о владельце компьютера, его пристрастиях, например, информацию о получаемых из сети файлах, посещаемых сайтах, установленном программном обеспечении. Шпионские программы используют в основном фирмы-разработчики программного обеспечения в маркетинговых целях;

- вместе с запрашиваемой информацией в компьютеры может загружаться и ненужная информация - баннеры и иная реклама (спам). Хотя сами по себе эти объекты не могут вызвать потерю или искажение информации на ваших компьютерах, однако они существенно увеличивают время загрузки страниц, особенно при работе через модем.

Тех, кто получает или пытается получить незаконный доступ к данным через Интернет, называют хакерами. Во многих странах принято законодательство, ставящее действия хакеров вне закона, и многие из них уже привлечены к ответственности. Тем не менее, вал компьютерных преступлений не спадает – более того, он нарастает год от года. Защиту компьютерных сетей многих крупных фирм и государственных организаций хакеры уже испытывали на прочность, и нередко им удавалось найти в ней бреши.

Если раньше, чтобы взломать систему, требовались некоторые усилия, то в наши дни существуют программы, которые делают это автоматически. Их могут использовать даже дети, не имеющие специальных знаний и опыта. В Интернете эти программы можно найти без труда. Многие из них распространяются по сети в виде почтовых вложений. Если такая программа попадает в компьютер пользователя, она посылает сигнал о своем местонахождении своему владельцу. Таким образом хакер может следить за удаленным компьютером незаметно для пользователя. Он получает возможность фиксировать все движения курсора и нажатия клавиатуры на этом компьютере и может легко узнать номер кредитной карточки или пароли.

Не следует думать, что хакеров интересует только «крупная рыба». Все чаще они атакуют не защищенные или слабо защищенные от вторжения домашние компьютеры и сети, подключенные к Интернету. Атака может исходить также изнутри- от программы-шпиона, проникшей на компьютер, например, в качестве вложения в письмо-спам.

Для обеспечения безопасности и защиты информации на компьютерах локальной сети необходимо использование целого ряда мер, которые можно объединить в четыре группы:

- установка всех обновлений операционной системы;
- настройка в операционной системе режимов максимальной безопасности;
- использование антивирусного программного обеспечения с регулярно обновляемыми вирусными базами;
- использование защитного экрана или брандмауэра (firewall).

В этой главе мы подробно рассмотрим практическую реализацию этих мер.

## Установка всех обновлений Windows XP

В операционных системах семейства Windows постоянно обнаруживаются уязвимости различных систем и служб, которые называют также «дырами» в системе безопасности. Эти дыры позволяют вирусам проникать на компьютер, а злоумышленникам - получать возможность управления системой. Корпорация Microsoft регулярно выпускает обновления для операционных систем, называемые «заплатами», позволяющие устранить тот или иной изъян в системе безопасности. Первым шагом в обеспечении безопасности каждого компьютера в отдельности и локальной сети в целом является установка всех обновлений системы безопасности Windows XP или Windows 2000 (защищать операционные системы Windows 98/Me бесполезно).

Для поддержания операционной системы Windows в обновленном состоянии используются обновления двух типов: наборы (service packs) и заплаты (hotfix).

Наборы для обновления (service packs) - это тщательно протестированные группы обновлений, выпущенные на основании анализа проблем с той или иной разработкой Microsoft, возникших у пользователей. Как правило, они исправляют несоответствия, выявленные в продукте с момента его запуска в широкую продажу. Наборы для обновления кумулятивны - в дополнение к новым исправлениям каждый последующий набор содержит в себе предыдущий. Наборы обеспечивают совместимость продуктов с новыми версиями драйверов и программного обеспечения и исправляют проблемы, выявленные в процессе эксплуатации или дополнительного тестирования. Их необходимо устанавливать сразу же после выпуска. Примером набора обновления является Service Pack 1 для Windows XP.

В свою очередь заплатами (hotfix) называется оперативное исправление определенного дефекта или уязвимости в системе защиты. Разрозненные обновления включаются затем в выпускаемые наборы для обновлений.

Для обновления операционной системы существуют два взаимодополняющих средства, которые корпорация Microsoft рекомендует применять совместно:

- Microsoft Windows Update (Средство обновления Microsoft Windows);
- автоматическое обновление.

Эти средства помогают поддерживать программное обеспечение в актуальном состоянии путем установки самых последних обновлений продуктов корпорации Майкрософт.

Windows Update (Средство обновления Microsoft Windows) - это программа и интерактивный Web-узел, с которого можно загружать и устанавливать обновления Windows, постоянно поддерживая на высоком уровне безопасность и производительность компьютера. Windows Update работает с операционными системами Windows NT Server 4.0, Windows Millennium Edition (Windows Me), Windows 2000, Windows XP, Microsoft Windows Server 2003 и позволяет в любое время просматривать, выбирать и устанавливать самые последние улучшения, усовершенствования системы, обновления безопасности и драйверы для компьютера. Программа просматривает компьютер и предлагает набор обновлений, подходящих именно для данного компьютера.

Автоматическое обновление - это служба операционной системы, которая автоматически доставляет на компьютер важные обновления Windows. Она помогает решить проблемы, которые могут быть причиной уязвимости компьютера перед атаками компьютерных вирусов и сетевых червей. Служба автоматического обновления находит обновления, наиболее подходящие для данного компьютера, автоматически загружает их и устанавливает в указанное время, если это предусмотрено настройками. Важно не забывать до наступления времени обновления сохранять копии данных, так как для завершения процедуры установки процесс автоматического обновления может потребовать перезагрузки компьютера.

Обновления, существенно необходимые для работы компьютера, рассматриваются как ключевые обновления и автоматически выбираются для установки с помощью Windows Update и автоматического обновления. Критические обновления предназначены для исправления обнаруженных ошибок и защиты компьютера от известных неполадок безопасности. Автоматическое обновление поддерживают операционные системы Windows Me, Windows 2000 с установленным пакетом Service Pack 3 (SP3) или более поздним - Windows XP, Windows Server 2003.

## Установка обновлений с узла Windows Update

Самый простой способ установить обновления операционной системы - это запустить Windows Update и следовать инструкциям, появляющимся на экране. Посмотрим, как это сделать практически.

Значок **Windows Update** обычно находится в меню кнопки **Пуск** (Start). Если значка **Windows Update** в этом меню нет, можно выбрать в главном меню команду **Справка и поддержка** (Help and Support), после чего в открывшемся окне **Центр справки и поддержки** (Help and Support Center) после подключения к Интернету щелкнуть мышью на ссылке **Обновление системы с помощью веб-узла Windows Update** (Keep your computer up-to-day with Windows Update) или же обратиться по адресу **windowsupdate.microsoft.com.**

После соединения с Web-узлом Windows Update одним из указанных способов вы увидите его первую страницу (Рис. 5.1).

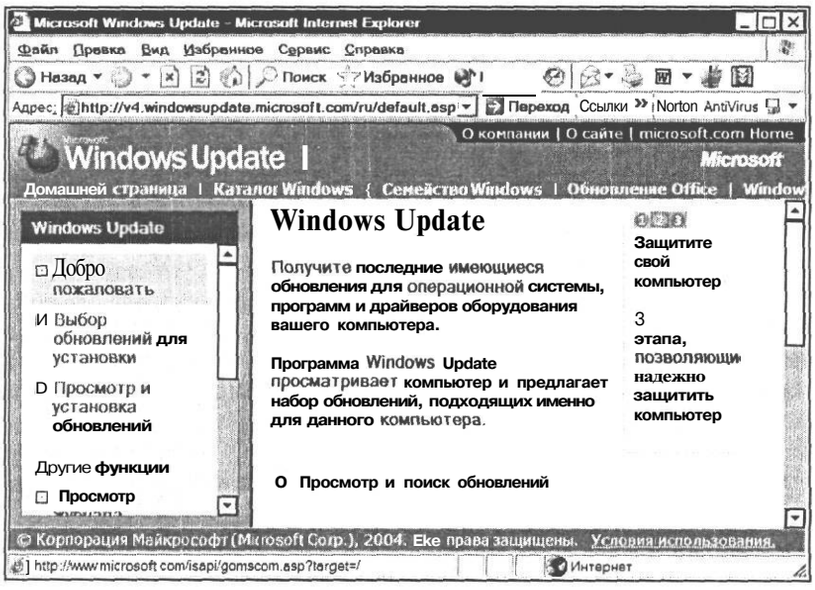



*Рис. 5.1. Первая страница Web-узла Windows Update*

➤ Щелкните мышью на ссылке **Просмотр и поиск обновлений** (Scan for Updates).

Программа выполнит поиск доступных обновлений для вашего компьютера. Это может занять некоторое время.

Когда поиск будет закончен, на экране появится сообщение о количестве найденных критических обновлений (Рис. 5.2). Напомним, что критические обновления предназначены для исправления обнаруженных ошибок и защиты компьютера от известных неполадок безопасности. Вы увидите также информацию о других обновлениях для вашей операционной системы и драйверов. Количество дополнительных обновлений указывается в левой части окна.

➤ Щелкните мышью на ссылке **Просмотр и установка обновлений** (Review and install updates).

Для отправки вызова за пределы локальной сети следует в поле открывающегося списка для ввода или выбора адреса ввести один из следующих адресов:

- IP-адрес компьютера;
- адрес сервера каталога и электронной почты;
- номер телефона.

После ввода адреса необходимо нажать кнопку |☎| - **Вызвать** (Place Call).

Если это возможно, способ вызова определяется автоматически. В противном случае на экран выводится диалог **Вызов** (Place A Call) (Рис. 7.24). Данный диалог можно открыть также, нажав кнопку |☎| - **Вызвать** (Place A Call), когда поле открывающегося списка адресов пустое.

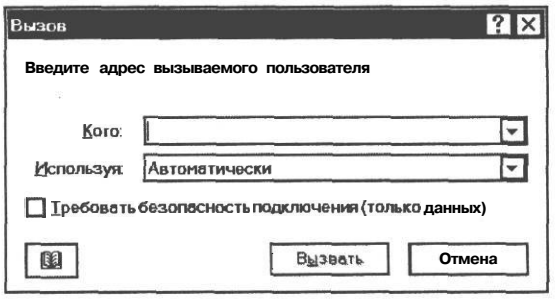



*Рис. 7.24. Диалог **Вызов** (Place A Call)*

В поле ввода **Кого** (To) указывается имя вызываемого компьютера.

В открывающемся списке **Используя** (Using) следует выбрать нужный тип подключения. Набор элементов в нем может изменяться в зависимости от установленных служб.

**Если установить флажок Требовать безопасность подключения (только данных)** (Require security for this call (data only)), то данный вызов будет безопасным. При этом NetMeeting будет шифровать все данные, отправляемые или получаемые с помощью программ Разговор (Chat), Доска (Whiteboard), общих программ или в файлах, которыми обмениваются участники. В безопасных вызовах недоступны средства передачи звука и изображений, поскольку NetMeeting не поддерживает их шифрование. Во время встречи не могут совместно использоваться безопасные и небезопасные вызовы. Все вызовы должны быть одного типа. Если возможность размещения безопасных вызовов отсутствует, данный флажок недоступен.

Если обеспечение безопасности построено на последовательных вызовах, для отправки вызова следует пользоваться кнопкой |☎| – **Вызвать** (Place Call), а не адресной строкой или ярлыком. При вызове через открывающийся список адресов или через ярлык диалог **Вызов** (Place A Call) с флажком **Требовать безопасность подключения (только данных)** (Require security for this call (data only)) не отображается.

Если в диалоге **Вызов** (Place A Call) нажать кнопку [ ], откроется диалог **Поиск пользователя** (Find Someone), с помощью которого можно выполнить поиск абонентов в доступных списках, в частности в каталоге Интернета Microsoft. Подробнее об этом будет рассказано далее.

Для просмотра списка недавно вызывавшихся абонентов следует открыть открывающийся список адресов в рабочем окне NetMeeting.

Отправить вызов можно также другими, перечисленными ниже способами.

## Вызов через сервер каталогов

Как уже отмечалось, в Интернете существуют специальные серверы каталогов, содержащие информацию о всех подключенных пользователях NetMeeting. Подключившись к одному из серверов, вы можете просмотреть список пользователей и выбрать в нем нужного абонента. Кроме того, допускается подключение к серверам каталогов, предоставляемым и обслуживаемым другими организациями. Чтобы просмотреть список доступных серверов, посетите Web-страницу NetMeeting по адресу **http://www.microsoft.com/netmeeting/**.

Для вызова через сервер каталогов следует предварительно указать программе, к какому серверу каталогов следует подключаться.

➤ Выберите команду меню **Сервис** ◆ **Параметры** (Tools ◆ Options). На экране появится диалог **Параметры** (Options) с открытой вкладкой **Общие** (General) (Рис. 7.25).

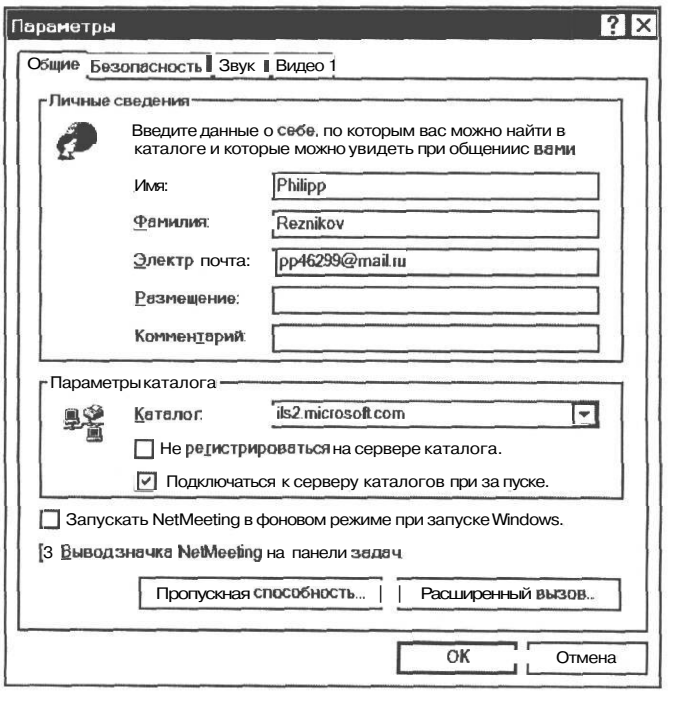



*Рис. 7.25. Вкладка **Общие** (General) диалога **Параметры** (Options)*

➤ В поле открывающегося списка **Каталог** (Directory) группы **Параметры каталога** (Directory Settings) укажите имя нужного сервера каталогов.

При работе с приложением NetMeeting по локальной сети или через привратника (об этом далее) доступные серверы каталогов в этом открывающемся списке представлены не будут.

Ваше имя и почтовый адрес не будут присутствовать в каталоге, к которому выполняется подключение, если установить флажок **Не регистрироваться на сервере каталога** (Do not list my name in the directory).

Чтобы подключение выполнялось автоматически, установите флажок **Подключаться к серверу каталогов при запуске** (Log on to a directory server when NetMeeting starts).

> Закройте диалог **Параметры** (Options) нажатием кнопки **OK.**

После такой установки вы будете либо автоматически подключаться к серверу каталогов при каждом запуске NetMeeting, либо сможете подключаться к нему вручную, нажав кнопку | 📖 | - **Поиск пользователя в каталоге** (Find Someone in a Directory) в рабочем окне NetMeeting и в открывающемся списке Выберите папку (Select a directory) появившегося диалога **Поиск пользователя** (Find Someone), выбрав имя сервера каталога.

При отсутствии подключения к серверу каталогов сохраняется возможность поступления вызовов от пользователей, которым известен ваш IP-адрес.

## Вызов по IP-адресу

Каждый компьютер при каждом сеансе подключения к Интернету получает уникальный адрес, называемый IP-адресом, благодаря которому становится возможной связь в сети. Этот адрес состоит из четырех частей, разделенных точками. Каждая часть может принимать числовое значение от 0 до 255, например 254.42.36.254. Зная IP-адрес компьютера в Интернете, вы легко можете вызвать его владельца.

IP-адрес может быть статическим и динамическим. Статический IP-адрес остается постоянным в каждом сеансе подключения к Интернету. Его можно получить у поставщика услуг Интернета за дополнительную плату. Это лучший вариант для быстрого вызова из NetMeeting. Достаточно ввести в адресное поле статический IP-адрес вызываемого компьютера и нажать кнопку | ☎ | – **Вызвать** (Place Call).

Но большинство пользователей при подключении к Интернету получают динамический IP-адрес, который не бывает постоянным, а меняется при каждом сеансе связи. Поэтому, чтобы вызвать пользователя с динамическим IP-адресом, следует предварительно получить от него по электронной почте, телефону, факсу или другим способом его IP-адрес. Чтобы получить входящий вызов, следует предварительно послать вашему абоненту ваш динамический IP-адрес и ожидать вызова, не разрывая связь с провайдером.

Как определить IP-адрес текущего подключения к Интернету?

➤ После подключения к Интернету в программе NetMeeting выберите команду меню **Справка * О программе** (Help ◆ About Windows NetMeeting). Откроется диалог **О программе** (About Windows NetMeeting), в нижней части которого вы увидите **IP-адреса** (IP Addresses) текущего сеанса подключения (Рис. 7.26).

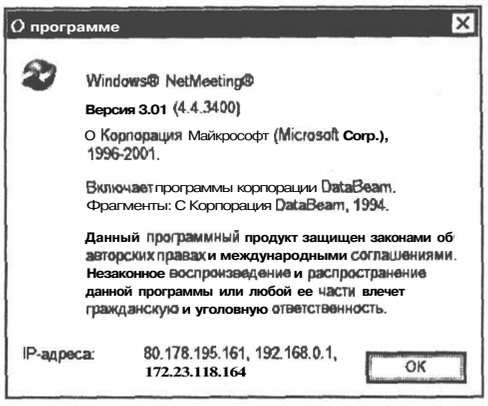



*Рис. 7.26. Диалог* ***О программе*** *(About Windows NetMeeting)*

Если в диалоге указано несколько адресов, то следует использовать первый.

Если на компьютере не установлена программа Winsock 2, IP-адрес в диалоге **О программе** (About Windows NetMeeting) не отображается. В таком случае он может быть определен следующим способом.

- Нажмите кнопку **Пуск** (Start) на **Панели задач** (Taskbar) и в появившемся главном меню Windows выберите команду **Программы * Стандартные * Командная строка** (Programs ◆ Accessories ◆ Command Prompt). Появится окно **Командная строка** (Command Prompt).
- В окне **Командная строка** (Command Prompt) при установленной связи с провайдером Интернета введите команду **ipconfig** и нажмите клавишу Enter. Вы получите IP-адреса всех сетевых адаптеров (Рис. 7.27).

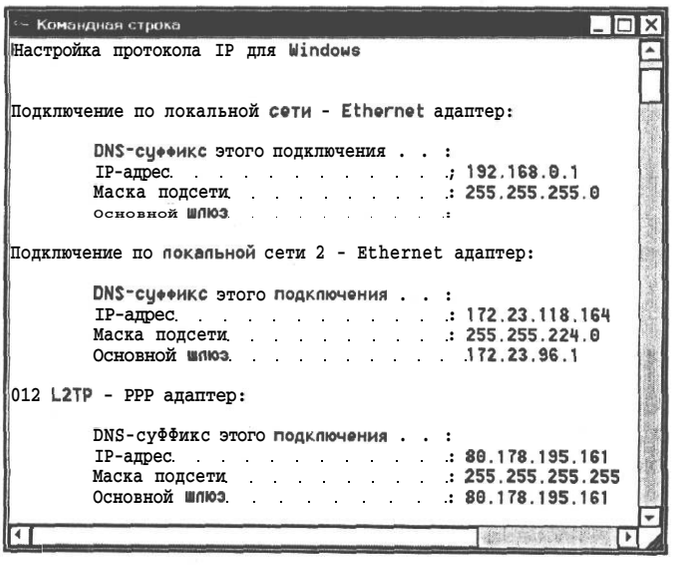



*Рис. 7.27. Определение IP-адреса текущего подключения*