ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Сколько вокруг нас компьютерных сетей! Редкое учреждение обходится без локальной сети, и все больше сетей появляется в квартирах, домах, районах. Вместе с локальными сетями развиваются и сети глобальные. Сегодняшний Интернет способен на то, о чем раньше никто и не догадывался. Очень может быть, что компьютерные сети постепенно заменят собой все остальные виды дистанционного общения, обычную почту, например. Кстати, в некоторых странах начинается сокращение числа почтовых отделений, так как надобность в них постепенно снижается.

Интернет уже сейчас неплохо выполняет функции телефона, а иногда и видеотелефона. Но книга, которую вы держите в руках, посвящена преимущественно локальным сетям. Почему? Да потому что глобальные сети — это, в сущности, множество локальных сетей, соединенных линиями связи.

У локальных сетей есть особенности, и одной из них посвящена эта книга. Особенность эта заключается в том, что создать простую локальную сеть под силу любому пользователю ПК.

Компьютерные сети — это целый мир интереснейших событий, сведений и технологий. Над основными технологиями локальных сетей работают уже несколько десятилетий. К примеру, протокол IP используется и в локальных сетях, и в глобальных. Эволюционируют сетевые функции операционных систем, улучшается оборудование, создается новое программное обеспечение — и все время появляются новые способы использования компьютерных сетей.

Итак, книга, которую вы держите в руках, посвящена локальным сетям: их истории, основным технологиям, практике построения сетей, сетевому программному обеспечению, вопросам безопасности, настройкам операционных систем для работы в сетях, сетевому оборудованию и многому другому. Книга предназначена для широкого круга пользователей — от начинающих до достаточно опытных. Возможно, опытным пользователям многое из того, о чем здесь говорится, уже известно. Но автор уверен, что и они найдут здесь для себя кое-что интересное. Ведь компьютерные сети — тема практически неисчерпаемая.

Начинающий пользователь, которому известно, чем компакт-диск отличается от дискеты, узнает из этой книги, что такое TCP и IP, научится создавать локальные сети, управлять ими и работать с сетевым обору-

дованием. Здесь он изучит возможности множества сетевых программ и узнает много любопытнейших сведений из истории компьютерных сетей. Внимательно изучив книгу, вы станете продвинутым в сетевых вопросах пользователем.

Практическая часть книги ориентирована на операционную систему Windows XP, модемные соединения с Интернетом и локальные Ethernet-сети. Кроме ОС Windows XP автор уделяет внимание другим операционным системам, например все еще актуальной Windows 98 и не самой новой, но по-прежнему широко используемой Windows 2000. Мы разберемся в функционировании беспроводных сетей, отдадим немало сил интеграции в домашнюю локальную сеть карманных компьютеров на базе Windows Mobile 2003 и, разумеется, уделим внимание вопросам безопасности. Кроме того, мы разберем особенности работы с сетевым программным обеспечением. Также книга содержит описания некоторых полезных программ, которые помогут вам сделать вашу домашнюю сеть лучше.

Почему домашнюю? Не советую вам устанавливать какие-нибудь программы на офисные компьютеры, особенно такие, как файрволлы и антивирусы. Как правило, у каждой сети есть хозяин — администратор. Когда-то давно один человек сказал мне замечательную фразу: «В сети хозяин должен быть один». Это действительно так. К примеру, если вы поставите на свой рабочий ПК файрволл — полезную, в общем-то, программку, то существует ненулевая вероятность, что с этого самого момента с вашим компьютером (особенно если он предоставляет каким-либо другим компьютерам сети свои ресурсы), да и вообще с сетью могут начать твориться странные вещи. Словом, никаких сетевых программ на офисных ПК — если вы не являетесь хозяином офисной сети. Думаю, теперь мы можем начать наш путь к освоению компьютерных сетей. Обещаю, что будет интересно.

ЧАСТЬ 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

Глава 1
ЧТО ТАКОЕ КОМПЬЮТЕРНАЯ СЕТЬ?

Некоторые думают, что история — это очень скучно. Не согласен! Мне, да и многим другим компьютерщикам, очень интересно читать компьютерные документы двадцатилетней давности. (Это, кстати, один из признаков человека, по-настоящему интересующегося компьютерами и информационными технологиями.) Когда читаешь о том, что было 10, 20, 30 или 50 лет назад, часто возникает желание «вернуться» назад: посмотреть своими глазами на первые опыты программистов и инженеров, пообщаться с машинами, описания которых мирно покоятся на страницах учебников истории, и попытаться передать какую-нибудь информацию по сетям тех времен. А раз так, начнем с краткой истории сетей передачи данных.

1.1. ИСТОРИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Сети передачи данных — явление гораздо более древнее, чем можно представить. Передавать данные людям понадобилось задолго до появления первого компьютера. Эту главу я бы мог начать с описания событий 1837 года, когда Сэмюэл Морзе изобрел электромеханический телеграф. И, хотя именно это изобретение стало точкой отсчета сетей передачи данных, нашу историю мы начнем с гораздо более поздних событий, которые имеют к компьютерным сетям, окружающим нас, самое прямое отношение.

Все началось в 60-х годах прошлого века. Тогда основными сетями передачи информации были телефонные сети. Компьютеры начинали играть заметную роль в военном деле, образовании и в других отраслях.

БОЛЬШИЕ КОМПЬЮТЕРЫ И ГЛОБАЛЬНЫЕ СЕТИ

Пользователь и компьютер в те годы общались на основе мейнфрейма — большого, мощного по тем временам и ужасно дорогого компьютера. Общались с ним при помощи перфокарт или с пользовательских терминалов. Время шло, и компьютерщики осознали, что территориально раз-

деленные огромные, дорогие компьютеры неплохо было бы объединить при помощи линий связи и совместно использовать данные, ресурсы компьютеров, вести совместные разработки и так далее.

Примерно в то же время существовал доступ к центральному компьютеру с территориально удаленных терминалов через телефонную сеть (рис. 1.1) — это очень напоминало современный dial-up доступ к Интернету, хоть скорость связи была далека от сегодняшней.

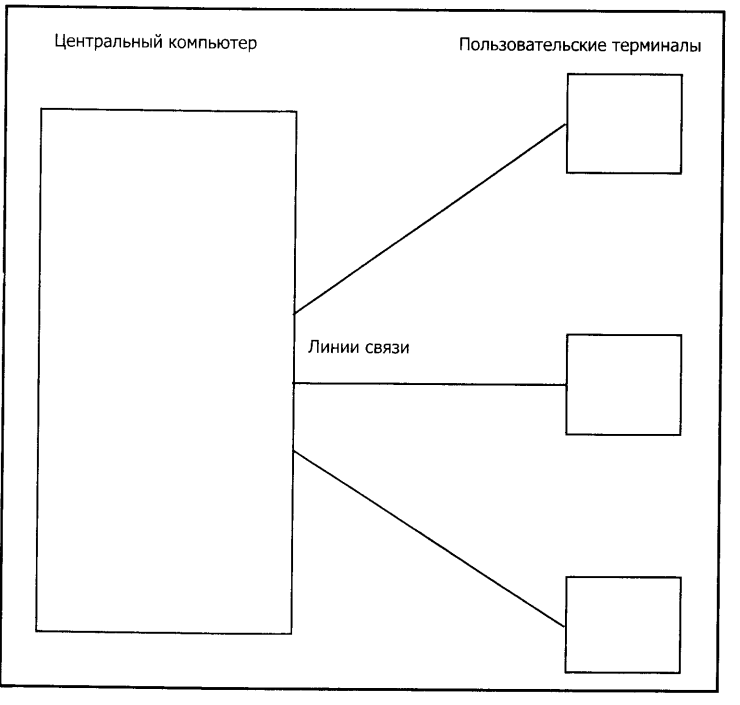


Рис. 1.1. Взаимодействие терминалов с центральным компьютером

Телефонные сети тех времен были сетями с коммутацией каналов. Это важное понятие в сфере компьютерных сетей, и на нем мы остановимся подробнее.

КОММУТАЦИЯ КАНАЛОВ И КОММУТАЦИЯ ПАКЕТОВ

Коммутация каналов (рис. 1.2) предусматривает выделение отдельного канала передачи данных на все время соединения. Этот канал будет занят передаваемыми данными и обеспечит постоянную гарантированную скорость передачи данных.

На рис. 1.2 подписями A1 — A6 обозначены абоненты или компьютеры, а подписями K1 — K5 — коммутаторы или маршрутизаторы.

Схемы сетей с коммутацией каналов очень похожи на сети с коммутацией пакетов. Разница между ними заключается в логике работы сети.

Так, если представить сеть, изображенную на рис. 1.2 в качестве сети с коммутацией каналов, то, например, для связи между узлами A1 и A4 придется создать составной канал передачи данных, проходящий, например, через коммутаторы K1, K4, K5. Такой канал будет обслуживать одно только это соединение, а другие абоненты не смогут использовать ресурсы этого канала, пока абоненты A1 и A4 обмениваются данными.

Коммутация каналов удобна, да и просто необходима в голосовых сетях. Разговаривая по телефону, мы слышим своего собеседника не через слово, а постоянно, равно как и он нас. Но если речь идет о неравномерной передаче данных, такой тип соединения нерационален.

Вот пример. Пользователь соединяется с компьютером и дает ему какую-нибудь команду. В течение нескольких секунд линия занята. В следующие несколько секунд компьютер отрабатывает эту команду. Еще несколько секунд, и он шлет пользователю результат. Получается, что в течение определенного времени линия простаивает, а это нерационально. Но схема коммутации каналов не позволит чьим-нибудь данным «занять» эту линию даже в момент явного простоя.

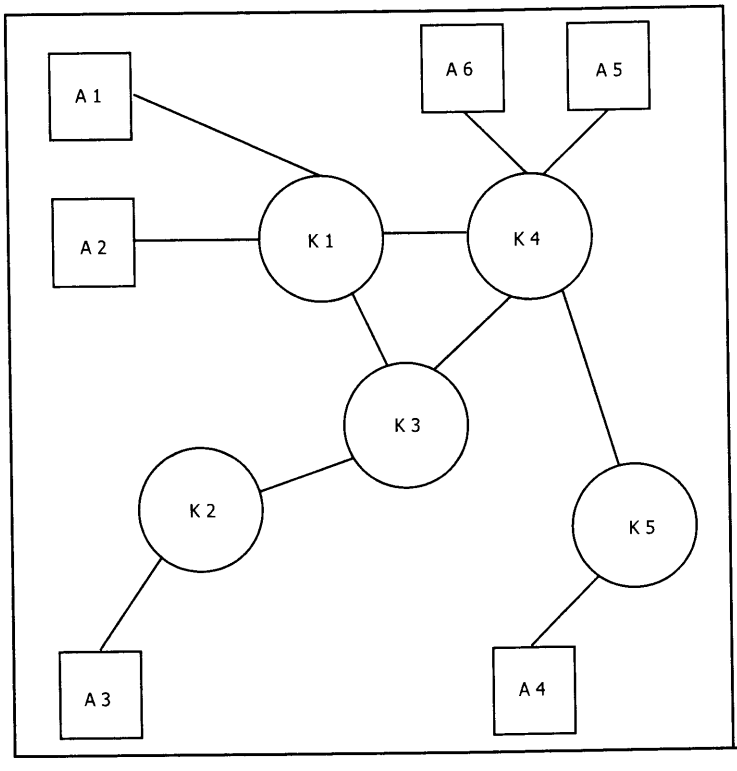


Рис. 1.2. Коммутация каналов и коммутация пакетов

Если бы современный Интернет использовал идеологию коммутации каналов, тогда после вашего соединения с каким-нибудь сервером, путь от вас до которого лежит через множество маршрутизаторов, вашему со-

единению был бы выделен отдельный канал (пусть виртуальный — это не меняет дела), который был бы недоступен для других пользователей даже во время вашего простоя. Часть пропускной способности линий связи использовалась бы нерационально, а учитывая количество узлов в современном Интернете и то, что один узел и даже обычный пользовательский компьютер могут одновременно общаться с десятком серверов, делаем вывод: коммутация каналов — слишком большая роскошь для Интернета.

Здесь я говорю о логике работы сети, о ее транспортном уровне (что это такое, вы узнаете очень скоро), а на физическом уровне коммутация каналов — взять те же dial-up соединения — самое обычное дело.

Другое дело — коммутация пакетов (под пакетами здесь понимаются пакеты данных). Сети с коммутацией пакетов — это сегодняшняя действительность. При коммутации пакетов данные пользователей разбиваются на некоторые последовательности, называемые пакетами, и в таком виде отправляются по сети. В сети одновременно находятся пакеты разных пользователей, которые доставляются коммуникационным оборудованием до адресатов. Получается, что пользователь загружает сеть только тем трафиком, который он генерирует, не затрачивая ресурсы сети впустую. Современный Интернет — самый яркий пример сети, построенной на коммутации пакетов, — и даже не коммутации, а маршрутизации.

Представим, что на рис. 1.2 изображена сеть с коммутацией пакетов. Пусть это будет некоторая часть Интернета. Понятно, что для соединения компьютеров A1 и A2 уже нет нужды занимать ресурсы сети на все время соединения. К тому же пакеты от A1 к A2 могут путешествовать не только путем K1, K4, K5, но и K1, K3, K4, K5.

Первые научные работы о принципах сетей с коммутацией пакетов относятся к началу 60-х годов. Причем разработкой идей коммутации пакетов одновременно занялись три независимые группы исследователей по всему миру — из MIT, Rand Institute (США) и NPL (National Physical Laboratory, Англия). Исследования в области сетей с коммутацией пакетов стали основой, на которой базируются сегодняшний Интернет и другие сети.

Через некоторое время эти исследования вылились в исследовательскую программу Advanced Projects Research Agency (ARPA), в рамках которой была создана первая сеть с коммутацией пакетов, известная как ARPAnet. К 1972 году, когда в сети ARPAnet имелось уже 15 узлов, был разработан первый протокол передачи данных между компьютерами. Этот протокол назывался Network Control Protocol (NCP). В 1972 году была написана первая почтовая программа. Сеть ARPAnet, разработка сетевого программного обеспечения, протоколов, оборудования — все это стало настоящим технологическим прорывом! После этого дальнейшее распространение сетей стало лишь вопросом времени.

СЕТИ РАСПРОСТРАНЯЮТСЯ

После того, как сетевые концепции были в той или иной мере отработаны на ARPAnet, стали появляться другие компьютерные сети. Среди них ALOHAnet, Telenet, Transpac и другие. Это были глобальные сети. Да, да — история компьютерных сетей начинается именно с глобальных систем! Но в 1972 году Роберт Меткалф, работавший тогда в одной из лабораторий Xerox, разработал принципы Ethernet-сетей, которые впоследствии охватили весь мир, породив неимоверное количество локальных сетей. Стандарт Ethernet, которому мы посвятим немало времени, продолжает развиваться, распространяться и сегодня.

При изучении взаимодействия различных сетей родились понятие network of networks (сеть сетей) и термин Interneting, который описывал работу в такой сети. Эти исследования велись при поддержке DARPA. Сегодня слово Interneting переводится как взаимодействие сетей. А от Interneting до Интернет всего один шаг. Тогда же были сформулированы принципы открытой сетевой архитектуры, которые применяются и сегодня:

- возможность автономной работы;
- предоставление услуг по принципу Best Effort — то есть с максимальными усилиями со стороны сети;
- возможность восстановления испорченных при передаче данных;
- децентрализованное управление сетью и применение маршрутизаторов.

Эти принципы легли в основу протокола TCP. Ранние версии TCP не похожи на сегодняшние, но преемственность сохранена: некоторые части первых реализаций TCP существуют и сегодня как модули действующего протокола.

Разработки в области TCP, преимущественно направленные на взаимодействие приложений, привели к выделению протокола IP и разработке протокола UDP. Мы рассмотрим все эти протоколы в соответствующих главах. Кстати, TCP, IP и UDP — это фундамент современного Интернета. А заложен был этот фундамент в конце 70-х годов XX века.

Интересно, что протокол Ethernet, на котором сейчас функционирует огромное количество локальных сетей, изначально задумывался именно как протокол для связывания компьютеров, принтеров и другой периферии в единую рабочую среду. Собственно говоря, так Ethernet-сети и используются.

Между тем в 70-х годах развитие сетей продолжилось. Среди сетей тех времен можно отметить DECnet — она была построена в 1975 году компанией Digital Equipment Corporation, работали сети компаний Xerox и IBM. Опыт копился, и к началу 80-х годов для широкого распространения и развития сетей все было готово.

КОМПЬЮТЕРНЫЕ СЕТИ

В начале 80-х годов в США развернулись проекты по связыванию университетских компьютеров в единую сеть. Эту сеть использовали для научных целей. Среди университетских сетей того времени известны BITnet, CSNET, NFSNET и некоторые другие. Пропускная способность магистральных каналов передачи данных в то время редко когда достигала полутора мегабит в секунду. Но для того времени это было очень много.

РОЖДЕНИЕ TCP/IP

Первого января 1983 года увидел свет официально признанный стандарт TCP/IP. Он заменил применявшийся в ARPAnet протокол NCP. Тогда же появилась система доменных имен — DNS (Domain Name System), то есть способ преобразования IP-адресов так, чтобы они хорошо воспринимались человеком. Например, какой-нибудь сайт, скажем www.mysite.com, может иметь IP-адрес 212.192.152.200. Конечно, использовать в обиходе имя сайта проще, чем IP-адрес.

Родина ARPAnet — США. Но развитием сетей занимались и в других странах. Во Франции развивался проект Minitel, базирующийся на протоколе X.25. В Minitel использовались серверы и недорогие терминалы со встроенными модемами. Эта сеть была во Франции популярна, когда французское правительство позволило всем желающим бесплатно пользоваться Minitel-терминалами. Сеть Minitel к середине 90-х годов представляла собой огромную сеть, которой пользовалось около 20% жителей страны. Интересно, что Minitel представляла собой весьма неплохую аналогию современного Интернета, но была постепенно задушена широким, всемирным распространением своего американского «соперника».

Тем временем развитие IP-сети набирало мощь. В 1990 году прекращает существование наша старая знакомая ARPAnet и начинается эра предоставления доступа к ресурсам сети, — теперь уже сети Интернет, — на коммерческой основе. В этом же году появляется первый провайдер интернет-доступа — The World.

WWW

Одним из главных событий 1990 года, однако, стало не исчезновение ARPAnet, а разработка Всемирной Паутины — World Wide Web. «Паутину» разработал Тим Бернерс-Ли, сотрудник CERN — Европейской лаборатории физики элементарных частиц. Правда, гипертекст не был абсо-

лютной новинкой: первые теоретические работы в этой области относятся аж к 1945 году. Однако свежесть идеи от этого не уменьшилась, а Интернет получил платформу для бурного развития сервисов и приложений. Тим Бернерс-Ли разработал все четыре ключевых компонента современного Интернета: язык HTML, протокол HTTP, Web-сервер и Web-браузер.

В самом начале WWW был исключительно текстовой системой, но позднее Web-браузеры стали графическими. Графическими браузерами мир пользуется и по сей день.

В середине 90-х в сферу WEB-браузеров вторглась корпорация Microsoft со своим Internet Explorer. Альтернативный ему Netscape Navigator имеет куда более длинную историю и ведет происхождение от первого графического браузера Mosaic.

НАШИ ДНИ

Конец 90-х годов и наши дни — годы бурного роста и развития Интернета и сетевых технологий. Растут скорости передачи данных. Еще недавно самым быстрым был гигабитный Ethernet, а сейчас идут эксперименты на 10-гигабитном. Сети становятся беспроводными. Технология Wi-Fi в разных ее модификациях представляет собой довольно удобную замену проводных сетевых адаптеров в домашних локальных сетях. Растет число публичных точек Wi-Fi-доступа, и поддержкой Wi-Fi оснащаются многие ноутбуки, КПК и даже некоторые мобильные телефоны.

Для построения сетей городского масштаба можно использовать технологию Wi-Max, которая тоже освобождает пользователей и провайдеров от проводов. Запускаются коммуникационные спутники для создания глобальных беспроводных компьютерных сетей. Интернет растет так быстро, что уже сейчас всерьез задумываются о применении 128-битной схемы адресации, предусмотренной протоколом IP v6. Современный протокол IP v4 использует 64-битную систему адресов. Это очень много даже с учетом некоторых зарезервированных диапазонов адресов. Но и этого скоро может не хватить. В Интернете сегодня миллиарды сайтов, и один только российский сегмент Сети насчитывает около 17 миллионов пользователей. IP-телефония начинает серьезно конкурировать с обычными телефонными сетями. Да что там телефония — не так давно была представлена технология передачи запахов по Сети! В Интернет сегодня вкладываются огромные средства, да и он сам стал, без преувеличения, нервной системой современной экономики.

Уже несколько лет идет работа над проектами Internet2 и Planet Lab. Первый призван стать новой физической структурой Интернета, принеся в него невиданные доселе скорости, а второй — приспособить логиче-

скую структуру Сети к современным условиям. К примеру, современный Интернет не имеет «врожденных» механизмов для борьбы с вирусами и червями. Вам известно, что вирусные эпидемии случаются довольно часто, а антивирусное программное обеспечение порой генерирует едва ли не больше трафика, чем, например, сетевой червь, рассылающий свои копии по электронной почте. Все эти проблемы и призваны решить вышеупомянутые и многие другие исследовательские проекты.

Сети меняют мир вокруг нас, превращаясь в настоящую параллельную реальность, в котором люди, а порой даже не сами люди, а их идеальные воплощения живут, работают и общаются. Вот к чему привела более чем столетняя история событий, изобретений и разработок. Сети стали главной инфраструктурой современного мира, и можно не объяснять, какое значение имеют в этом мире пользовательские сетевые навыки. Приобрести эти навыки можно разными способами, в том числе и с помощью изучения этой книги.

Компьютерное образование — это постоянный, непрекращающийся процесс. Никто не может с уверенностью утверждать, что он знает и умеет достаточно много, — ведь в компьютерной отрасли каждый день происходит что-то новое. И чем больше человек узнает о компьютерах и о сетях, тем лучше он понимает, как мало знает и как ограничен его кругозор.

Но не будем отвлекаться от основной темы от компьютерных сетей. А раз так — переходим от, несомненно, интересной истории к еще более интересной практике: сейчас мы рассмотрим классификацию компьютерных сетей.

Как только заходит разговор о компьютерах и сетях, следует быть особенно внимательным: в этой области не существует ни мелочей, ни теоретических «излишеств». Здесь имеет значение буквально каждое слово.

1.2. ЛОКАЛЬНЫЕ И ГЛОБАЛЬНЫЕ СЕТИ

Определимся с терминами и основными свойствами сетей.
Схематическое изображение соотношения локальных и глобальных сетей вы видите на рис. 1.3.

Локальные сети называют LAN (Local Area Network). Это общепринятая аббревиатура. Как правило, локальными сетями называют сети, соединяющие компьютеры в радиусе до 1–2 километров.

Физической основой локальных сетей служат такие технологии, как, например, Fast Ethernet, обеспечивающий пропускную способность 100 Мбит/с, Gigabit Ethernet на 1000 Мбит/с или один из вариантов Wi-Fi. Все они достаточно универсальны для реализации различных сервисов, которые требуют большой пропускной способности сети.

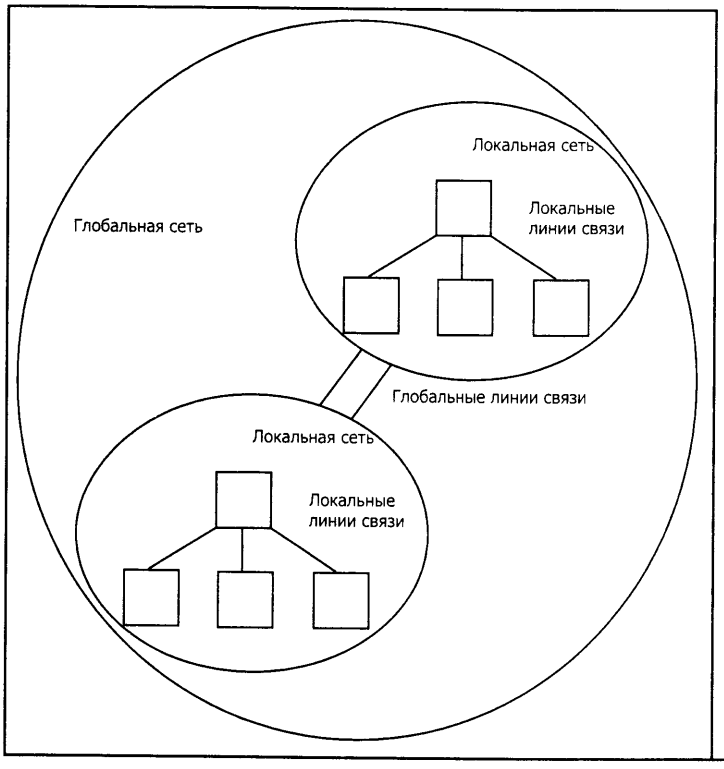


Рис. 1.3. Соотношение локальных и глобальных сетей

Что это за сервисы? Передача больших объемов информации за весьма умеренную плату или вовсе без таковой — если, например, сеть принадлежит какой-либо организации и используется для внутрипроизводственных нужд. Кроме того, локальные сети представляют собой благодатную среду для развития сетевых игр.

Но LAN при всей их универсальности обладают одним серьезным недостатком — и даже не недостатком, а особенностью, которая на определенном этапе превращается в недостаток. Заключается эта особенность в ограниченности расстояний. Для разных технологий локальных сетей это разные цифры, но рано или поздно возникает потребность в связи на больших расстояниях. «Чистые» локальные сети такую связь осуществить не могут. Поэтому на сцену выходят глобальные сети, WAN (Wide Area Network). Есть еще некий Metropolitan Area Network промежуточный вариант сети — сеть масштаба города — MAN.

MAN — высокоскоростная сеть, которая приближается по скоростям передачи данных к локальным сетям, но прокладывается в масштабах городов и служит для связи городских локальных сетей. Для обычных пользователей, то есть для нас с вами, интереснее локальные сети. Но локальные сети сближаются с глобальными. Технологиям сегодняшнего дня присуща конвергенция (взаимное проникновение), ну а случай с сетями — самый яркий тому пример.

Конечно, технологии, применяемые для передачи данных в локальных и глобальных сетях, различны. Если вы научитесь строить простые Ethernet-сети, то это не значит, что вы сможете точно так же создать подобие глобальной сети. Но на общем уровне тенденции их развития одинаковы.

Глобальные линии связи становятся все быстрее — и тут же распространяется высокоскоростной доступ к глобальным сетям через локальные сети. К примеру, локальная сеть предприятия соединяется с Интернетом посредством выделенной линии — довольно быстрого соединения. В свою очередь, Интернет все чаще используют в качестве среды для построения виртуальных сетей: сети центрального офиса и филиала могут быть связаны воедино при помощи глобальной сети. Выросли скорости магистральных каналов глобальных сетей — и мы тут же видим лавинообразное развитие мультимедийных сервисов, да и сам WWW все больше ориентируется на высокоскоростные линии связи. Локальные и глобальные сети в своем развитии сталкиваются с одинаковыми проблемами. Возьмем, скажем, проблему безопасности — ей уделяют много внимания и в локальных, и в глобальных сетях.

1.3. ВЫВОДЫ

Полагаю, теперь у вас есть представление о компьютерных сетях. В следующих главах мы поговорим об основах передачи данных, о линиях связи и сетевом оборудовании.

ГЛАВА 2
ПЕРЕДАЧА ДАННЫХ, ЛИНИИ СВЯЗИ

В этой главе рассказывается об основах передачи данных и о линиях связи. Здесь же мы впервые заведем разговор о сетевом оборудовании. Вы также познакомитесь с характеристиками кабелей, чаще всего используемых для монтажа проводных локальных сетей, и с теоретическими основами их монтажа.

2.1. ЛИНИИ СВЯЗИ

Что для сети важнее: хорошие линии связи или надежные серверы? Ответа на этот вопрос нет: важно и то и другое.

Рассмотрим различные линии связи, применяемые в локальных сетях, и некоторые их важнейшие характеристики.

ВИДЫ ЛИНИЙ СВЯЗИ

Линию связи можно представить как систему, через которую передаются сигналы. Если рассмотреть линии связи поближе, то окажется, что они представляют собой совокупность аппаратуры передачи данных, то есть физических сред, через которые эти данные передаются, и других устройств, так или иначе участвующих в передаче.

В первом приближении линии связи можно разделить на аналоговые и цифровые. Примером аналоговой линии связи может служить, например, модемное соединение с провайдером. Отличительной особенностью аналоговых линий связи является то, что их сигнал носит непрерывный характер — диапазон его значений находится в неких пределах и может принимать бесконечное множество значений. Цифровые же линии связи отличаются фиксированным набором значений, которые может принимать передаваемый по линии сигнал.

Помимо цифровых и аналоговых, среди линий связи выделяются кабельные каналы и радиоканалы. Эти последние — не что иное, как среда передачи данных для беспроводных сетей.

На кабельных системах остановимся подробнее: ведь именно они — основа популярных локальных Ethernet-сетей.

Сегодняшние кабельные системы основаны на так называемой витой паре. Витая пара — это кабель, состоящий из нескольких скрученных между собой проводов, заключенных в общую изоляцию. Различают неэкранированную и экранированную витые пары.

- ❑ Экранированная витая пара называется STP (Shielded Twisted Pair) и представляет собой скрученные провода, заключенные в экранирующую оплетку
- ❑ Неэкранированная витая пара называется UTP (Unshielded Twisted Pair, или Unscreened Twisted Pair) и, как ясно из названия, не имеет дополнительного экранирования.

Для полноты изложения упомяну и другие типы кабелей.

- Коаксиальный кабель, состоящий из центральной медной жилы, заключенной в экранирующую оплетку. Этот кабель все реже встречается в современных локальных сетях, так как он в основном вытеснен витой парой.
- Оптоволоконный кабель в качестве несущей среды использует оптическое волокно. Он поддерживает очень высокие скорости передачи данных. Оптоволоконная линия связи защищена от помех. Оптические кабельные системы применяются там, где нужны высокие скорости и высокая надежность линий.

ВИТАЯ ПАРА (TWISTED PAIR)

Рассматривая подробности характеристик витой пары, начнем с кабеля UTP.

Кабель UTP отличается невысокой стоимостью и достаточно хорошими характеристиками, о которых будет сказано чуть ниже. Именно поэтому UTP так часто применяется в строительстве современных локальных сетей. Кабель UTP состоит из скрученных между собой проводов, заключенных в общую оплетку.

Провода кабеля UTP скручены не произвольно, а в соответствии со строго определенными параметрами: от параметров скрутки зависят характеристики кабеля. Поэтому, если, например, произошел разрыв такого кабеля, то его лучше заменить, а не пытаться восстановить своими силами. Правильно вы его не скрутите, зато ухудшите характеристики сети.

Кабели в сети должны удовлетворять определенным индустриальным стандартам. Это нужно для обеспечения совместной работоспособности устройств разных производителей. Среди UTP-кабелей существует несколько категорий.

- UTP 1 категории — это устаревший стандарт. Разрешите мне не стесняться в выражениях: помянутый кабель — это телефонная лапша, то есть он предназначается для передачи голоса и низкоскоростной передачи данных и сегодня для построения сетей не применяется.
- UTP 2 категории — тоже устарел.
- UTP 3 категории — устарел.
- UTP 4 категории — это чуть улучшенный UTP 3 категории. Электрические характеристики кабеля UTP 4 категории лежат в диапазоне до 20 МГц. Сегодня этот кабель устарел и применяется крайне редко.
- UTP 5 категории — его электрические характеристики определены в диапазоне до 100 МГц. Его вариант называется UTP 5e (рис. 2.1). Это наиболее широко применимый стандарт, поэтому вскоре его придется рассмотреть подробнее.
- UTP 6 категории — характеристики определены до частоты 200 МГц.
- UTP 7 категории — характеристики определены до частоты 600 МГц.

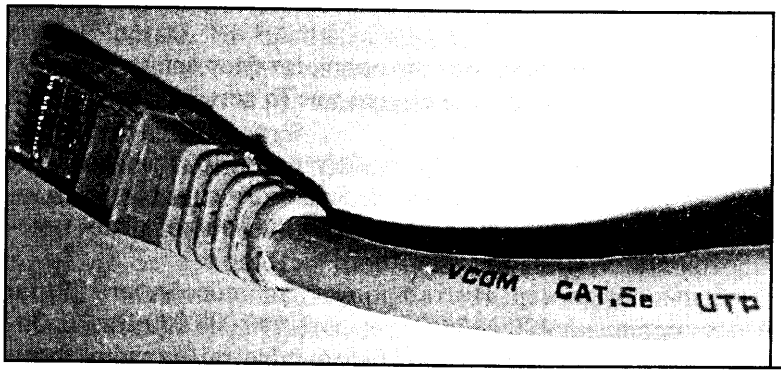


Рис. 2.1. UTP категории 5e

Для кабелей существует несколько общеупотребительных стандартов. Вышеперечисленные категории кабелей стандартизованы именно по этим стандартам:

- ❑ Европейский стандарт EN50713;
- ❑ Международный стандарт ISO/IEC 11801;
- ❑ Американский стандарт ANSI/TIA/EIA 586-B.2.

Помимо разделения на категории, каждый кабель имеет определенные характеристики. Их много, и рассмотрение всех этих характеристик не входит в наши задачи. Мы остановимся лишь на основных параметрах, чтобы слова и фразы вроде Attenuation или Near End Cross Talk не ставили вас в тупик. Рассматривая эти характеристики, мы приведем примеры «из жизни» UTP 5 категории как самого распространенного и востребованного для нас с вами стандарта.

ПРОПУСКНАЯ СПОСОБНОСТЬ И ПОЛОСА ПРОПУСКАНИЯ

Пропускная способность — это скорость передачи данных по линии связи. В качестве единицы пропускной способности используется бит в секунду. Именно бит, так как байты, которыми мы пользуемся «в повседневной жизни», в сущности — величина, базирующаяся на битах.

В качестве единицы пропускной способности сети можно использовать такой показатель, как пакет в секунду, но в конечном счете все сводится к битам в секунду.

Бит — наименьшая единица информации. Бит может принимать два состояния — единица или ноль. Передача данных в современных сетях связи ведется последовательно, то есть один байт передается побитно. Бит в секунду — это очень мало, и, чтобы не иметь дела с гигантскими числами, гораздо чаще используются такие единицы скорости, как килобиты в секунду (Кбит/с), мегабиты в секунду (Мбит/с), гигабиты в секунду (Гбит/с). Другие величины пока не получили широкого распространения, но, учитывая бурное развитие сетевой отрасли, осталось совсем немного до терабитов в секунду (Тбит/с) и... и так далее.

Килобиты и мегабиты в сетевой отрасли соответствуют принятой в других отраслях науки десятичной системе счисления. То есть 1 Кбит/с — это 1000 Бит/с.

Но основы информатики учат, что 1 килобайт равен 1024 байтам — ну и так далее. Как же перейти от «сетевого» десятичного счисления килобитов и мегабитов к привычным для компьютерщиков килобайтам и мегабайтам?

Разберем небольшой пример. Пусть пропускная способность линии передачи данных составляет 100 Мбит/с, то есть 100 000 000 Бит/с. Заметьте: это значение в битах. Перейти от битов к байтам (которые, напомню, состоят из 8 битов) очень просто — значение скорости в битах надо разделить на 8. Что же, делим — и получаем 12 500 000 Байт/с.

100 000 000 Бит/с : 8 = 12 500 000 (Байт/с)

Теперь нужно перейти к килобайтам. Для этого полученные 12 млн. байт в секунду делим на 1024 и, округлив, получаем 12 207 Кбит/с.

12 500 000 (Байт/с) : 1024 = 12 207 (Кбит/с)

И, наконец, перейдем от килобайтов к мегабайтам.

12 207 (Кбит/с) : 1024 = 11,9 (Мбит/с)

Получается, что 100 «метрических» Мбит/с — это «всего» 11,9 «компьютерных» Мбит/с, а вовсе не 100 мегабайт в секунду. Но вряд ли вы получите даже эти 12 мегабайт в секунду: на деле скорость передачи из-за помех в кабелях будет еще меньше.

Качество передачи данных по линии связи определяется параметром *Bit Error Rate*, или, сокращенно, BER. На современных линиях связи этот

параметр довольно низок — он изменяется от 10^{-4} до 10^{-9} в различных линиях связи. Разумеется, чем меньше значение BER, тем лучше.

Полоса пропускания определяет непрерывный диапазон частот синусоидального сигнала, при которых этот сигнал передается по кабелю без значительных искажений [1]. Чем шире полоса пропускания, тем больше максимально возможная скорость передачи информации по линии связи.

Между пропускной способностью линии и полосой пропускания существует определенная зависимость. Есть несколько формул, определяющих эту зависимость. Например, формула Шеннона [1].

$C = F \log_2 (1+ SNR)$

В этой формуле:

C — максимальная пропускная способность линии, бит в секунду;

F — ширина пропускной способности линии, герц;

SNR — соотношение сигнал/шум, дБ.

Из формулы видно, что реальная пропускная способность зависит от полосы пропускания и от соотношения сигнал/шум. Теоретически это соотношение может быть бесконечно большим, то есть линия связи — опять же теоретически — может обладать неограниченной пропускной способностью. Но практика вносит свои коррективы: для повышения пропускной способности линии можно либо повышать мощность сигнала, что приводит к усложнению передатчика, либо снижать мощность шума, что еще сложнее.

Ну а еще можно увеличивать полосу пропускания линии, что и делается на практике.

Есть еще одна формула, для понимания которой нужно обладать определенным запасом теоретических знаний. Это формула Найквиста [1], которая определяет зависимость пропускной способности линии от ширины полосы пропускания и способа кодирования информации. Итак, вот эта формула.

$C = 2F \log_2 M$, где M — количество состояний сигнала, при помощи которого кодируется информация. Формула Найквиста не учитывает соотношение сигнал/шум, но даже без его учета очевидно, что, используя способ кодирования, применяющий большее количество значимых состояний сигнала, можно получить более высокую скорость передачи данных при тех же физических характеристиках линии.

ПОМЕХИ

Продолжая разговор о свойствах кабеля, рассмотрим помехи и их классификацию. Нужно понимать, что рекомендации, касающиеся обращения с кабелями, далеко не случайны.

- Не рекомендуется восстанавливать поврежденные UTP или STP-кабели. Чтобы сеть могла полноценно функционировать, поврежденный кабель следует заменить новым.
- Не рекомендуется прилагать к проводам нагрузки, растягивающие их. Кабелям противопоказаны сильные сгибы, сжатия и так далее.

ATTENUATION (ЗАТУХАНИЕ)

Затухание — это относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты [1]. Конкретные значения затухания имеют смысл именно для определенной частоты сигнала. Затухание измеряется в децибелах на метр.

Мощность сигнала, распространяющегося по линии связи, падает. Чем меньше падает мощность, тем лучше связь. Именно поэтому длина линий связи ограничена и весьма строго оговаривается в стандартах локальных сетей.

NEXT (ПЕРЕКРЕСТНЫЕ НАВОДКИ НА БЛИЖНЕМ КОНЦЕ)

Параметр *Near End Cross Talk* — перекрестные наводки на ближнем конце — определяет помехоустойчивость кабеля к внутренним источникам помех. Дело в том, что так называемый наведенный сигнал, исходящий от соседней пары проводов UTP, может привести к существенному искажению сигнала, принимаемого по соседней паре. Получается, что мощный сигнал, передаваемый по одной паре, в самом начале своего пути может воздействовать на ослабленный сигнал, «прибывающий» по другой паре. Это и есть перекрестная наводка на ближнем конце.

Такие наводки могут быть причиной снижения эффективной скорости передачи или даже блокировки сетевого оборудования. Для технологий, предающих данные сразу по нескольким витым парам, имеет значение параметр PS NEXT (*PowerSum NEXT*). Он определяет суммарную мощность перекрестных наводок в кабеле.

Это, кстати, еще раз подтверждает вышеприведенные рассуждения о том, что с кабелями следует обращаться осторожно и не пытаться восстанавливать порванные провода.

ВОЛНОВОЕ СОПРОТИВЛЕНИЕ

Волновое сопротивление (полное сопротивление в сети) называют также импедансом. Единицей измерения волнового сопротивления является Ом. Это постоянная для кабеля величина. Номинальным значением импеданса для витой пары 5 категории может быть, например, 100 Ом.

Возможные отклонения от номинала могут быть вызваны низким качеством кабеля или разъемов: непостоянством диаметра проводника или свойств диэлектрика, нарушением симметричности витой пары. Изменение волнового сопротивления может быть результатом некачественной заделки проводов кабеля в контакты разъема, механическими нагрузками на кабель во время прокладки и в процессе использования.

Под механическими нагрузками понимаются растяжение кабеля, чрезмерный изгиб, скручивание, давление и так далее. Вот почему кабель требует к себе бережного отношения и плохо переносит восстановление после разрыва. Так что рассуждения о качестве прокладки или о том, как следует обращаться с кабелями, — это вовсе не пустой звук.

При передаче на высоких частотах (от 100 МГц) импеданс зависит также и от частоты передачи.

АКТИВНОЕ СОПРОТИВЛЕНИЕ

Активное сопротивление — это сопротивление постоянному току. Активное сопротивление зависит от длины кабеля.

ЕМКОСТЬ

Емкость — это свойство металлических проводников накапливать энергию [1]. В случае с сетями это свойство усугубляется тем фактом, что металлические провода, разделенные диэлектриком, образуют подобие конденсатора. Емкость — весьма нежелательное явление. Ограничивая полосу пропускания, она приводит к искажениям сигнала, и в результате скорость передачи данных падает.

ЭЛЕКТРИЧЕСКИЙ ШУМ

Источниками электрического шума, то есть электрических помех, которые выражаются в нежелательном переменном напряжении в проводнике, могут быть различные электроприборы. При этом шум может быть фоновым и импульсным.

Фоновый шум длится в течение относительно продолжительного времени, а его источниками могут быть лампы дневного света, компьютеры, микроволновые печи, офисная техника и так далее.

Источниками импульсных помех могут быть, например, сварочные аппараты.

Электрический шум измеряется в милливольтах.

ВОЗВРАТНЫЕ ПОТЕРИ

Возвратные потери иначе называются эхом передачи (*Return Loss, RL*). Эхо передачи — это параметр, который определяется отношением мощности передаваемого по линии сигнала к мощности отраженного. Эхо передачи приводит к искажению передаваемого сигнала и вызывается неоднородностями волнового сопротивления в линии передачи.

ХАРАКТЕРИСТИКИ КАБЕЛЯ

Диаметр проводника

Для классификации диаметра или площади сечения проводника чаще всего используется система AWG — *American Wire Gauge*. В этой классификации с увеличением номера уменьшается диаметр проводника.

Шаг скрутки проводов

Кабели UTP выпускаются в четырехпарном исполнении. Каждый проводник в таком кабеле имеет определенный цвет и шаг скрутки. Не во всех кабелях для передачи данных используются все линии.

Для соединения кабелей и оборудования используются стандартизированные вилки и розетки RJ-45 (рис. 2.2). Это восьмиконтактные разъемы, внешне напоминающие телефонные RJ-11, но шире последних.

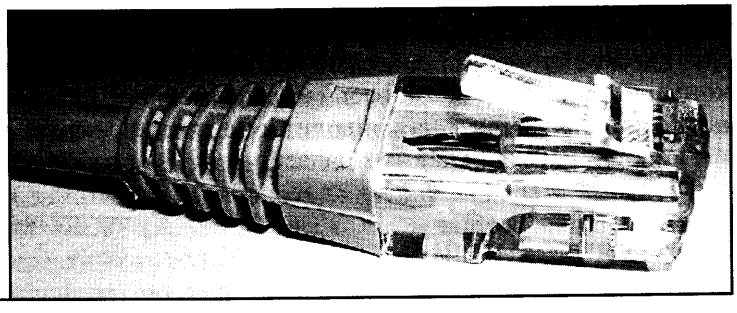


Рис. 2.2. Розетка RJ-45

Посмотрим на характеристики популярного кабеля UTP Cat. 5e. Характеристики такого кабеля определены до частоты 125 МГц.

Волновое сопротивление кабеля в диапазоне до 100 МГц равно 100 Ом. Допускаются отклонения ± 15 Ом.

Затухание принимает значение 20 дБ на частоте 1 МГц и доходит до 22,9 дБ на частоте 125 МГц.

Параметр NEXT тоже зависит от частоты и принимает на частоте 1 МГц значения не менее 75 дБ, а на частоте 125 Мгц — 41 дБ.

Активное сопротивление не должно превышать 170 Ом на километр.

Характеристиками кабеля UTP Cat. 5e мы и начнем, и закончим рассмотрение кабелей, так как в нашем случае потребуются характеристики именно этого кабеля — физической среды передачи данных. На приведенных выше характеристиках основаны некоторые правила работы с кабелями, о которых вы прочтете в одной из следующих глав.

2.2. СЕТЕВОЕ ОБОРУДОВАНИЕ

Посредством кабелей связывается различное сетевое оборудование. Существует много видов сетевого оборудования. Простейшим сетевым устройством (для применения в стандарте Ethernet) является повторитель (*repeater*). Это своего рода «продолжение кабеля» (рис. 2.3).

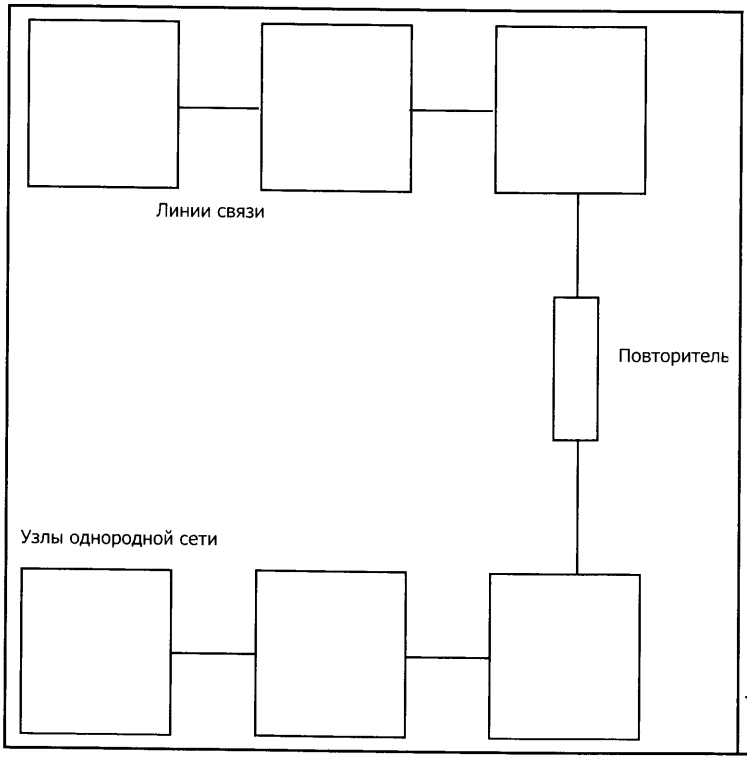


Рис. 2.3. Сеть с повторителем

Сетевое устройство упрощенно можно представить в виде некой совокупности портов, взаимодействие которых между собой подчинено определенному алгоритму. Под портами здесь понимаются сетевые интерфейсы, с помощью которых устройство может быть связано с другими устройствами.

Повторитель, получив на один из своих портов какой-то сигнал, просто повторяет его на других своих портах. Повторители в чистом виде

были нужны в те времена, когда важной физической составляющей сети являлся коаксиальный кабель. Эта технология устарела, но о ней стоит рассказать в двух словах.

Сеть на основе коаксиального кабеля строится следующим образом: например, пусть у нас есть три компьютера с сетевыми картами, к которым подключаются отрезки коаксиального кабеля, снабженного особыми Т-образными адаптерами. Получается, что для связи трех компьютеров понадобится как минимум два отрезка коаксиального кабеля, первый из них соединяет первый компьютер со вторым, второй — второй компьютер с третьим, а связь первого и третьего компьютеров производится через «посредника», то есть через второй компьютер (вернее, через тот самый Т-образный соединитель).

Возможности коаксиального кабеля ограничены: **для тонкого коаксиального кабеля сетей Ethernet максимальная длина одного сегмента не должна превышать 185 метров. При этом число подключений на один сегмент ограничивается тридцатью компьютерами.**

А что, если надо объединить в локальную сеть больше чем 30 компьютеров или если эти компьютеры разнесены территориально дальше, чем на 185 метров? Ответ прост — использовать повторитель. Кстати, повторители не позволят построить бесконечную сеть: удлинять с его помощью сеть можно лишь до определенного момента, после которого повторители уже не спасут.

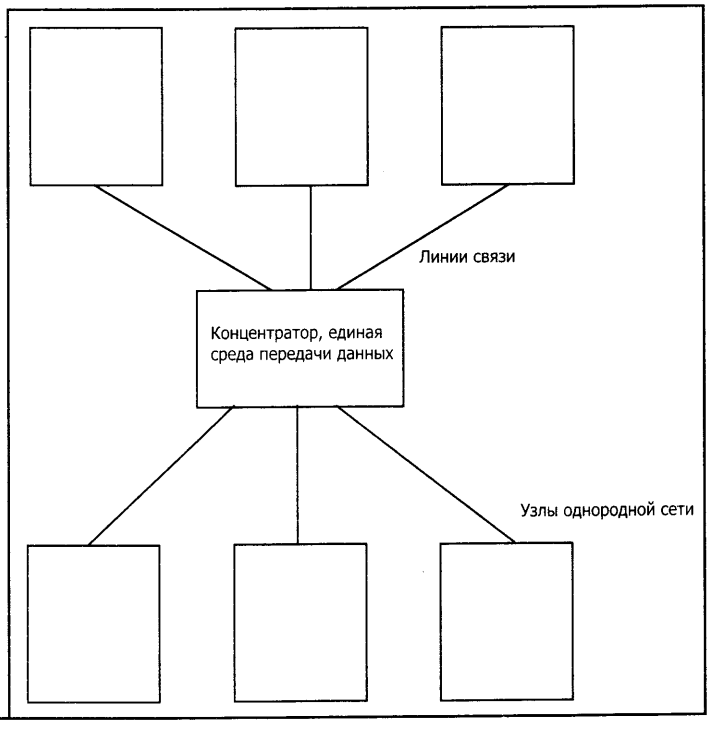
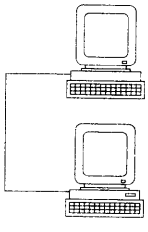


Рис. 2.4. Сеть на основе коммутатора или концентратора

В современных сетях повторители эволюционировали до **концентраторов**. В своем простейшем виде концентратор (рис. 2.4) — это повторитель, который связывает несколько компьютеров воедино. Если говорить о логике работы сети Ethernet с разделяемой средой передачи данных, то окажется, что обычный концентратор соединяет все подсоединенные к нему кабели в одну общую среду передачи данных. В качестве синонимов русскому слову «концентратор» используются английские слова *concentrator* или *hub*. Последнее слово, то есть *хаб*, часто применяется для характеристики других устройств, которые куда «умнее» обычного повторителя.

Если в одной Ethernet-сети работает достаточно много компьютеров, производительность сети падает. Так, например, если несколько компьютеров «захотят» передавать большие объемы данных, сеть будет перегружена и, несмотря на то, что каждому компьютеру выделяется определенное время для доступа к ресурсам общей среды передачи данных (а во многом и из-за этого), работа сети может замедлиться. Перегрузки может испытывать даже сравнительно небольшая сеть из десятка компьютеров. Построение Ethernet-сетей на основе единой разделяемой среды передачи данных — это хорошая идея, но не единственно возможная.

Сеть можно разделить на несколько взаимосвязанных сегментов, исходя, к примеру, из объема трафика, циркулирующего между группами компьютеров.



Предположим, что в сети из десяти компьютеров, «сидящих» на одной разделяемой линии, отчетливо выделяются две группы и большая часть трафика приходится на обмен данными внутри этих групп. Это могут быть, к примеру, рабочие группы или отделы организации. В этом случае логика подсказывает разделить одну сеть на две, чтобы компьютеры не мешали друг другу.

Помимо большей части трафика, циркулирующего между «рабочими группами», существует еще меньшая часть — обмен между группами. Для решения этой проблемы можно применить сетевое устройство, называемое **мостом** (*bridge*). Мост (рис. 2.5) располагается между двумя сегментами сети и пропускает в соседний сегмент только те пакеты данных, которые предназначены для компьютеров этого соседнего сегмента. Он не будет бездумно транслировать все, что попадает на его порты. Таким образом можно структурировать сеть и повысить эффективность ее работы.

Но мост — не слишком «умное» устройство. Мосты, к примеру, не допускают возникновения замкнутых контуров. Мост не знает топологии сети: он лишь следит за тем, с какого порта на него приходят пакеты

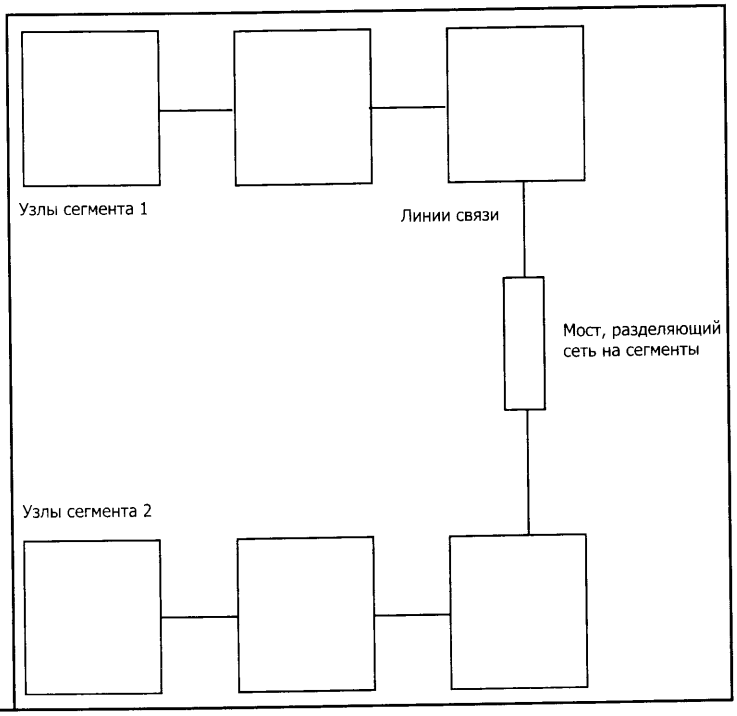


Рис. 2.5. Сеть, разделенная на сегменты мостом

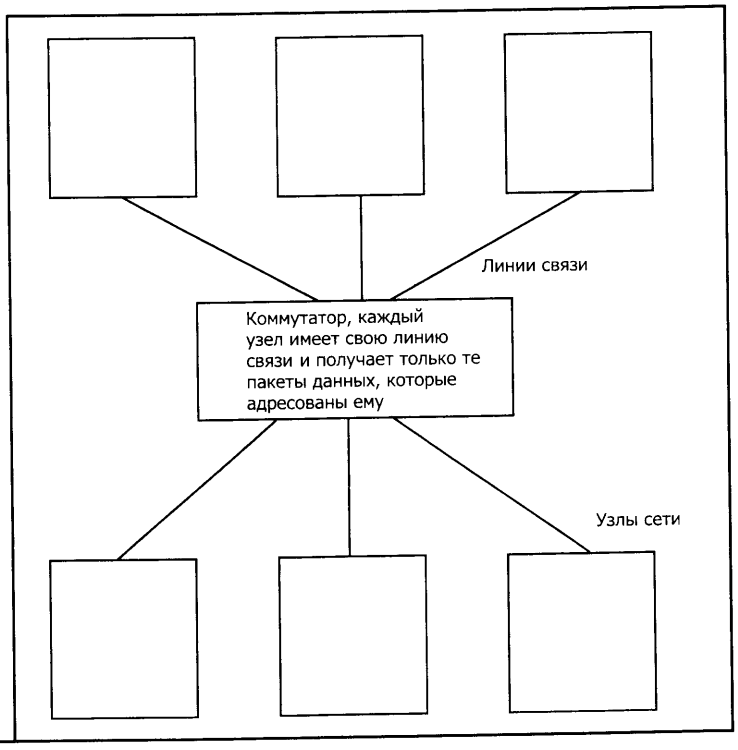


Рис. 2.6. Сеть на основе коммутатора

с определенным аппаратным адресом (это адрес, «зашитый» в сетевой карте), а потом отправляет на этот порт пакеты данных из других сегментов сети, предназначенные для этого адреса.

Продвинутым вариантом моста является **коммутатор** (*Switch*, или *Switching Hub*).

Фактически коммутатор (рис. 2.6) — это все тот же мост, каждый порт которого обрабатывает данные независимо от другого и может самостоятельно соединяться с другими портами. Коммутаторы очень популярны в современных Ethernet-сетях. Коммутатор для простых локальных сетей стоит около $ 20.

Но коммутатор — это еще не вершина сетевого оборудования. **Маршрутизатор** (*router*) куда умнее коммутатора.

Маршрутизаторы (рис. 2.7), в отличие от мостов, работают с адресами более высокого уровня, нежели аппаратные адреса, и потому прини-

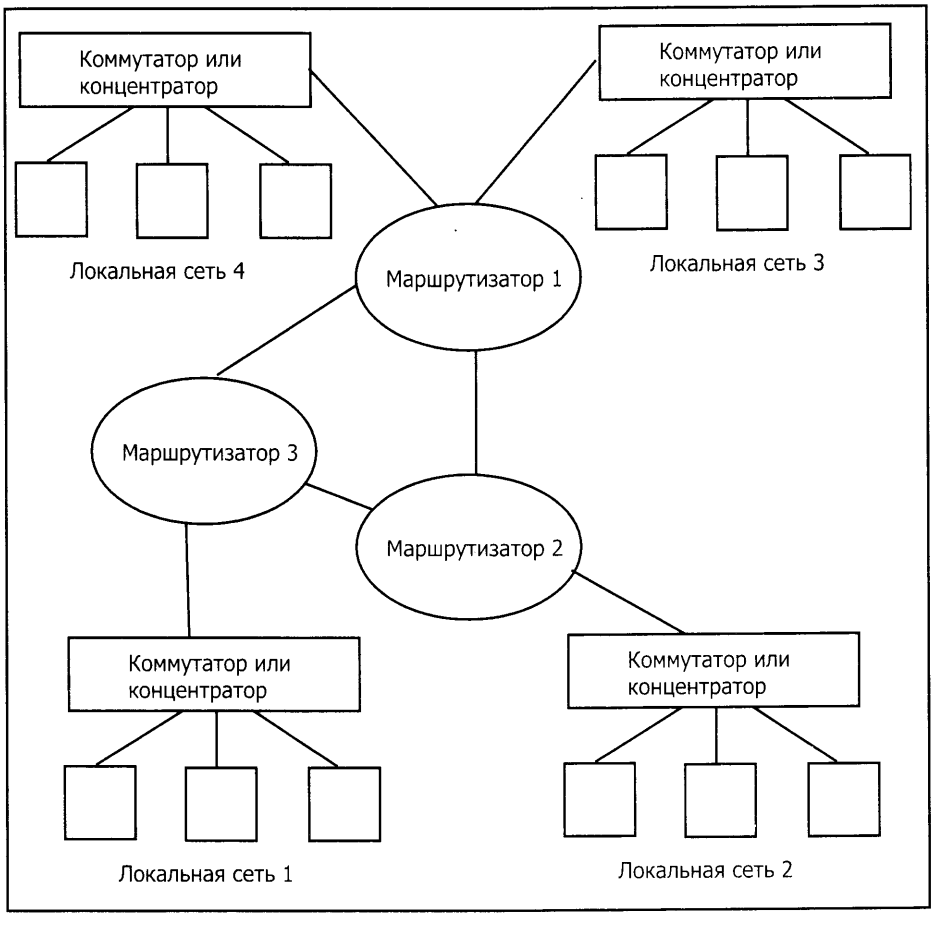


Рис. 2.7. Сеть, имеющая в своем составе маршрутизаторы

мают решения о приеме и передаче пакетов данных на более изощренном уровне. Они строят так называемые таблицы маршрутизации, которые позволяют им работать в сетях с замкнутыми контурами. Маршрутизаторы не просто предают пакеты на определенный порт, но выбирают наиболее рациональный маршрут, если есть варианты. К тому же маршрутизаторы могут объединять сети, выстроенные по разным сетевым технологиям.

Кроме маршрутизаторов, объединять разнородные сети может **шлюз**, или, в английской терминологии, *Gateway*.

2.3. ВЫВОДЫ

Финал этой главы насыщен техническими терминами, которые начинающим могут быть непонятны. Ни о чем не беспокойтесь и продолжайте читать дальше. Вскоре вы все поймете.

В следующей главе вас ждет продолжение рассказа о сетях. Из нее вы узнаете о семиуровневой модели OSI, топологиях сетей и о многом другом.

ЛИТЕРАТУРА

1. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. — СПб.: Питер, 2001.

Глава 3

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Чтобы сеть заработала, недостаточно иметь кабельную систему и сетевое оборудование. Для работы сети нужны слаженные действия составляющих ее подсистем. А построить работающую систему из множества разных компонентов можно, лишь если строго стандартизовать эти компоненты, связи между ними и многие другие параметры.

Целью любой стандартизации является выработка рекомендаций, которые в итоге позволяют строить системы из компонентов разных производителей. Скажем, кабель для нашей сети производит одна компания, разъемы — другая, сетевое оборудование — третья, программное обеспечение — четвертая. Как тут обойтись без стандартизации?

Стандартов, которые так или иначе затрагивают компьютерные сети, великое множество. Но из их числа самым важным для понимания сущности функционирования сетей стандартов является модель OSI. Ее разработали в 80-х годах прошлого столетия.

3.1. СТАНДАРТИЗАЦИЯ И СЕМИУРОВНЕВАЯ МОДЕЛЬ OSI

Сокращение OSI расшифровывается как *Open System Interconnection*, то есть взаимодействие открытых систем.

Описать сложный объект можно, представив его в виде отдельных взаимодействующих частей. Этот способ описания называется **декомпозиция**. Модель OSI — это пример декомпозиции некой сетевой системы, охватывающей все уровни сетевого взаимодействия. В этой модели семь уровней сетевых компонентов.

В ЧЕМ ПОЛЬЗА ОТКРЫТОЙ СИСТЕМЫ

Если разные производители оборудования создают устройства в соответствии с требованиями открытости, то эти устройства могут свобод-

но взаимодействовать друг с другом вне зависимости от того, кто их разработал и произвел. Открытые спецификации и стандарты, которые используются в индустрии компьютерных сетей, общедоступны. В соответствии с этими стандартами разные компании могут создавать совместимое оборудование и программное обеспечение. Конечно, идеальным вариантом была бы полная открытость систем, но зачастую это невозможно. Поэтому если хотя бы внешние интерфейсы какой-либо системы соответствуют принципам открытости, то взаимодействие других систем с такой «частично открытой» системой значительно облегчается.

Очевидно, что если корпорация будет создавать операционную систему, не содержащую подобных интерфейсов, эта ОС превратится в некую «вещь в себе». Приложения для такой ОС сможет разрабатывать только компания, которой принадлежит операционная система. Так и в случае с компьютерными сетями: чем система открытее, тем другим системам легче с ней взаимодействовать. Именно принцип открытости позволяет строить компьютерные сети из оборудования разных производителей. Именно из-за открытости возможна модернизация сети, ее быстрое и простое соединение с другими сетями и унификация. Да и в управлении такая сеть будет проще.

Интернет — это открытая система, построенная в соответствии с идеологией открытых систем и соответствующая модели OSI.

ЧТО ТАКОЕ ПРОТОКОЛ И ИНТЕРФЕЙС СИСТЕМЫ

Перед началом разговора о семиуровневой модели OSI определимся с очень важными понятиями, без знания которых дальнейший разговор не состоится. Эти понятия — интерфейс и протокол.

- **Протокол** — это «язык», на котором общаются одинаковые уровни двух связанных сетью систем.
- **Интерфейс** — это еще один «язык», понятный двум соседним уровням внутри одной системы (рис. 3.1.).

Чтобы лучше усвоить эти понятия, разберем пример: в соответствии с принципом декомпозиции разобьем на части процесс доставки письма адресату.

1. Вы пишете письмо, обычное «бумажное» письмо.

2. Исписанный лист вы кладете в конверт и опускаете его в почтовый ящик.

3. Почтальон вынимает письмо из ящика и несет его на почту. Прочитав адрес на конверте, он определяет, куда отправить письмо и, взяв еще несколько писем того же направления, передает их, скажем, транспортной службе почты.

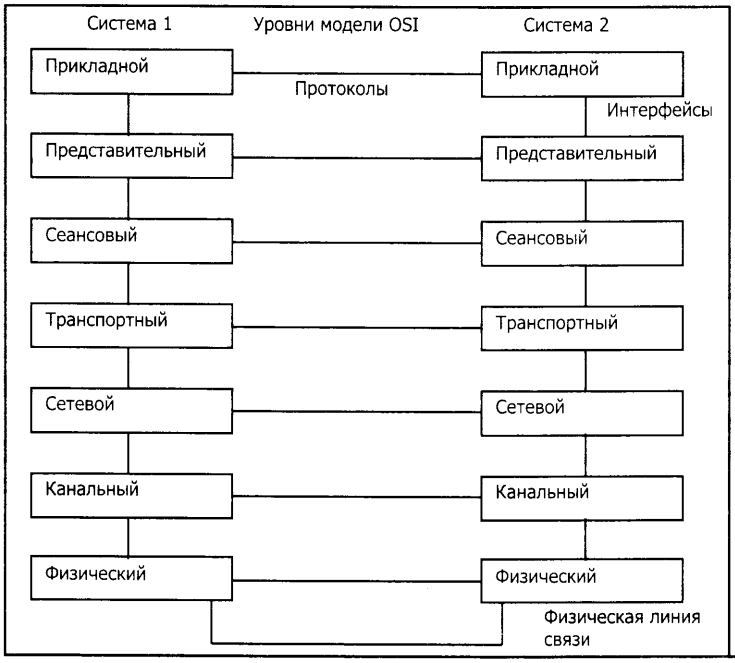


Рис. 3.1. Взаимодействие между уровнями модели OSI

4. В свою очередь транспортная служба доставляет письмо по адресу — в почтовый ящик получателя почты. При этом транспортная служба вначале доставит ваше письмо в почтовое отделение, которое расположено недалеко от дома адресата.

5. Затем другой почтальон прочтет адрес на конверте и положит его в нужный почтовый ящик.

Присмотримся к разным стадиям этого процесса. При написании письма вы обращаетесь непосредственно к его адресату: о чем-нибудь рассказываете ему или задаете вопросы. При этом вас не интересует способ доставки письма получателю, и в тексте письма вы никак не оговариваете путь его прохождения. Вы не общаетесь ни с почтальонами, ни с транспортными службами, а только с адресатом и только на русском языке. Надписав конверт и опустив его в почтовый ящик, вы не интересуетесь, кто и что будет с ним делать дальше: вас это не касается.

А теперь попробуем разбить нашу «почтовую систему» на составные части и определить в ее терминах понятий «протокол» и «интерфейс». Итак, пусть наша почтовая система состоит из трех уровней.

- Первый уровень находится на самом верху системы — это вы и ваш адресат. Назовем этот уровень «Уровень адресатов».
- Второй уровень — это почтальоны, которые забирают и разносят почту. Пусть это будет «Уровень почтальонов».
- Третий, низший уровень нашей системы, физически представлен почтовым транспортом. Назовем его «Транспортным уровнем».

Мы получаем две «Почтовые системы»: одна — наша, а другая — нашего корреспондента. Так вот, взаимодействие между двумя одинаковыми уровнями двух связанных сетью систем — это и есть протокол. Протокол, на котором вы общаетесь с вашим корреспондентом, это обычный русский язык. Протокол, на котором общаются почтальоны, — это язык адресов и почтовых индексов, а протокол транспортного уровня нашей почтовой системы — это разные железнодорожные станции, порты, аэропорты и так далее.

Теперь займемся интерфейсом, то есть языком, который понятен двум соседним уровням одной системы. Запечатав письмо в конверт и надписав адрес, вы вступаете во взаимодействие с почтальоном, который, в свою очередь, вступает во взаимодействие с транспортной системой почты. Адрес, который вы написали, а почтальон прочитал, — это и есть интерфейс вашего письма.

Точно так же взаимодействуют разные уровни эталонной модели OSI. Обсуждение этой модели мы начнем с низшего, физического уровня.

ФИЗИЧЕСКИЙ УРОВЕНЬ

По-английски нижний уровень модели OSI называется *Physical Layer*. Задача физического уровня — передавать биты данных по физическим линиям связи. Спецификации физического уровня определяют параметры сред передачи данных — это, например, полоса пропускания, затухание, волновое сопротивление, активное сопротивление, задержки при распространении сигнала и так далее (рис. 3.2). Помимо физических характеристик сред эти спецификации определяют физические характеристики сигналов. К этому же уровню относятся спецификации интерфейсных разъемов кабелей.

Вы уже поняли, что описанные в предыдущей главе характеристики кабелей имеют отношение к физическому уровню модели OSI.

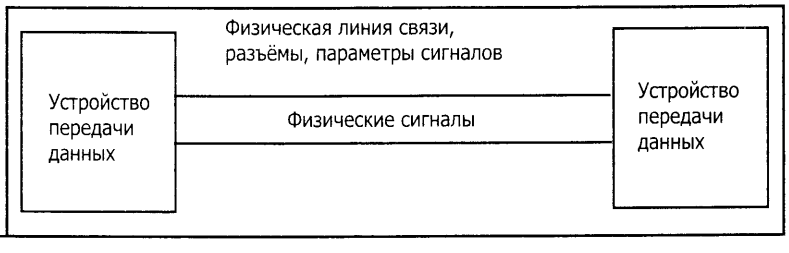


Рис. 3.2. Физический уровень

Устройствам физического уровня нет дела, что за данные они передают. Для них главное — сгенерировать, передать и распознать некую последовательность импульсов через физическую среду передачи данных. Переданные биты затем будут обработаны и в виде неких данных «пойдут» к более высоким уровням OSI.

Примером протокола физического уровня можно назвать спецификацию 100Base-TX для технологии Ethernet. В качестве среды передачи данных этот стандарт предусматривает использование кабеля UTP 5 категории, в качестве разъемов — RJ-45. Этот же стандарт описывает множество других физических характеристик. На физическом уровне работают, например, повторители.

Следующий уровень OSI — канальный уровень.

КАНАЛЬНЫЙ УРОВЕНЬ

Канальный уровень, он же *Data Link Layer* (рис. 3.4), — это уровень более «интеллектуальный», чем физический.

Задача физического уровня — передача битов данных в соответствии с физическими спецификациями передачи данных. Физический уровень не «задумывается» о том, что один и тот же канал могут попеременно использовать различные пары связывающихся компьютеров. Физическому уровню нет дела, случаются ли сбои при передаче данных или все идет хорошо. Биты на физическом уровне передаются неразделенным сплошным потоком: задача этого уровня состоит лишь в том, чтобы передать полученные от верхнего уровня данные.

А канальный уровень уже оперирует самими данными. Он разбивает поток данных, поступающих с высшего уровня, на куски, которые называются кадрами (*frame*). Каждый кадр оформляется особым образом. При этом помимо полезных данных передаются контрольные данные, в кадр включаются адреса принимающего и передающего оборудования и так далее.

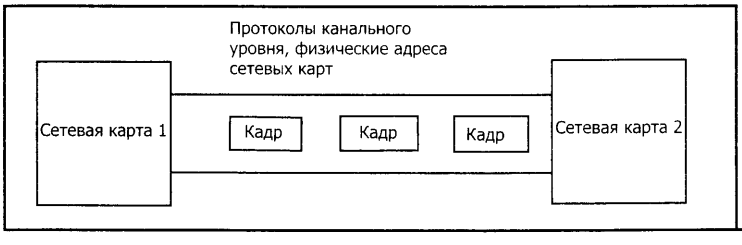


Рис. 3.3. Канальный уровень

Если получатель получит поврежденный кадр (целостность кадров проверяется путем подсчета контрольной суммы), канальный уровень повторит передачу.

Протоколы канального уровня, в случае с использованием разделяемой среды передачи данных, следят за тем, чтобы линия передачи была свободна в момент передачи. Примером протокола канального уровня можно привести протокол Ethernet.

На канальном уровне работают, например, мосты, коммутаторы, сетевые адаптеры. Нужно понимать, что каждое сетевое устройство так или иначе работает на всех уровнях OSI, на канальном уровне устройства, которые я назвал, наиболее функциональны.

Протокол канального уровня — это весьма интеллектуальная система, которая способна эффективно заниматься доставкой сообщений между двумя компьютерами (или между двумя другими устройствами). И все же «способностей» канального уровня не хватает для обеспечения работы сложной сети. Нужен еще один уровень!

К примеру, протокол канального уровня может определять способы доставки данных между двумя компьютерами в сети строго определенной структуры. Но если сеть немного усложнится (а такое поведение присуще неоднородным глобальным сетям), то возможностей канального уровня не хватит.

Разумеется, глобальные сети тоже используют канальный уровень для передачи данных. Но передача на канальном уровне осуществляется лишь между двумя «соседними» устройствами, а если речь заходит о передаче данных между устройствами, разделенными множеством разнородных сетей, передающих эти данные, особое значение приобретают протоколы следующего за канальным уровня — уровня сетевого.

СЕТЕВОЙ УРОВЕНЬ

Сетевой уровень, или *Network Layer*, расположен над канальным уровнем и служит для построения единой транспортной системы, основой которой могут стать сети, использующие различные принципы передачи данных. Схему такой сети вы видите на рис. 3.4 — здесь в качестве протокола сетевого уровня показан IP.

Канальный уровень «заведует» доставкой информации между узлами одной сети, построенной по определенной технологии. Протоколы канального уровня не умеют организовывать обмен данными между двумя сетями, построенными по разным технологиям. Заметьте, кстати: в этой главе мы довольно часто использовали термин «сеть». В случае с сетевым уровнем этот термин принимает особое значение.

Сеть в терминах сетевого уровня модели OSI — это совокупность компьютеров, объединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенного для этой топологии [1].

Сетевой уровень заведует доставкой данных между сетями. Ему нет дела до подробностей передачи данных на канальном уровне: ведь протоколы сетевого уровня оперируют адресами, отличными от тех, которые используются протоколами канального уровня.

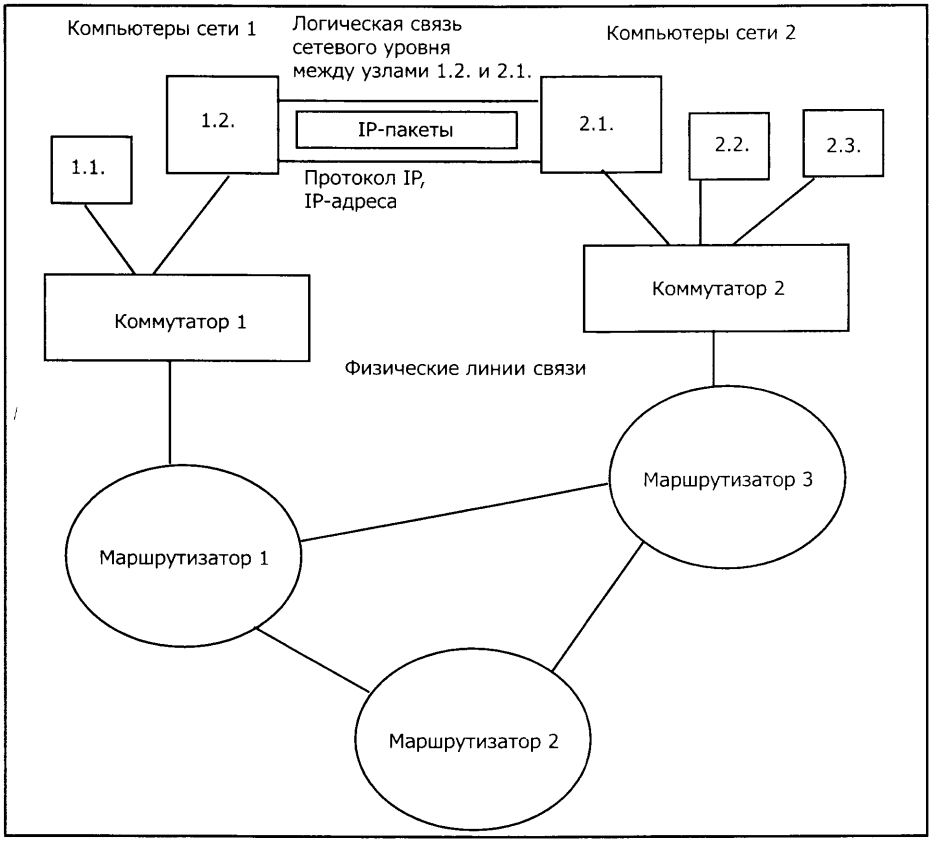


Рис. 3.4. Сетевой уровень

Одним из самых характерных устройств сетевого уровня является маршрутизатор. Руководствуясь адресами этого уровня, он осуществляет маршрутизацию трафика и выбирает самые рациональные пути его прохождения.

Если канальный уровень оперирует кадрами (*frame*), то сетевой имеет дело с пакетами (*packet*). Примером протокола сетевого уровня является IP, входящий в стек TCP/IP.

К сетевому уровню относится также протокол IPX стека IPX/SPX. Это так называемые маршрутизируемые протоколы (Routed Protocols) — протоколы, которые занимаются доставкой информации в сети. К этому же уровню относятся специфические протоколы, с помощью которых маршрутизаторы управляют трафиком. Эти так называемые протоколы маршрутизации (*Routing Protocols*) служат для сбора и анализа информации о топологии сети. Они, не перенося по сети данные, которые могут быть полезны пользователю, тем не менее играют важную роль.

Над сетевым уровнем расположен еще более высокий уровень — транспортный.

ТРАНСПОРТНЫЙ УРОВЕНЬ

Протоколы транспортного уровня (*Transport Layer*) обеспечивают надежную передачу данных для протоколов более высоких уровней или для приложений (рис. 3.5). При этом можно выбирать уровень надежности, то есть сложности процедур, который бы обеспечил более высокому уровню достаточный уровень сервиса.

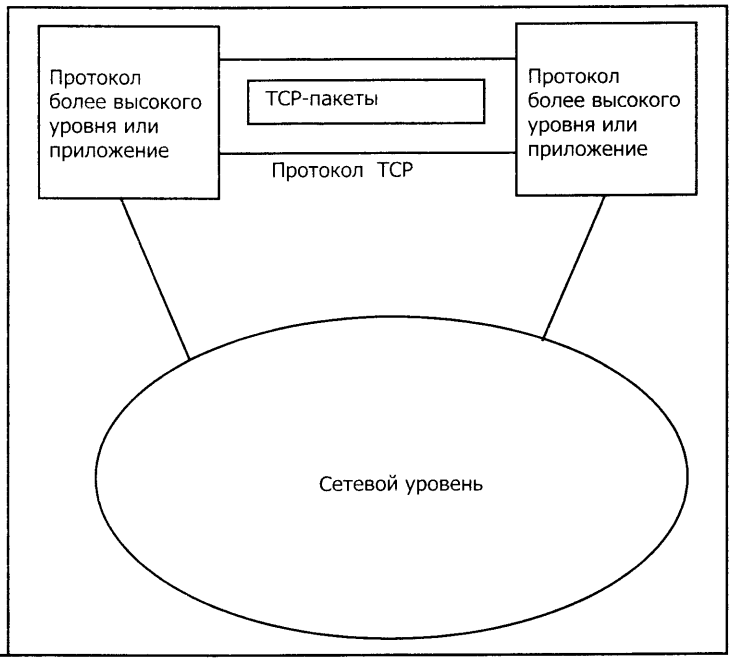


Рис. 3.5. Транспортный уровень

К примеру, в качестве приоритетных задач можно выбрать обнаружение и исправление ошибок, или высокую срочность доставки, или восстановление аварийно прерванной связи. Тип сервиса протокола транспортного уровня для различных сетей может быть разным.

Локальная сеть, чьи линии связи надежны, может обойтись методами восстановления потерянных данных более низких уровней, не тратя вычислительные ресурсы на реализацию сложных методов коррекции ошибок на транспортном уровне. С другой стороны, какая-нибудь медленная и ненадежная линия связи глобальной сети может потребовать пристального наблюдения за ошибками именно со стороны протоколов транспортного уровня.

К протоколам транспортного уровня относятся протоколы TCP и UDP стека TCP/IP и SPX протокола IPX/SPX. Как правило, функции транспортного уровня целиком реализованы программными средствами — в отличие от трех низших уровней, в реализации которых важное место занимают технические средства.

* * *

Мы рассмотрели четыре нижних уровня сетевой системы. Обобщенно их принято называть сетевым транспортом, то есть системой, которая обеспечивает исключительно транспортные функции сети, не задумываясь о характере передаваемых данных. Эти протоколы по большей части представлены физически существующими устройствами, реализующими их. А вот оставшиеся три уровня системы OSI являются исключительно программными надстройками над сетевой транспортной системой. Их основная задача — предоставление сетевых услуг приложениям. Итак, рассмотрим сеансовый уровень.

СЕАНСОВЫЙ УРОВЕНЬ

Сеансовый уровень (*Session Layer*) служит для управления ходом взаимодействия процессов. Он, к примеру, может применяться для синхронизации двух «общающихся» сторон. Как правило, этот уровень существует лишь формально, и его функции включают в себя протоколы следующего за ним уровня — уровня представлений.

УРОВЕНЬ ПРЕДСТАВЛЕНИЙ

Уровень представлений (Presentation Layer) работает с передаваемыми данными на уровне формы представления передаваемой информации. Это означает вот что: уровень представлений нужен, чтобы обеспечить взаимодействие, понимание уровней приложений. Он заключает в себе некие «переводчики» для разных «языков» более высокого уровня. Уровень представлений, не изменяя содержания передаваемых данных, может определенным образом обрабатывать их форму. Например, такая обработка может заключаться в перекодировке данных или в их шифровании. В качестве протокола уровня представлений можно назвать протокол SSL стека TCP/IP. Этот протокол служит для шифрования данных.

За уровнем представлений идет высший уровень модели OSI — уровень процессов и приложений, или прикладной уровень.

УРОВЕНЬ ПРОЦЕССОВ И ПРИЛОЖЕНИЙ

Прикладной уровень (*Application Layer*) — это набор протоколов, позволяющих пользователям работать с ресурсами сети (рис. 3.6). В качестве единицы данных протоколов прикладного уровня выступают сообщения (*message*).

В качестве примеров протокола уровня процессов и приложений можно привести протоколы SMTP (*Simple Mail Transfer Protocol*), FTP

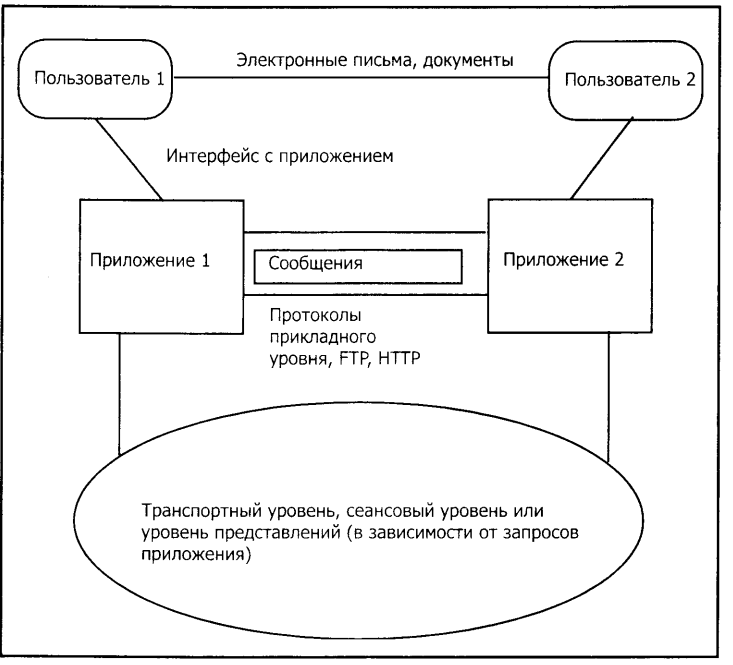


Рис. 3.6. Уровень процессов и приложений

(*File Transfer Protocol*) из стека TCP/IP и так далее. Возьмем протокол FTP: он служит для передачи файлов. Существуют специальные программы — FTP-клиенты, обладающие графическим интерфейсом и позволяющие в привычной для пользователя среде Windows оперировать ресурсами FTP-серверов.

Команды пользователя, которые он подает, например, перетаскивая файлы из одного окна программы в другое или нажимая на кнопки, преобразуются в команды протоколов FTP, которые передаются FTP-серверу. На этом простом примере можно увидеть взаимосвязь приложения и протокола прикладного уровня. При желании пользователь может воспользоваться простой коммуникационной программой и вводить FTP-команды вручную.

Рассмотрим теперь процесс взаимодействия пользователя с HTTP-сервером по протоколу HTTP (*Hyper Text Transfer Protocol,* то есть протокол передачи гипертекста).

1. Пользователь запускает веб-браузер и вводит веб-адрес (URL) нужного ему ресурса. Введенные данные (сообщение в терминах уровня процессов и приложений) передаются уровню представлений. Отметим, что такого рода сообщения имеют, как правило, заголовок, содержащий служебную информацию и тело сообщения, в котором записаны полезные данные, — не правда ли, похоже на наш пример с отправленным по почте письмом?

2. Дальше это сообщение передается уровню представлений, который снабжает его своим собственным заголовком и передает сообщение сеан-

совому уровню, который, в свою очередь, снабжает это сообщение собственным заголовком. И так далее — до тех пор, пока сообщение не примет вид, пригодный для передачи по ближайшему к пользователю сетевому интерфейсу. Пусть это будет, например, модемное соединение компьютера пользователя с провайдером. После того, как данные переданы модему провайдера, они проходят часть пути «вверх» по лестнице уровней OSI.

3. Доведя сообщение до сетевого уровня, то есть, превратив его в IP-пакет, содержащий IP-адрес, система провайдера, имеющая выход в Интернет, маршрутизирует этот пакет на нужный выход. При прохождении пакета по Интернету он снова и снова то «опускается» до физического уровня на линиях передачи данных, то опять «поднимается» до сетевого уровня на маршрутизаторах.

4. Наконец наш пакет достиг целевого сервиса. Там он «поднимается» до прикладного уровня, и сервер, распознавая команду пользователя, которая содержит URL какой-нибудь веб-странички, хранящейся на этом сервере, высылает пользователю (вернее, веб-браузеру) эту страничку. Содержимое страницы снова проходит длинный путь по Интернету, достигает браузера и отображается в нем. При этом вовсе не обязательно, чтобы страничка шла от сервера к браузеру тем же путем, по которому шел запрос от браузера к серверу, — тут все зависит от решений, которые принимают маршрутизаторы.

Все это и просто, и сложно. Я даже думаю, что «в первом чтении» многое вам осталось непонятным. Что ж, придется перечитать, постараться вникнуть в эту главу и, возможно, законспектировать особо «темные» места. Не пугайтесь трудностей: мне известно совершенно точно, что знание эталонной модели OSI вскоре позволит вам разобраться со стеком протоколов TCP/IP и некоторыми другими популярными стеками протоколов. Разобравшись в структуре модели OSI, вы легко разложите в соответствии с этой структурой информацию о протоколах.

Между прочим, существует стек протоколов, построенный в строжайшем соответствии с моделью OSI. Он так и называется: стек протоколов OSI. Он не слишком распространен, и о нем мы больше упоминать не будем, а будем ориентироваться на наиболее популярные TCP/IP, IPX/SPX и еще один прекрасный стек протоколов по имени NetBIOS.

3.2. СТЕКИ КОММУНИКАЦИОННЫХ ПРОТОКОЛОВ

Все коммуникационные протоколы определенным образом стандартизированы. Стек коммуникационных протоколов — это набор протоколов различных уровней, которые обеспечивают взаимодействие в сети. Под взаимодействием здесь понимается взаимодействие физических ус-

тройств — если речь идет о протоколах физического уровня эталонной модели OSI; взаимодействие программ, если речь идет о протоколах прикладного уровня, и так далее.

Русское слово «стек» произошло от английского *«stack»*, которое переводится как «куча», «груда», «множество». Понятие «стек» нашло широкое применение в компьютерной науке. Обычно оно используется в случаях, когда надо определить совокупность объектов, имеющих иерархическую структуру, — как, например, в случае со стеком коммуникационных протоколов.

Стеки коммуникационных протоколов TCP/IP и IPX/SPX в качестве физического уровня могут использовать Ethernet-устройства. Но вот высшие уровни для каждого стека — свои.

Все эти стеки соответствуют модели OSI не слишком строго. Дело в том, что модель OSI разрабатывалась на основе практики создания сетей и уже существующих протоколов, а не наоборот.

СТЕК TCP/IP

Сегодня самый распространенный в мире протокол — стек TCP/IP, который ведет свою историю еще от сети ARPAnet. Название свое он получил от пары протоколов: протокола IP сетевого уровня модели OSI, который обеспечивает доставку данных между узлами, и протокола TCP транспортного уровня, который делает эту доставку надежной. Помимо этих двух протоколов, стек включает в себя множество других.

TCP/IP — основной протокол Интернета, и этим все сказано: с ним работают десятки миллионов компьютеров во всем мире. На основе TCP/IP работает все больше локальных сетей. Стек TCP/IP за десятки лет своего развития вобрал в себя немало других протоколов: это и протоколы для обеспечения работы гипертекстовых служб WWW — HTTP, и почтовые протоколы SMTP и POP, и специальные протоколы для шифрования и дешифровки передаваемых данных «на лету», SSL например.

Реализация протокола достаточно сложна, и для его работы в глобальных сетях требуются специальные сервисы, например система доменных имен DNS (*Domain Name System*). Поддержка таких служб стоит дорого, но без них Интернет работать не сможет. Этот протокол прекрасно проявляет себя при маршрутизации — кстати, без маршрутизаторов Интернет тоже не смог бы работать.

На свете не существует простых в установке и настройке стеков протоколов. Но при всей сложности установки и администрирования сетей на базе TCP/IP этот стек предоставляет администраторам весьма значительные возможности и в масштабах Интернета, и для локальных сетей.

Стек TCP/IP поддерживает удобную систему адресации, обладает возможностью фрагментации пакетов, то есть умеет подстраивать их размеры при передаче через сети, построенные на основе разных технологий. Стек TCP/IP поддерживается подавляющим большинством современных операционных систем.

TCP/IP — центральный протокол для самых распространенных настольных ОС, то есть для разных реализаций разные Windows и Unix.

TCP/IP приобрел всемирное распространение из-за того, что был в свое время реализован в некогда популярной ОС Unix. История этого стека протоколов насчитывает более двадцати лет. Но есть еще один стек протоколов, который до недавнего времени тоже был весьма распространен. Я имею в виду стек коммуникационных протоколов IPX/SPX.

СТЕК IPX/SPX

Стек IPX/SPX (*Internetwork Packet Exchange/Sequenced Packet Exchange*) — это фирменная разработка компании Novell. Стек IPX/SPX разрабатывался для сетевой операционной системы Novell NetWare в 80-х годах и не утерял популярности и по сей день. Поддержка этого стека протоколов встроена даже в Windows XP.

Протокол IPX определяет формат передаваемых по сети пакетов и взаимодействие с сетевым программным обеспечением. Этот протокол находится на сетевом уровне модели OSI, а на транспортном ее уровне расположен протокол SPX.

Преимущество IPX/SP, которое позволило ему стать чрезвычайно популярным в 90-х годах прошлого века, заключалось в том, что он был ориентирован и на довольно слабые персональные компьютеры, и на работу в небольших локальных сетях. В частности, он очень вольно обращался с так называемыми широковещательными рассылками пакетов, а скажем, в TCP/IP, изначально рассчитанном на работу в больших сетях, такое недопустимо.

Если бы в Интернете действовали принципы установления соединения, основанные на широковещательных рассылках, то Интернета, каким мы его знаем, просто не существовало бы. То, что хорошо для маленькой локальной сети и даже для корпоративной сети среднего размера, для Интернета неприемлемо.

Стек IPX/SPX продолжает развиваться, но ему уже не видать прежней популярности: мир работает с TCP/IP, и с этим ничего не поделать.

СТЕК NETBIOS

Стек NetBIOS разработан IBM как сетевое расширение BIOS и предназначен для работы в простых локальных сетях. Стек протоколов NetBIOS (*Network Basic Input/Output System*) состоит из протоколов NetBIOS

и SMB (*Server Message Block*). Расположены они, соответственно, на сеансовом и транспортном (NetBIOS) и уровне представлений и прикладном уровне (SMB) модели OSI. Современная реализация NetBIOS называется NetBEUI и используется в сетях Microsoft.

3.3. ТОПОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ

Простейшей топологией локальной сети можно назвать сеть из двух компьютеров. Например, если пару компьютеров, оснащенных сетевой картой, связать кабелем (разведенным особым образом), получим сеть на основе стандарта Ethernet. Но локальная сеть из более чем двух компьютеров всегда строится с применением топологии локальных сетей, предусмотренной стандартами их построения.

Вот определение топологии локальной сети [1]: под топологией вычислительной сети понимается конфигурация графа, вершинам которого соответствуют компьютерные сети (иногда и другое оборудование например, концентраторы), а ребрам — физические связи между ними.

Но это определение подразумевает глобальные сети, а мы основное внимание уделяем локальным сетям. Локальная же получится, если на место компьютерных сетей в вершинах графа поставить отдельные компьютеры. Как бы там ни было, запомним: **топология — это способ связи нескольких компьютеров в сеть.**

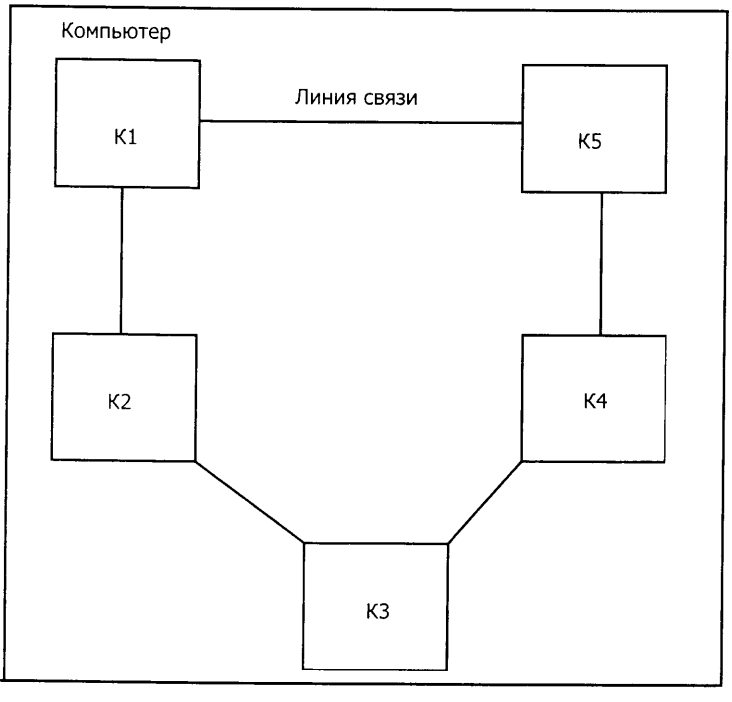


Рис. 3.7. Кольцевая топология локальных сетей

О простейшей топологии мы говорили в начале этого раздела: это одна связь, соединяющая два узла. На нее похожа так называемая кольцевая топология (рис. 3.7), когда все узлы сети соединены в **кольцо**. При этом данные, как правило, передаются от компьютера к компьютеру в одном направлении. Эта топология используется в некоторых типах локальных сетей.

Другая очень распространенная топология носит название **общей шины** (рис. 3.8). Эта топология характерна для сетей Ethernet, построенных на основе коаксиального кабеля. Серьезный минус общей шины состоит в том, что нарушение контакта в одном из соединений или повреждение одного из отрезков кабеля разбивает сеть на два независимых сегмента, фактически разрушая ее.

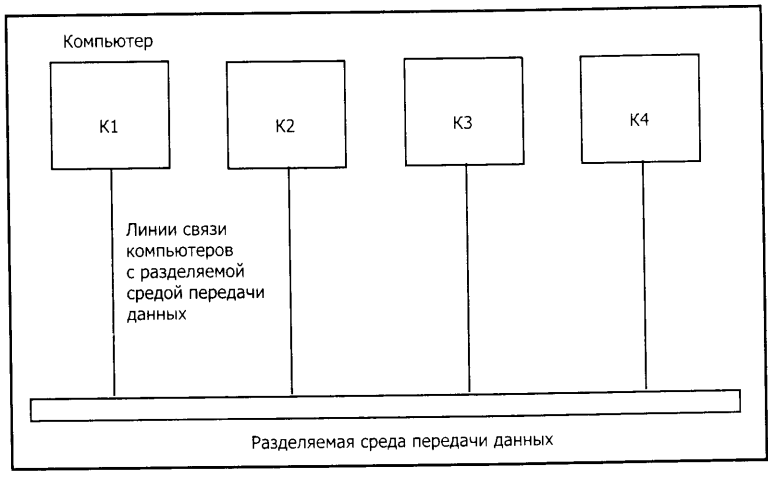


Рис. 3.8. Топология «Общая шина»

В свое время эта топология была чрезвычайно распространена: старые сети на основе коаксиального кабеля можно встретить и сегодня.

Второй серьезный недостаток топологии общей шины состоит в том, что пропускная способность линии делится между всеми компьютерами сети. Этого недостатка отчасти лишена сеть, построенная по топологии **«звезда»** (рис. 3.9). Центром такой «звезды» может быть повторитель или коммутатор.

- Поставив в центр «звезды» повторитель, мы получаем все ту же самую «общую шину», стянутую в точку, с отдельными линиями для каждого компьютера.
- Если сделать центром «звезды» коммутатор, который позволяет одновременное общение нескольких компьютеров, получается качественно иная сеть.

Но если в некоторый момент сразу несколько компьютеров захотят общаться с одним и тем же компьютером, этот «плюс» окажется несущественным. Для нас важнее другое преимущество «звезды»: ее надежность. Повреждение одного кабеля или разъема отрежет от сети — «звезды» всего один компьютер, а сеть в целом останется рабочей.

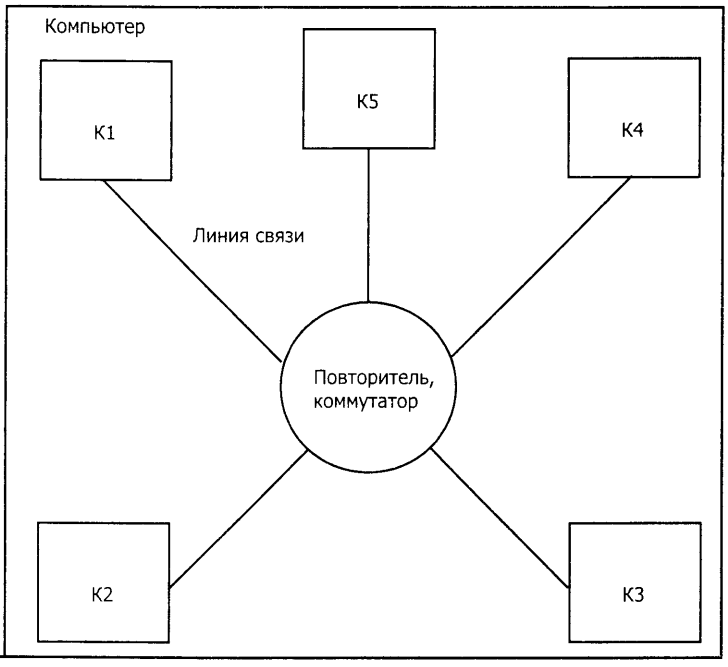


Рис. 3.9. Топология «Звезда»

Недостаток «звезды» состоит в сравнительно высокой стоимости оборудования. И все же «звездная» топология — самая распространенная сегодня топология локальных сетей по технологии Ethernet. В качестве центра сети все чаще используется коммутатор: из-за его дешевизны такое решение оправдывает себя даже в простой домашней сети.

Разновидностью топологии «звезда» является топология, соединяющая в иерархическую структуру сразу несколько сетей, построенных по топологии «звезда». Дело в том, что коммутаторы могут объединяться в иерархическую сеть. Для достаточно больших сетей это оправданно. В результате такого объединения получаем **«иерархическую звезду»**.

Топологии «звезда» и «иерархическая звезда» сегодня распространены больше всех: по ним строятся и локальные, и глобальные сети.

Следующая разновидность — **полносвязная** топология. В этом случае каждый компьютер сети имеет по одному интерфейсу для связи с другими. Например, в сети из пяти компьютеров (рис. 3.10) каждый из них должен иметь по четыре сетевых адаптера, а количество связей между всеми этими компьютерами достигнет десяти.

Не слишком рационально, не так ли? Ведь в случае обычной «звезды» для пяти компьютеров понадобилось бы всего пять связей и хватило бы пяти сетевых карт, — правда, пришлось бы «украсить» центр звезды концентратором, но это не меняет общей картины.

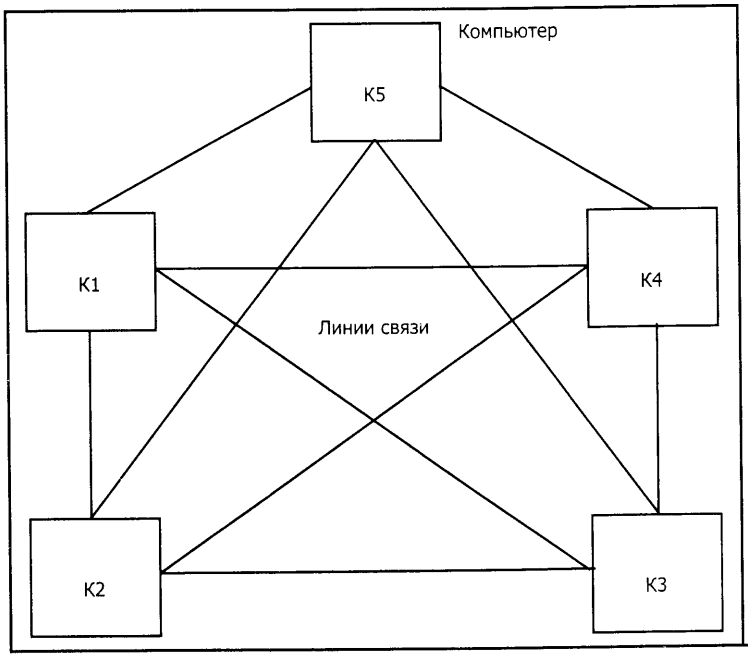


Рис. 3.10. Полносвязная топология

Ячеистая топология — вариант полносвязной. Здесь отсутствует часть связей между узлами. Такая топология присуща глобальным сетям: в них от некоторых узлов линии связи могут идти к нескольким другим узлам.

Если же говорить о глобальных сетях в целом, равно как и о сложных, больших локальных сетях предприятий, то окажется, что существуют так называемые смешанные топологии, — несколько разнородных локальных сетей, связанных общими магистралями в единую сеть.

В сетях любой топологии, кроме полносвязной, вынужденно применяется совместное использование линий связи. Линии связи, используемые несколькими устройствами передачи данных, еще называют разделяемыми линиями связи. Самым характерным примером использования разделяемой линии передачи данных является сеть, построенная по технологии Ethernet на базе коаксиального кабеля.

Сеть, построенная по топологии «звезда» на основе повторителя, логически очень похожа на сеть, в основе которой лежит коаксиальный кабель. Разница лишь в том, что каждый компьютер связан с повторителем индивидуальным кабелем в отличие от сети на коаксиале, где компьютеры связаны одним кабелем или сегментами кабеля, объединенными в единую линию передачи данных. Обратите внимание: в сети с повторителем, несмотря на наличие отдельных линий связи, все кабели составляют единую среду передачи данных. Такая сеть надежнее, чем сеть на коаксиале, но не имеет принципиальных преимуществ перед ней. А вот звездообразная топология с коммутатором в центре — это пример использования индивидуальных линий связи и индивидуальной среды

передачи данных. Коммутатор способен одновременно связывать несколько компьютеров между собой, изолируя отдельные пары связанных компьютеров от других машин.

3.4. РОЛИ КОМПЬЮТЕРОВ В СЕТИ

Современные компьютерные сети содержат компьютеры преимущественно двух типов: серверы и пользовательские рабочие станции. Перед продолжением разговора о ролях компьютеров в сети, мне хотелось бы подробнее остановиться на толковании понятий «сервер» и «клиент» (рис. 3.11).

Слово «сервер» в применении его к сетям имеет несколько значений. Сервером называют компьютер или приложение, которые предоставляют свои ресурсы другим приложениям. Компьютер-сервер — это, как правило, достаточно мощный компьютер. У серверов разные задачи. Бывают файловые серверы — сетевые хранилища нформации. Принт-сервер используется как посредник между другими компьютерами и подключенными к нему принтерами. Веб-сервер — это компьютер, который предоставляет другим компьютерам веб-услуги. Эти роли типичны для серверов локальных сетей.

Программная и аппаратная составляющие понятия «сервер» особенно близки, когда речь идет о веб-сервере. Так, в программном понимании веб-сервер — это программа, которая предоставляет другой программе — клиенту — некие ресурсы. Клиентское же программное обеспечение (к примеру, известный всем Internet Explorer) запрашивает у серверного ресурсы или данные.

В глобальных сетях и, в частности, в Интернете существуют серверы, занятые исключительно поддержанием работоспособности сети. Это DNS-серверы.

Итак, **в сетях компьютер может быть либо сервером, либо клиентом**. Исключение — небольшие сети, где один и тот же компьютер в разное время может выполнять различные функции. Например, пользовательская рабочая станция может быть одновременно принт-сервером, который предоставляет подключенный к нему принтер в качестве устройства для печати всем компьютерам сети.

В точности так же, как компьютеры, которые делятся на клиентские и серверные машины, некоторые операционные системы имеют клиентские и серверные версии. К примеру, у операционной системы Windows 2000 есть версия Windows 2000 Server, которая позволяет создавать сети со сложной логической структурой, поддержкой сотен пользователей и управлять политиками безопасности. Знакомая многим ОС Windows

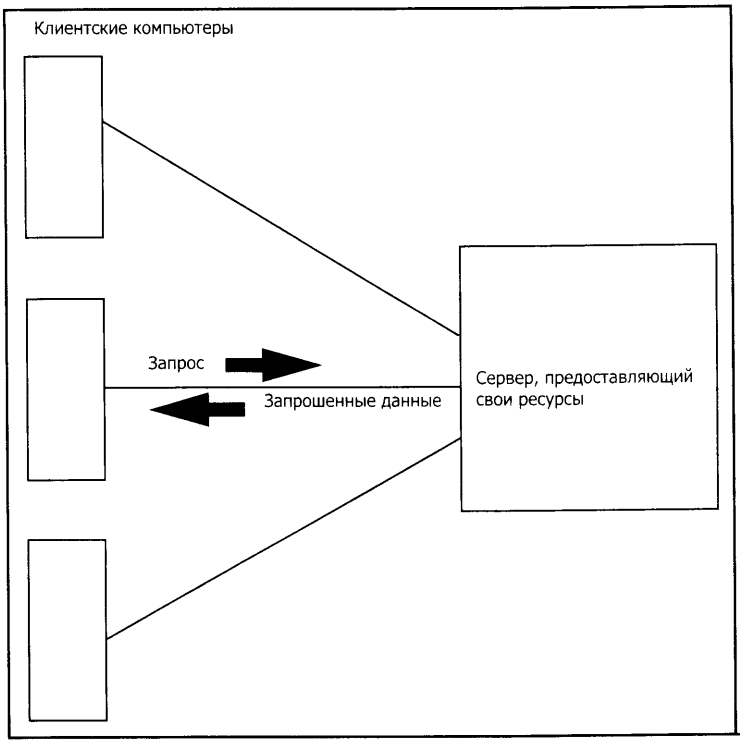


Рис. 3.11. Взаимодействие клиентов и сервера

2000 Professional — это клиентская версия Windows 2000 Server. Использование такой серверной ОС подразумевает достаточно мощный сервер, который в качестве рабочей станции лучше не использовать: серверная операционная система сильно нагружает компьютер, и работать на нем не очень приятно.

С другой стороны, сервер — это компьютер, который должен работать как можно стабильнее. Любое вмешательство пользователя в его работу (даже если пользователь не трогает средств администрирования сервера) потенциально опасно для его стабильной работы, а значит, и для всей сети.

В качестве сервера годится и не самый мощный компьютер, если оптимизировать его работу, например отключить ненужные службы.

Глава 4

БАЗОВЫЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

Эта глава посвящена самым «горячим» и современным технологиям построения локальных сетей. Рассмотрим некоторые вопросы стандартизации и практического применения этих технологий.

4.1. СТАНДАРТИЗАЦИЯ ТЕХНОЛОГИЙ ЛОКАЛЬНЫХ СЕТЕЙ

В прошлой главе мы затронули проблему стандартизации кабелей для локальных сетей. Сейчас речь пойдет о технологиях локальных сетей.

КТО ПИШЕТ СТАНДАРТЫ

Организация, которая занимается стандартизацией технологий локальных сетей, называется IEEE (*Institute of Electrical and Electronics Engineers*) — Институт инженеров по электротехнике и радиоэлектронике.

В начале 80-х годов прошлого века эта организация занялась развитием стандартов локальных сетей. Группа стандартов локальных сетей 802 получила нумерацию по номеру рабочей группы, которая трудилась над вопросами локальных сетей. Эта группа стандартов за годы работы сделала очень многое, но работа по стандартизации продолжается и сейчас.

Сегодня в состав рабочей группы 802 входит множество подгрупп, каждая из которых занимается определенными стандартами. Нас с вами интересуют следующие подгруппы и разрабатываемые ими стандарты.

- 802.1 — группа разработки *Internetworking* — стандартов объединения сетей, общих для всех локальных сетей. Например, они определяют логику работы некоторых сетевых устройств вроде мостов, которые способны соединять различные сети, способы создания виртуальных локальных сетей и так далее.
- 802.2 — группа разработки *Logical Link Control* (LLC) — методов управления логической передачей данных.
- 802.3 — группа разработки стандарта Ethernet, использующего метод доступа CSMA/CD. Здесь разрабатывают стандартоы передачи

* * *

Рассмотрим технологии Ethernet и Wi-Fi подробнее. Каждой из этих технологий можно посвятить отдельную книгу, но мы остановимся на тех особенностях, которые важны для практического создания небольших локальных сетей.

4.2. IEEE 802.11 — WI-FI

Начнем с беспроводных сетей: ведь будущее именно за ними. Точнее, не будущее, а настоящее.

В основе беспроводных сетей лежит передача данных по радиоканалу. Сегодня распространены три стандарта беспроводных сетей: 802.11b, 802.11g, 802.11a. Беспроводные сети группы стандартов IEEE 802.11x имеют несколько названий, и вы можете столкнуться с любым из них.

- Чаще всех встречается обозначение WLAN (*Wireless Local Area Network*): по-русски эти слова значат «беспроводная локальная сеть».
- Так как принципы работы беспроводных локальных сетей и проводных Ethernet-сетей очень похожи (например, по используемым методам доступа к среде), иногда их называют RadioEthernet-сети. Это название устарело и сегодня используется очень редко.
- Локальные беспроводные сети сегодня модно называть словом Wi-Fi. Это сокращение от английских слов *Wireless Fidelity*. Переводятся эти слова как «беспроводная преданность».

Вернемся к стандартам. Вначале рассмотрим стандарт 802.11b: он был принят в 1999 году как расширение стандарта 802.11 и сегодня стал самым распространенным. Скорость передачи данных по этому стандарту достигает 11 Мбит/с.

Вы скажете, что это немного? Но простенький сетевой адаптер для ПК, который работает в стандарте 802.11b и подключается к компьютерному USB-порту, стоит около $ 25. Желающих воспользоваться беспроводной локальной сетью за эту небольшую сумму найдется немало. К тому же сетевые карты стандарта 802.11b встраиваются сейчас в ноутбуки, а сравнительно недорогие КПК среднего и высокого уровня тоже имеют Wi-Fi-адаптер этого стандарта. Большинство точек доступа к беспроводным сетям, или, как их еще называют, хотспотов, рассчитаны именно на технологию 802.11b.

Стандарт 802.1 предполагал гораздо более медленную передачу данных — 1 или 2 Мбит/с.

С принятием стандарта 802.11b появились новые скорости — 5,5 и 11 Мбит/с. Стандартом предусмотрен частотный диапазон от 2,4 до

2,4835 Ггц. Теоретически сети этого стандарта могут передавать данные на расстояние более 100 км в условиях прямой видимости. На практике дела обстоят не так радужно: беспроводные сети покрывают радиус в десятки или, в лучшем случае, сотни метров. Виной этому сравнительно слабые передатчики и помехи при прохождении сигнала. Мощность радиосигнала ослабляется стенами и металлическими предметами на пути его прохождения. Поэтому дальность связи в разных условиях может варьироваться в весьма широких пределах, которых, впрочем, обычно хватает для создания офисной или домашней беспроводной сети.

Частота, на которой работает оборудование 802.11b, выбрана не случайно: она предназначена для безлицензионного, свободного использования в промышленности, науке и медицине. В странах СНГ этот диапазон лицензируется, что предполагает его дополнительную помехоустойчивость.

Стандарт 802.11b описывает так называемый коллизионный метод множественного доступа к среде — CSMA/CA, очень похожий на метод доступа к каналу передачи данных стандарта Ethernet. Подробнее об этом методе доступа к среде мы поговорим немного ниже, а здесь лишь отметим, что такое использование среды передачи данных подходит для передачи информации, некритичной к полосе пропускания канала и его доступности в конкретный момент времени. А вот для передачи, скажем, голоса это не подходит.

Существует два способа построения Wi-Fi сети. Они называются Ad Hoc.

СЕТИ AD HOC

Это самый простой и дешевый способ построения беспроводной сети. Он заключается в создании простой одноранговой локальной сети из нескольких компьютеров. Такая сеть называется Ad Hoc, но иногда можно встретить название *Independent Basic Service Set* (рис. 4.1).

В такой сети могут работать обычные стационарные компьютеры, ноутбуки, КПК и другие устройства, оснащенные WLAN-адаптером. Сеть Ad Hoc почти не требует дополнительных капиталовложений: достаточно соответствующим образом настроить сетевые адаптеры беспроводной сети и программное обеспечение, и сеть заработает.

Преимущества сетей Ad Hoc — дешевизна исполнения, высокая мобильность, простота установки (подчеркну: *сравнительная простота*. Ведь настройка даже простейшей WLAN требует некоторых знаний). Недостатки у сетей этого типа тоже есть. Размер такой сети ограничен десятью одновременно работающими клиентами. Ограничен и физический размер сети (физическое расстояние между компьютерами), а так-

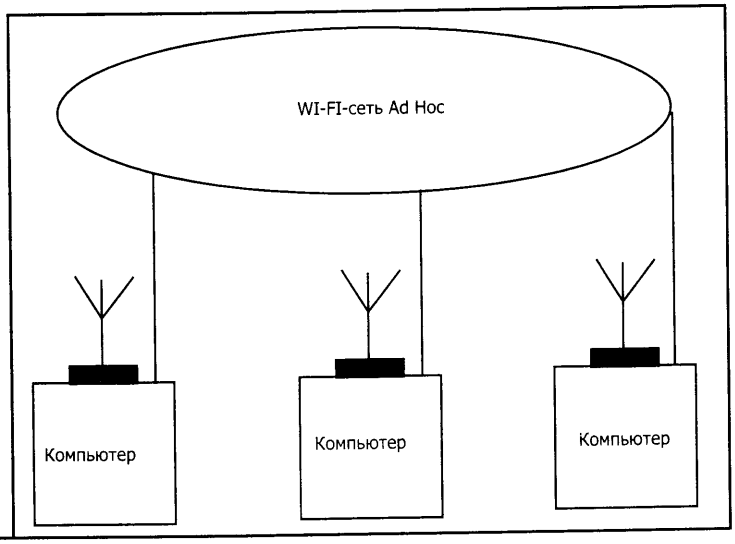


Рис. 4.1. Схема Ad Hoc сети

же возможность связи с компьютерами, обладающими проводными интерфейсами. Конечно, можно соорудить нечто вроде маршрутизатора, связывающего локальную сеть Ethernet и беспроводную сеть, но работоспособность такой сети сомнительна.

СЕТИ INFRASTRUCTURE

В сетях Infrastructure (рис. 4.2) важную роль играет так называемая точка доступа, или, по-английски, *Access Point*.

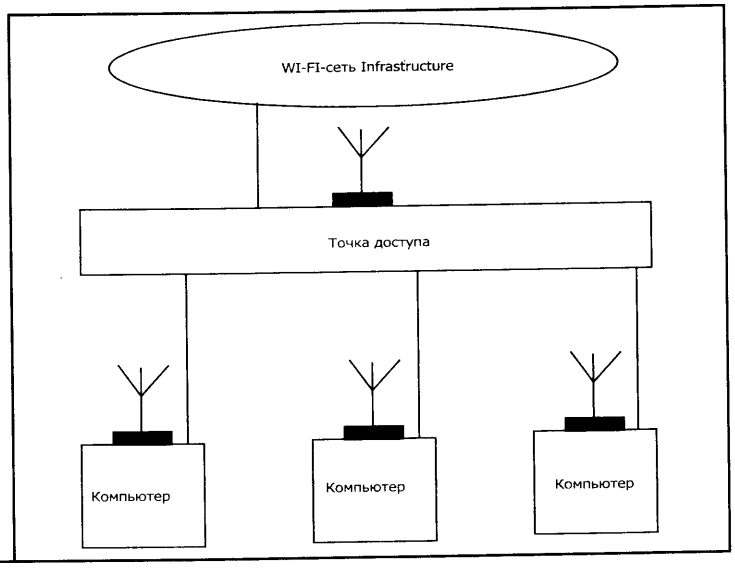


Рис. 4.2. Схема сети Infrastructure

Точка доступа — это отдельное устройство, снабженное Wi-Fi адаптерами и внешними антеннами. Помимо адаптеров беспроводной сети, такая точка доступа может содержать интерфейсы для подключения ее к локальной сети. Как видите, здесь мы получаем еще и мост между проводными и беспроводными сетями.

Применение точки доступа позволяет создавать сети, распределенные территориально, потому что точки доступа можно связывать между собой.

Существует два режима работы подобной сети. Первый называется BSS — *Basic Service Set* — и предусматривает использование одной точки доступа для всех целей. Второй называется ESS — *Extended Service Set* — и предусматривает объединение нескольких BSS-сетей в единую инфраструктуру. Связи между базовыми станциями в таком случае могут быть организованы с применением радиоканала или с использованием кабелей.

СЕТИ, СТАНДАРТЫ, ПРОБЛЕМЫ

Все это прекрасно, но вот скорость 11 Мбит/с — это слишком мало. Поэтому были разработаны стандарты IEEE 802.11a и 802.11g.

Стандарт IEEE 802.11a работает в диапазоне частот 5 ГГц, а максимальная пропускная способность поднимается до 54 Мбит/с. Остальные параметры сети, о которых рассказывалось выше, практически не изменились. Вот только оборудование стоит дороже.

Стандарт 802.11g примечателен тем, что работает в том же частотном диапазоне, что и 802.11b, полностью совместим с оборудованием этого стандарта, но обеспечивает пропускную способность до 54 Мбит/с, как и стандарт 802.11a. Этот стандарт из группы 802.11 считается самым перспективным. Кстати, именно для этого стандарта существуют различные фирменные улучшения, внесенные разработчиками «железа». Некоторые из этих разработок позволяют довести скорость соединения более чем до 100 Мбит/с.

Внимание всех, кто так или иначе пользуется беспроводными сетями, приковано к вопросам их безопасности. Если с проводной сетью все более или менее ясно — по крайней мере проводная сеть позволяет физически контролировать подключение «чужих» компьютеров, — то с беспроводной все немного сложнее.

Если, скажем, в вашем офисе работает WLAN, это значит, что она передает ваши данные на определенное расстояние, находящееся за его стенами. Некий условный «шпион», вооруженный соответствующей техникой (обычным ноутбуком или даже КПК), при желании сможет перехватить ваши коммерческие секреты. Правда, сейчас существуют достаточно эффективные средства защиты информации в беспроводных сетях, например шифрование. Подробнее о безопасности и о дру-

гих практических аспектах работы беспроводных сетей читайте в одной из следующих глав. А сейчас позвольте представить вашему вниманию некоторые подробности о технологии Ethernet.

4.3. IEEE 802.3 — ETHERNET

ИСТОРИЯ

Прежде чем начать разговор о некоторых технических подробностях технологии Ethernet, расскажу о том, почему эта технология получила такое название. Ethernet создал Роберт Меткаф (Robert Metkalf) с коллегами из лабораторий Xerox в 1972 году. Сеть использовалась для связи компьютеров (точнее, персональных рабочих станций) Xerox Alto между собой, с серверами и принтерами. Пропускная способность первой Ethernet-сети была равна 2,94 Мбит/с. Первая экспериментальная сеть Меткафа называлась *Alto Aloha Network*. В 1973 он сменил это название на «Ethernet» подчеркивая тот факт, что система может поддерживать различные компьютеры, а не только Xerox Alto. Его выбор основывался на слове Ether (эфир) и описывал одно из существенных свойств системы (точнее, кабельной системы сети): биты данных доставлялись до каждого из подключенных к сети компьютеров.

МЕТОД CSMA/CD

От множества стандартов спецификации 802.3 стандарт Ethernet отличается средой передачи данных, или, говоря проще, кабелями, используемыми для связи. Метод доступа к среде передачи данных у стандарта Ethernet называется CSMA/CD, что означает *Carrier Sense Multiply Access with Collision Detection*, то есть «метод коллективного доступа с опознанием несущей и обнаружением коллизий».

Принципы, положенные в основу технологии Ethernet, были опробованы в радиосети Гавайского университета, которая называлась Aloha. Как видите, налицо преемственность — Ethernet создана на основе опыта, полученного при создании радиосети, а Wi-Fi, которая, в сущности, использует аналогичный способ доступа к среде, построена в некоторой степени на базе Ethernet.

Метод доступа CSMA/CD используется в сетях с общей средой передачи данных. В нашем случае это кабель. Такая система очень проста,

но одновременно в ней могут общаться лишь два компьютера, а остальные ждут, когда освободится среда передачи данных. В то же время данные, переданные одним из компьютеров, могут легко приниматься всеми остальными машинами. При таком подходе сеть как бы делится между всеми компьютерами.

Как видно из названия метода доступа CSMA/CD, в сети возможны исключительные ситуации. Они называются коллизиями и возникают, когда две станции начинают передачу в одно и то же время (с некоторым сдвигом по времени). В результате работа сети останавливается на некоторое, очень небольшое время, а потом передача данных возобновляется.

Сущность CSMA/CD заключается в том, что компьютеры «слушают» сеть и пытаются передавать данные только тогда, когда сеть не занята никем. Если вдруг окажется, что два компьютера начали передачу данных почти одновременно, в сети возникнет коллизия и передаваемые данные смешаются. Тогда компьютеры снова «замолкают» и снова пытаются захватить среду в соответствии с определенным алгоритмом. Это очень упрощенное описание, но оно дает представление о принципе CSMA/CD.

ЕЩЕ НЕМНОГО О СТАНДАРТЕ 802.3

Остановимся подробнее на разных реализациях стандарта 802.3. Различают следующие варианты этого стандарта.

10Base-5 — это Ethernet сеть, использующая в качестве среды передачи данных так называемый толстый коаксиальный кабель (диаметр кабеля около 10 мм). Эта сеть имеет пропускную способность 10 Мбит/с. Стандарт этот устарел.

10Base-2 — Ethernet сеть на базе «тонкого» (5 мм) коаксиального кабеля. Пропускная способность такой сети равняется 10 Мбит/с. Как и вышеприведенный, этот стандарт тоже устарел.

10Base-T — в качестве среды передачи данных используется UTP-кабель 3-й категории. Пропускная способность сети — 10 Мбит/с. Этот вариант стандарта опять же устарел, хотя современные сети на основе витой пары во многом похожи на 10Base-T.

10Base-FL — это все тот же 10 Мбит/с Ethernet, использующий в качестве среды передачи данных оптоволокно.

100Base-TX — современный Ethernet, обладающий пропускной способностью 100 Мбит/с и в качестве физической основы сети использующий витую пару. Этот стандарт предусматривает применение различных кабелей, однако для нас с вами важна его реализация на UTP 5-й категории, а точнее UTP cat. 5e.

100Base-4 — это сеть 100 Мбит/с, использующая витую пару UTP cat. 3. Устаревший вариант.

100Base-FX — то же самое, но на оптоволокне.

10 GIGABIT ETHERNET

Эти три последние реализации Ethernet объединены общим названием Fast Ethernet. Есть еще Gigabit Ethernet — это Ethernet на 1000 Мбит/с (1000Base-X, 1000Base-LX, 1000Base-SX, 1000Base-CX, 1000Base-T). В качестве физической среды передачи данных он может использовать коаксиальный кабель, оптоволокно, витую пару.

Помимо Gigabit Ethernet существует 10 Gigabit Ethernet (например, 10000Base-LX4). Как следует из названия, эта технология поддерживает скорость соединения 10 Гбит/с. Решения на базе Gigabit Ethernet сегодня очень дороги, поэтому они интересны лишь крупным компаниям, нуждающимся в высокоскоростных линиях связи.

10 Gigabit Ethernet в целом очень похож на «прежние» сети Ethernet. Самое существенное изменение состоит в том, что в Gigabit Ethernet применяется другой способ доступа к среде. Разработчики, желая «вывести» локальные сети на 10 Gigabit Ethernet за пределы локальных сетей, отказались от способа доступа к среде CSMA/CD. Еще одно серьезное различие касается физической среды передачи данных: все варианты физических связей между устройствами в 10 Gigabit Ethernet строятся на основе оптоволоконного кабеля. То есть ни витой пары, ни коаксиального кабеля в 10 Gigabit Ethernet не найти.

В случае с Fast Ethernet пригодны все поддерживаемые им физические среды передачи данных, однако и здесь особенно пригодится витая пара, хотя и оптоволокно, и коаксиальные кабели также нельзя назвать неудачным выбором. Но самым важным для нас с вами является стандарт 100Base-TX.

100BASE-TX

Стандарт 100Base-TX имеет определенные ограничения на структуру сети, построенной в соответствии с ним. Другие стандарты, о которых шла речь выше, тоже имеют особенности и ограничения, но они интересны преимущественно для изучения истории сетей, поэтому их мы их здесь обсуждать не будем. А вот краткая информация о 100Base-TX читателю может пригодиться, даже если ему не придется строить большие сети масштаба предприятий.

Максимальный размер сегмента сети в стандарте 100Base-TX равняется 100 метрам. Это означает, что вы можете подключить к коммутатору несколько компьютеров 100-метровыми кабелями (рис. 4.3).

В сети Ethernet очень важным является понятие домен коллизий, то есть сегмент сети, все узлы которого способны распознать коллизию независимо от того, где произошла эта коллизия. Для того, чтобы все узлы, входящие в домен коллизий, могли вовремя распознать коллизию (и чтобы они корректно отрабатывали другие процедуры сетевого

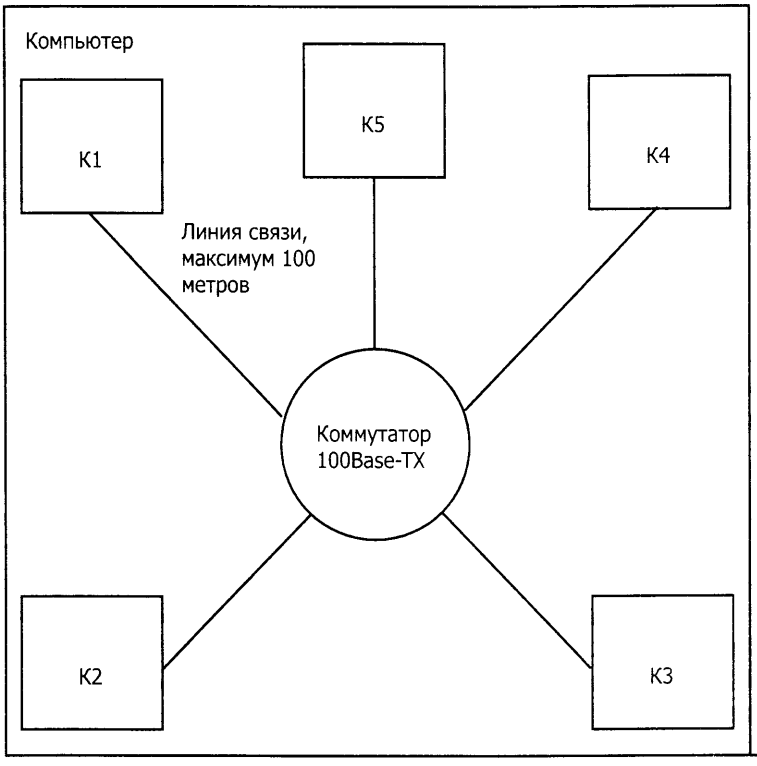


Рис. 4.3. Структура сети 100Base-TX на основе коммутатора

взаимодействия), вводится ограничение на максимальную длину кабелей. Кабели и сетевое оборудование вносят определенную задержку в распространение сигнала по сети, отсюда и ограничения.

Применение маршрутизаторов снимает ограничение на общую длину сети: маршрутизатор делит сеть на несколько доменов коллизий, узлам которых нет необходимости распознавать коллизии, произошедшие в соседних доменах.

Следующий стандарт, который имеет шансы стать достаточно популярным, а уж некоторых пользователей он точно заинтересует.

4.4. HPNA

Существует альтернатива стандартным Ethernet-решениям или домашним беспроводным сетям: это технология построения так называемых HomePNA-сетей. HomePNA — сравнительно новый стандарт локальных сетей, разработанный Home Phoneline Networking Alliance и предназначенный, как следует из названия, специально для домашнего использования.

Особенностью этого стандарта является то, что в качестве среды передачи данных используется обычная домашняя телефонная проводка.

Сетевые адаптеры подключаются к компьютерам и к телефонным розеткам. Таким образом мы словно бы получаем обычную Ethernet-сеть, передающую данные по телефонным проводам.

Сегодня существует HomePNA версий 1.0 и 2.0. Они различаются скоростями передачи данных. Первая поддерживает скорость до 1 Мбит/с, а вторая — до 10 Мбит/с. Сети этого стандарта в некоторых реализациях могут работать на скоростях до 32 Мбит/с, но реальная максимальная скорость передачи данных лежит на уровне 10–15 Мбит/с.

Сеть на основе HPNA соответствует требованиям стандарта 802.3, однако она не нуждается в концентраторах, коммутаторах и прочем сетевом оборудовании. Сеть может работать на домашней линии, не мешая своей работой ни обычным телефонам, ни даже аналоговым модемам, часто использующимся для выхода в Сеть.

4.5. ВЫВОДЫ

В этой главе мы обсудили базовые технологии построения локальных сетей. Вы уже успели убедиться в том, что сегодня самой перспективной является технология проводных сетей Ethernet 100Base-TX и группа технологий беспроводных сетей, имеющая одно общее название Wi-Fi. В следующих главах мы еще не раз вернемся к этим двум технологиям.

Глава 5
ПРОТОКОЛЫ

В этой главе мы подробнее остановимся на протоколах TCP/IP и входящих в него протоколах разных уровней, а также на протоколах IPX/SPX и NetBIOS/SMB.

Стек протоколов TCP/IP сегодня наиболее распространен и наиболее востребован. Этот стек универсален, он подходит как для соединения пары компьютеров, стоящих в пяти метрах друг от друга, так и для построения всемирной глобальной сети Интернет. Решительно невозможно дать полное описание всех технологий TCP/IP, так как за десятки лет существования они пополнились множеством спецификаций и дополнительных протоколов. Однако знание основ TCP/IP помогает обычным пользователям, не говоря о системных администраторах, глубже понимать принципы сетевого взаимодействия устройств. Эти основы также пригодятся нам при настройке сети в Windows.

Зная основы TCP/IP, вы сможете хорошо представить себе даже такую (на первый взгляд) сложную для понимания вещь, как процедура оптимизации интернет-соединения по коммутируемой линии, а также множество более «приземленных» вещей. Другие стеки мы рассмотрим скорее для полноты изложения, так как локальных сетей, построенных исключительно на них, сейчас не найти. Но эти другие протоколы не упразднены и могут использоваться в локальных сетях наравне с TCP/IP.

Начнем с форматов представления данных в компьютере.

5.1. ФОРМАТЫ ДАННЫХ

ДВОИЧНАЯ СИСТЕМА

Как известно, компьютер работает с двоичными данными. Все, что хранится на жестких дисках компьютера, и все, что передается по компьютерным сетям, выводится на экраны мониторов и печатается на принтерах, все это изначально существует в двоичной форме. Только нули и единицы — высокие и низкие уровни сигнала, намагниченные и ненамагниченные участки жесткого диска и заряженные или разряженные конденсаторы.

Десятичная система счисления построена на применении десяти цифр — от нуля до девятки. Эта система счисления позиционная, то есть значимость той или иной цифры для конечного результата зависит от ее позиции.

Десятичные числа мы воспринимаем не задумываясь, интуитивно. Это напоминает навыки быстрого чтения, когда человек читает не по буквам или по слогам, а целыми словами. С десятичными цифрами человеческое сознание связывает определенные образы, поэтому числа в этой системе мы воспринимаем автоматически. И все же задумаемся над тем, как получаются десятичные цифры. Например, возьмем несколько чисел и попробуем «почитать» их «по буквам».

Например, число, состоящее из одной цифры — «5». Здесь, кажется, нечего «читать по слогам». Пока примем это утверждение и перейдем дальше. Берем двузначное число — «25». На первый взгляд, никаких «доказательств» того, что это именно «двадцать пять», не требуется. Но попробуем разложить это число на составные части. Получится примерно следующее: $2\times10+5$. Уже интереснее — в записи появляется десятка — основание десятичной системы счисления. Идем дальше и берем число 347. Раскладываем его, и у нас получается $3\times100+4\times10+7$. А если дальше разложить, получится вот что: $3\times10\times10+4\times10+7$. Ну и, наконец, ключевой момент наших изысканий — $10\times10=10^2$. Пишем $3\times10^2+4\times10+7$.

Вспомним, что любое число в первой степени равняется самому себе, а любое число в нулевой степени равняется единице. Разложив таким образом число 12345, мы получим следующее: $1\times10^4+2\times10^3+3\times10^2+4\times10^1+5\times10^0$.

Вот и все — для того, чтобы унифицировать запись, мы добавили значок степени (первой и нулевой) и получили правило вычисления значения числа в десятичной системе счисления, которым неосознанно пользуемся, читая такие числа.

Запишем теперь то, что получилось, в общем виде.

Основание степени, то есть основание нашей системы счисления, обозначим как Q.

Позицию цифры обозначим P. Позиция цифры в десятичной системе будет показателем степени, в которую надо возводить основание.

В результате получаем универсальный алгоритм для перевода числа из любой системы счисления в десятичную:

$N_{10} = N_x\times Q^{(P1)}$, где основание числа N указывает на основание системы счисления.

Двоичное число может состоять лишь из нулей и единиц. При их записи используется точно такая же позиционная система, как и при записи десятичных чисел. Например, двоичное число «0» — это ноль и в десятичной системе счисления. «1» — это тоже единица. По приведенной выше формуле для двоичного счисления

$1_{10} = 1_2\times2^0$

Идем дальше. Чему будет равно двоичное число 11? Ответ: $1\times2^1+1\times2^0=3$. Точно так же получаем значение числа 101:

$1\times2^2+0\times2^1+1\times2^0=5$.

Можете проверить эти вычисления в стандартном калькуляторе Windows. Он умеет переводить числа из одной системы счисления в другую.

Для этого нужно выбрать в меню **Вид калькулятора** строку **Инженерный** и переключить его на ввод двоичных чисел при помощи переключателя Bin. Введите число 101 и, переведя опять в Dec, получите в ответ цифру 5.

Продолжаем переводы двоичных чисел. Известно, что байт состоит из восьми битов. Итак, переводим в десятичную систему число 11111111. Получаем 255. Вам это число ничего не напоминает? Оно чрезвычайно распространено в компьютерной технике. Части IP-адреса тоже заканчиваются на числе 255 (по крайней мере в использующейся сейчас реализации протокола IP). Кстати, в компьютерной науке счет начинается не с 1, а с 0, поэтому в диапазон байта попадают 256 значений — от 0 до 255.

ШЕСТНАДЦАТЕРИЧНАЯ СИСТЕМА

Если с двоичной системой счисления все понятно, то шестнадцатеричная система чаще всего вызывает недоумение. Главный вопрос тех, кто впервые слышит о ней, звучит следующим образом: «Зачем это все?» А вот зачем: шестнадцатеричные числа удобны для представления полубайтов, то есть половинок двоичного числа, состоящего из восьми цифр. Шестнадцатеричная система, как видим, нужна для облегчения работы с двоичными числами. Она использует для записи чисел не десять цифр, как делает это десятичная, и не две, как двоичная, а целых шестнадцать.

Двоичные цифры громоздки для записи, но с ними приходится работать. Переводить десятичные числа в двоичные сложно, и делать это в уме способны не все. А шестнадцатеричные цифры вполне поддаются такому переводу, особенно если попытаться выучить таблицу соответствия двоичных и шестнадцатеричных кодов.

Арабы, которые изобрели десятичную систему счисления, не придумали символов больше девятки, поэтому в шестнадцатеричной системе приходится использовать буквы латинского алфавита от A до F. Посмотрите на табл. 5.1. Здесь наглядно представлено соответствие десятичных, двоичных и шестнадцатеричных цифр. Для того чтобы сделать данные понятнее, двоичные цифры дополнены до четырех знаков путем добавления «лишних» нулей.

Таблица 5.1. Соответствие чисел разных систем исчисления

Десятичные числа	Двоичные числа	Шестнадцатеричные числа
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Как видите, все очень логично. Перевод чисел из двоичной в шестнадцатеричную систему счисления и обратно — это легкая процедура, не требующая вычислений.

Мы обсуждали перевод чисел в десятичную систему счисления и конверсию между двоичной и шестнадцатеричной системами. А как перевести десятичное число в иную систему счисления?

Для двоичной системы это выглядит так: делим десятичное число на два, записывая остаток справа налево. Посмотрите на табл. 5.2. Здесь наглядно изображен процесс такого перевода.

Таблица 5.2. Перевод из десятичной системы счисления в двоичную

Десятичное число	Двоичное число
155/2=77 (остаток 1)	1
77/2=38 (остаток 1)	1
38/2=19 (остаток 0)	0
19/2=9 (остаток 1)	1
9/2=4 (остаток 1)	1
4/2=2 (остаток 0)	0
2/2=1 (остаток 0)	0
1/2=0 (остаток 1)	1
155	10011011

Ну, давайте же, задавайте ваш вопрос: «Зачем мне это все, если я просто хочу построить маленькую локальную сеть и подключиться к Интернету?» Ответ прост — все это нужно, чтобы понимать, что именно вы делаете.

Что касается систем счисления, имейте в виду: представления IP-адресов, о которых мы поговорим дальше, могут быть представлены в разных системах счисления.

5.2. АДРЕСАЦИЯ

Чтобы понимать основы функционирования сетей, рассмотрим применяемые в сетях способы адресации. Существует три типа сетевых адресов (рис. 5.1).

Проще всех так называемые **символьные адреса**. Например, компьютер в локальной сети может иметь символьное имя «Computer1» или даже на русском языке — «Компьютер1», а сервер может называться просто «Server» или «Сервер».

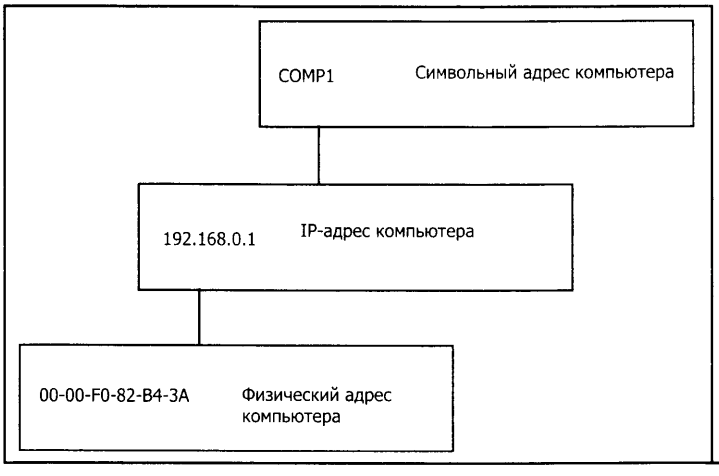


Рис. 5.1. Иерархия адресов, используемых в TCP/IP сетях

Такие адреса удобны: они легко запоминаются, и при их создании можно использовать любые логические ассоциации, которые могут быть вызваны расположением компьютера или пользователями, которые на нем работают. Но, если говорить об использовании этого типа адресации для работы машин, окажется, что символьные адреса имеют нерегулярную структуру, то есть машине работать с таким именем будет трудно. К тому же символьные адреса бывают очень длинными, а это неудобно.

Доменные имена компьютеров — это разновидность символьных. Они имеют иерархическую структуру, но также не могут обеспечить должную лаконичность и регулярность и потому не годятся в качестве «внутренних» адресов сетей.

Поэтому в больших сетях (и не только в больших) для адресации используются короткие, но информативные с точки зрения машины **составные числовые адреса**. Например, распространенный протокол IP оперирует адресами примерно такого вида: xxx.xxx.xxx.xxx. Эти адреса

называются IP-адресами. Схема IP-адресации поддерживает иерархическое построение адреса: часть адреса его отводится под так называемый номер сети, а другая часть — под номер узла в этой сети.

Но тема сетевой адресации не исчерпывается составными числовыми адресами. Существуют еще **аппаратные адреса**. Как правило, это адреса физических устройств передачи данных, сетевых адаптеров например. Аппаратные адреса обычно жестко привязаны к оборудованию: они могут прошиваться в ПЗУ тех же сетевых адаптеров.

У такого подхода есть сильные и слабые стороны. С одной стороны, нет нужды выполнять ручную работу по заданию аппаратных адресов. С другой стороны, получается вот что: при смене сетевой карты IP-адрес компьютера остается неизменным, а вот аппаратный — физический адрес — меняется. Правда, это не такая уж большая проблема.

Недостатком аппаратных адресов можно назвать то, что они «плоские», то есть не поддерживают иерархического построения адреса. Правда, если вспомнить, что роль аппаратных адресов заключается в доставке данных от одного физического устройства к другому (вспомните модель OSI), то получается, что иерархия здесь и не нужна.

Все эти сведения пригодятся, когда мы займемся созданием собственной сети.

А теперь — обещанный TCP/IP.

5.3. TCP/IP

В общих чертах со стеком TCP/IP мы уже знакомы. Поэтому сразу начнем с описания адресации компьютеров в TCP/IP сети. Это один из ключевых вопросов взаимодействия компьютеров, на решение которых и направлено применение любого протокола.

Особое значение адресация имеет для межсетевого взаимодействия. Собственно говоря, вся мощь и красота TCP/IP видна именно в глобальной сети, объединяющей невероятное количество других сетей, не говоря уже о просто невообразимом количестве отдельных компьютеров.

АДРЕСАЦИЯ В TCP/IP-СЕТЯХ

Вспомним, какие адреса могут иметь компьютеры. Вспомнили? А теперь привяжем это представление к модели OSI.

Предположим, что имеется компьютер, оснащенный сетевым адаптером Ethernet-сети. Во-первых, этот компьютер имеет физический адрес — так называемый MAC-адрес (от названия *Media Access Control*)

сетевой карты. Во-вторых, он имеет IP-адрес, который нас интересует сейчас больше всего. Этот адрес находится на сетевом уровне OSI. И, в-третьих, этот компьютер в локальной сети может иметь символьный адрес вроде «Computer1», а в глобальной — иерархическое, то есть доменное имя наподобие «computer1.net.ru». Это, строго говоря, еще не все адреса нашего компьютера, но мы ограничимся этими тремя, так как они описывают схему его взаимодействия с другими системами.

Физический, или локальный, адрес предназначен для передачи данных между физическими устройствами, находящимися в пределах одной подсети. Такой адрес может применяться для передачи данных в локальной сети. Это «плоский» адрес: он не содержит информации о принадлежности устройства к какой-то сети. Поэтому, зная физический адрес компьютера, находящегося в одной сети, передать ему сообщение из другой сети (отделенной от первой, скажем, маршрутизатором) просто невозможно.

Но устройства с разными физическими интерфейсами также не смогут обмениваться сообщениями напрямую, даже если они находятся в одной сети. Например, если к одной и той же локальной сети один компьютер подключен при помощи Ethernet-адаптера, а второй по Wi-Fi через точку доступа, то «физического разговора» между компьютерами не получится, хоть они и находятся в одной сети. Именно для обеспечения межсетевого взаимодействия компьютеров и существуют **адреса сетевого уровня, то есть IP-адреса**.

IP-адрес состоит из четырех байтов. Они записываются в виде четырех чисел, разделенных точками, и выглядят примерно так: 169.254.100.123. Существует особая классификация IP-адресов, в соответствии с которой они делятся на несколько классов. Взгляните на табл. 5.3, где показана структура IP-адресов разных классов.

Класс IP-адреса	Первый байт	Второй байт	Третий байт	Четвертый байт
Класс A	0 номер сети	Номер узла	Номер узла	Номер узла
Класс B	10 номер сети	Номер сети	Номер узла	Номер узла
Класс C	110 номер сети	Номер сети	Номер сети	Номер узла
Класс D	1110 адрес группы	Адрес группы	Адрес группы	Адрес группы
Класс E	11110 зарезервировано	Зарезервировано	Зарезервировано	Зарезервировано

Таблица 5.3. Классы IP-адресов

Сеть, обладающая адресом класса A, имеет однобайтовый номер сети, а остальные три байта отведены под номер узла. Несложно подсчитать, что сеть класса A может содержать 2^{24} узлов. Эта сеть может иметь номер от 1.0.0.0 до 126.0.0.0. Сетей класса A очень мало, зато каждая из них может содержать множество узлов.

Сеть класса B имеет двухбайтовый номер сети, а остальное отведено под номера узлов — номера сетей изменяются в диапазоне от 128.0.0.0 до 191.255.0.0, а количество узлов в каждой сети может составлять 2^{16}.

У сетей класса C под номер сети отведено целых три байта. Получается, что номер сети может изменяться от 192.0.0.0 до 223.255.255.0. А вот узлов в сети класса C может быть меньше всего — всего 2^8. Кстати, именно сети класса C наиболее распространены.

Адреса класса D могут использоваться для рассылки широковещательных сообщений определенной группе узлов. Это так называемый Multicast-адрес. Такие адреса применяются в первую очередь для организации потоковой передачи мультимедийных данных большому количеству пользователей. Узлы, которые хотят принимать данные от какого-то источника, объединяются в группу, члены которой и получают сообщения с таким адресом.

Адреса класса E зарезервированы для будущих применений.

Помимо вышеописанных адресов существуют зарезервированные адреса, которые используются особым образом. К примеру, адрес, первый байт которого равен 127, применяется для тестирования сетевой подсистемы отдельно взятого компьютера. Если программа отправит пакет с таким адресом, то этот пакет, не выйдя за пределы компьютера, пройдется по всем уровням сетевой подсистемы и вернется к этой программе. Этот адрес также называют адресом обратной связи, или *loopback*.

Есть среди IP-адресов и так называемые широковещательные (*broadcast*). Они бывают двух видов. Первый вид — это адрес, состоящий из единиц (в двоичном представлении). Пакет с таким адресом должен быть разослан всем узлам той сети, в которой находится отправитель. Другой вид широковещательного адреса предназначен для рассылки сообщений узлам определенной сети. Адрес узла в таком сообщении состоит из единиц (опять же в двоичной записи), а номер подсети может изменяться.

Эта классификация имеет смысл для сетей, включаемых в Интернет.

Номера сетей, входящих в состав Интернета, назначаются централизованно, но администратор локальной сети может назначить компьютерам своей сети практически любые IP-адреса. Но и здесь есть свои правила, чтобы разделять трафик локальных сетей от интернет-трафика.

Заметим, что применяемая сегодня версия протокола IP, называемая IP v4, поддерживает описанные здесь четырехбайтные адреса. Разработана версия IP v6, которая использует адреса, состоящие из 16 байт. Возможно, переход на IP v6 станет одним из следующих шагов в развитии Интернета. Дело в том, что даже такого огромного количества адресов, которые предусмотрены в IP v4, в недалеком будущем может просто не хватить для всех, кто желает подключить свои сети к Интернету.

Если сеть существует отдельно от Интернета, администратор может назначать ее узлам произвольные адреса (кроме тех, применение которых оговорено особо, — например, те, первый байт которых равняется 127, и им подобные). Стандартами определены несколько диапазонов адресов, предназначенных специально для локальных сетей. Эти адреса не обрабатываются маршрутизаторами в Интернете, что предотвращает попадание нежелательного трафика в Сеть.

Диапазоны адресов локальных сетей существуют в различных классах. Для класса A — это одна сеть 10.0.0.0, для класса B — это сети от 172.16.0.0 до 172.31.0.0, а для класса C предусмотрены номера сетей в диапазоне 192.168.0.0–192.168.255.0. Это, повторюсь, номера сетей.

Как же быть с номерами узлов в подсети? Как различать номер сети и номер узла в IP-адресе? Ответ на этот вопрос дают так называемые **маски подсети**.

Эти маски похожи на IP-адреса, но они не несут адресной информации, а лишь говорят о том, какую часть адреса считать адресом подсети, а какую — адресом узла. Обратите особое внимание на эту информацию. Если данные о распределении интернет-адресов нужны больше «для общего развития», то знание вопросов взаимодействия масок подсетей и IP-адресов — это самая что ни на есть практика.

Маска подсети — это четырехбайтное число, которое определяет, какую часть адреса считать адресом подсети, а какую — IP-адресом узла. Например, пусть IP-адрес узла будет 169.234.93.171, а маска подсети — 255.255.0.0. Если представить адрес и маску в двоичном виде (табл. 5.4), то адресом подсети будет та часть IP-адреса, которой соответствуют единицы в записи маски, а адресом узла — та ее часть, которая содержит нули.

IP-адрес в десятичной записи	IP-адрес в двоичной записи
169.234.93.171	10101001.11101010.01011101.10101011
Маска подсети 255.255.0.0	11111111.11111111.00000000.00000000
Адрес подсети 169.234.0.0	10101001.11101010.00000000.00000000
Адрес узла 0.0.93.171	00000000.00000000.01011101.10101011

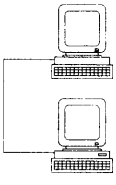
Таблица 5.4. IP-адрес и маска подсети

Таблица наглядно иллюстрирует применение масок подсети. Эта информация понадобится нам, когда мы займемся настройкой параметров IP в Windows. В случае с локальной сетью многие настройки делаются системой автоматически, но возможность их ручной модификации и, повторюсь, понимания своих действий мы с вами закладываем именно сейчас, рассматривая особенности построения IP-адреса.

IP-адреса бывают динамическими и статическими. Разница между ними заключается в том, что статический IP-адрес назначается вручную (а иногда программным обеспечением) и не изменяется, а динамический IP-адрес может меняться при каждом подключении компьютера в сети.

Динамический IP-адрес может быть назначен компьютеру так называемым DHCP-сервером. Сервер DHCP расшифровывается как *Dynamic Host Configuration Protocol* (динамический протокол конфигурации хостов) и позволяет динамически настраивать параметры компьютеров, подключающихся к сети. При помощи DHCP можно настраивать IP-адреса и локальных компьютеров, и тех, что выходят в Интернет, скажем, через модем.

DHCP-сервер каждый раз назначает компьютеру, входящему в сеть, уникальный IP-адрес. Как правило, этот адрес всякий раз новый. Такая ситуация вполне допустима для обычных пользовательских компьютеров, но в некоторых случаях требуются статические IP-адреса. К примеру, статические адреса имеют интернет-серверы, предоставляющие пользователям свои ресурсы, да и в локальной сети, особенно в небольшой, ручное назначение IP-адресов иногда может быть очень удобным.



Однажды я занимался администрированием небольшой сети на базе Windows 2000. Всем машинам в этой сети я назначил статические IP-адреса, причем номера узлов в этих адресах соответствовали нумерации компьютеров в зале, то есть наклеенным на них номерам и именам компьютеров. Например, компьютер, на который была наклеена цифра 7, мог иметь символьное имя T7.Tih.ru (в сети была установлена поддержка доменных имен, развернута полноценная AD с поддержкой нескольких сотен пользователей, сеть не была подключена к Интернету напрямую, поэтому вышеприведенное доменное имя не имело особого значения) и IP-адрес 192.168.0.7. Таким образом, узнать IP-адрес компьютера не составляло особого труда, что удобно при использовании некоторых специальных программных средств для дистанционной работы с компьютерами.

ПОДРОБНОСТИ О ПРОТОКОЛАХ

То, о чем пойдет речь в этом разделе, имеет важное значение для понимания основ сетевой безопасности. Здесь мы разберем понятия «связь с установлением соединения» и «связь без установления соединения».

IP — это своего рода сетевой транспорт, который занимается доставкой данных через составные сети. Средствами IP осуществляется маршрутизация пакетов. IP работает без установления соединения, выполняя «черновую» работу по доставке пакетов данных по сети. Его цель — доставлять пакеты данных по определенному адресу, не задумываясь об их целостности. IP умеет фрагментировать слишком большие пакеты: одно

и то же сообщение протокола более высокого уровня может быть разбито на несколько фрагментов, которые независимо путешествуют по сети в поисках адресата и, дойдя до него, снова собираются в исходное сообщение. Протоколу IP все равно, что передавать, но поверх IP работают более «умные» протоколы, в частности TCP — *Transport Control Protocol и UDP — Universal Datagram Protocol.*

TCP отвечает за надежную доставку сообщений. Прежде чем начинать передачу, он устанавливает соединение, а в процессе передачи контролирует передаваемые данные и при необходимости проводит повторные передачи. TCP оперирует так называемыми сегментами данных, а IP работает с пакетами. Сегмент TCP образуется путем «вырезания» определенного количества байт из поступившего потока данных более высокого уровня. TCP не занимается структурированием этих данных, точно так же как и IP, и не задумывается над тем, что он передает. Но если задача IP — доставить данные через систему сетей, то задача TCP — надежная передача этих данных с использованием IP в качестве транспорта.

Расскажем подробности того, как все происходит. Пусть наш TCP получил порцию байтов, нарезал ее на сегменты, упаковал эти сегменты в IP-пакеты и передал то, что получилось, протоколу IP. Протокол IP, то есть программно-аппаратные средства, реализующие его возможности, проанализировал адрес назначения и инкапсулировал его в структуры передачи данных протокола более низкого уровня (в кадры Ethernet, например). Эти структуры и протоколы, пройдя путь между двумя узлами одной сети, опять «поднимаются» до IP, который решает пути их дальнейшего прохождения.

Задача TCP — надежная доставка данных между процессами и приложениями. На одном компьютере может работать несколько приложений, которые взаимодействуют с сетью. Средство операционной системы, позволяющее прикладным процессам взаимодействовать с коммуникационными протоколами, называется портом. Разные прикладные службы имеют разные номера портов. Получается, что процесс в сети может быть охарактеризован IP-адресом узла и номером порта этого процесса. Иногда номер порта и IP-адрес в совокупности называют сокетом (*Socket*), и тогда это слово используется как синоним слова «порт».

На том же уровне OSI, на котором расположен TCP, есть еще один похожий протокол, называемый UDP. В отличие от TCP протокол UDP, как и IP, работает без установки соединения. Он не содержит средств подтверждения доставки данных, и приложение, использующее UDP, само должно позаботиться о целостности данных, которые оно передает. Также как TCP, протокол UDP оперирует понятием сокетов.

Теперь обсудим третий вид адресов, использующихся в TCP/IP. Это символьные, логически понятные человеку адреса. Такие адреса имеют иерархическую структуру и называются еще доменными именами. В небольшой сети из пяти компьютеров можно обойтись без доменной структуры имен, но если сеть растет и разделяется на несколько подсетей, то без такой адресации не обойтись.

Части доменного имени записываются через точку. Слово «домен имен» здесь понимается как некая совокупность имен, у которых совпадают старшие составные части. Например, пусть старшая часть доменного имени будет «.ru» (на деле самая старшая часть всех доменных имен Интернета — это точка «.», но она обычно не принимается во внимание). Все имена узлов, у которых их старшая часть будет «.ru», образуют один домен имен (в данном случае — это пространство доменных имен русского Интернета). Это, например, всем известные yandex.ru, rambler.ru и так далее.

Для того чтобы TCP/IP-сеть, узлы которой имеют символьные доменные имена и IP-адреса, могла работать, эти два типа адресов нужно поставить в соответствие друг с другом. Например, человек, набирающий в окне «Адрес» своего интернет-браузера адрес «yandex.ru», может не знать IP-адрес, используя который, его браузер будет связываться с вышеупомянутым сайтом.

Чтобы устанавливать соответствия между доменными именами и IP-адресами в Интернете, существуют специальные серверы, называемые DNS-серверами, то есть *Domain Name System* серверами. Они помогают определять IP-адрес узла по его доменному имени. В локальных TCP/IP сетях тоже есть нечто подобное, но здесь нет нужды выделять в них отдельный сервер — особенно в малых сетях. В этих случаях функции разрешения имен выполняет ПО, работающее на компьютерах клиентов.

Говоря о разрешении имен относительно пары «IP-адрес — доменное имя», следует отметить, что разрешения требует и связка адресов «физический адрес — IP адрес». Эта задача возложена на протокол стека TCP/IP, называемый ARP. Эта аббревиатура означает *Address Resolution Protocol*, то есть протокол, который занимается определением физического адреса узла по его IP-адресу.

Мы разобрали несколько тонкостей стека протоколов TCP/IP. По крайней мере, этого хватит, чтобы в следующих главах изучить материалы по сетевой безопасности, настройке TCP/IP на компьютере, вопросы подключения ПК к Интернету и оптимизации этого подключения. А дальше мы займемся изучением некоторых особенностей стека IPX/SPX.

5.4. IPX/SPX

IPX/SPX сегодня относится к семейству малопопулярных протоколов. Разработчик этого стека, компания Novell, и в наши дни занимается его развитием, но его время прошло. И все же IPX/SPX порой используется в современных локальных сетях, реализуя некоторые дополнительные функции. Если вы пользуетесь старыми программами, которые рассчитаны на IPX/SPX, вам будет полезна некоторая дополнительная информация об этом стеке протоколов.

Для начала рассмотрим общую структуру протоколов стека IPX/SPX.

Физический и канальный уровень этого стека совпадает со стеком TCP/IP, то есть стек IPX/SPX может работать в тех же Ethernet-сетях,

на том же оборудовании, сетевых картах и кабелях. Различия начинаются уже на сетевом уровне.

Сетевой уровень IPX/SPX представлен протоколом IPX (у TCP/IP это IP). IPX, аналогично IP, занимается доставкой сообщений узлам сети без установления соединения. При этом его не заботит надежность доставки информации. За надежную доставку информации отвечает протокол SPX, расположенный на транспортном уровне модели OSI. Его аналогом, как вы понимаете, является TCP. Протокол SPX работает с установлением соединения, он умеет восстанавливать потерянные или поврежденные пакеты.

На прикладном уровне стека IPX/SPX расположены протоколы SAP и NSP. Эти протоколы могут работать с протоколом IPX непосредственно, без привлечения SPX. Концептуальное отличие IPX/SPX от TCP/IP состоит в том, что первый изначально разрабатывался для применения в небольших локальных сетях, а второй был обобщением опыта создания глобальных сетей. Поэтому по прошествии времени интерес общества к этим стекам протоколов менялся.

Реализация TCP/IP требует серьезных аппаратных ресурсов (особенно актуально это было в 90-е годы), а протокол IPX/SPX чрезвычайно экономичен, что и определило его былую популярность.

Адрес узла в стеке IPX/SPX складывается из четырехбайтового номера сети, шестибайтового номера узла и двухбайтового номера сокета. Посмотрите на табл. 5.5, где схематично изображен такой адрес.

Номер сети	Номер узла	Номер сокета
4 байта	6 байт	2 байта

Таблица 5.5. Структура адреса IPX/SPX

В качестве номера узла в стеке используется физический адрес сетевого оборудования (MAC-адрес сетевой карты, например). Это очень важный момент — адрес узла в TCP/IP не имеет ничего общего с его физическим адресом.

Номер сети в IPX/SPX имеет фиксированный размер, а TCP/IP позволяет пользоваться масками подсетей. В результате мы получаем потенциально более быструю (особенно на медленных ПК 80–90-х годов), чем в TCP/IP, реализацию сетевых функций, но за скорость приходится расплачиваться универсальностью. Если TCP/IP гарантированно будет работать с сетью с любой физической архитектурой, то с IPX/SPX могут возникнуть проблемы. (Эти проблемы не коснутся нас с вами, строителей небольших локальных сетей)

Так же как и TCP/IP, протокол IPX/SPX позволяет осуществлять маршрутизацию пакетов между сетями. И, возможно именно IPX/SPX стал бы основой современного Интернета, если бы не удобство TCP.

Еще один стек протоколов, с которым вы можете столкнуться на практике, называется NetBIOS.

5.5. NETBIOS

NetBIOS — это немаршрутизируемый протокол. Он не знает понятия «сеть» и работает только с плоскими локальными адресами. Несмотря на такую ограниченность, то есть пригодность только для построения локальных сетей, NetBIOS существует до сих пор. Имена NetBIOS представляют собой произвольные символьные последовательности длиной до 16 символов.

В современных условиях NetBIOS в чистом виде не используется. Он работает через TCP/IP, предоставляя свои сервисы прикладным программам.

Существует реализация NetBIOS, называемая NetBEUI (*NetBIOS Extended User Interface*). NetBEUI был разработан в 1985 году.

5.6. ВЫВОДЫ

Полагаю, что прочитанные вами пять глав заложили достаточную базу для глубокого восприятия дальнейшего материала. Знакомясь с технологиями локальных сетей, равно как и с другими технологиями, лучше придерживаться такой стратегии: не останавливаться на непонятных местах, а продолжать читать дальше. Могу поспорить, что понимание «непонятностей» придет рано или поздно. Люди воспринимают информацию поразному, и то, что одному понятно сразу, другому может быть неясным.

Практическая работа, самостоятельные попытки настройки оборудования и программного обеспечения упрощают понимание теории. Но практика без теории превращается в малоосмысленную деятельность по случайному поиску каких-то установок системы, которые заставляют ее работать. Но и теория без практики — лишь набор бесполезных данных. А вот когда вы, вооружившись теорией, приступите к практической работе над установкой и настройкой сети, тогда все станет на свои места.

С чего начинать — с теории или с практики? Ни то, ни другое: теорию следует дополнять практикой, а практику — теорией. Такой путь подразумевает некую нелинейность изложения материала, но написанная таким образом книга была бы слишком сложна для восприятия. Поэтому спасибо всем, кто дочитал до этого места — и давайте читать дальше. В следующих главах речь пойдет об установке оборудования и настройке операционных систем для работы в сети.

Основное внимание мы уделим популярной ОС Microsoft Windows XP, но не оставим без внимания Windows 98 и Windows 2000. Однако Windows XP станет основой, на примере которой будет рассмотрено практически все.

Прежде чем заниматься настройками ПО, поговорим о физических особенностях подключения тех или иных устройств к компьютеру.

ЧАСТЬ 2

СЕТЕВОЕ ОБОРУДОВАНИЕ

ГЛАВА 6
СЕТЕВОЕ ОБОРУДОВАНИЕ

Вторая часть книги посвящена сетевому оборудованию, его установке и настройке, а также решению разного рода проблем, которые могут при этом возникнуть.

В этой главе мы коснемся характеристик некоторых наиболее популярных сетевых устройств, а также особенностей их физической инсталляции в систему. Программной установке и настройке этих устройств посвящается отдельная глава.

6.1. СЕТЕВЫЕ АДАПТЕРЫ

В нашем случае в качестве сетевых адаптеров выступают PCI-карты и USB-устройства.

Интерфейс USB сейчас занимает первые места в хит-параде компьютерных решений, поэтому довольно широко распространены сетевые устройства с этим интерфейсом. Но сетевые адаптеры для FastEthernet в большинстве случаев выпускаются в формате PCI-карты.

Установка такой карты может вызвать трудности у неподготовленных пользователей. Здесь бывает две крайности. Некоторые из пользователей, решив, что им море по колено, смело открывают корпус, делают все, что считают нужным, попутно разбираясь в особенностях установки на собственном опыте. Такой подход часто оправдывает себя, но порой случаются досадные недоразумения, которые, как правило, заканчиваются походом бесстрашного пользователя в сервисный центр.

Что же делать? Да просто быть аккуратным и соблюдать простые правила безопасной работы с подобными устройствами. Прежде чем работать в открытом системном блоке, познакомьтесь с правилами техники безопасности. «Безопасность» следует понимать в широком смысле слова: советы, которые я даю ниже, равно касаются и вашей безопасности, и сохранности здоровья вашего электронного друга.

Перед тем как открыть системный блок, рекомендуют отключить от него электропитание. А я добавлю: следует отключить от питания и все остальное, а затем поставить системник в удобное для работы место. На-

пример, аккуратно положить его на стол. Так вы обеспечите себе удобство работы и избежите некоторых опасностей, о которых чуть дальше.

Открыв системный блок, не спешите браться руками за платы или микросхемы. На всякий случай первым делом прикоснитесь рукой к чему-нибудь металлическому. Например, к радиатору отопления. Дело тут вот в чем. Тело человека имеет определенный электрический потенциал. Если он серьезно разнится с потенциалом компьютера, то при первом прикосновении разность потенциала сравняется. Если ваше тело сильно заряжено, то, прикоснувшись к заземленному предмету, вы почувствуете что-то вроде легкого удара током. Так бывает, когда долго «общаешься» с CRT-мониторами. Кроме того, одежда и волосы тоже способны электризоваться. Если разность потенциалов вашего тела и ПК сравняется через какую-нибудь микросхему, то существует ненулевая вероятность порчи этой микросхемы. Такое бывает крайне редко — вот и пусть бывает... с кем-нибудь другим, а не с вами.

Открыв системный блок, осмотрите его и продумайте, что вы будете делать и как. После этого приступайте к работе. В нашем случае работа заключается в установке сетевой карты. Она ставится в PCI-разъем (рис. 6.1).

Прежде чем устанавливать карту в разъем, убедитесь, что снята защитная крышка (заглушка), которая есть на задней части системного блока против каждого разъема.

Некоторые системные блоки, особенно из тех, что подороже, имеют фиксаторы этих крышечек. В корпусах подешевле кусочек металла, который прикрывает неиспользуемый слот, просто выламывают. Это надо делать отверткой. Возможно, понадобятся плоскогубцы. Работайте осторожно: ведь сорвавшаяся отвертка или резко отскочившая металлическая пластинка — не самые желанные гости в открытом системном блоке.

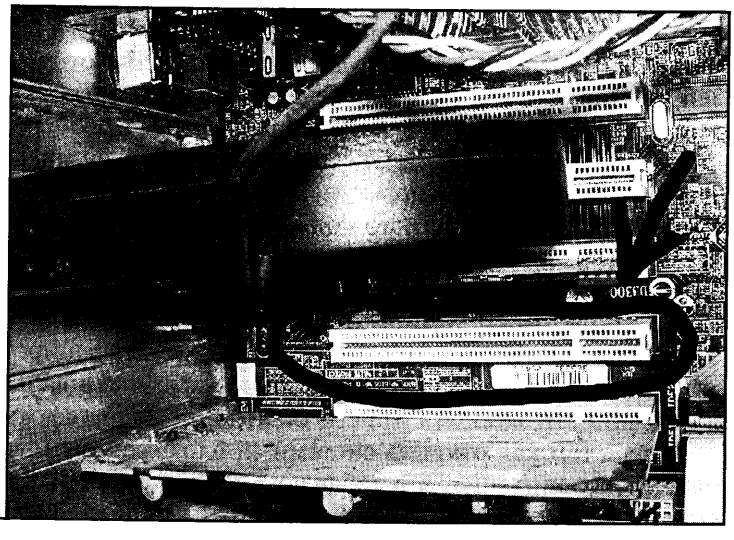


Рис. 6.1. Разъем PCI для установки сетевой карты

Подготовив место для установки карты, аккуратно выньте ее (рис. 6.2) из пластикового антистатического пакета, в которые они обычно упаковываются, и, стараясь не касаться интерфейсной части, установите в разъем.

Установка карты в разъем PCI не требует физической силы. Установить ее неправильно у вас не получится. Этот этап установки обычно проходит без проблем. После установки убедитесь, что карта установлена равномерно, без перекосов, и закрепите ее винтом — это такой же винтик, которым завинчивается системный блок.

Не пренебрегайте закреплением карты! Даже если кажется, что она жестко зафиксирована в разъеме, может случиться, что вы сами сдвинете ее с места, воткнув в ее разъем кабель. К тому же работающий компьютер подвергается воздействию разного рода вибраций — от работы кулеров, жесткого диска, CD-привода. Поэтому незакрепленная карта рано или поздно «вылезет» из слота.

Часто оборудование комплектуется драйверами на CD или хотя бы на дискете, но бывают и так называемые OEM-варианты карт. Они поставляются в пластиковых пакетиках безо всяких излишеств вроде драйверов.

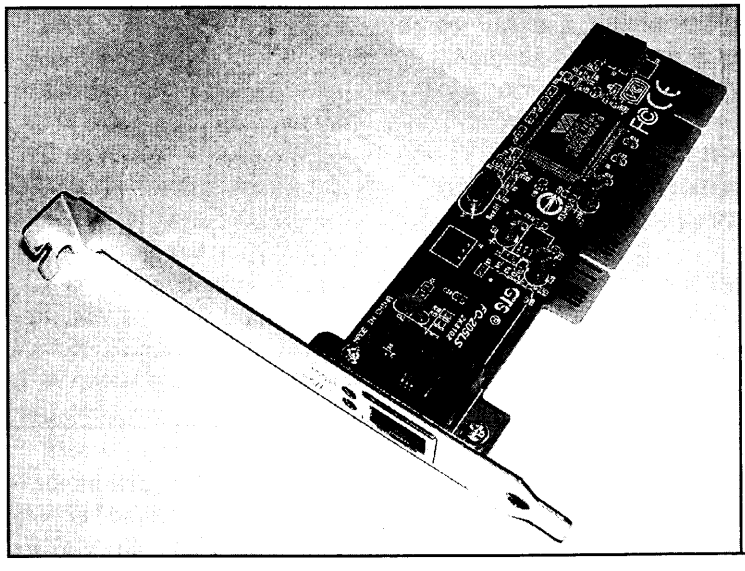


Рис. 6.2. Сетевая карта Fast Ethernet Genius GF100TXV

Про выгоды и неудобства OEM-поставок сказано немало слов. С одной стороны, пользователь, покупающий OEM-оборудование, платит за него меньше. С другой стороны, приятнее купить красиво упакованное устройство, снабженное драйверами, а иногда и бонусными программами.

Словом, физическая установка PCI-карты не должна вызвать у вас ни малейших проблем. С физической же установкой устройства, которое подключается по USB, проблем не может быть в принципе. Разъем USB просто невозможно воткнуть неправильно! Кроме того, подключать устройство к USB-порту можно и при выключенном, и при включенном компьютере. Это так называемое горячее подключение, которое характерно для современных интерфейсов.

Кабелем USB чаще всего подключаются Wi-Fi адаптеры (рис. 6.3). Дешевые адаптеры выполняются в виде USB-брелоков, и обычно вместе с ними поставляется USB-удлинитель. У такой конструкции есть серьезный минус: если системный блок вашего компьютера находится где-нибудь под столом, связь на некотором расстоянии от него (особенно если это расстояние «пересечено» стенами и другими предметами) затруднена. Поэтому при покупке такого адаптера следует задуматься о поиске как можно более длинного USB-удлинителя или о том, как поставить компьютер, а вместе с ним и приемо-передающую антенну повыше.

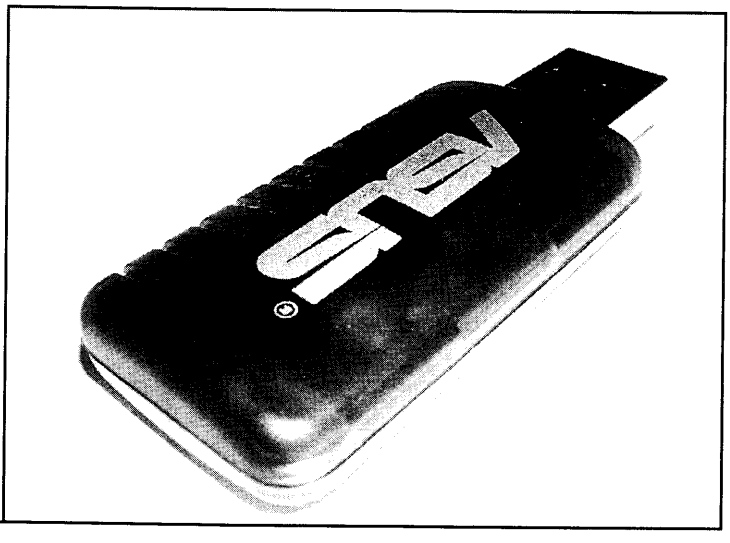


Рис. 6.3. Wi-Fi адаптер Asus WL-161

Альтернативой в деле построения домашней локальной сети является уже упоминаемая технология HomePNA. Отметим, что сейчас HPNA-адаптеры сравнительно дороги. Например, обычная PCI-карта этого стандарта стоит около $ 50. За эти деньги можно построить Ethernet-сеть для пяти–восьми компьютеров на базе коммутатора, или объединить пару компьютеров беспроводной Wi-Fi сетью. Хотя HPNA, особенно при снижении цен на оборудование, может стать хорошим решением для домашних пользователей.

Перечислим оборудование, на примере которого мы будем далее рассматривать настройку локальных сетей.

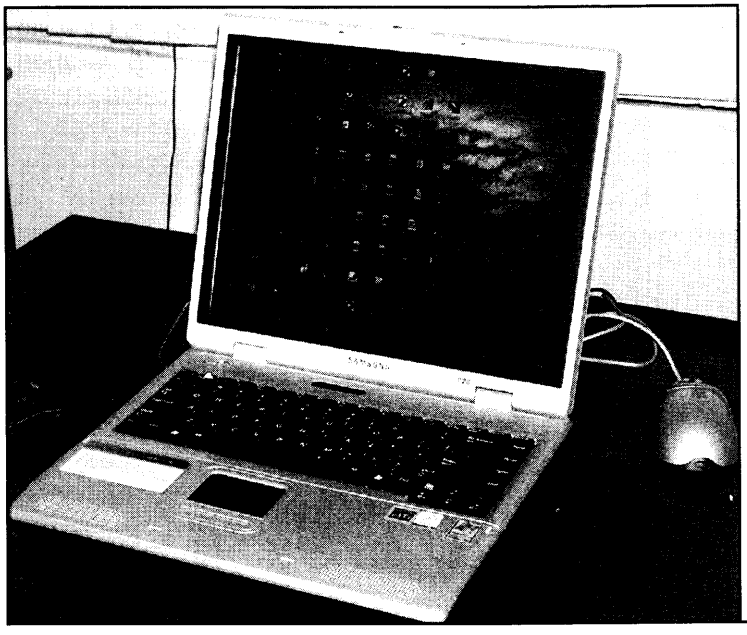


Рис. 6.4. Samsung P28-DGH

В качестве сетевой карты выступает карточка Fast Ethernet Genius GF100TXV. Она собрана на чипе от VIA и в документации называется VIA VT6105 Rhine III Fast Ethernet Adapter. Эта карта установлена в настольный ПК на базе Athlon XP 1,8+, оснащенном 256 Мб DDR RAM и 40 GB HDD. В качестве кабелей — UTP 5 категории.

В качестве второго ПК в нашем примере выступает ноутбук Samsung P28-DGH (рис. 6.4) с интегрированным сетевым адаптером Broadcom 440x 10/100 Integrated Controller. Это оборудование, которое относится к проводной части наших экспериментов.

В качестве беспроводного испытательного полигона будем использовать все тот же настольный компьютер, оснащенный беспроводным адаптером ASUS WL-161 — это устройство стандарта 802.11b, и ноутбук со встроенной беспроводной сетевой картой Agere Wireless Mini PCI Card того же стандарта 802.11b.

Мы подробно разберем вопросы интеграции в беспроводную сеть КПК на базе Windows Mobile 2003 — это Fujitsu Siemens Pocket LOOX 420 (рис. 6.5) со встроенным адаптером Wi-Fi стандарта 802.11b.

Немало времени мы отведем модемам. Тестовыми экземплярами послужат модем Zyxel Omni 56K PCI (рис. 6.6), встроенный в ноутбук SENS LT56ADW, и пара беспроводных модемов, проще говоря — сотовых телефонов, оснащенных встроенными модемами. Это Motorola C650 (рис. 6.7), выступивший в качестве GPRS-модема, который можно соединить с настольным ПК посредством дата-кабеля, и Alcatel 535 (рис. 6.8). Кроме этого, такой телефон имеет все шансы «подружиться» с КПК посредством инфракрасного порта.

В качестве хаба для построения проводной сети использовался недорогой восьмипортовый коммутатор Compex PS2208B (рис. 6.9)

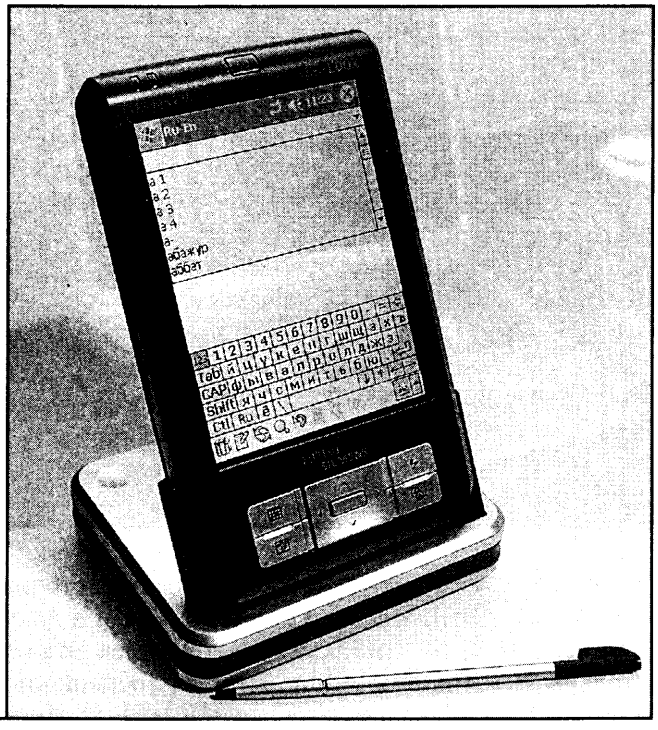


Рис. 6.5. Fujitsu Siemens Pocket LOOX 420

В следующем разделе мы подробнее рассмотрим функции маршрутизации. Это нужно, чтобы сделать один из вышеперечисленных ПК маршрутизатором и посмотреть, что из этого всего выйдет.

6.2. КОММУТАТОРЫ, КОНЦЕНТРАТОРЫ, МОСТЫ, МАРШРУТИЗАТОРЫ

КОММУТАТОР

Коммутатор — это центр проводной Ethernet-сети. До недавнего времени были распространены Ethernet-концентраторы, но сегодня простой коммутатор для локальной сети из нескольких ПК стоит довольно дешево. Такой коммутатор имеет несколько RG-45 разъемов для подключения сетевого оборудования.

Таким оборудованием могут быть настольные ПК и ноутбуки, оснащенные сетевыми картами, а также, например, принтеры, поддерживающие подключение к Ethernet-сетям.

В простой локальной сети коммутатор — самое неприхотливое устройство. Он представляет собой логическое продолжение кабельной системы или сети, не требующее дополнительной настройки. После установки в компьютеры сетевых адаптеров достаточно воткнуть сетевые кабели в разъемы на сетевых картах и на хабе, и физическая часть работ по созданию сети может считаться завершенной.

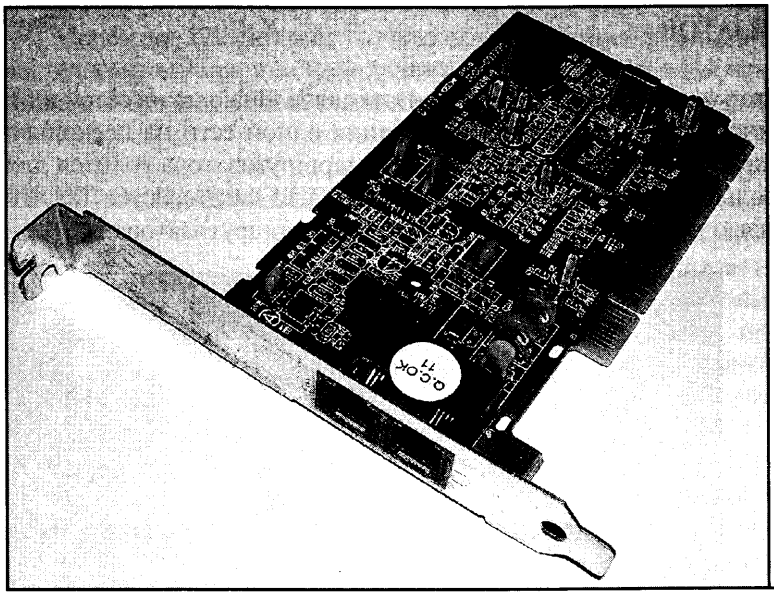


Рис. 6.6. Zyxel Omni 56K PCI

ТОЧКА ДОСТУПА

Точки доступа, использующиеся при построении беспроводных сетей, обычно управляются через веб-интерфейс.

Маршрутизаторы в их физическом воплощении для домашней или малой сети не нужны. Во-первых, они довольно дороги, а во-вторых, домашняя сеть редко когда объединяет больше двух компьютеров. Правда, в маршрутизации может нуждаться и малая сеть, если понадобится соединить два сегмента сети, построенные по разным технологиям. Это может быть, к примеру, сегмент на Wi-Fi и на Fast Ethernet. В таком случае можно воспользоваться специальной точкой доступа, которая свяжет воедино проводную и беспроводную сеть.

Этот вариант подойдет, если потребуется соединить две достаточно большие беспроводные и проводные сети. Правда, придется пойти на дополнительные затраты. Но если у вас, скажем, в офисе есть большая беспроводная сеть и если вы не являетесь ее администратором, тогда там, во-первых, обойдутся без вашего вмешательства, и, во-вторых, велика вероятность, что подобная точка доступа уже существует. Поэтому

в этой книге мы рассмотрим настройку в качестве маршрутизатора одного из компьютеров сети, обладающего и проводным, и беспроводным интерфейсами.

А раз так — остановимся подробнее на принципах работы маршрутизаторов.

МАРШРУТИЗАТОР

Маршрутизатор — это сетевое устройство для связи нескольких сетей или, как бы странно это ни звучало, для разбиения одной сети на несколько разных. Последний вариант использования маршрутизатора годится для достаточно больших Ethernet-сетей, и вас он вряд ли заинтересует. Так что займемся связью нескольких сетей посредством маршрутизатора.

Рис. 6.7. Motorola C650

Маршрутизатор, как уже говорилось, работает на третьем, сетевом уровне модели OSI. Классический маршрутизатор содержит несколько портов и строит таблицу маршрутизации. Эта таблица содержит информацию о «расстоянии» до того или иного узла и о том, на какой порт маршрутизатора необходимо отправить пакет данных, предназначенный для этого узла. Маршрутизатор анализирует адресную информацию маршрутизируемых протоколов (IP, IPX и так далее) и принимает решение о том, на какой из своих портов отправить полученные данные. При этом маршрутизатор должен определить оптимальный путь отправки данных.

В малой сети главная задача маршрутизатора — соединять сети, построенные по разным технологиям. А эта функциональность достаточно

легко может быть реализована обычным ПК, имеющим несколько сетевых интерфейсов и соответствующее программное обеспечение. Мы рассмотрим реализацию такой маршрутизации в одной из следующих глав.

6.3. МОДЕМЫ

Модемное соединение — чрезвычайно популярный способ подключения компьютера или небольшой локальной сети к Интернету. Правда, модем — это медленное соединение, зато сравнительно дешевое.

ТЕЛЕФОННЫЕ МОДЕМЫ

Модем — английское слово-неологизм, составленное из двух слов *Modulator/Demodulator* (модулятор/демодулятор). С помощью модема цифровые данные, с которыми работает компьютер, преобразуются в аналоговую форму, пригодную для передачи по телефонным линиям, и, наоборот, аналоговые сигналы превращаются в цифровые, понятные компьютеру.

Модемы — последовательные устройства передачи данных. Одновременно они передают или принимают лишь один бит информации.

Модемы выпускаются в различных конструктивных вариантах. Они бывают внутренними и внешними. Если один и тот же модем реализован в обоих вариантах, то разница между ними заключается в отсутствии у внутреннего модема отдельного блока питания, корпуса и, естественно, индикаторов состояния модема на корпусе. Отсутствие внешних индикаторов, а также то, что при зависании модема (это бывает крайне редко, по крайней мере если пользоваться качественным модемом известного производителя вроде Zyxel) приходится перезагружать весь компьютер, часто заставляет пользователей делать выбор в пользу внешних модемов.

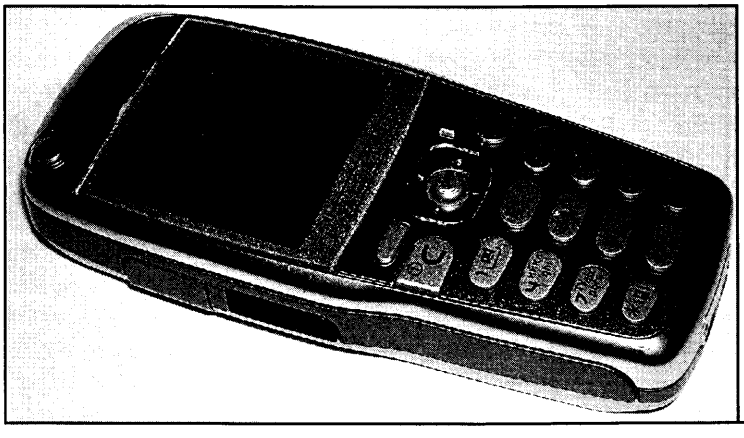


Рис. 6.8. Alcatel 535

Но внешний модем при прочих равных условиях немного дороже внутреннего. В целом же выбор между внутренним и внешним модемом — дело вкуса, так как и те и другие работают совершенно одинаково.

Существует странный класс устройств, называемых программными модемами, или софт-модемами. Логика работы такого модема ничем не отличается от работы обычного модема. Вся разница заключается в том, что софт-модем не имеет собственных вычислительных ресурсов, и вся обработка информации, которой занимается обычный модем, перекладывается на центральный процессор компьютера. Обычный модем, если посмотреть на его внутреннее устройство, похож на компьютер в миниатюре: у него есть свой процессор, ПЗУ, микросхемы, обеспечивающие обмен информацией с другими устройствами, или, как их еще называют, интерфейсные микросхемы. А у типичного софт-модема есть лишь интерфейсные микросхемы.

Софт-модемы дешевле обычных, но такая экономия весьма сомнительна. Качественный аппаратный модем предпочтительнее софт-модема.

Бывают софт-модемы, встроенные в материнские платы. Что делать: пользоваться тем, что уже имеется, или покупать отдельное устройство? Попробуйте поработать с программным модемом и решите, устраивает ли он вас и не нужен ли аппаратный модем взамен того, что уже есть и так.

На компьютерные мощности находится немало охотников. На мощном современном компьютере помимо операционной системы, съедающей немало ресурсов, работает куча нужных программок: антивирусы, файрволлы и, естественно, прикладные программы пользователя. Когда вы выходите в Интернет при помощи программного модема, на систему ложится дополнительная нагрузка. Работа программ на перегруженном компьютере замедляется, а соединение с Интернетом, осуществляемое софт-модемом,

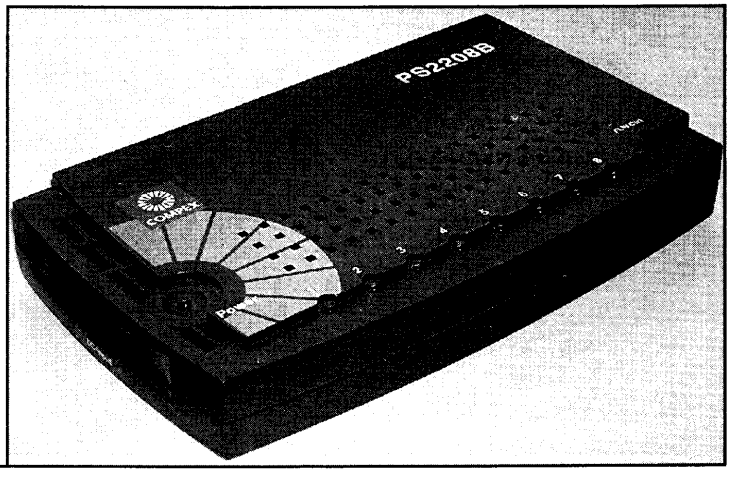


Рис. 6.9.
Compex PS2208B

тоже может замедлиться, а то и разорваться. Современные компьютеры достаточно мощны и часто «не замечают» работы софт-модема, но пользователю, выбирающему модем, следует знать особенности его работы.

Рассмотрим способы подключения модема к компьютеру.

Внутренние модемы подключаются через PCI или PCI-Express. Внешние модемы подключаются либо по все еще здравствующему COM-порту, либо по вездесущей USB. И те и другие выполняют свои задачи очень хорошо. Правда, установка USB-модемов не всегда проходит гладко. COM-модем можно установить очень быстро, чуть ли не с закрытыми глазами, а вот USB — не всегда. Зато после установки проявляются все удобства USB-модема: как и все USB-устройства, его можно отключать и подключать даже при работающем компьютере.

Подключение внутреннего модема состоит в его установке в свободный слот материнской платы или подсоединении к поддерживаемому им интерфейсу. Для подключения COM-модема компьютер надо выключить, а если речь идет о USB-модеме, то следует поступать в соответствии с инструкцией к нему.

Некоторые инструкции по установке устройств предупреждают, что подключение модема (или другого USB-устройства) до установки драйверов может вызвать проблемы.

Подключая к модему телефонный кабель, убедитесь, что вы вставляете его в нужное гнездо. Дело в том, что модемы имеют как минимум два гнезда — Line и Phone. Одно из них (Line) служит для подключения к телефонной линии, а второе (Phone) — для подключения к этой линии телефона. Телефон можно подключить и как-нибудь по-другому, к примеру воспользовавшись специальной телефонной розеткой на несколько устройств. Но слишком большое количество устройств на одной телефонной линии ухудшает ее параметры и приводит к снижению и без того не слишком высокой скорости модемного соединения.

В области модемов, так же как и в области локальных сетей, существуют стандарты, которые определяют параметры оборудования, протоколы коррекции ошибок, сжатия информации и передачи данных. Уже несколько лет в среде модемов нет никаких заметных новостей. Пока максимальная скорость передачи данных, предусматриваемая стандартом ITU-T V.92, находится на уровне 56 Кбит/с. Как правило (полагаю, что это подтвердят пользователи модемов), зачастую не удается достичь даже этой скорости.

Важное для модемов значение имеют протоколы сжатия информации и коррекции ошибок. Поясним этот тезис. Телефонная линия подвержена воздействию различных помех. Порой старые аналоговые АТС сами по себе являются главной помехой в установлении быстрого соединения. С этим ничего не поделаешь, но стандарты коррекции ошибок и сжатия данных помогают несколько скрасить неприятные моменты

плохих линий связи. Здесь надо учесть, что, пересылая с помощью модема файл, сжатый каким-нибудь архиватором, вы вряд ли сможете добиться от встроенных алгоритмов модема дополнительного сжатия, а вот коррекция ошибок — это всегда важно и всегда нужно. Среди применяемых сегодня протоколов сжатия данных можно отметить V.42, а среди стандартов сжатия данных — V.44.

Использование модема предусматривает выполнение некоторых простых правил безопасности. Если технологии локальных сетей, которые мы рассматривали раньше, по умолчанию находятся внутри здания, то модем — это устройство, связывающее компьютер при помощи телефонной проводки, иногда проходящей по воздуху, с АТС. В телефонный провод, расположенный на улице, может ударить молния. Удар молнии в телефонный провод — событие редкое, но вполне реальное, и, если вы пользуетесь модемом и знаете, что ваши телефонные провода проходят «по воздуху», — помните, что ваша техника находится под угрозой. Поэтому во время грозы лучше отключить модем от телефонной линии.

Иногда рекомендуют использовать специальные защитные устройства — фильтры телефонной сети. Эти фильтры позволяют защитить модем от перепадов напряжения в телефонной сети: по разным причинам там иногда бывают сильные всплески. Хорошие и недешевые модемы, как правило, имеют собственные средства для борьбы с перепадами напряжения.

СОТОВЫЙ ТЕЛЕФОН В КАЧЕСТВЕ МОДЕМА

Все, что было сказано выше, относилось к обычным проводным модемам, используемым на простых телефонных линиях. Но сегодня растет популярность GPRS-модемов, которые часто представляют собой обычные мобильные телефоны со встроенным модемом, подключенным к компьютеру.

Существуют и специальные GPRS-модемы. Они чаще всего выполнены в формате PCMCIA и предназначены для использования совместно с ноутбуками. Такой модем стоит примерно столько же, сколько самая последняя и функциональная модель сотового телефона.

Теоретически GPRS-соединение может предоставить пользователю скорость соединения до 172 Кбит/с, но на практике эта цифра в несколько раз ниже. Дело в том, что российские GSM-сети ориентированы на передачу голосового трафика, и скорость GPRS-соединения может быть очень низкой, особенно в рабочее время суток. Однако здесь все зависит от местности, где вы пытаетесь произвести соединение.

Что бы там ни говорили, а GPRS-модем — это очень удобно, особенно тогда, когда под рукой нет ничего лучше. Владельцы ноутбуков и КПК,

которым приходится, скажем, проводить много времени в дороге, уже оценили преимущества беспроводного Интернета и давно им пользуются.

Сегодня весь мир развивает сотовые сети третьего поколения, или 3G-сети. Пользователи встретили такие сети довольно прохладно, но их развитие продолжается. В России тоже есть проекты таких сетей, например «СкайЛинк». Основные отличие таких сетей от «традиционных» GPRS-сетей (их иногда называют 2,5G-сетями) состоит в скорости передачи данных. Она может колебаться, в зависимости от технологии построения сети третьего поколения, в очень широких пределах — от сотен килобит в секунду до мегабитных скоростей. Правда, как и в случае с GPRS, фактическая скорость соединения может отличаться от заявленной в меньшую сторону.

Коммутируемый доступ в Интернет по обычному модему оплачивается повременно, и, если вы в течение часа соединения не передали ни одного бита, вы оплатите этот час полностью. Правда, стоимость телефонного Интернета сейчас весьма невысока. GPRS-соединение позволяет оператору мобильной связи организовывать тарификацию не за время соединения, а за трафик. Получается, что вы можете сутками «висеть» на GPRS-канале, заплатив лишь за переданную вами информацию.

ИНТЕРФЕЙСЫ БЕСПРОВОДНЫХ МОДЕМОВ

Существует несколько интерфейсов взаимодействия беспроводных модемов с компьютерами. Первый тип соединения — проводной. Сотовые телефоны (или беспроводные модемы, как мы назвали их ранее) могут подключаться к компьютерам и при помощи дата-кабелей. Каждой модели телефона нужен собственный дата-кабель. Иногда (крайне редко!) один и тот же кабель может работать с несколькими моделями одного и того же производителя. Например, это телефоны от Motorola — многие из них поддерживают соединение с ПК по Mini-USB кабелю.

Способы кабельного соединения тоже разнятся. Устаревший, но все еще существующий вариант такого соединения предусматривает использование дата-кабеля для COM-порта. Вариант поновее — это уже порядком примелькавшееся решение на базе USB. Обычно у пользователя сотового телефона нет выбора — конкретная модель телефона, как правило, поддерживает лишь один тип кабеля. Однако USB-соединение все же быстрее, да и управляться с телефоном, поддерживающим такое соединение, куда легче. Проводные комплекты созданы как для настольных ПК и ноутбуков, так и для КПК. Видимо, провода будут нужны еще долгое время, но их уверенно вытесняют беспроводные средства связи — инфракрасные порты и Bluetooth-адаптеры.

IrDA — *Infrared Data Association* (Ассоциация инфракрасной передачи данных) — это протокол ближней беспроводной связи. Инфракрас-

ная связь (к примеру, пульты дистанционного управления) существует уже довольно давно.

Как это бывает обычно, на первых этапах использования технологии среди производителей не было единства и каждый делал инфракрасные устройства по-своему. В 1993 году Hewlett-Packard собрала множество ведущих производителей электронной техники на совещание, посвященное стандартам инфракрасной связи. В результате была образована Ассоциация инфракрасной передачи данных, которая существует до сих пор.

Особенность стандарта IrDA заключается в том, что для передачи данных используется световое излучение с длиной волны 850–900 нм. Скорость передачи данных в этом стандарте изменяется от 9,6 Кбит/с до, в новых его реализациях, 16 Мбит/с и даже больше. Ассоциация инфракрасной передачи данных ведет работу над дополнительными спецификациями стандарта, применение которых позволит поднять скорость передачи данных до 100–500 Мбит/с.

Носитель информации в IrDA — свет, а это накладывает на его использование определенные ограничения. Плюсы IrDA заключаются в низкой стоимости оснащения сотовых телефонов и другой техники инфракрасным портом и в достаточно высоком уровне защищенности канала связи: ведь свет не проходит сквозь непрозрачные предметы, а учитывая маломощность инфракрасного передатчика, канал передачи данных может быть «взломан» лишь с достаточно близкого расстояния.

Если говорить о дальности инфракрасной связи, то более или менее качественная инфракрасная связь возможна на небольшом расстоянии — от метра и меньше.

Ограниченное расстояние передачи данных — это существенный минус. К тому же связь по IrDA-каналу может быть неустойчивой, особенно если пользоваться ею в транспорте для соединения сотового телефона с ноутбуком. Стоит портам ноутбука и сотового немного сместиться, и связь прерывается.

Здесь следует учитывать, что свет исходит из инфракрасного приемопередатчика в виде конуса, который должен быть направлен на другой инфракрасный порт.

Еще одним недостатком стандарта является то, что по IrDA могут одновременно общаться лишь два устройства: в нашем случае это сотовый телефон, выступающий в роли беспроводного модема, и компьютер.

Несмотря на все недостатки стандарта, инфракрасные порты продолжают встраивать в мобильные телефоны, ими оборудуют ноутбуки и КПК. В последнее время, однако, производители техники постепенно отходят от инфракрасных портов. Например, во многие ноутбуки их уже не встраивают, и все больше производителей сотовых отдают предпочте-

ние более скоростным и надежным стандартам передачи данных. Но при желании вы сможете оборудовать ваш ПК инфракрасным портом — стоят они сейчас около $ 30.

Другая технология, которая вызывает сегодня наибольший интерес в области связи мобильных устройств друг с другом и с настольными собратьями, называется Bluetooth.

История этого стандарта начинается в 1998 году, когда группа компаний: Ericsson, Intel, IBM, Toshiba и Nokia — начала разработку Bluetooth (в переводе на русский — «Синий зуб»), или, сокращенно, BT. Технология была названа так в честь датского короля Харальда Блатана, жившего в X веке: он славился способностью легко находить общий язык со своими вассалами. По мысли разработчиков, Bluetooth-устройства должны были так же свободно «разговаривать» друг с другом. Через некоторое время после начала исследований к «первопроходцам» присоединились другие фирмы, и вместе они занялись работой над новым стандартом беспроводной связи.

Главными идеями, которые были положены в основу разработок, стали экономичность, маленькие размеры модуля связи, дешевизна и максимальная простота использования. Стандарт Blutetooth планировался как универсальный, соединяющий любые устройства друг с другом. Среди них — сотовые телефоны, гарнитуры hands-free, КПК, ноутбуки, настольные компьютеры, компьютерная периферия и так далее.

Среди преимуществ «Синего зуба» можно отметить дальность действия — до 10–15 метров. На таком расстоянии могут связываться устройства стандарта Bluetooth 1.1, а в стандарте Blutetooth 1.2 «разговор» уже может происходить на 100 метрах.

Так как для связи используются радиоволны, непрозрачные предметы для них уже не помеха. Скорость передачи данных по Bluetooth-каналу может достигать 721 Кбит/с.

Для передачи данных используется диапазон частот 2400–2483,5 МГц, который во многих странах не лицензируют. Государственная комиссия по радиочастотам при Министерстве связи России узаконила использование Bluetooth в указанном диапазоне частот в 2003 году.

Если говорить о преимуществах BT перед IrDA, можно отметить возможность одновременного «общения» семи устройств — при этом получается некое подобие небольшой локальной сети. Что до безопасности, то с ней у Bluetooth все хорошо. Конечно, существует потенциальная возможность несанкционированного доступа к данным, передаваемым по BT-каналу, или подключение злоумышленника к устройству, сотовому, например, оборудованному BT-адаптером. Но реальная опасность не слишком высока.

Bluetooth встраивают во все большее количество моделей телефонов, КПК среднего и высокого уровня оснащают BT-адаптерами, но встро-

енный BT присущ ноутбукам ценой начиная от $ 2000. BT-адаптер, который одинаково хорошо подойдет для настольного ПК или ноутбука, стоит сейчас в районе $ 40, если не меньше.

Как видите, соединить ПК, КПК или ноутбук с сотовым телефоном можно без особых проблем. Как правило, стоимость коммуникационных средств, если они не встроены в устройства, не превышает $ 40 (это цена дата-кабелей, BT-адаптеров и инфракрасных портов).

6.4. ЕЩЕ НЕСКОЛЬКО СЛОВ О КАБЕЛЯХ

Обжим — это неразъемное соединение, обеспечивающее надежное электрическое и механическое сопряжение кабеля и контактов разъема. В процессе обжима производится соединение проводников кабеля с соответствующими контактами вилки разъема, после чего сама вилка закрепляется на кабеле.

Правильный, качественный обжим кабеля имеет большое значение для нормальной работы сети. Если кабель не слишком длинный, скажем метров 10–15, то огрехи в обжиме могут быть незаметны. Ну а если длина кабеля метров 50, любые неточности могут отрицательно повлиять на работу сети: сеть либо не будет работать вообще, либо будет работать, но не на максимальной скорости.

Для использования в домашних условиях подойдут кабели с заводской обжимкой. Обычно они продаются отрезками по 5 метров (бывают и другие длины) и с установленными разъемами RJ-45.

Но такие кабели уместны далеко не всегда. Что делать, если вам нужен кабель подлиннее или покороче? Здесь можно пойти двумя путями.

- Кабель нужной длины вам могут обжать там, где вы его приобретаете. Это, кстати, наиболее предпочтительный вариант. Для обжима кабелей существуют специальные обжимочные инструменты.
- Если у вас есть обжимочный инструмент, значит, вы и сами знаете, что с ним делать. Если такого инструмента нет, то обжать кабель можно обычной отверткой. Правда, качество обжима может от этого пострадать.

Рассмотрим схемы расположения проводников UTP 5-й категорий для наиболее часто используемого сегодня восьмижильного кабеля.

Есть **две** стандартные схемы обжима. **Одна** схема обжима состоит в том, что разводка проводников на одном конце кабеля соответствует разводке на другом. Такая схема применяется для соединения сетевых карт и портов коммутатора: кабель, обжатый таким образом, подойдет для монтажа сети на основе коммутатора. **Другой вариант** обжима позволяет связывать одним кабелем две сетевые карты напрямую, создавая локальную сеть из пары компьютеров без использования коммутатора.

Рассмотрим наиболее распространенную схему распределения пар проводников в кабеле, определенную стандартом EIA-T568B (табл. 6.1).

При использовании схемы EIA-T568B пары скручиваются таким образом:

1. Синий — бело-синий
2. Оранжевый — бело-оранжевый
3. Зеленый — бело-зеленый
4. Коричневый — бело-коричневый

Номер контакта разъема	Конец кабеля 1	Конец кабеля 2
1	Бело-оранжевый (БО)	Бело-оранжевый
2	Оранжевый (О)	Оранжевый
3	Бело-зеленый (БЗ)	Бело-зеленый
4	Синий (С)	Синий
5	Бело-синий (БС)	Бело-синий
6	Зеленый (З)	Зеленый
7	Бело-коричневый (БК)	Бело-коричневый
8	Коричневый (К)	Коричневый

Таблица 6.1. Разводка кабеля для соединения «сетевая карта — хаб»

Как видите, одинаковые провода соединяют одинаковые выходы разъема RJ-45. Чтобы расположить проводники правильно, розетку нужно ориентировать таким образом, как показано на рис. 6.10.

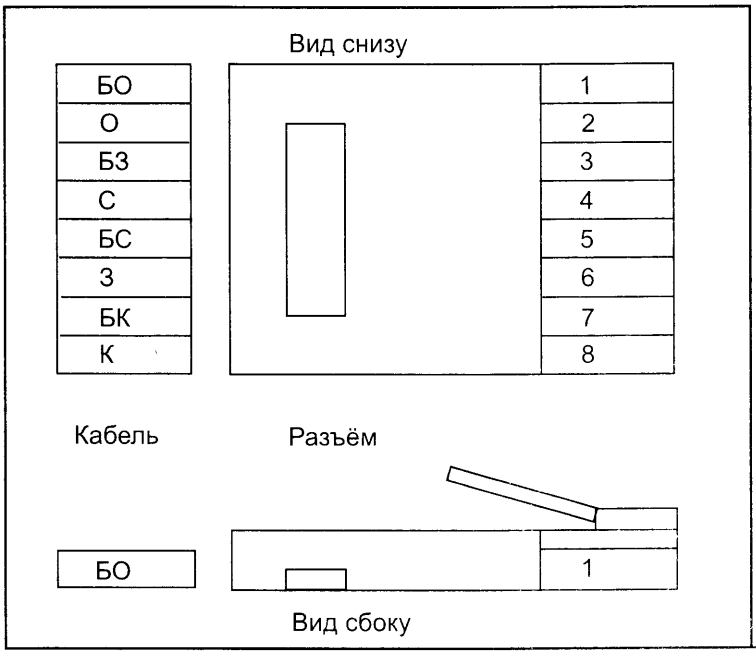


Рис. 6.10. Расположение кабеля и разъема при заделке кабеля и нумерация позиций

В табл. 6.2. приведен порядок разводки кабеля для соединения «сетевая карта — сетевая карта».

Таблица 6.2. Разводка кабеля для соединения «сетевая карта – сетевая карта» (кроссовер)

Номер контакта разъема	Конец кабеля 1	Конец кабеля 2
1	Бело-оранжевый	Бело-зеленый
2	Оранжевый	Зеленый
3	Бело-зеленый	Бело-оранжевый
4	Синий	Синий
5	Бело-синий	Бело-синий
6	Зеленый	Оранжевый
7	Бело-коричневый	Бело-коричневый
8	Коричневый	Коричневый

Как видно из таблицы, здесь меняются местами лишь четыре провода. Так мы напрямую соединяем приемник одной сетевой карты с передатчиком другой, и наоборот.

Подготовив кабели и разъемы, нужно зачистить концы кабеля, удалив внешнюю изоляцию. Сделать это можно острым ножом. При этом старайтесь не повредить провода внутри кабеля. Можно снять с кабеля изоляцию длиной сантиметра 3–4, чтобы потом было легче выпрямлять провода. Выпрямив провода, обрежьте кабель таким образом, чтобы в результате осталось примерно 12–15 миллиметров распрямленных проводов. Собираясь обжимать длинный кабель, постарайтесь не выходить за пределы 12 миллиметров. После этого наденьте разъем на кабель так, чтобы нужные проводники попали в соответствующие им желобки разъема. Сами провода зачищать не нужно.

На последнем этапе заделки провода его нужно обжать. Обжимный инструмент все сделает сам, а если такого инструмента нет, то ваши действия должны быть следующими: сначала аккуратно обожмите контакты при помощи отвертки — так, чтобы они, врезавшись в соответствующие провода, обеспечили надежное соединение, а потом зажмите до щелчка фиксатор кабеля.

6.5. ВЫВОДЫ

О физических вопросах подключения оборудования мы поговорили достаточно. А раз так — переходим к обсуждению программных технологий.

ГЛАВА 7
НАСТРОЙКА СЕТЕВОГО ОБОРУДОВАНИЯ

Установив оборудование, не торопитесь закрывать крышку системного блока и не подключайте к нему сразу все кабели. Сначала проверьте, «видит» ли система установленное вами устройство, и только потом, выключив компьютер, закройте корпус, подключите всю периферию и приступайте к установке программ.

В этой главе мы разберем установку и настройку следующего оборудования: сетевой карты VIA VT6105 Rhine III Fast Ethernet Adapter (производство Genius), беспроводного адаптера Asus WL-161 и модема Zyxel Omni 56K PCI.

Начнем с сетевой карточки, которая обеспечивает 100 Мбит/с Ethernet.

7.1. ОПЕРАЦИОННАЯ СИСТЕМА

В основном мы будем работать с операционной системой Windows XP. Некоторые моменты мы рассмотрим и на примере других ОС, но Windows XP — это основа. Она сегодня наиболее распространена, ею оснащаются новые компьютеры, она поддерживает множество устройств, удобна в работе и достаточно безопасна, особенно если регулярно устанавливать обновления от Microsoft.

Обратите внимание: здесь имеется в виду Windows XP Home Edition с установленным комплектом обновлений SP2 (а некоторые вещи мы разберем на примере Windows XP Professional). Service Pack 2 для Windows XP был выпущен Microsoft еще в прошлом году, и в нем множество новшеств, многие из которых касаются именно сетевых вопросов.

Если вы еще не установили SP2, сделайте это поскорее.

Windows XP Home Edition не содержит некоторых возможностей Windows XP Professional. Но в общем случае для дома ОС Windows XP Home Edition является отличным выбором, а при желании вы легко примените все, что знаете, к Windows XP Professional.

Следующий ниже рассказ о драйверах тоже построен на примерах из Windows XP. В Windows 98 и 2000 все очень похоже на XP, поэтому здесь и далее будут рассматриваться только очень серьезные отличия Windows 98 и Windows 2000 от Windows XP.

7.2. ПОИСК ДРАЙВЕРОВ

Часть устройств операционная система устанавливает самостоятельно. Обычно есть смысл заменить драйверы на более свежие, особенно в случае с видеокартами. Драйверы же остальных устройств, определенных и установленных автоматически, лучше менять лишь в том случае, если устройство работает неправильно.

Я уже говорил, что купил сетевую карту VIA VT6105 Rhine III Fast Ethernet Adapter в OEM-исполнении и к ней не приложили даже драйверов. Привыкнув, что драйверы оборудования Windows XP обычно ставит автоматически, я не придал этому никакого значения и, установив карту в компьютер, обнаружил, что драйверов для нее в системе нет. Тогда я пошел в Сеть и начал искать их там.

Где же найти нужный драйвер? У вас несколько путей. Первый — пойти на сайт производителя устройства и поискать там. Другой путь — особенно для устаревшего или просто достаточно старого, но нужного оборудования — поискать в онлайновых архивах. Еще можно походить по знакомым и попробовать обнаружить в их коллекциях CD что-нибудь подходящее.

Особо комичная ситуация возникает, если компьютер не имеет драйверов модема, и этот модем не устанавливается как стандартный. У меня один раз было такое — одна хорошая знакомая попросила настроить ей компьютер, ОС которого стала себя странно вести. Я так и не понял окончательно, что же было с этим компьютером — разбираться времени и желания не было, а работало все из рук вон плохо, висло и сбоило. Например, ужасные странности творились с файловой системой вышеописанного ПК. В корневом каталоге диска C обнаружилось целых 2 папки с именем Windows, с которой машина преспокойно работала параллельно даже в DOS, специально запущенной для проверки этого факта. Такого я вынести не мог, поэтому решил поступить кардинально — Format C:, а потом ставить систему.

У меня был новенький компьютер. Диски с драйверами лежали рядом в целлофановых пакетиках, поэтому я, не мудрствуя лукаво, сделал все, что хотел, и приступил к установке устройств. Принтер, видеокарта, сканер и другие заработали сразу и без проблем, но тут оказалось, что к маленькому, размером с компьютерную мышь USB-модему драйверов нет.

Была коробка от модема, была инструкция к модему, был диск с какой-то программой для модема, но драйверов не было. Исследовав прилагавшийся к модему диск на предмет следов драйверов, и получив в ответ невнятное сообщение ОС о том, что «в указанной папке сведения об оборудовании отсутствуют», я решил атаковать проблему «в лоб».

Запустив мастер нового оборудования, я попытался установить модем как нечто стандартное. Это нечто пыталось выйти в Интернет, после чего наглухо висло. История с модемом затянулась на несколько дней, пока я, добравшись до онлайнового архива драйверов производителя модема, не нашел то, что нужно.

Но вернемся к нашей сетевой карте.

Остановился я на том, что стандартных драйверов на нее обнаружить не удалось, поэтому пришлось мне лезть за ними в Сеть. Ниже я опишу логику поиска драйверов на сайте производителя.

Для начала, если вы не слишком дружите с английским, запаситесь англо-русским словарем: некоторые производители не имеют русскоязычных сайтов, поэтому приходится продираться сквозь дебри классификации устройств этих производителей и вникать в английские понятия. В моем случае, правда, все было на русском, каталог оборудования оказался понятно организован, поэтому драйверы я нашел сразу. Посмотрите на рис. 7.1. Здесь изображена стартовая страничка сайта Genius.ru. Обратите внимание на то, что на первой странице расположен каталог оборудования.

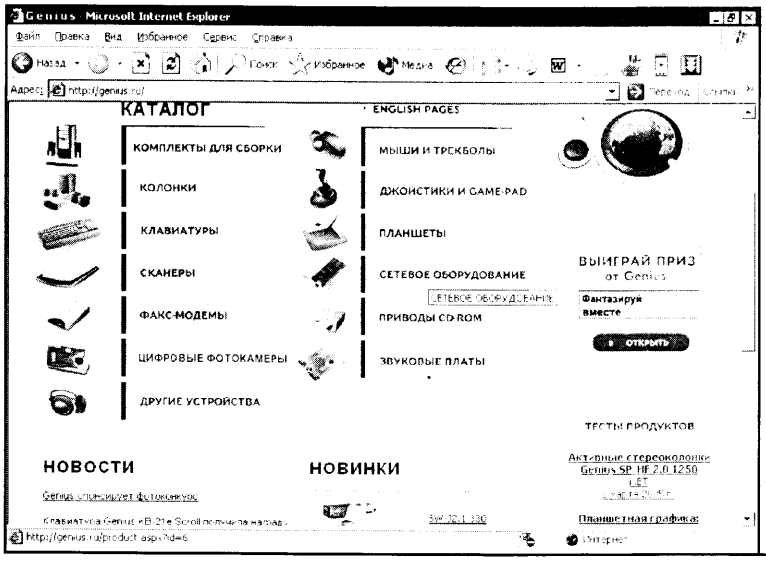


Рис. 7.1. Каталог оборудования Genius

Здесь достаточно выбрать соответствующий пункт в каталоге оборудования, — в нашем случае это сетевое оборудование — перейти на страничку сетевого оборудования (рис. 7.2) и, найдя там ссылку на страничку искомой сетевой карты, перейти на нее (рис. 7.3) и скачать нужный драйвер.

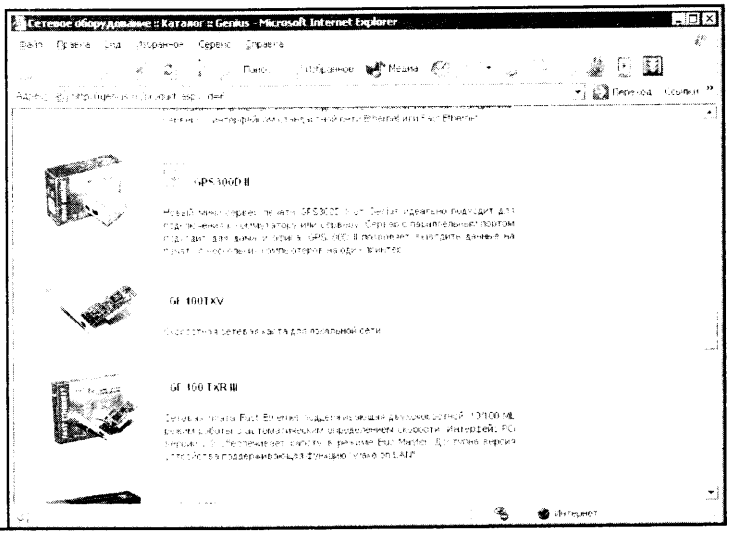


Рис. 7.2. Поиск страницы оборудования

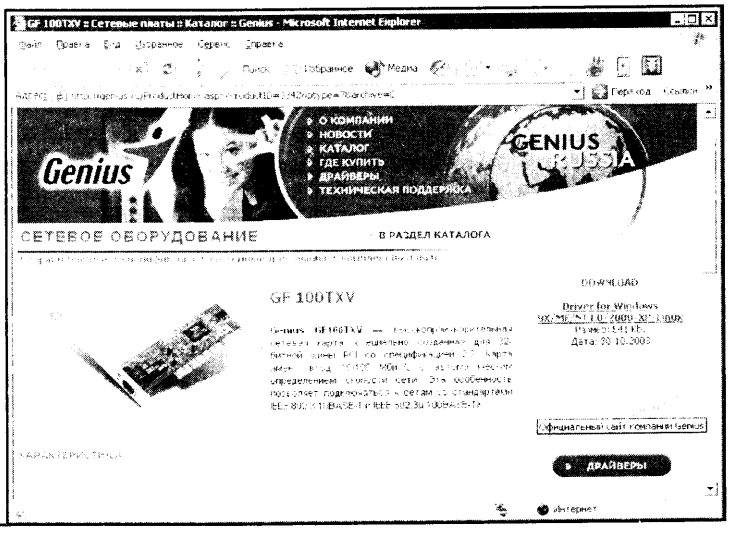


Рис. 7.3. Страничка устройства и загрузка драйверов

Для загрузки драйверов выберите ссылку Download и, дождавшись загрузки ZIP-архива, извлеките его содержимое в какое-нибудь подходящее место.

Прежде чем заниматься установкой драйверов, желательно проанализировать содержимое папки с драйверами. Посмотрите на рис. 7.4. Здесь изображен внешний вид папки с драйверами.

В этой папке мне хотелось найти файл с именем Setup.exe или Install.exe, который взял бы всю работу по установке на себя. Но такого файла не оказалось, поэтому пришлось все делать самому. Этот процесс, однако, не составляет особой сложности, особенно когда знаешь, что и как делать.

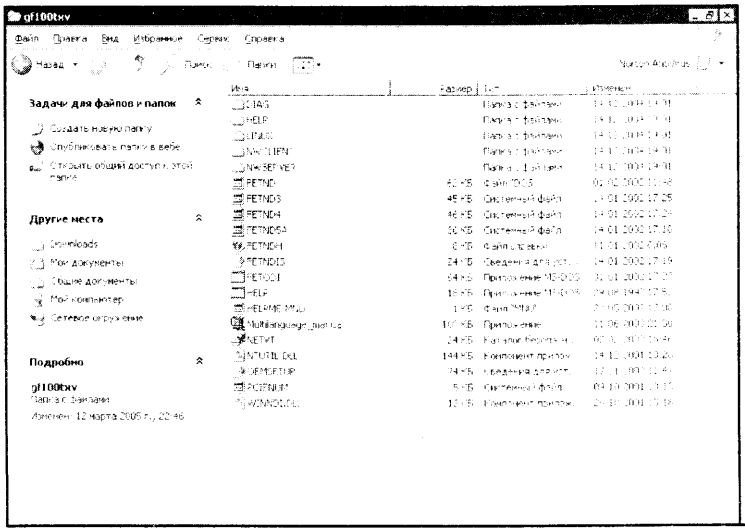


Рис. 7.4. Папка с драйверами

7.3. РУЧНАЯ УСТАНОВКА ДРАЙВЕРОВ СЕТЕВОЙ КАРТЫ

Если драйверы требуют ручной установки, выберите следующий порядок действий. Во-первых, надо сделать щелчок правой кнопкой мыши по значку **Мой компьютер** на **Рабочем столе** и в выпавшем контекстном меню выбрать пункт **Свойства**. Посмотрите на рис. 7.5 — здесь изображен процесс выбора этого пункта меню.

После выбора этого пункта вы увидите окно свойств компьютера. Оно содержит множество вкладок, но нас сейчас интересует вкладка **Оборудование** (рис. 7.6). На нее вам и следует перейти.

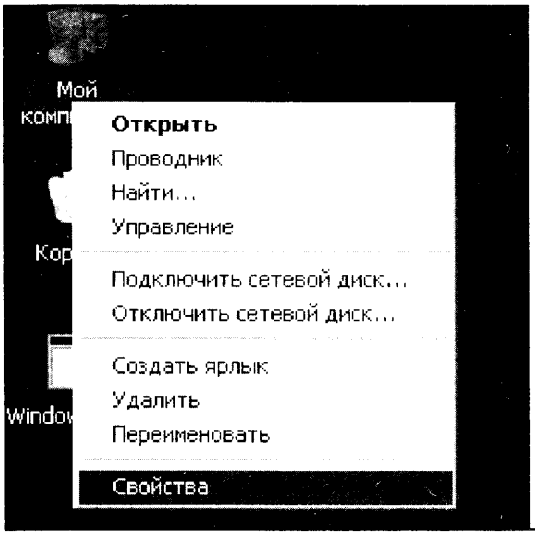


Рис. 7.5. Открытие окна свойств системы

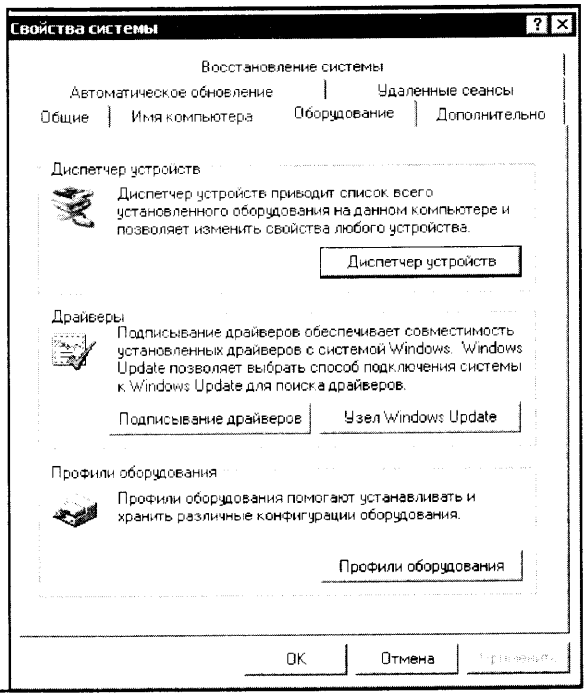


Рис. 7.6. Вкладка Оборудование в окне свойств системы

Когда вы перешли на эту вкладку, нажмите на кнопку **Диспетчер устройств**. Откроется окно **Диспетчера устройств**, где перечислены все установленные в систему устройства.

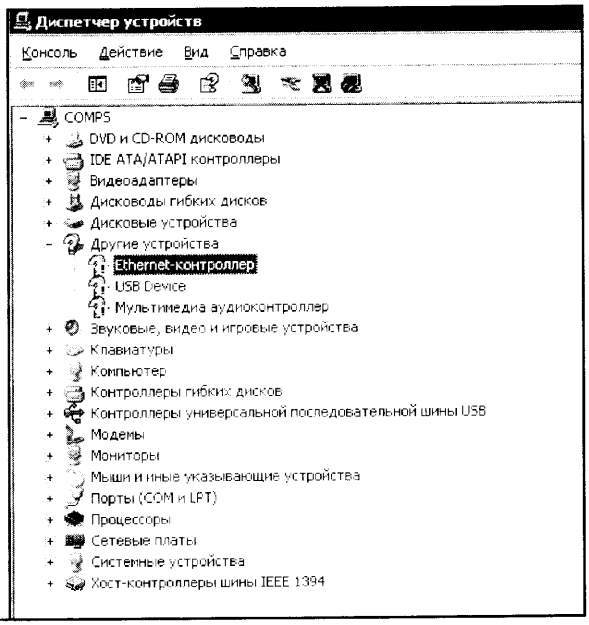


Рис. 7.7. Анализ конфигурации компьютера с помощью Диспетчера устройств

На рис. 7.7 изображено окно диспетчера устройств. Обратите внимание на значки, выделенные восклицательными знаками. Они сгруппированы в отдельную категорию, что позволяет понять, какие устройства еще не инсталлированы в систему должным образом.

Видя такую картину, начинаем ее анализировать. Первый вопросительно-восклицательный знак подписан как **Ethernet-контроллер** — тот самый, драйверов которого в системе не нашлось. Второй значок называется **USB Device** — он имеет отношение к Wi-Fi адаптеру, подключаемому к компьютеру по USB, и его установкой мы займемся чуть ниже.

Третий значок не относится к сетевым устройствам, но его появление вызвано тем, что я не проинсталлировал драйверы для звуковой карты, встроенной в материнскую плату тестового компьютера.

Раз мы хотим установить драйверы для Ethernet-контроллера, щелкаем правой кнопкой мыши по значку с этим контроллером и в появившемся меню выбираем **Свойства** (рис. 7.8).

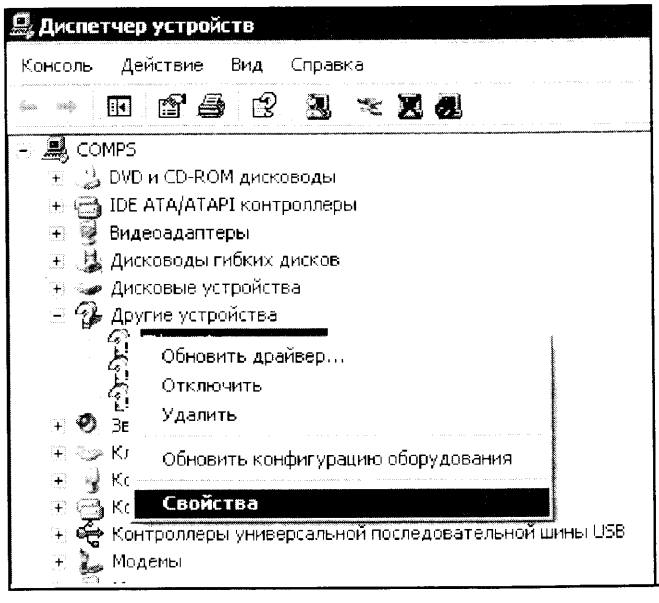


Рис. 7.8. Открытие окна свойств устройства

После щелчка по пункту меню **Свойства** вы увидите окно свойств оборудования. Там, как это обычно бывает в подобных окнах, можно найти массу вкладок, которые служат для характеристики устройства. Обратите внимание на первую из вкладок, которая будет видна сразу после открытия этого окна. Эта вкладка содержит информацию о том, что устройство работает неправильно, и о том, что драйверы для него не установлены (рис. 7.9).

В случае установки драйверов для нового устройства можно обойтись и кнопкой **Переустановить**, но в более сложных случаях полезной может

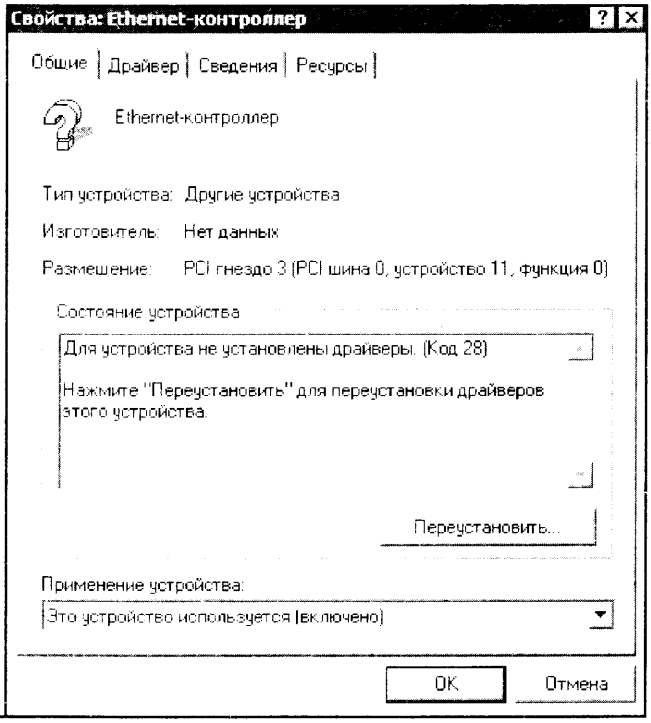


Рис. 7.9. Просмотр свойств устройства

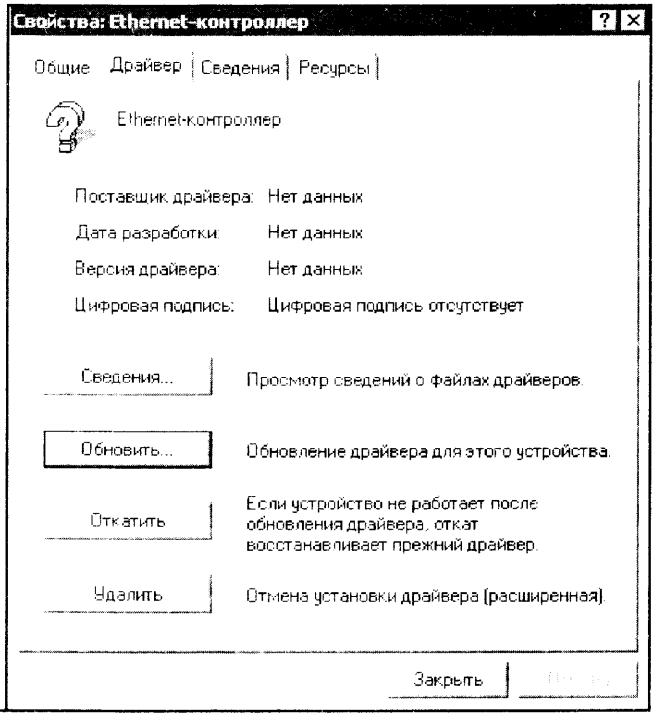


Рис. 7.10. Вкладка Драйвер окна свойств системы

стать вкладка **Драйверы**. Посмотрите на рис. 7.10. Здесь вы можете видеть вкладку **Драйверы** окна свойств устройства.

Если вы хотите начать установку нового драйвера, то на вкладке **Драйвер** достаточно нажать кнопку **Обновить**. Действие этой кнопки аналогично действию кнопки **Переустановить**... вкладки **Общие** того же окна. Но вкладка **Драйвер** существует далеко не случайно. Обратите внимание на кнопки **Сведения**, **Откатить** и **Удалить**.

Кнопка **Сведения** показывает информацию об установленном драйвере устройства. Эта информация может понадобиться вам при обращении в сервис-центр в случае каких-то проблем с устройством.

Кнопка **Откатить** позволяет восстановить прежний драйвер. Это может быть полезным в случае, если вы занимаетесь подбором драйверов для какого-то устройства: например, вы установили драйвер, с которым проблемное устройство работает, но не так, как вам хотелось бы. Вы можете экспериментировать с драйверами, после каждого неудачного эксперимента откатываясь к старому драйверу.

Также кнопка Откатить чрезвычайно полезна в случаях обновления драйверов. Вообще, если какое-то устройство (исключая, наверное, лишь видеокарту) работает нормально, то нет особого смысла обновлять его драйверы. Не факт, что оно будет работать лучше с новыми драйверами, хотя в их установке обычно нет ничего плохого — драйвера улучшают, дорабатывают, поэтому попробовать в любом случае стоит.

Итак, вы установили новый драйвер, и тут оказалось, что ваше устройство начинает вести себя странно. Не спешите, однако, сразу «сносить» новый драйвер — попытайтесь почитать комментарии производителя на тему возможных неполадок — может быть, все дело в неправильной настройке драйвера на вашем компьютере. Если ошибки продолжаются — это значит, что вам ничего не остается, как откатить установку драйвера, вернувшись к прежнему. Также в такой ситуации можно удалить драйвер, воспользовавшись соответствующей кнопкой на вкладке Драйвер окна свойств устройства, и установить старый драйвер заново.

Но вернемся к установке драйверов для нашей сетевой карты. Посмотрите на рис. 7.11. Здесь изображена стартовая страничка Мастера установки нового оборудования.

Windows XP очень любит веб-узлы Microsoft, но она не идет на них бесконтрольно. В нашем случае нет нужды обращаться к узлу Windows Update: драйвер и так лежит в одной из папок на нашем жестком диске. А раз так, выбираем в окне **Мастер обновления оборудования** пункт **Нет, не в этот раз** и нажимаем кнопку **Далее**. После чего попадаем на следующее окно установки драйверов (рис. 7.12).

Мастер хочет уточнить у нас действие, которое следует выполнить дальше. Его интересует способ поиска драйверов для устройства. Если с устройством поставляется установочный диск — достаточно вставить

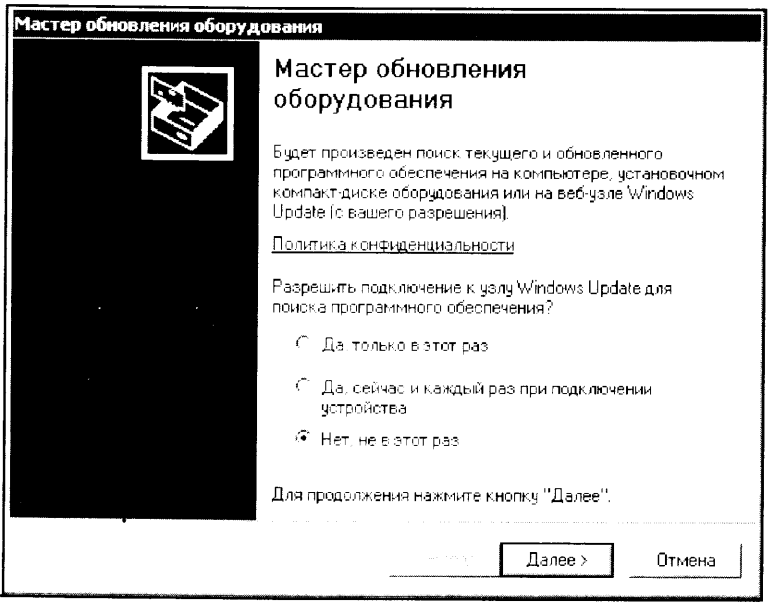


Рис. 7.11. Начало установки нового драйвера

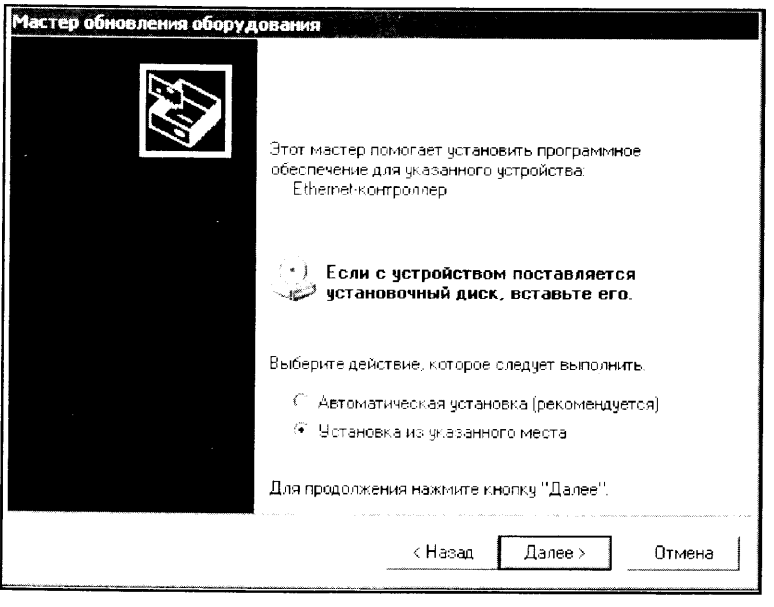


Рис. 7.12. Выбор типа продолжения установки

его в дисковод и, выбрав пункт **Автоматическая установка**, дождаться сообщения о том, что все завершено успешно. Но мы хотим пройти весь путь по установке драйвера сами, поэтому выбираем пункт **Установка из указанного места**. Такой подход полезен при подборе драйверов для устройства. Если система не в состоянии сама найти нужный драйвер, тогда остается найти этот драйвер самому.

Посмотрите на рис. 7.13.

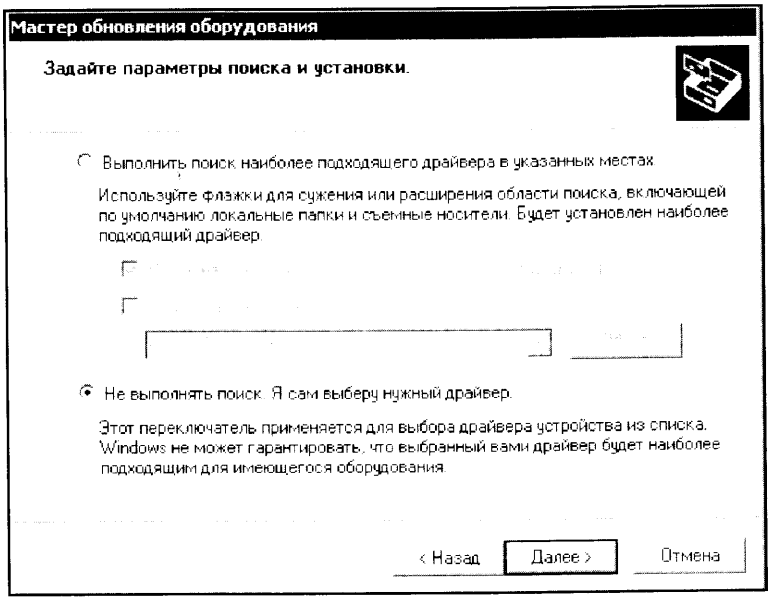


Рис. 7.13. Выбор места для поиска драйвера

Здесь вы видите окно, в котором **Мастер обновления оборудования** спрашивает у вас о том, где следует искать драйверы. В общем случае можно выбрать пункт **Выполнить поиск наиболее подходящего драйвера в указанных местах**, а потом, нажав кнопку **Обзор**, включить в область поиска папку с вашими драйверами, но здесь мы выберем пункт **Не выполнять поиск**.

Мастер предупреждает, что `Windows не может гарантировать, что выбранный вами драйвер будет наиболее подходящим для имеющегося оборудования`. Но в данном случае мы точно знаем, что наш драйвер только что скачан с официального сайта производителя оборудования и предназначен для работы в Windows XP, поэтому можно смело выбирать данный пункт и продолжать установку.

Такой способ позволит вам установить вручную любое устройство даже в том случае, если Windows не в состоянии определить его или найти драйверы для него.

Итак, нажимаем кнопку **Далее** и попадаем в следующее окно **Мастера обновления оборудования** (рис. 7.14).

В этом окне Мастер отдает все на ваше усмотрение. Выбирайте из списка типов устройств тот, который лучше соответствует тому, которое вы хотите устанавливать. В нашем случае это пункт **Сетевые платы**. Выбираем его и продолжаем установку.

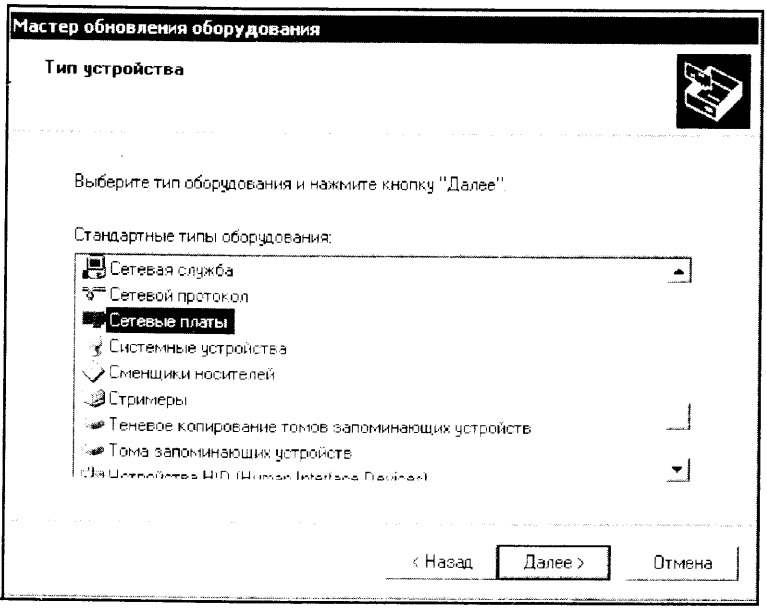


Рис. 7.14. Выбор типа оборудования

Иногда Windows вообще никак не определяет устройство, подключенное к компьютеру, поэтому данный шаг позволит вам установить даже то, что Windows не видит буквально в упор.

Следующим шагом (рис. 7.15) является выбор конкретного драйвера.

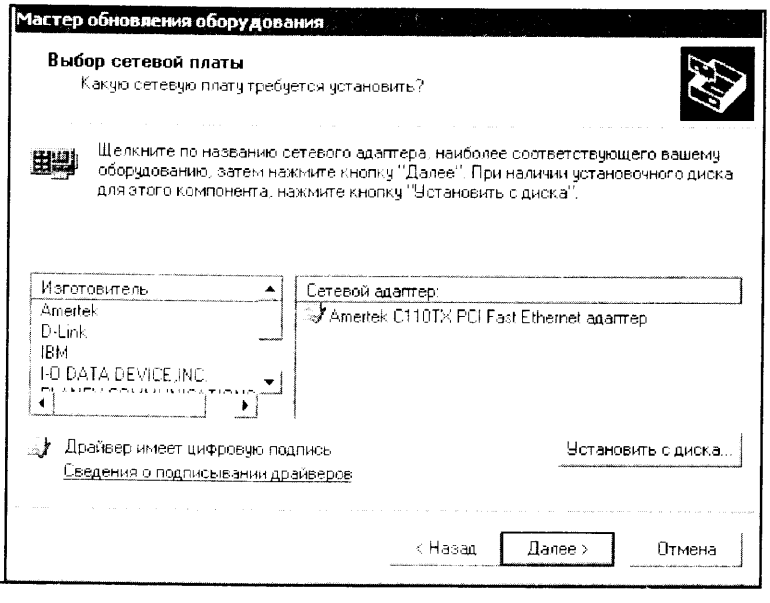


Рис. 7.15. Выбор драйвера

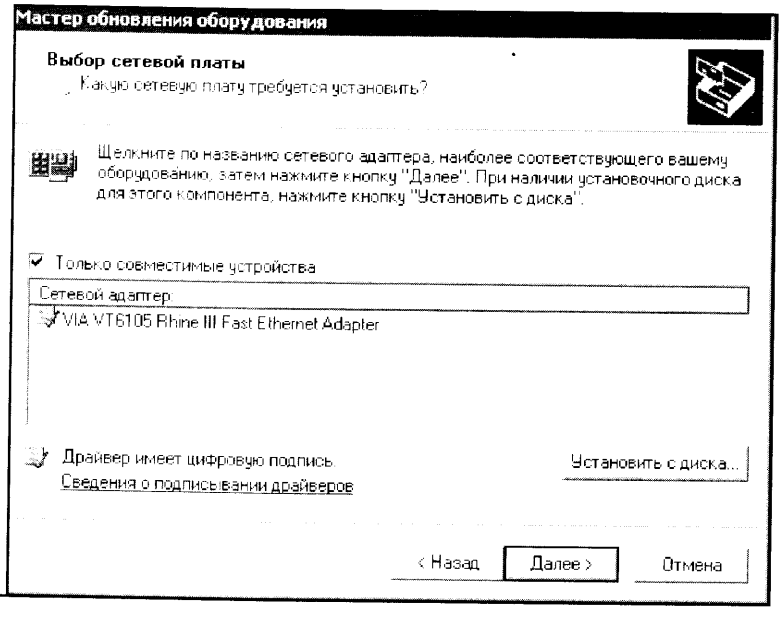


Рис. 7.17. Выбор конкретного драйвера для установки

Это сделано не зря. Windows точно определила устройство, и, когда мы показали ей несколько драйверов, она безошибочно выбрала среди них нужный. Обратите внимание: мы устанавливаем сетевую карту Genius GF100TXV, а в строке наименования драйвера написано нечто совершенно другое — VIA VT6105 Rhine III Fast Ethernet Adapter.

Это не ошибка и не опечатка. Просто фирма-производитель Genius, создавая свою карту Genius GF100TXV, использовала компоненты от VIA, которые определяются как VIA VT6105 Rhine III Fast Ethernet Adapter. Это нормальное явление, и встречается оно достаточно часто.

Однако бывают особо тяжелые случаи, когда система не может определить драйвер самостоятельно. Тогда следует вручную выбрать драйвер из полученного списка. В данном случае выбрать драйвер вручную без дополнительных исследований, заключающихся либо в открывании системного блока и изучении маркировки микросхем на карте, либо в более внимательном изучении сайта производителя, было бы непросто, хотя в таких случаях может помочь обычный перебор драйверов. Так можно делать, когда драйверов немного.

Ну вот и все. Устройство установлено в системе, и в последнем появившемся окошке сообщается, что Мастер завершил установку программ для нашей карточки. Осталось лишь нажать кнопку **Готово** в этом окне и посмотреть еще раз на **Диспетчер устройств** (рис. 7.18).

Окно диспетчера устройств выглядит преображенным: в разделе неизвестных устройств стало меньше одним вопросительным знаком, а в разделе сетевых плат добавилась наша VIA VT6105 Rhine III Fast Ethernet Adapter.

Правда, то, что плата установлена, еще не гарантирует того, что она работоспособна. Но если процесс установки проходил достаточно глад-

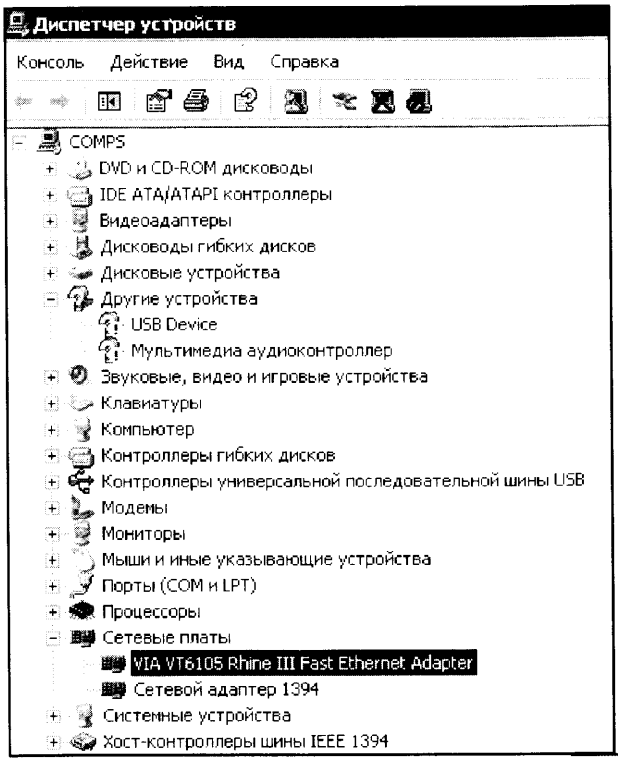


Рис. 7.18. Анализ окна диспетчера устройств после установки сетевой карты

ко, компьютер не перезагружался самопроизвольно и не было большого количества сообщений об ошибках, то с высокой долей уверенности можно говорить о том, что устройство установлено верно.

Приведенная выше методика ручной установки драйверов сетевой карты универсальна. С ее помощью вы можете установить практически любое устройство, подобрать драйверы и привести свой компьютер в работоспособное состояние.

Но установка драйверов на этом не закончилась. На все том же рис. 7.18 остались еще вопросы. Нас особенно интересует тот вопросительный знак, который называется USB Device. Этот девайс — не что иное, как беспроводной адаптер, подключенный к ПК посредством USB. Теперь мы установим и его.

7.4. АВТОМАТИЧЕСКАЯ УСТАНОВКА ДРАЙВЕРОВ WI-FI АДАПТЕРА

Выше мы прошли длинный путь ручной установки драйверов. Но есть и другой способ их инсталляции.

Часть устройств комплектуется программами для автоматической установки их драйверов на компьютер. В нашем случае таким устройством стал адаптер беспроводной сети ASUS WL-161. Этот адаптер по-

ставлялся в аккуратной, размером с компакт-диск и толщиной около сантиметра коробочке, которая содержала сам адаптер, USB-удлинитель и диск с драйверами. Не мудрствуя лукаво, вставляем диск в привод — срабатывает автозагрузка (рис. 7.19) и запускается стартовая программа инсталляции ПО.

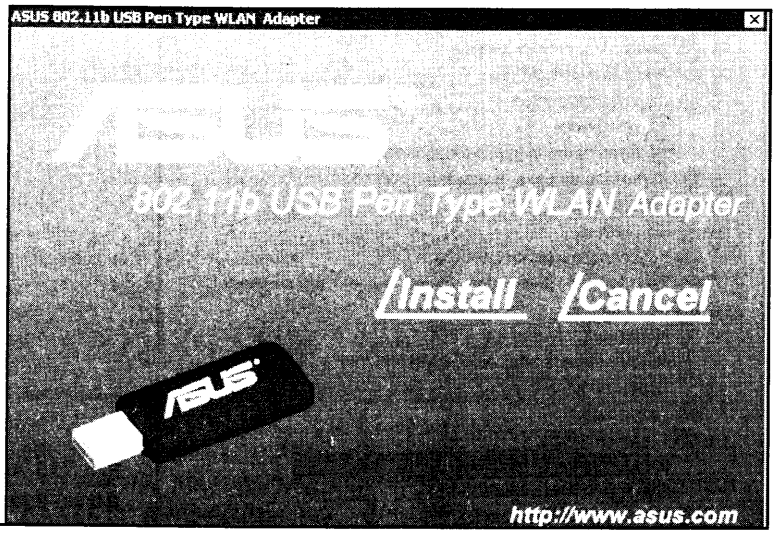


Рис. 7.19. Начало установки Wi-Fi адаптера

Меню стартового окошка установки драйверов на беспроводной адаптер предельно лаконично: здесь **Install** — начать инсталляцию — **Cancel** — отменить. Нажимаем **Install** и попадаем в следующее окно

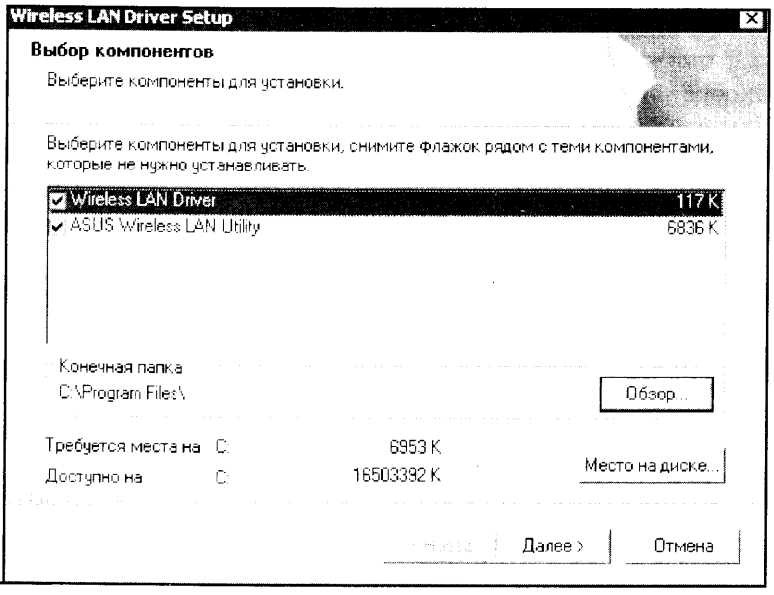


Рис. 7.20. Установка драйверов беспроводного адаптера

установщика, где нужно всего лишь нажать на кнопку **Далее**. А вот дальше появляется окошко (рис. 7.20), которое требует некоторых размышлений.

Программа просит нас определиться с тем, какие компоненты фирменного ПО мы хотим устанавливать. Wireless LAN Driver — это обязательный компонент нашей установки, без него адаптер просто не сможет работать, а вот ASUS Wireless LAN Utility — это уже дело добровольное (особенно в Windows XP).

Такое утилиты служат, как правило, либо для упрощения процесса конфигурирования устройства, либо для хранения различных профилей для разных беспроводных сетей, либо для чего-то подобного. Можно обойтись и без этих утилит, ограничившись стандартными средствами Windows, но зачем от них отказываться? К тому же для жесткого диска современного компьютера дополнительные 6 мегабайт, что требуются для установки этих утилит, погоды не сделают. А раз так — ставим все галочки (вернее, оставляем их по умолчанию) и нажимаем кнопку **Далее**. Вот, собственно говоря, и вся установка беспроводного адаптера — и спасибо ASUS за качественный софт.

Чтобы убедиться в том, что адаптер установлен и правильно распознан системой, идем снова в уже известный вам диспетчер устройств (рис. 7.21) и изучаем его раздел, посвященный сетевым адаптерам.

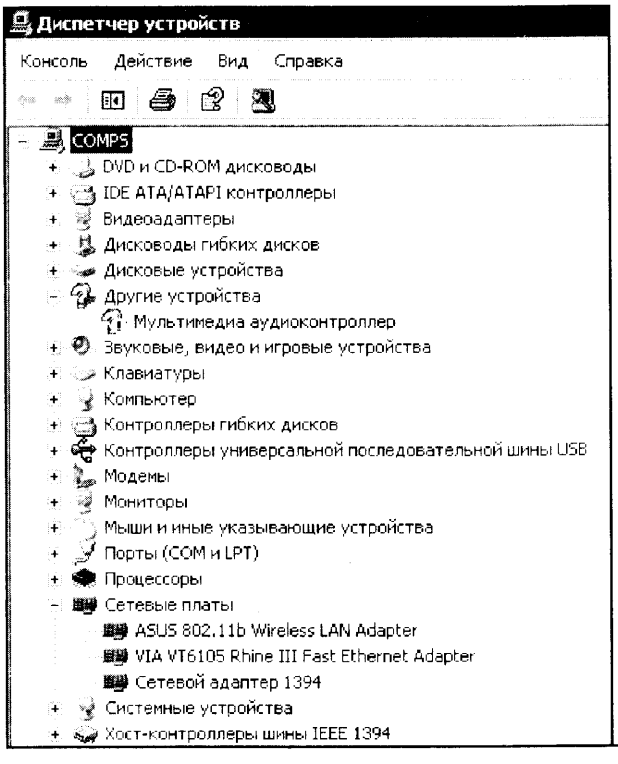


Рис. 7.21. Анализ конфигурации в диспетчере устройств

В этом разделе обнаруживаются уже целых три карты. Среди них — искомый Wi-Fi адаптер. Не открывая пока свойств этого адаптера, переходим к модемным вопросам.

Как и в случае с установкой сетевой карты, установка Wi-Fi адаптера прошла гладко, поэтому с большой долей уверенности можно говорить о том, что все будет работать правильно.

7.5. УСТАНОВКА МОДЕМА, ПРОВЕРКА ОБОРУДОВАНИЯ

Выше мы инсталлировали сетевые карты, а сейчас займемся модемом. В общем случае модем может быть установлен либо вручную — так, как мы поступили с PCI-картой, либо при помощи автоматической установки с использованием CD производителя или программы, загруженной с его сайта.

В нашем случае система самостоятельно определила модем. Он отображается в окне диспетчера устройств (рис. 7.22) без каких бы то ни было предупредительных значков.

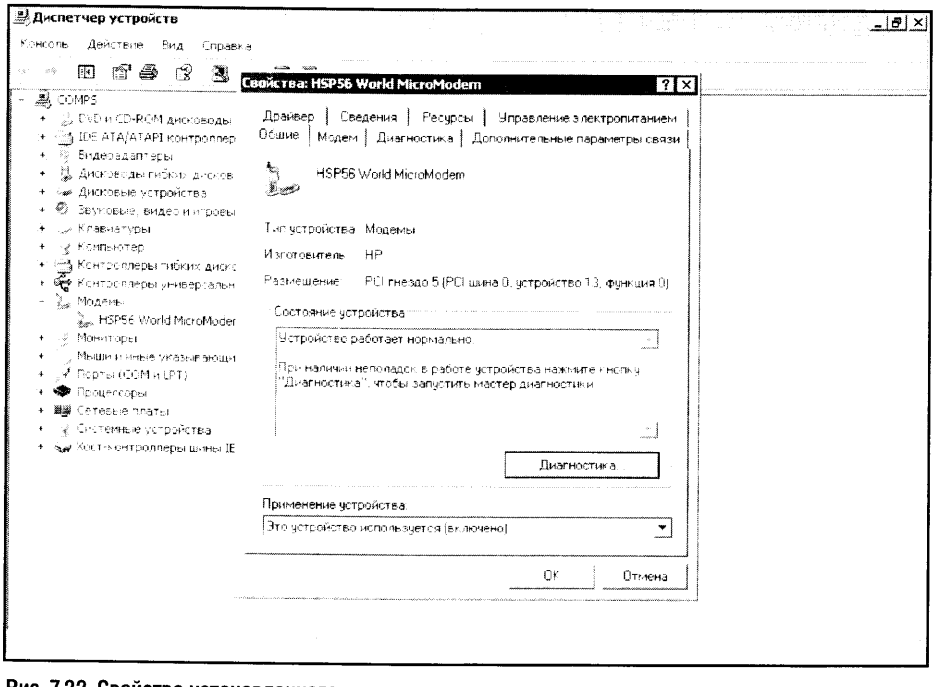


Рис. 7.22. Свойства установленного модема

Но иногда модемы определяются системой неправильно. Устройство вроде бы установлено, а если попытаться протестировать его, окажется, что он не отзывается на системные команды.

Для проверки модема существует специальное средство, доступное на вкладке **Диагностика** окна свойств модема.

Не обращайте внимания на кнопку **Диагностика** вкладки **Общие** этого окна. Эта кнопка вызывает, безусловно, полезную процедуру, где система, задавая вам вопросы о неполадках, пытается дать советы по их устранению. Однако в нашем случае модем только что установлен, неполадок пока нет, но мы хотим убедиться, что драйверы модема установлены верно и система может с ним общаться.

Опасения по поводу модема возникли у меня не случайно. Модем называется Zyxel Omni 56K PCI, а здесь написано, что это модем HSP56 World Micro Modem. Я ничего не имею против этого Micro Modem'a, но, чтобы удостовериться, что система не ошиблась, нужно его протестировать.

Посмотрите на рис. 7.23. Здесь изображена вкладка **Диагностика** окна свойств модема.

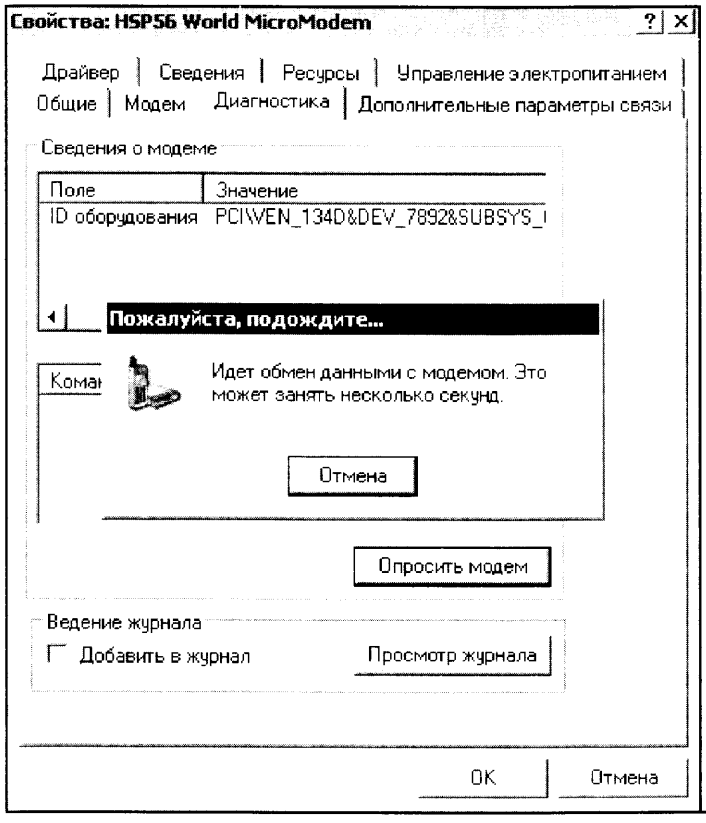


Рис. 7.23. Опрос состояния модема

Чтобы начать опрос, надо, переключившись на вкладку **Диагностика**, нажать там кнопку **Опросить модем**. Обратите внимание на то, что здесь видно небольшое окошко с заголовком **Пожалуйста, подождите...** Это окно говорит о том, что в идет опрос модема. Если опрос окажется успешным — тогда вы увидите примерно следующее (рис. 7.24).

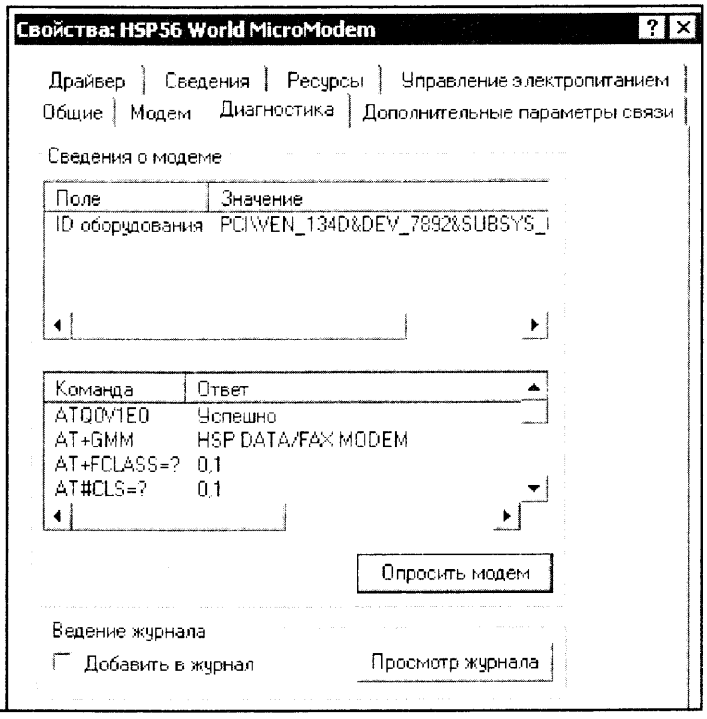


Рис. 7.24. Успешный опрос модема

Обратите внимание на то, что в ранее пустой нижней части рамки **Сведения о модеме** появились какие-то строчки. Это так называемые AT-команды, которые посылал модему компьютер, и ответы модема. Если ответы есть — это стопроцентная гарантия того, что модем установлен и настроен правильно и все будет работать.

А вот проверка других устройств — сетевой карты и беспроводного адаптера — заключается, во-первых, в осмотре внешнего вида их значков в диспетчере задач. Если никаких восклицательных знаков здесь нет, значит, все в порядке. Во-вторых, можно открыть их свойства и посмотреть на то, что сообщает система. Например, вот свойства беспроводного адаптера (рис. 7.25).

Как видите, все нормально. Но окончательный вывод о том, что все действительно хорошо, можно делать только тогда, когда заработают беспроводная локальная сеть, проводная сеть и подключение к Интернету.

Вы заметили, сколько разных вкладок в окнах свойств сетевых устройств и модема? Они скрывают массу параметров. Некоторые из них мы обсудим немного позже, а пока остановимся на вопросах установки принтеров.

Зачем нам принтер? Очень просто: принтер часто выступает в качестве разделяемого ресурса локальной сети. Поэтому мы рассмотрим его установку, а в одной из следующих глав сделаем общим для всей сети.

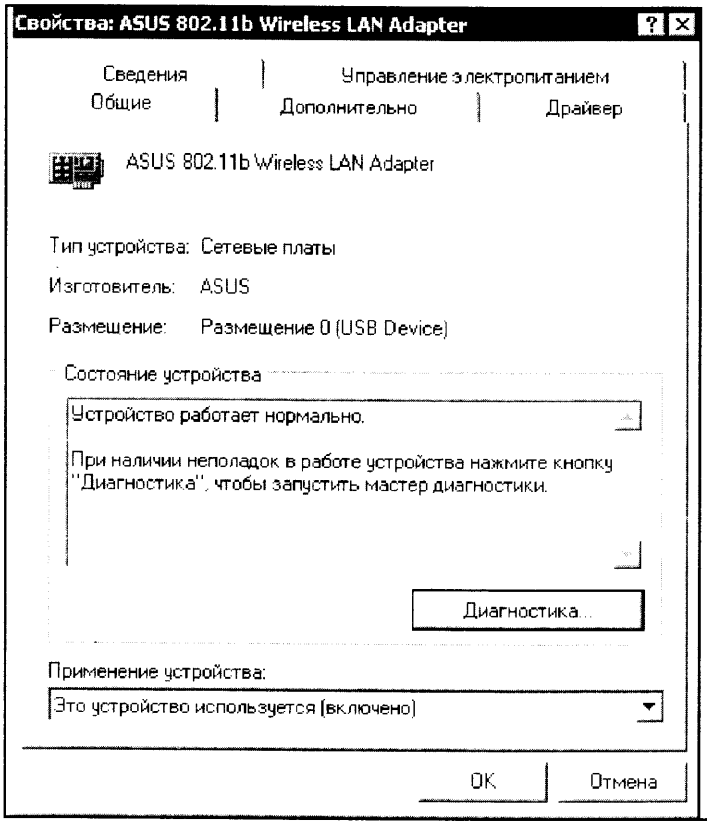


Рис. 7.25. Окно свойств беспроводного адаптера

7.6. УСТАНАВЛИВАЕМ ПРИНТЕР

Установка принтера может вестись различными способами. Современные принтеры подключаются к компьютеру с помощью интерфейса USB. К принтерам обязательно прикладываются диск с программным обеспечением и подробная инструкция по установке.

Я не буду приводить выдержки из этих инструкций, все они немного разные. Если вы будете устанавливать принтер, внимательно читайте их и строго выполняйте последовательность действий, которую предлагают производители.

Однажды мне пришлось быть свидетелем невозможности установки принтера — это был недорогой, но весьма пригодный для домашних пользователей принтер Canon Pixma IP1000. Как я ни вчитывался в инструкцию, чего только ни делал, компьютер его не видел. Вернее, не видел не полностью и вел себя при этом чрезвычайно странно. Позже оказалось, что все дело в дешевом кабеле, который дали в магазине в придачу к принтеру, и на нормальном кабеле все заработало отлично.

Итак, первый способ установки принтера, особенно USB-принтера, — фирменный компакт-диск и строгое следование инструкциям производителя. Иногда, особенно в случае LPT-принтеров, система находит их, но установить самостоятельно не может. Тогда в окне диспетчера устройств в разделе принтера можно наблюдать желтые вопросики и восклицательные знаки. В этом случае установка принтера практически ничем не отличается от установки сетевого адаптера, которую мы выполняли выше. Очень возможно, что принтер будет автоматически опознан системой и установлен без вашего вмешательства.

Бывает, что принтер подключен к компьютеру, но диспетчер устройств его не видит, а диска с программным обеспечением просто нет. Так получается, если нужно установить очень старый принтер. Но и в этом случае принтер можно установить с помощью третьего способа установки драйверов для новых устройств, то есть с помощью средств панели управления.

Посмотрите на рис. 7.26.

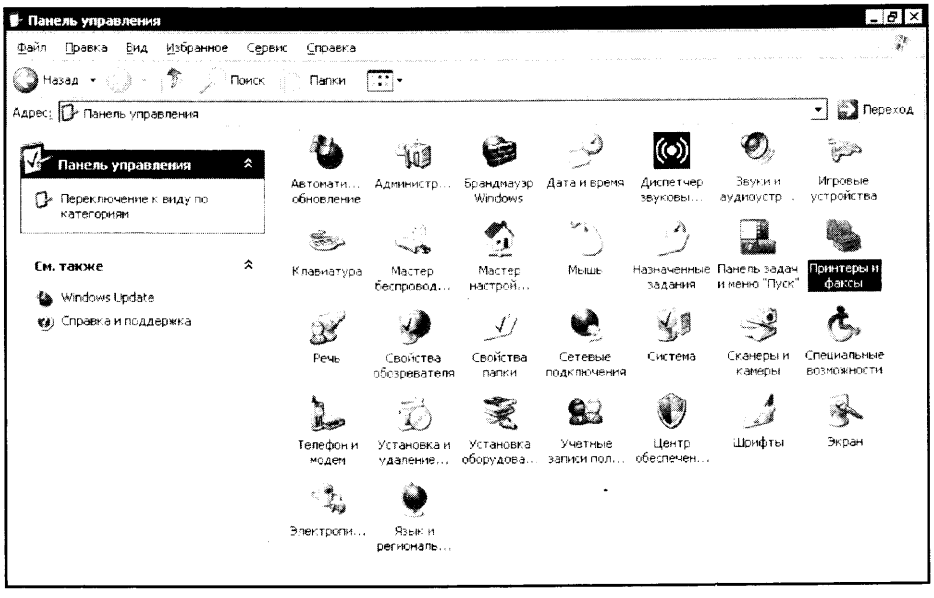


Рис. 7.26. Панель управления

Здесь изображена панель управления в классическом виде. Значок **Принтеры и факсы**, который нас сейчас интересует, выделен. Нажимаем его и попадаем на страницу управления принтерами (рис. 7.27).

Здесь, как видите, принтеров не обнаружено. Но в левой части окна **Принтеры и факсы** есть ссылка, запускающая **Мастер установки принтера**. Нажимаем ее и начинаем установку.

Обратите внимание на первое окно этого Мастера (рис. 7.28).

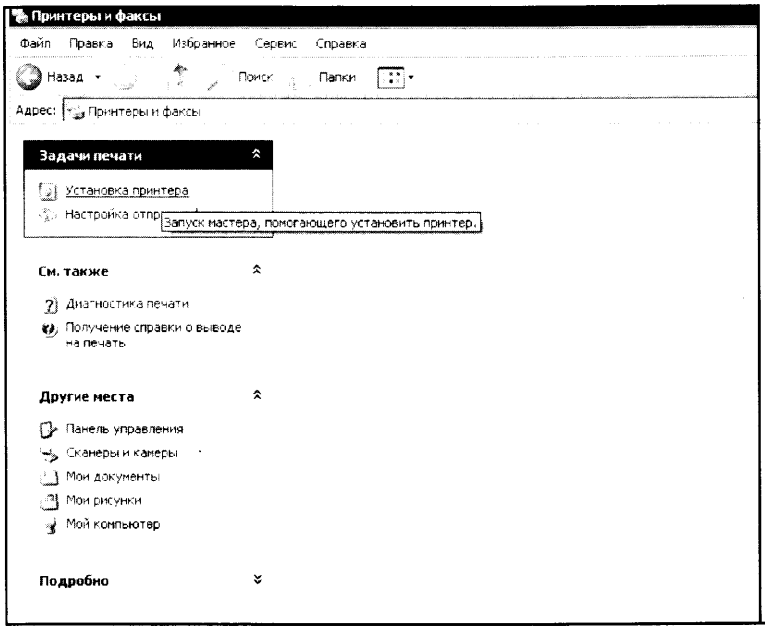


Рис. 7.27. Окно управления принтерами

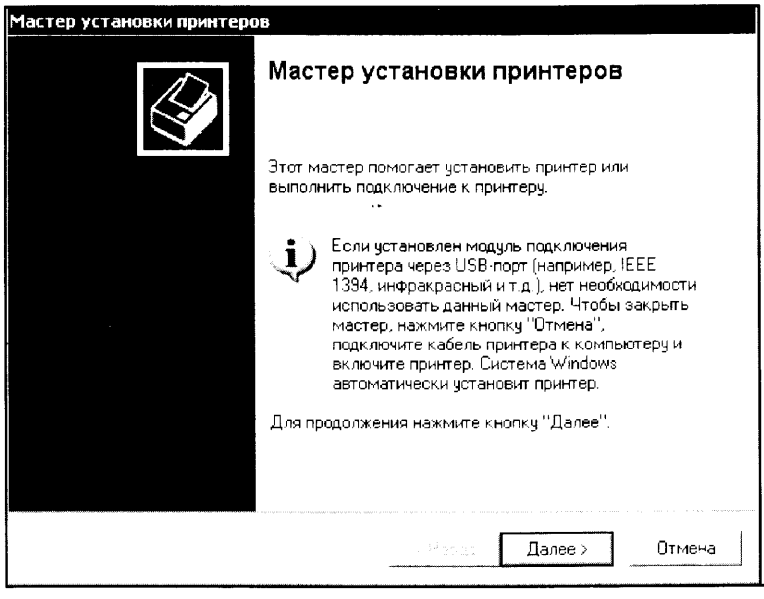


Рис. 7.28. Первое окно Мастера установки принтера

Здесь Мастер предупреждает пользователя о том, что если принтер подключается по USB, Fire-Wire или инфракрасному порту, то система справится с ним сама и в использовании Мастера нет нужды. Как правило, установка таких принтеров проводится средствами фирменных программ производителя. Но в нашем случае не остается ничего, кроме кнопки **Далее**, и мы попадаем в следующее окно Мастера (рис. 7.29).

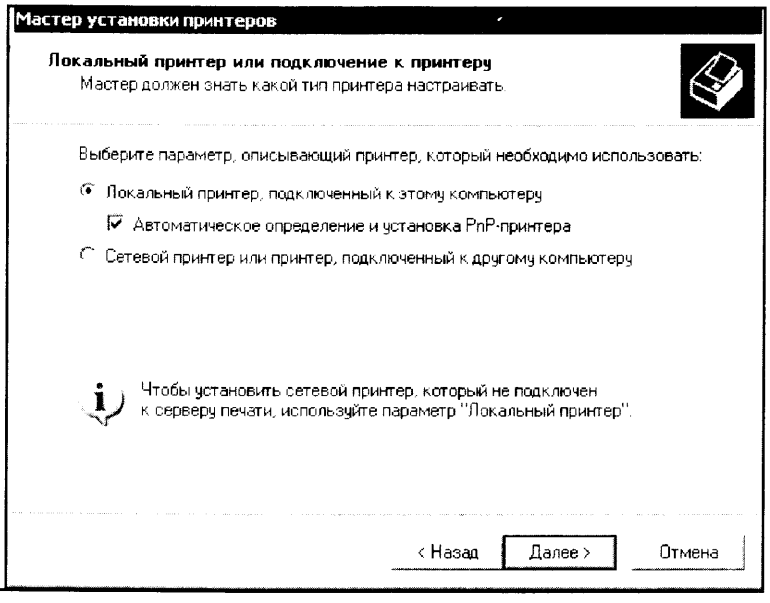


Рис. 7.29. Выбор параметров установки принтера

В нашем случае это локальный принтер. В надежде, что система все-таки найдет его драйвер сама, ставим галочку **Автоматическое определение и установка PnP принтера**. Технология PlugAndPlay (PnP, нечто вроде «Включай и играй») позволяет системе опознавать PnP устройства и автоматически устанавливать драйверы для них.

В этом окошке есть еще один параметр, к которому мы еще вернемся, когда будем устанавливать принтер на других компьютерах нашей сети.

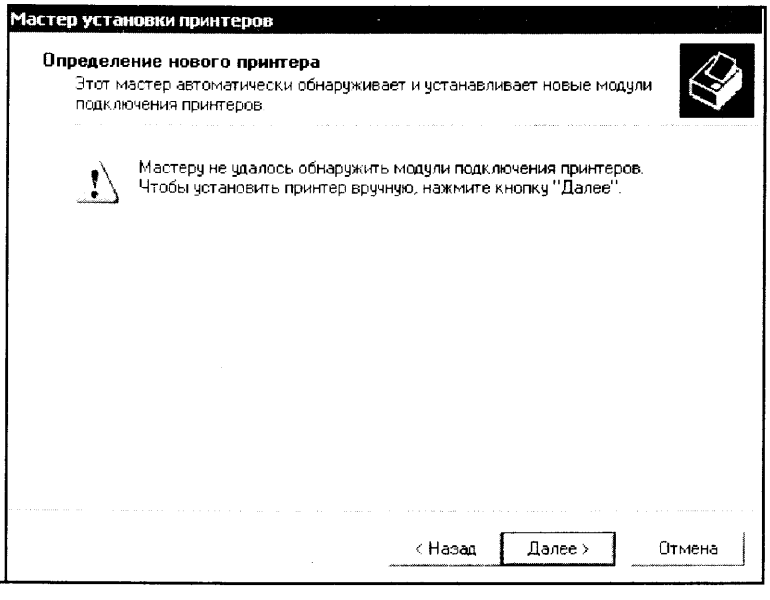


Рис. 7.30. Сообщение об ошибке

Следующий этап установки был ознаменован сообщением об ошибке (рис. 7.30).

Ну не хочет он опознаваться системой, и все тут. А раз так — нажимаем **Далее** и начинаем ручной выбор установок принтера (рис. 7.31).

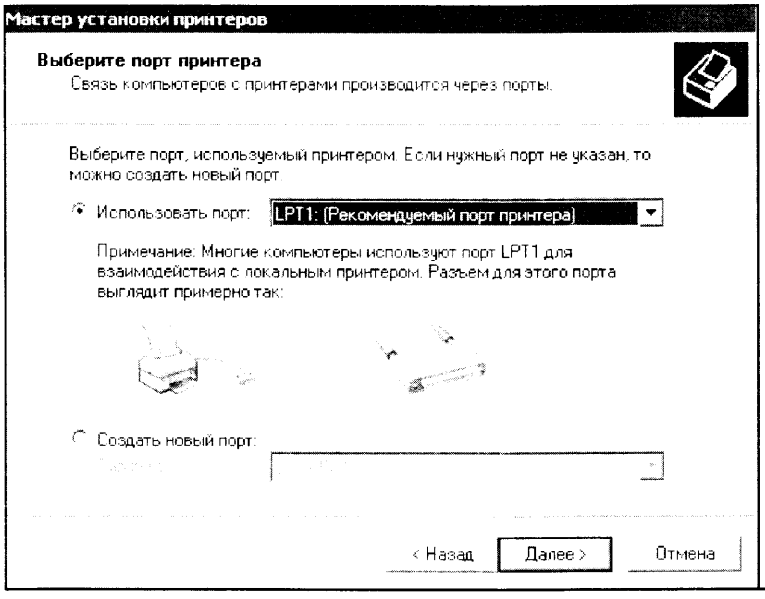


Рис. 7.31. Выбор порта принтера

После того как порт выбран, наступает этап, который уже знаком вам по предыдущему примеру инсталляции. На рис. 7.32 изображено окно

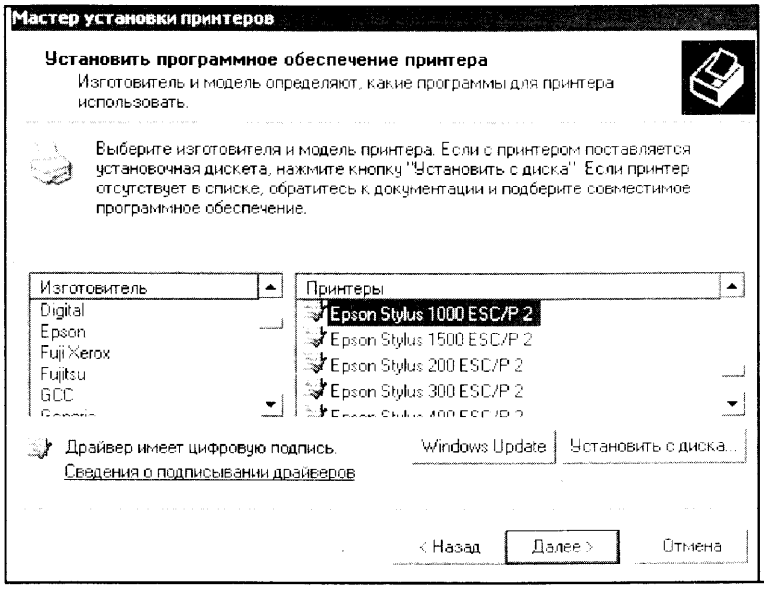


Рис. 7.32. Поиск драйвера принтера

выбора драйвера принтера. В этот раз драйвер удалось найти среди стандартных драйверов, входящих в комплект Windows XP.

Установка подходит к финалу. Выбрав драйвер принтера, остается только нажать на кнопку **Далее**, в следующем окне программы задать имя принтера и, несколько раз ответив **Далее**, получить на выходе сообщение об успешном завершении работы. Посмотрите на рис. 7.33. Здесь изображено окно, предшествующее окончательной установке драйверов.

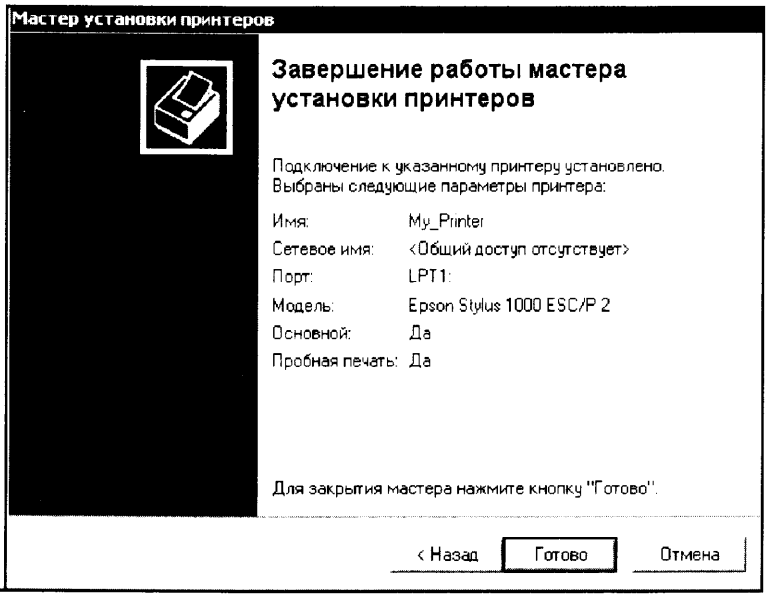


Рис. 7.33. Завершение установки принтера

Обратите внимание на то, что в параметрах принтера включена установка, запускающая печать пробной страницы. Ее можно и не включать, но лучше удостовериться, что все работает так, как надо, иначе потом, если окажется, что принтер не работает, почти весь ваш труд будет потрачен впустую. Лучше сразу, по горячим следам, установить принтер и заставить его работать правильно.

7.7. ВЫВОДЫ

Оборудование мы установили, инсталлировали драйверы, а теперь время настраивать локальную сеть. В следующих главах мы установим и настроим Ethernet-сеть, Wi-Fi сеть, подключим компьютер к Интернету с помощью модема и займемся общими ресурсами сети.

ЧАСТЬ 3

НАСТРОЙКА СЕТЕЙ

ГЛАВА 8
ПОДКЛЮЧЕНИЕ К ИНТЕРНЕТУ, НАСТРОЙКА INTERNET EXPLORER И OUTLOOK EXPRESS

В этой части мы займемся настройкой локальной сети в Windows XP и Windows 98, коснемся вопросов сетевой безопасности и рассмотрим сетевое программное обеспечение. Немало внимания мы уделим современным мобильным технологиям для работы с локальными и глобальными сетями.

Здесь мы постараемся рассмотреть самые разные аспекты работы с локальными сетями. А так как локальные и глобальные сети существуют в тесной взаимосвязи, мы коснемся и вопросов работы в сети Интернет.

Одна из главных задач этой книги, да и любой книги, посвященной компьютерам, создать у читателя целостную картину того или иного направления компьютерной науки. Такая картина компьютерного мира (или его части, сетей например), позволит вам по-новому взглянуть на различные явления, с которыми вам предстоит иметь дело, общаясь с этими умными устройствами.

Чтобы сделать приведенные ниже сведения пригодными для любых ситуаций, мы разберем различные способы осуществления одних и тех же действий: процессы ручной и автоматической настройки проводной и беспроводной сети и вопросы подключения компьютера к Интернету. С Интернета мы и начнем, разобрав работу с Мастером подключения к Интернету. Это подключение понадобится нам чуть позже, когда мы займемся «выпусканием» в Сеть компьютеров нашей локалки.

Разберем стандартный способ подключения к Интернету при помощи модема и настройку некоторых популярных продуктов для работы в Сети. На этой главе, однако, разговор о подключении к Интернету закончен не будет — в одной из следующих глав будет описан алгоритм подключения ПК к Интернету с использованием сотового телефона в качестве модема.

Мы начинаем наш разговор не с локальных сетей, которым посвящена эта книга, а с подключения компьютера к глобальной сети. В этом есть глубокий смысл — часто выход в Интернет бывает первой «сетевой ласточкой», которая приходит к пользователю. К тому же локальная

сеть — это хорошо, но без Интернета современному пользователю не прожить и дня.

Несмотря на тривиальность процедуры, подключение к Сети способно вызвать некоторые сложности у неподготовленных пользователей. Пока у вас не будет хотя бы начального опыта в этой области, все будет казаться вам слишком сложным. Но только очень вас прошу: не пытайтесь заучивать что-нибудь наизусть или пытаться находить все ответы на ваши вопросы в книгах — гораздо важнее развитие ваших компьютерных знаний и компьютерной интуиции. И помните: знаний никогда не бывает много, а интуиция, не подкрепленная теорией, напоминает игру в русскую рулетку.

Поэтому не будем играть в опасные игры и начнем с подключения к Интернету.

8.1. ПОДКЛЮЧЕНИЕ К ИНТЕРНЕТУ

Залог успешного подключения к Интернету — правильно установленный модем. Как установить его, вы узнали из прошлой главы. А вот о том, что с ним делать дальше, читайте дальше.

Windows имеет одно замечательное средство, автоматизирующее процесс подключения к Интернету. Когда вы впервые щелкаете по значку Internet Explorer в свежеустановленной Windows XP, она запускает Мастер подключения к Интернету, который спрашивает вас о том, что вы хотите делать дальше (рис. 8.1).

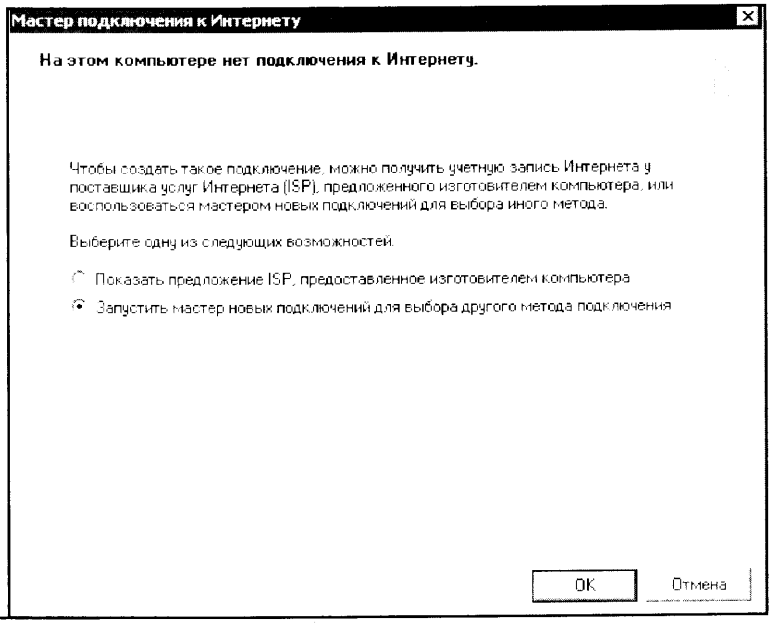


Рис. 8.1. Создание подключения на новом компьютере

В этом окне вам достаточно выбрать пункт **Запустить мастер новых подключений** для выбора другого метода подключения. Следующим шагом установки будет первое окно Мастера новых соединений. Из элементов, которые требуют внимания пользователя, это окно содержит лишь кнопку **Далее**, поэтому мы сразу переходим к следующему окну (рис. 8.2).

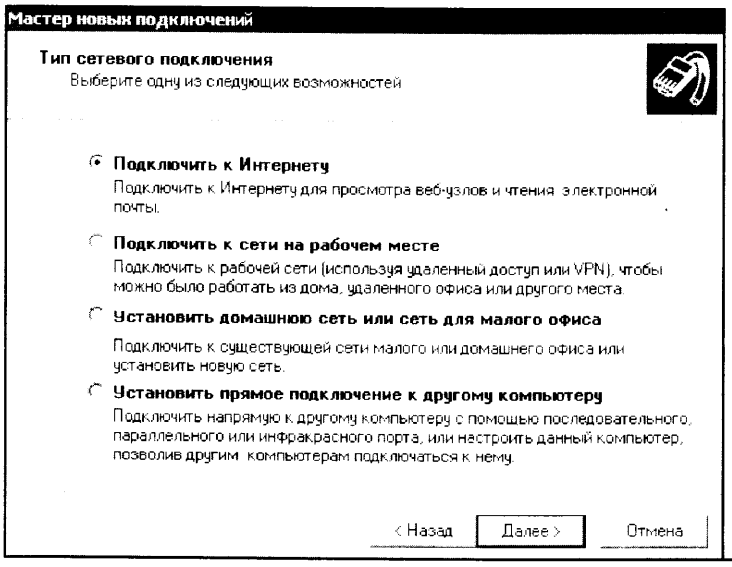


Рис. 8.2. Выбор типа устанавливаемого подключения

Здесь следует выбрать первый пункт — **Подключить к Интернету**. Кстати, как вы можете видеть, это окно позволяет устанавливать и другие подключения, но, забегая вперед, скажу, что установка локальной сети может осуществляться не только с помощью этого Мастера.

Следующий шаг установки подключения к Интернету заключается в выборе способа подключения и получения регистрационных данных. Так, здесь (рис. 8.3) вы можете либо выбрать поставщика услуг Интернета из списка — лучше не выбирать этот пункт, так как здесь вы не найдете местного интернет-провайдера. Пункт **Использовать компакт-диск поставщика услуг Интернета** тоже выбирается довольно редко — по крайней мере, мне неизвестны провайдеры, которые выполняют подключение клиентов таким образом.

Самым важным для нас с вами является пункт **Установить подключение вручную**, так как мы рассматриваем наиболее распространенное сегодня dial-up-подключение.

Подключения такого рода чаще всего устанавливаются пользователями самостоятельно, без помощи обслуживающего персонала провайдера. Дело в том, что если вы будете устанавливать, скажем, ISDN-соединение, модернизируя свою телефонную сеть, с настройками вам помогут люди из сервисной службы провайдера. А вот к модемам все так привыкли, что не считают нужным заботиться о них.

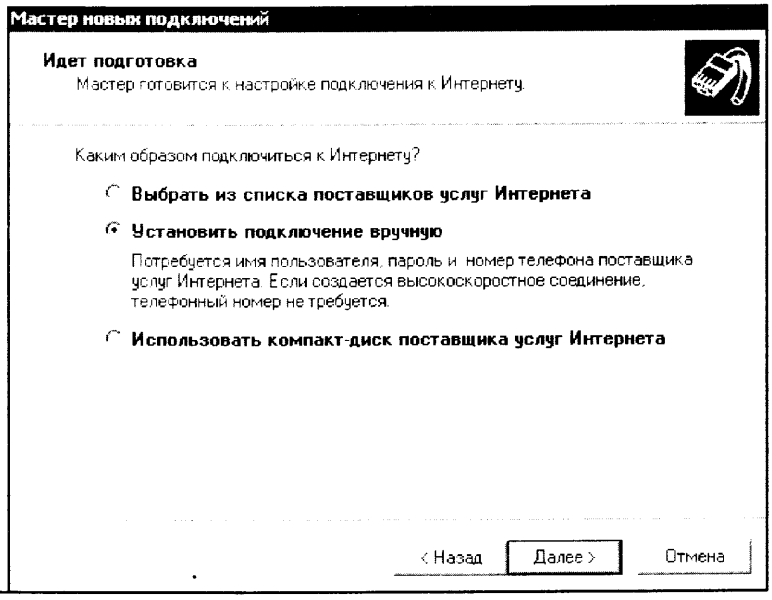


Рис. 8.3. Выбор способа подключения

В подсказке около пункта **Установить подключение вручную** говорится, что для подключения вам понадобятся имя (логин) и пароль, выдаваемые вашим провайдером. Значит, самое время посмотреть на свежекупленную интернет-карточку, на которых провайдеры пишут имена и пароли.

Ну а если вы подключаетесь к провайдеру, который пока не выпустил собственных пластиковых интернет-карт, то вам, скорее всего, логин

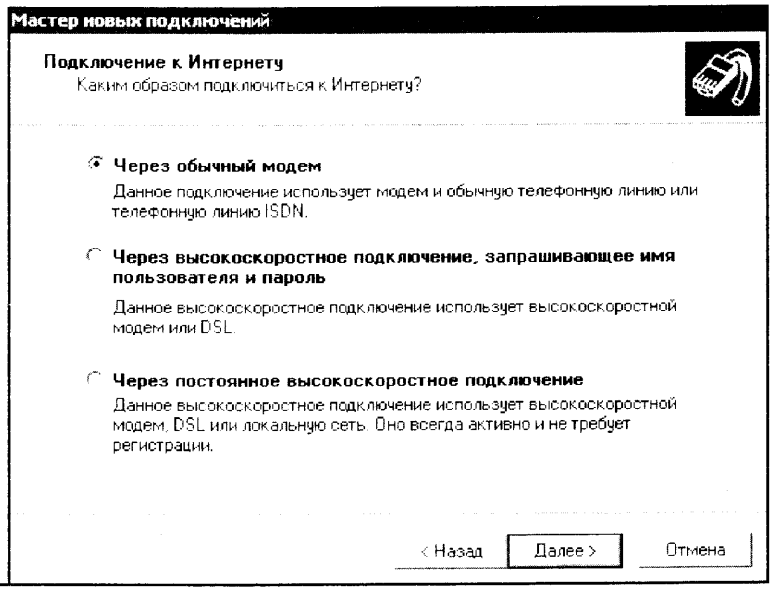


Рис. 8.4. Выбор способа подключения к Интернету

и пароль выдали в офисе провайдера. Вероятно, они напечатаны в договоре об обслуживании.

Следующий этап подключения — выбор типа подключения (рис. 8.4).

В данном случае выбрано подключение через обычный модем. Если вы подключаетесь через иное устройство, выбирайте другой тип подключения и следуйте инструкциям Мастера.

С этого момента Мастер начинает задавать вам различные вопросы. Он попросит ввести имя подключения — это имя может быть любой угодной вам комбинацией цифр или букв, латиницей или кириллицей. А вот следующее окно, куда нужно ввести номер модемного пула провайдера, требует некоторого внимания. Посмотрите на рис. 8.5. Здесь изображен процесс ввода номера провайдера.

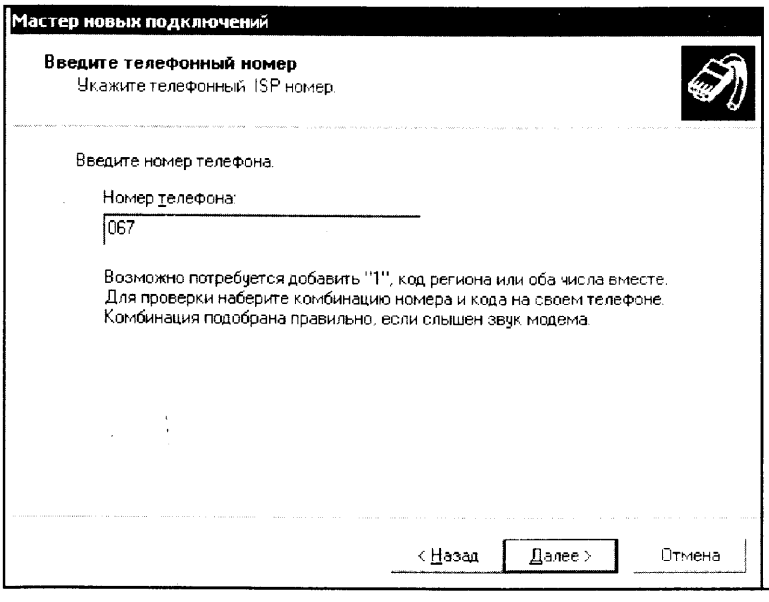


Рис. 8.5. Ввод номера для дозвона к провайдеру

Обратите внимание, что телефонный номер вводится без всяких посторонних значков или черточек. Если номер местный, его вводят без кода города и кода страны.

Иногда невозможность установить соединение с Интернетом заключается именно в неправильном вводе номера — вы ввели его с вышеупомянутыми черточками в качестве разделителей цифр или с ненужным кодом страны или города и так далее.

Бывают случаи, когда в тоновом режиме набора номера модем соединяется с модемом провайдера, а в импульсном — наоборот. Это надо учитывать, если вдруг с подключением к Интернету возникают какие-то проблемы.

В написании номера можно использовать латинские буквы **p** для задания импульсного способа набора номера и **t** — для задания тонового набора.

Следующий этап установки заключается во вводе имени и пароля пользователя. Здесь будьте внимательны, особенно при вводе пароля. Дело в том, что в целях секретности символы пароля не отображаются в строке ввода: вместо символов там появляются жирные точки (рис. 8.6).

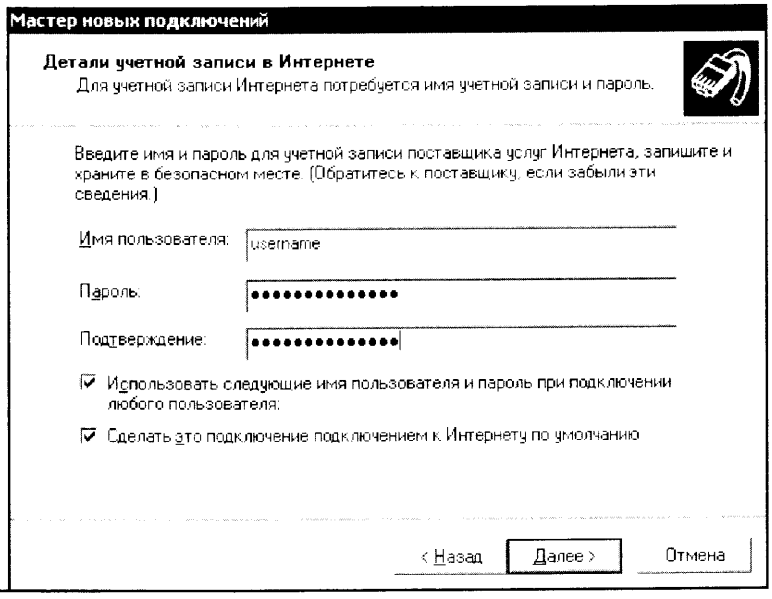


Рис. 8.6. Ввод имени пользователя и пароля

Вот и весь процесс подключения. Нажав кнопку **Далее**, вы попадете на финальную страницу Мастера, где останется нажать на кнопку **Готово** и попытаться подключиться к Интернету. Как правило, сразу это не получается: Internet Explorer не хочет загружать устанавливаемую по умолчанию интернет-страничку. Это значит, что от настройки подключения к Интернету мы плавно переходим к настройке IE для работы в Интернете. Этот браузер вместе с почтовой программой Outlook Express является для многих основным интернет-инструментом, возможностей которого хватает для комфортной работы. Только эти инструменты надо правильно настроить.

Windows XP, как и другие версии Windows, имеет встроенный веб-браузер — Internet Explorer. Браузер IE является одним из наиболее распространенных в мире. Это мощный обозреватель интернет-ресурсов, для работы с которым нужны определенные навыки. До недавнего времени, а именно — до выхода SP2, он требовал довольно сильной «доработки» путем установки ПО сторонних производителей. К примеру, IE не умел блокировать всплывающие окна и другой мусор, который в изобилии встречается на веб-страницах.

Правда, IE и сегодня не идеален, но достаточно сказать, что большинство создателей сайтов ориентируются при создании своих сайтов именно на этот браузер. Хороший стиль программирования при построении сайта включает его адаптацию и к Internet Explorer, и к Mozilla Firefox — второму по популярности браузеру, но мне встречались странички, которые прекрасно себя чувствовали в IE, но отказывались работать в Mozilla и в еще одном известном браузере, довольно быстром, который называется Opera.

Понятно, что все дело в том, под какой браузер делался тот или иной сайт. Продвинутому пользователю ничего не стоит установить новый браузер и работать с ним, а новичку нужно что-нибудь попроще. Вот мы и займемся вопросами настройки Internet Explorer'а.

8.2. НАСТРОЙКА ПАРАМЕТРОВ INTERNET EXPLORER

Чтобы получить доступ к настройкам IE, достаточно запустить его и выбрать пункт меню **Сервис ▸ Свойства обозревателя**. На рис. 8.7 вы можете видеть первую вкладку свойств IE, которая называется **Общие**.

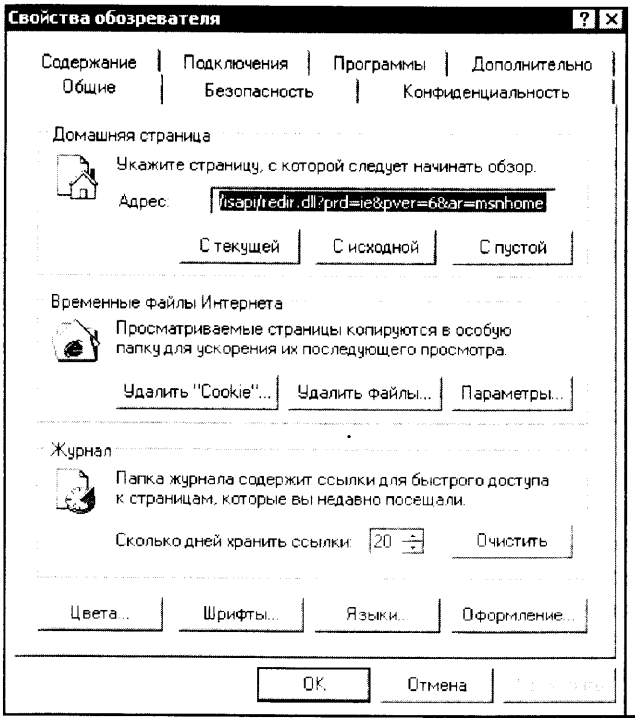


Рис. 8.7. Вкладка Общие окна свойств IE

Здесь собраны параметры, которые позволяют настроить некоторые важные свойства Internet Explorer.

Группа параметров **Домашняя страница** позволяет установить страницу, с которой начинается обзор интернет-ресурсов. Но такую страницу можно и не назначать: некоторые находят удобным входить в Интернет «с чистого листа». Для этого нужно нажать кнопку **С пустой**. Так вы, открыв IE, сможете самостоятельно ввести URL (веб-адрес) нужной вам интернет-странички. Но если вам нравится начинать день в Интернете с просмотра определенной страницы, введите в строку **Домашняя страница** веб-адрес этого сайта. Кнопка **С исходной** устанавливает в качестве стартовой страничку одного из разделов сайта Microsoft.

Параметры группы **Временные файлы Интернета** интересны тем, что порой позволяют освобождать немало места на жестком диске вашего компьютера. Если вы владелец мощного современного компьютера и вам не жаль отдать под «ненужности» несколько сотен мегабайт дискового пространства, то можете особо не обращать внимания на удаление временных файлов. А вот владельцам машин послабей, особенно тем, кто интенсивно использует Интернет, следует присмотреться к этому параметру.

Теперь о *Cookies*. Это небольшие файлы, которые содержат историю вашей работы с тем или иным веб-ресурсом. Именно благодаря этим файлам серверы «запоминают» ваш визит. Если вы хотите, чтобы ваши интернет-привычки остались для окружающих секретом, можете после каждого сеанса работы нажимать кнопку, удаляющую файлы-*cookies*. В остальных случаях это значения не имеет: можете удалять, а можете и не удалять.

Параметры, касающиеся настройки **Журнала**, позволяют задавать срок хранения ссылок на посещенные вами ресурсы. Если вы занимаетесь долгосрочным проектом, связанным с поиском информации в Сети, параметр **Сколько дней хранить ссылки** для собственного удобства можно значительно увеличить. Ну а если ссылки на посещенные вами ресурсы вам больше не нужны — нажимайте на **Очистить** и начинайте веб-серфинг с чистого листа.

Следующая вкладка окна настройки свойств IE называется **Безопасность** (рис. 8.8) Здесь можно настраивать параметры безопасности при работе в Интернете.

С настройками этого уровня, особенно теми, которые появляются после щелчка на кнопке **Другой**, следует обходиться очень аккуратно. Если вы не уверены в том, что вы все делаете правильно, лучше оставить все как есть. Правда, параметры безопасности, настраиваемые в этом окне, даже если установить все на максимально безопасную работу, все равно не отменяют необходимости пользоваться файрволлом и антивирусом.

Вкладка, посвященная конфиденциальности работы в Сети (рис. 8.9), позволяет управлять параметрами работы с *cookies*. Некоторые сайты, требующие авторизации, отказываются работать с браузером, если *cookies* в нем заблокированы. Поэтому лучше выбрать среднее значение параметра конфиденциальности.

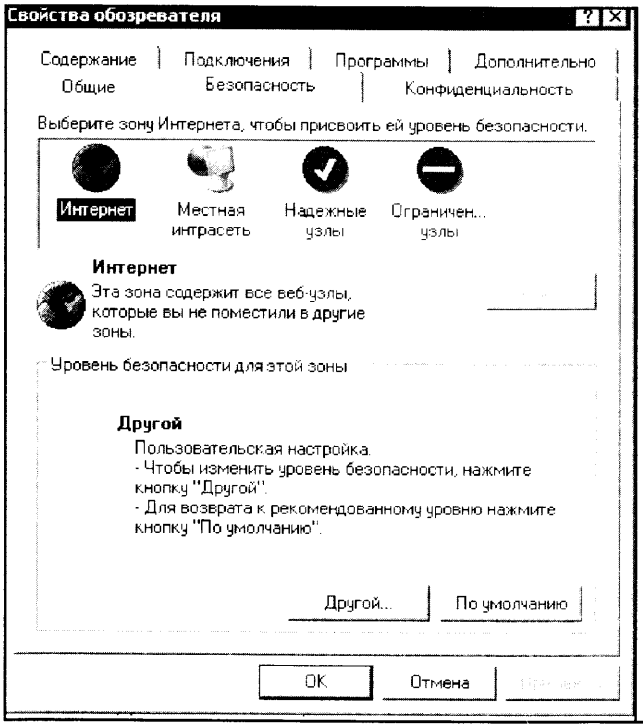


Рис. 8.8. Настройка параметров безопасности

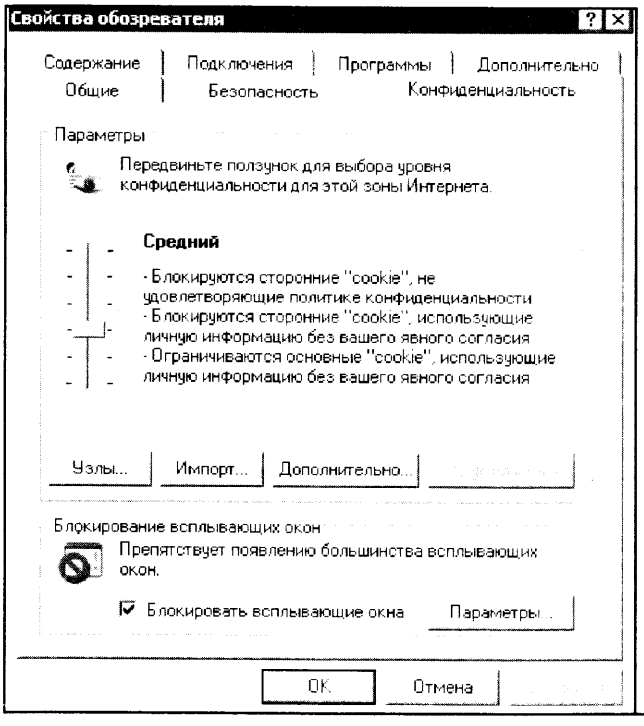


Рис. 8.9. Настройка параметров конфиденциальности

Это же окно содержит рамку **Блокирование всплывающих окон**. Блокируйте их, не задумываясь! Ничего хорошего в них нет, а время, ресурсы и трафик пользователя они пожирают с большим аппетитом. Блокировка всплывающих окон — одно из нововведений Service Pack 2. Раньше IE не умел блокировать всплывающие окна и для этого приходилось использовать программы сторонних разработчиков.

Вкладка **Дополнительно** (рис. 8.10) содержит некоторые дополнительные параметры настройки IE.

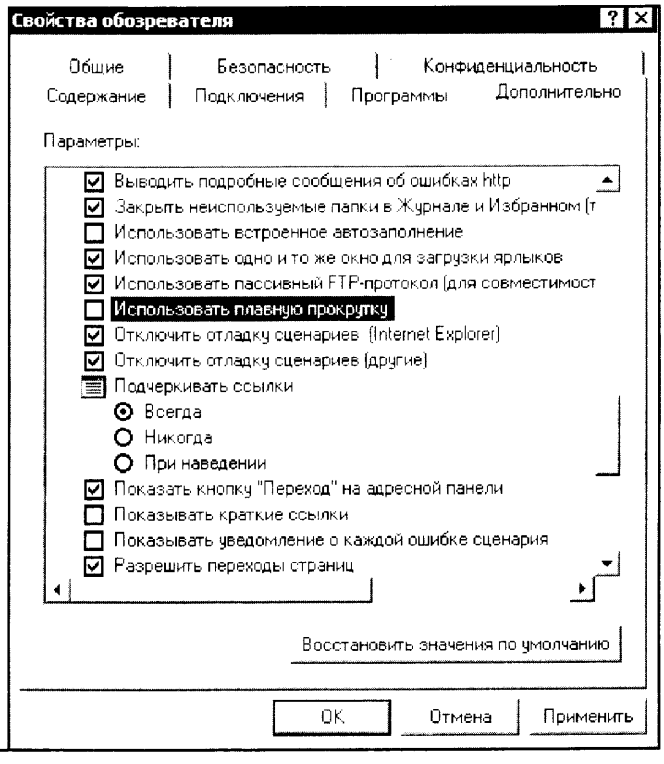


Рис. 8.10. Настройка дополнительных свойств IE

Эти параметры очевидны, поэтому, просмотрев их, вы можете настроить браузер в соответствии со своими нуждами. Правда, понять, что для вас важно, а что — нет, вы сможете лишь после того, как некоторое время поработаете в Сети.

Могу дать совет владельцам LCD-мониторов и ноутбуков. На мой взгляд, с IE комфортнее работать, если отключить параметр **Использовать плавную прокрутку**. Это особенно важно для владельцев достаточно старых LCD, так как плавная прокрутка сильно «смазывает» текст.

Теперь переходим во вкладку **Программы** (рис. 8.11).

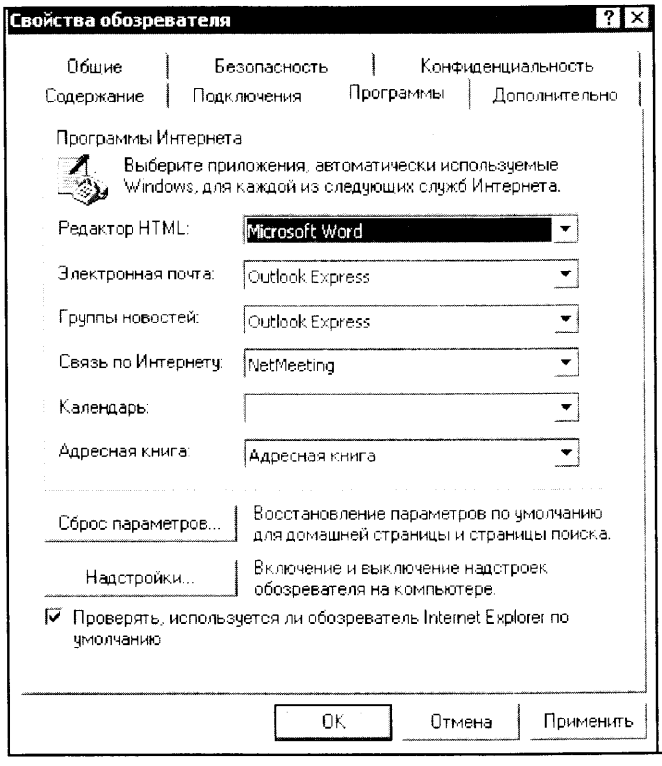


Рис. 8.11. Настройка программ, используемых совместно с IE

Если вы не пользуетесь программами сторонних производителей, параметры этой страницы можно оставить такими, какие они есть. Но при использовании какого-нибудь альтернативного браузера лучше отключить галочку **Проверять, используется ли обозреватель Internet Explorer по умолчанию**. Иначе вы станете свидетелем довольно забавной «войны браузеров»: то один, то другой из них будет пытаться стать браузером «по умолчанию», выводя соответствующие сообщения.

Теперь, «перепрыгнув» вкладку **Подключения**, к которой мы вернемся чуть позднее, рассмотрим вкладку **Содержание** (рис. 8.12).

Обратите внимание на установку **Ограничение доступа**. Если вы включите ограничение, а потом забудете пароль, то ситуация может обернуться неприятностями. (Однажды я и сам попал в такое положение: кому-то захотелось поразвлечься, закрыв доступ ко всем веб-сайтам, кроме yandex.ru.)

В группе параметров **Личные данные** самыми полезными являются параметры автозаполнения. Благодаря этой возможности IE вы можете, например, не вводить полностью имена и пароли для доступа к каким-нибудь онлайновым ресурсам. Введя начало имени пользователя на каком-нибудь сайте, вы, если все настроено по умолчанию, получите запрос от **Автозаполнения**. Вам будет предложено сохранить пароль доступа к этому ресурсу. Если за вашим компьютером работаете вы и только

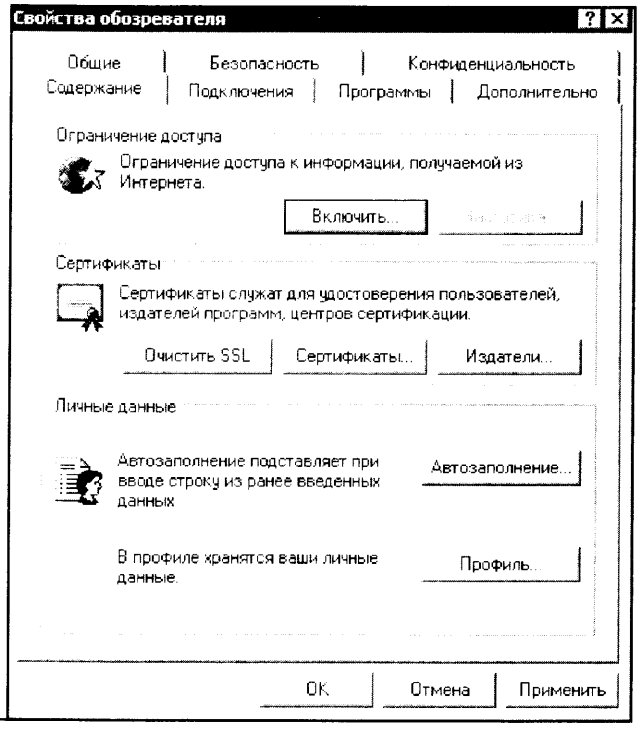


Рис. 8.12. Настройка содержания

вы и если пароль закрывает доступ к какому-нибудь не слишком важному ресурсу, то допустимо позволить сохранить этот пароль. Но если у вас есть хотя бы малейшее сомнение, пароль лучше не сохранять. Ведь любой, кто сядет за ваш компьютер, сможет получить доступ к вашим ресурсам и даже действовать от вашего имени. Ну а если вы хотите очистить сохраненные данные, нажмите на кнопку **Автозаполнение**... и в появившемся окне выполните требуемые действия по очистке данных форм и паролей.

Вот мы и подошли к той вкладке свойств Internet Explorer, из-за которой начали рассматривать все остальные. Это вкладка **Подключения** (рис. 8.13).

Обратите внимание на рамку **Настройка удаленного доступа и виртуальных частных сетей**. Здесь есть список подключений. Выше мы создали подключение к Интернету, которое называется **Мой провайдер**.

Помните, как мы, попытавшись войти в Интернет сразу после создания этого подключения, получили отказ, то есть сообщение о том, что IE не может отобразить страницу? Дело в том, что это подключение не было назначенным по умолчанию, которое следует использовать всегда.

Сразу под списком подключений есть несколько переключателей. Сразу после установки наше подключение может иметь свойство **Использовать при отсутствии подключения к сети**. Так как компьютер, на котором настраивалось подключение, имеет единственный выход

в Интернет именно через настроенное подключение, этому параметру нужно присвоить значение **Всегда использовать принятое по умолчанию подключение**. В нашем списке всего одно подключение, и оно будет отмечено как подключение по умолчанию.

Из этого же окна настройки IE можно создавать новые подключения: кнопка **Установить** запускает Мастер новых подключений, который мы рассмотрели выше. А вот управлять существующими подключениями можно при помощи кнопки **Настройка** в правой части рамки **Настройка удаленного доступа и виртуальных частных сетей**. Посмотрите на рис. 8.14. Здесь вы можете видеть окно настройки выбранного подключения.

В этом окне довольно много параметров, некоторые из них мы рассмотрим немного позже, когда будем обсуждать особенности подключения локальной сети к Интернету. Пока же сосредоточимся на свойствах конкретного подключения.

Эти свойства в окне представлены именем пользователя и паролем в рамке **Настройка удаленного доступа**. Это окно дает возможность доступа к свойствам подключения, где можно настроить массу других параметров. При нажатии кнопки **Свойства** появляется окно, позволяющее настраивать практически все доступные свойства подключения. Посмотрите на рис. 8.15. Здесь изображено окно свойств конкретного подключения, в нашем случае это подключение с именем **Мой провайдер**.

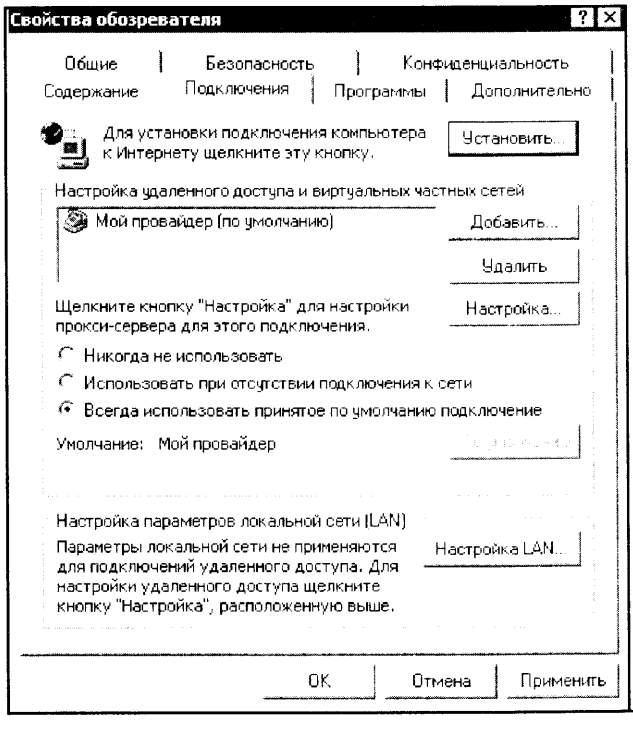


Рис. 8.13. Настройка свойств подключения к Интернету

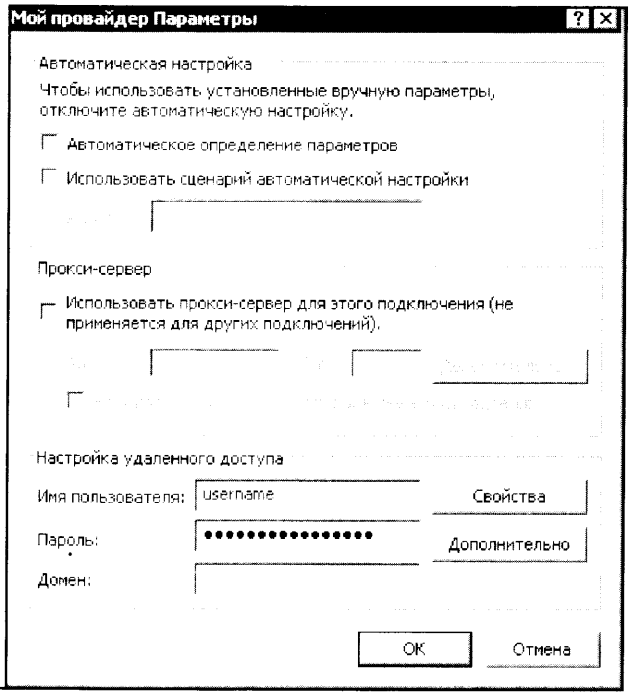


Рис. 8.14. Настройка параметров подключения

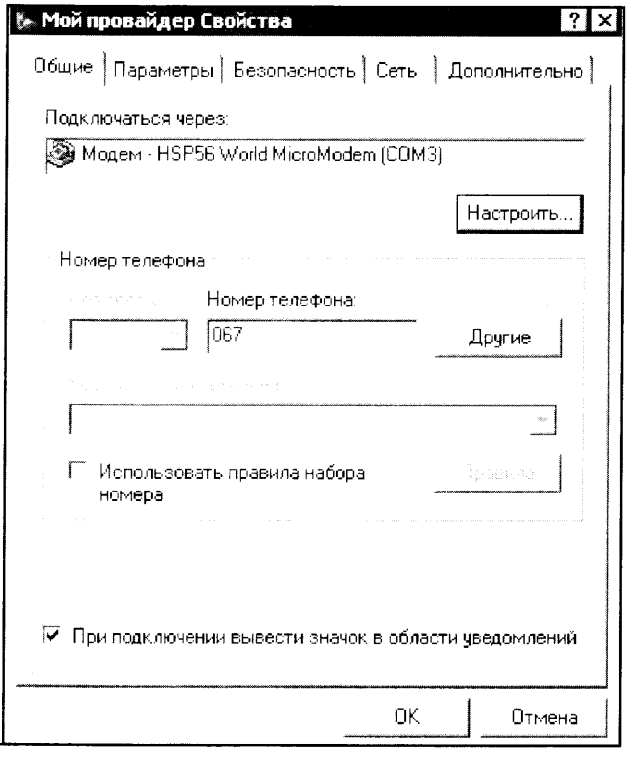


Рис. 8.15. Настройка свойств подключений

Так, на вкладке **Общие** можно поменять телефонный номер провайдера.

Кстати, иногда решить проблему невозможности подключения помогает выключение галочки Использовать правила набора номера. Если ее не снять, то номер вашего провайдера будет набираться с использованием правил набора номера, часто с ненужным для локальных звонков кодом города.

Полезен включенный по умолчанию параметр **При подключении вывести значок в области уведомлений**. Так вы точно будете знать, что в данный момент подключены к Интернету.

Теперь посмотрите на рис. 8.16. Здесь вы можете видеть вкладку **Параметры настройки свойств подключения**.

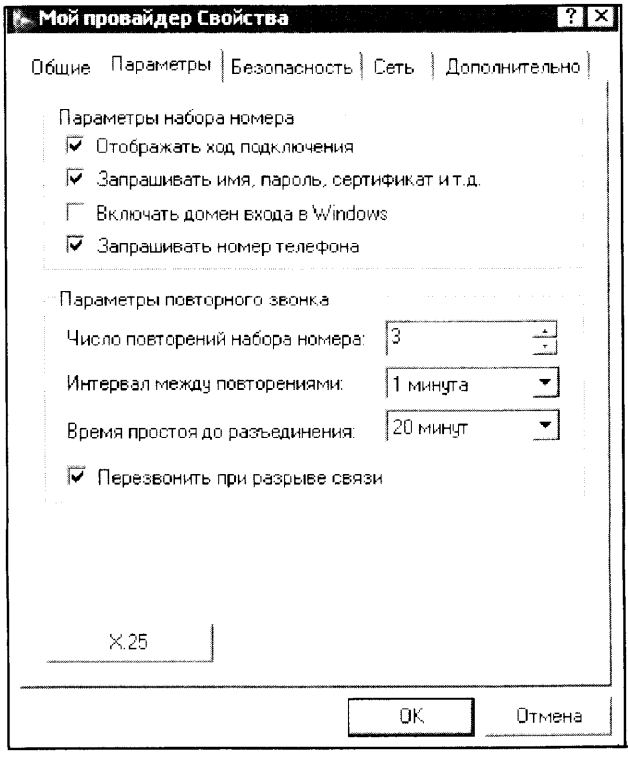


Рис. 8.16. Вкладка Параметры свойств подключения

Эта вкладка позволяет управлять параметрами набора номера и повторного звонка. Параметры набора номера можно оставить по умолчанию, а вот настройка параметров повторного звонка требует внимания.

Порой дозвониться до провайдера бывает сложно. Приходится снова и снова повторять набор номера. Установленный по умолчанию параметр, предусматривающий три повторных набора, подходит для работы

на качественных линиях, когда повторных звонков практически не требуется. А вот там, где с дозвоном бывают проблемы, его можно и даже нужно увеличить.

Например, подняв количество повторных наборов номера до десяти, вы избавите себя от ручного включения набора номера при работе на плохой линии. Ну а если провайдер перегружен, то есть заняты все линии доступа к Сети, а вам нужно срочно выйти в Интернет, можно установить этот параметр еще выше — например, двадцать наборов — и, включив набор, заниматься своими делами. Когда хотя бы одна из линий освободится, вы узнаете об этом первым.

Интервал между повторениями звонков можно оставить равным одной минуте. Но его можно и уменьшить: это поможет, если вы пытаетесь срочно дозвониться к занятому провайдеру. Время простоя тоже можно уменьшить: если вы забудете отключиться от Интернета после окончания работы, то потратите деньги впустую. Установив, скажем, 10 минут простоя, вы сможете застраховаться от глупых случайностей.

Учтите, однако, что если вы работаете с Сетью, передавая, например, файлы с помощью FTP-клиента, вас может «выбросить» из Интернета именно из-за автоотключения, которое может проигнорировать работу программы, произведенной не Microsoft.

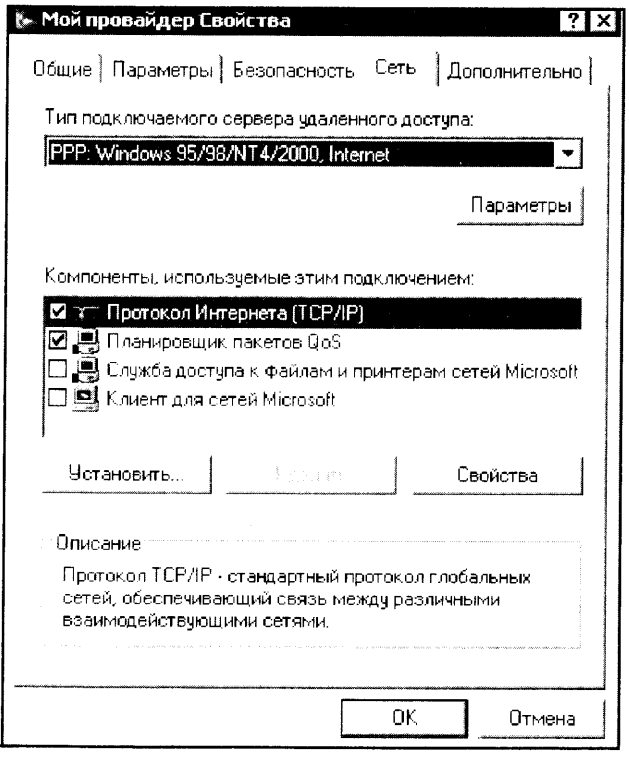


Рис. 8.17. Вкладка Сеть свойств подключения

Следующая вкладка окна настройки свойств подключения называется **Безопасность**. На этой вкладке лучше всего ничего не менять. Поэтому ее мы рассматривать пока не будем. А вот вкладку **Сеть** (рис. 8.17) рассмотрим подробнее: параметры этой вкладки весьма ощутимо влияют на безопасность компьютера в Интернете.

Обратите внимание на группу параметров, которая называется **Компоненты, используемые этим подключением**.

Настоятельно не рекомендуется включать дополнительные компоненты, кроме протокола TCP/IP. Дело в том, что дополнительные протоколы и службы — это дополнительные возможности для проникновения в ваш компьютер извне, дополнительные дыры и опасности.

TCP/IP также можно настраивать, но в большинстве случаев это делается автоматически. Поэтому пока не стоит заниматься этими настройками самостоятельно. Подробнее настройкой TCP/IP мы займемся немного ниже, когда будем говорить о ручной настройке локальной сети.

Учтите, однако, что если правила вашего провайдера требуют ручного назначения IP-адреса и некоторых других параметров вашего компьютера, то настройкой TCP/IP все же придется заняться.

Для настройки протокола надо выделить его в списке **Компоненты, используемые этим подключением** и, нажав на кнопку **Свойства**, настроить его параметры, о которых будет сказано ниже.

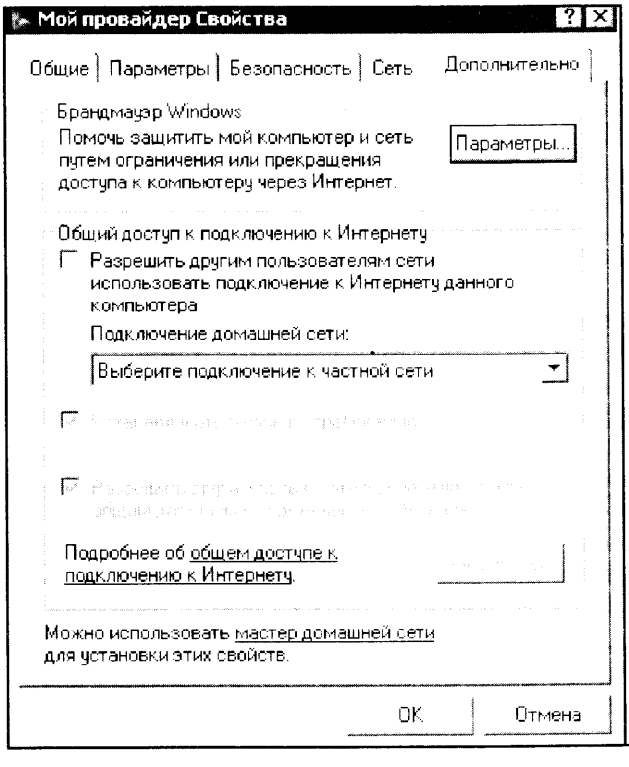


Рис. 8.18. Дополнительные параметры настройки подключения

Следующую вкладку этого окна (рис. 8.18) мы тоже пропустим, так как рассмотрению брандмауэра (это еще одно нововведение Windows XP SP2) будет посвящена отдельная глава, равно как и установке и настройке общего доступа к Интернету.

Надо сказать, что Windows содержит разные средства для выполнения одних и тех же действий. Так, например, общий доступ к Интернету может быть настроен и с помощью **Мастера установки локальной сети**, и соответствующей настройки свойства подключения Internet Explorer.

По возможности мы будем рассматривать наиболее рациональный и гибкий способ действий. Но в этой книге вы можете встретить несколько способов выполнения тех или иных задач. Дело в том, что разные люди имеют разные предпочтения, поэтому то, что удобно для одного, может быть неудобно для другого. Хорошая, гибкая программа всегда позволяет пользователю выбирать образ действий и чувствовать себя комфортно.

Подключение к Интернету мы настроили. Осталось проверить его работу. Закройте окно свойств подключения, введите в адресную строку Internet Explorer какой-нибудь интернет-адрес и нажмите **Enter**. Сразу же после этого появится окно установки соединения (рис. 8.19).

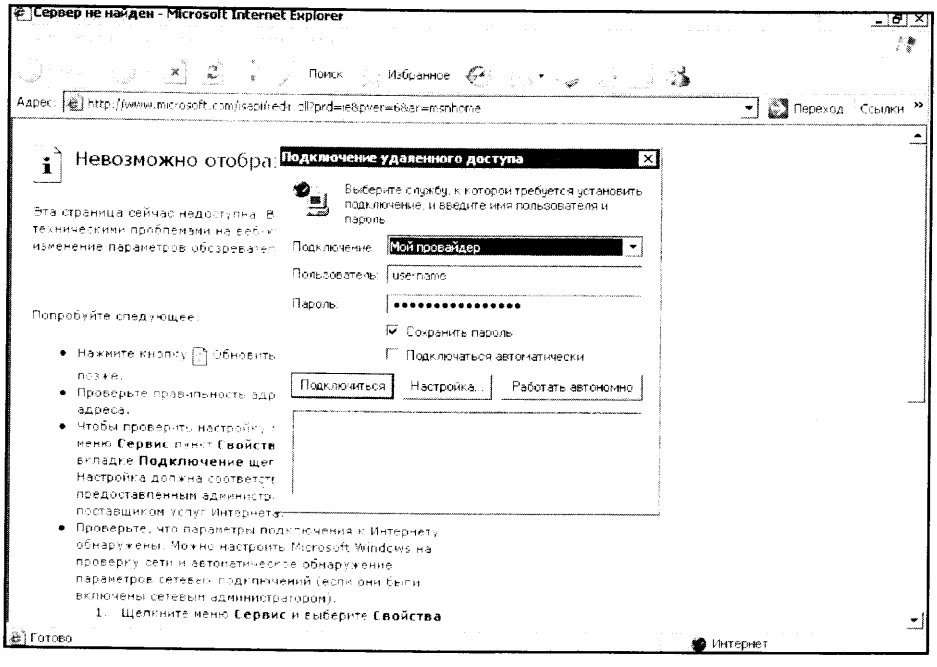


Рис. 8.19. Процесс подключения

Чтобы начать подключение, достаточно нажать на кнопку **Подключиться**. Модем наберет номер провайдера, и, если все пройдет успешно,

вы войдете в Сеть. При этом в системной панели Windows появится значок подключения в виде двух мигающих экранчиков.

Пара слов о настройке подключения средствами окна **Подключение удаленного доступа**. В этом окне есть параметры **Сохранить пароль** и **Подключаться автоматически**. Первый параметр можно включить, а вот второй включать нежелательно. Если вы разрешите компьютеру самостоятельно подключаться к Интернету, то он будет выполнять подключение всякий раз, как какой-нибудь программе вдруг что-нибудь понадобится в Сети, причем без вашего ведома.

Правда, при настройке соединения, используемого несколькими компьютерами локальной сети, тут нужно подумать. Сохранив пароль, вы избавите себя от необходимости вводить его каждый раз при подключении. Это удобно. Но сохраненный пароль может быть украден: ведь он хранится в системе, пусть и в зашифрованном виде. Но и ручной ввод пароля не гарантирует абсолютной безопасности, так как его тоже могут украсть с помощью программы, так называемого клавиатурного шпиона например. Так что думайте сами, включать эту установку или не включать.

После работы в Интернете вы должны отключиться, то есть прервать соединение. Это сделать легко — достаточно щелкнуть по значку соединения в системной панели и выбрать в выпавшем меню команду **Отсоединить**.

Раз уж мы взялись рассматривать вопросы подключения к Интернету, рассмотрим здесь же особенности настройки программы Outlook Express.

8.3. НАСТРОЙКА OUTLOOK EXPRESS

Многие начинающие пользователи испытывают затруднения при работе с электронной почтой. Затруднения эти бывают двух видов: сложности с открытием почтового ящика и проблемы с настройкой почтового клиента на автоматическую работу с этим самым почтовым ящиком. Разберем пример создания почтового ящика на популярном почтовом сервере Mail.ru, настроим Outlook Express, чтобы он автоматически забирал и отправлял почту, и протестируем полученную конструкцию.

А начнем мы с регистрации почтового ящика. Для этого надо войти на сервер, который предоставляет почтовые услуги. В нашем случае это будет Mail.ru.

Зайдя на главную страницу сервиса, нажмите на ссылку **Регистрация в почте**. Если вы регистрируетесь на другом сервере, то ссылка, ведущая к регистрации, может называться иначе, но в целом все выглядит именно так.

После этого вы попадете на страницу регистрации. Эта страница (рис. 8.20) содержит много вопросов, на которые система хочет получить ответы. Некоторые из них имеют критическую важность, и если ответы

на них неверны, то вы либо не сможете зарегистрироваться, либо, зарегистрировавшись, не сможете пользоваться своим почтовым ящиком (учетной записью, или аккаунтом).

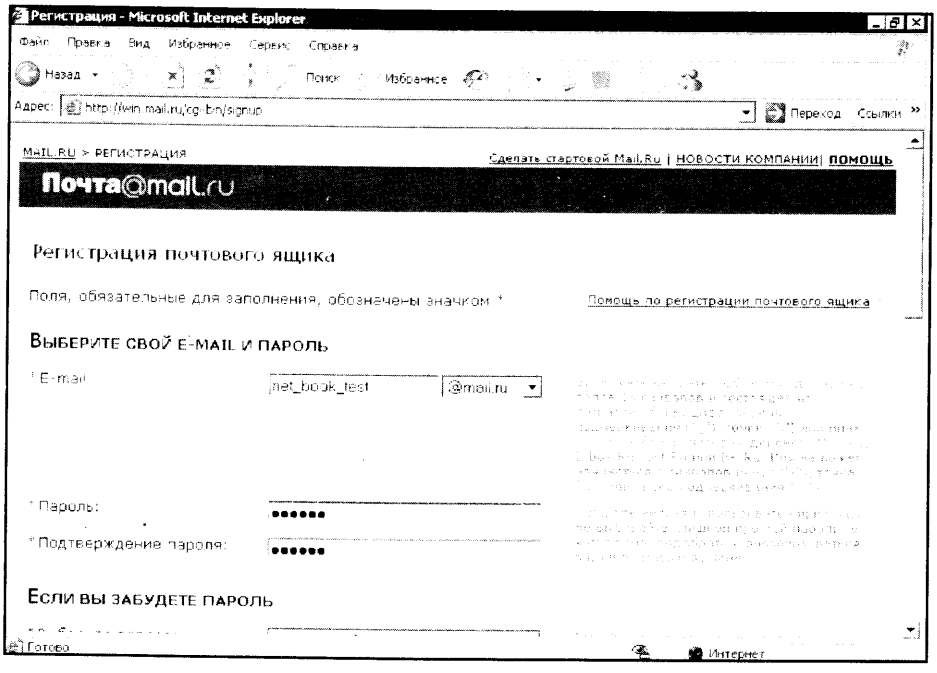


Рис. 8.20. Начало регистрации в почтовой системе

Самые важные поля, которые нужно заполнить, **E-mail** и **Пароль**.

В качестве адреса электронной почты в нашем примере выбрано слово net_book_test. В списке, который расположен сразу после поля ввода имени, можно выбрать домен. В нашем случае это Mail.ru.

В поле ввода пароля надо ввести пароль для доступа к системе. Ни в коем случае не используйте слишком простые пароли, то есть какие-нибудь слова, имена, даты. Такие пароли легко можно взломать. Представляете, что будет, если посторонний сможет рыться в вашей корреспонденции, писать письма от вашего имени и читать вашу переписку? Поэтому задавайте пароль, в котором сочетаются цифры, буквы и, возможно, другие символы — вроде скобок и звездочек. Чем длинней пароль, тем лучше. Слишком длинный пароль тоже выбирать не стоит, его трудно запомнить. Символов пять или восемь, и хватит.

При выборе пароля лучше всего сделать так: сначала придумайте пароль, запишите его в надежном месте, а потом, при регистрации почтового ящика, внимательно вводите этот пароль. При вводе пароля и подтверждения они отображаются в виде точек. Такой подход позво-

ляет защитить пароль от подглядывания: например, если вы регистрируете почту в интернет-клубе, кто-нибудь может его увидеть. А так все достаточно секретно.

Еще раз повторю: внимательно вводите оба варианта пароля. У меня однажды был случай, когда я, регистрируя почту на сервере своего интернет-провайдера, сначала ввел пароль, а потом записал то, что, как мне казалось, я напечатал. Этот пароль для меня до сих пор остается загадкой. Ну а ящик, конечно же, пришлось перерегистрировать.

Записав и введя пароль, переходим к группе параметров **Если вы забудете пароль** (рис. 8.21). Здесь надо выбрать вариант вопроса и придумать ответ. В качестве варианта ответа лучше вводить что-нибудь совершенно бредовое (а можно и вопрос свой придумать), но такое, чтобы вы легко могли, в случае чего, вспомнить этот бред. Если вы забудете пароль, система задаст вам этот вопрос и, если вы ответите правильно, напомнит забытый пароль.

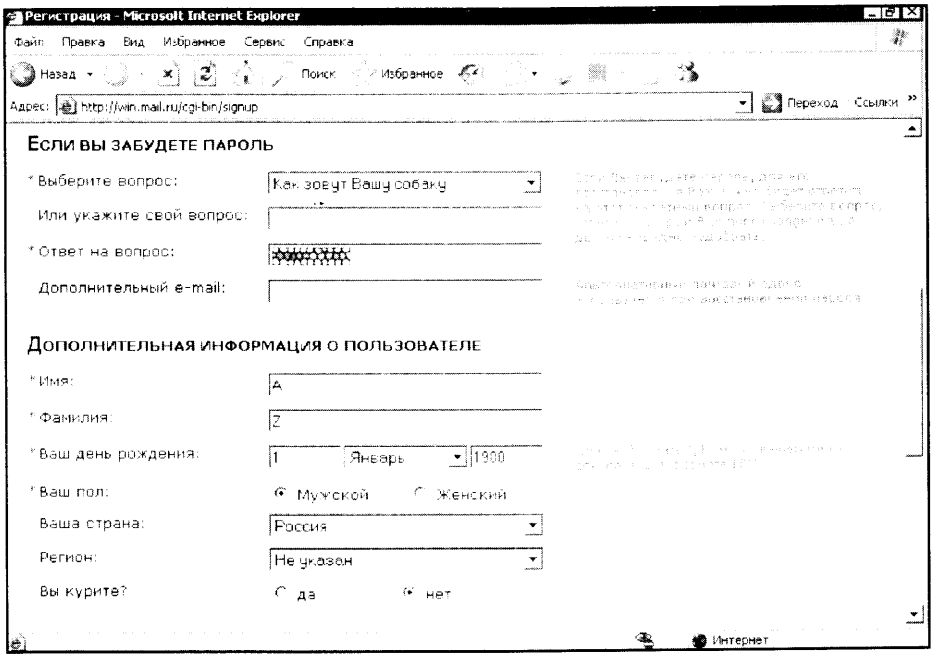


Рис. 8.21. Продолжение заполнения анкеты

В разделе **Дополнительная информация о пользователе** лучше сказать о себе всю правду: опять-таки, если вы забудете пароль и система спросит вас дату рождения, а вы ответите неверно, восстановить пароль будет невозможно.

Обратите внимание на то, что поля, обязательные для заполнения, помечены звездочками. Если их не заполнить, система откажется вас регистрировать.

Следующий этап регистрации заключается в заполнении особого поля, защищающего систему от автоматической регистрации учетных записей почты, которую могут проводить специально «обученные» этому делу роботы (рис. 8.22).

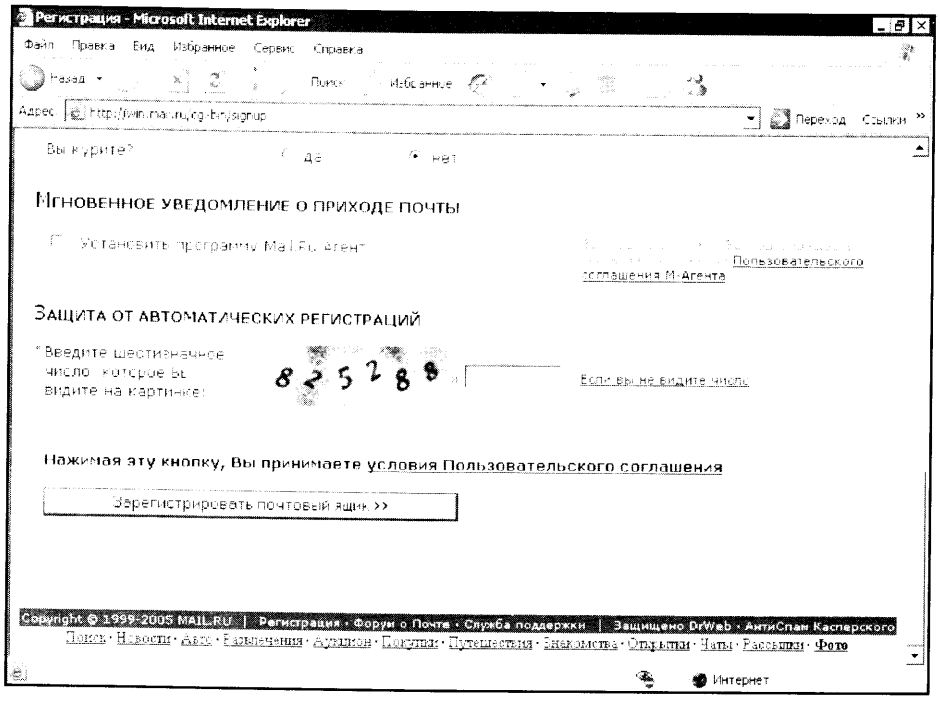


Рис. 8.22. Финальный этап регистрации

После того как все заполнено, осталось нажать на кнопку **Зарегистрировать почтовый ящик**, и вы, если регистрация успешна, попадаете на стартовую страничку почтового ящика.

Там все организовано довольно просто, поэтому с веб-интерфейсом почты вы разберетесь быстро. Единственное, что хочу добавить: после окончания работы с почтой не забывайте нажимать на кнопку **Выход** (рис. 8.23) — она находится в правом верхнем углу, а если вам что-то непонятно — внимательно почитайте справочные материалы на сервере. Там все очень хорошо объясняется. И если вам удалось зарегистрировать почтовый ящик, то все остальное не составит трудностей.

Чтобы получить дополнительную информацию о настройке почтового клиента на работу с почтой, можно воспользоваться разделом **Помощь**. Ссылка на него находится сразу над кнопкой **Выход**. Однако

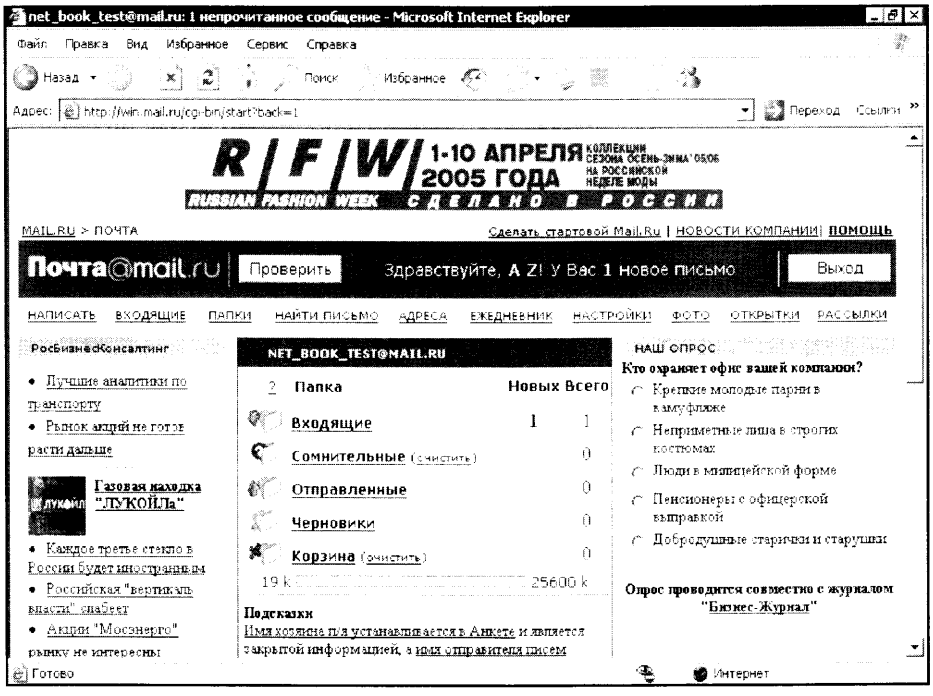


Рис. 8.23. Стартовая страничка веб-интерфейса почтовой программы

практика показывает, что материалы этого раздела сложны для восприятия неподготовленного пользователя, поэтому здесь мы, ориентируясь на тех, кто пока не знаком с тонкостями настройки почтовых клиентов, пошагово рассмотрим настройку **Outlook Express**.

В свежеустановленной Windows XP значок Outlook Express находится около значка Internet Explorer. После первой попытки запустить Outlook Express вам сразу же будет предложено создать учетную запись электронной почты. Эта процедура, особенно некоторые ее части, у начинающих пользователей вызывает определенные сложности.

Посмотрите на рис. 8.24. Здесь изображено первое окно Мастера, который помогает настроить учетную запись.

В качестве имени обычно удобно использовать свои настоящие имя и фамилию, чтобы получатели письма могли точно вас идентифицировать. Правда, Интернет — это очень свободное сообщество, поэтому, строго говоря, вы можете написать здесь все, что душе угодно.

Следующее окно (рис. 8.25) предназначено для ввода адреса вашей электронной почты. Этот тот самый адрес, регистрацией которого мы с вами занимались выше.

После ввода этого адреса наступает момент, на котором спотыкается подавляющее большинство начинающих. Вам нужно ввести адреса серверов входящей и исходящей почты, которые нигде в явном виде не фи-

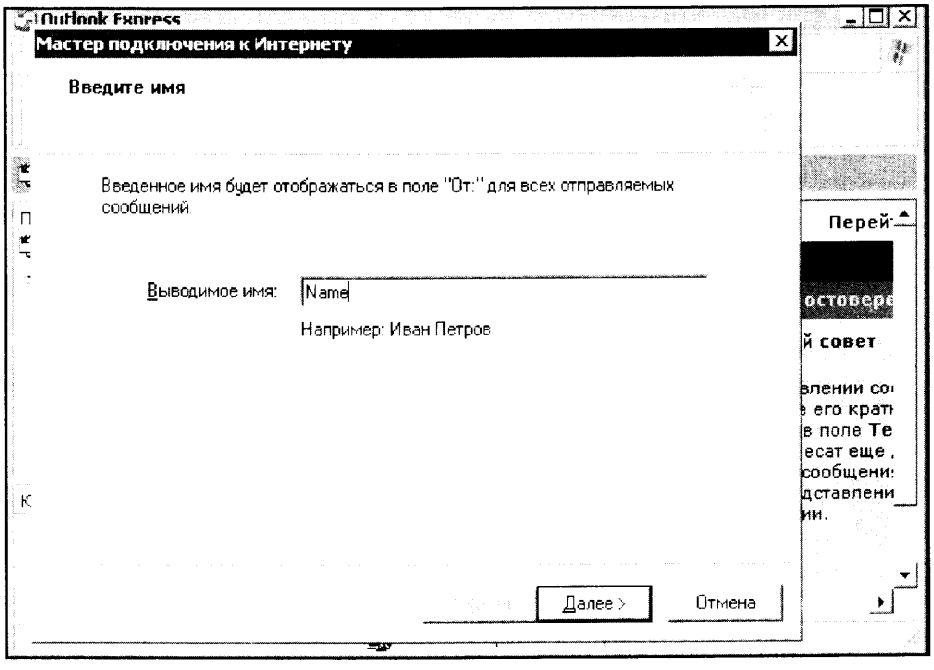


Рис. 8.24. Задание имени

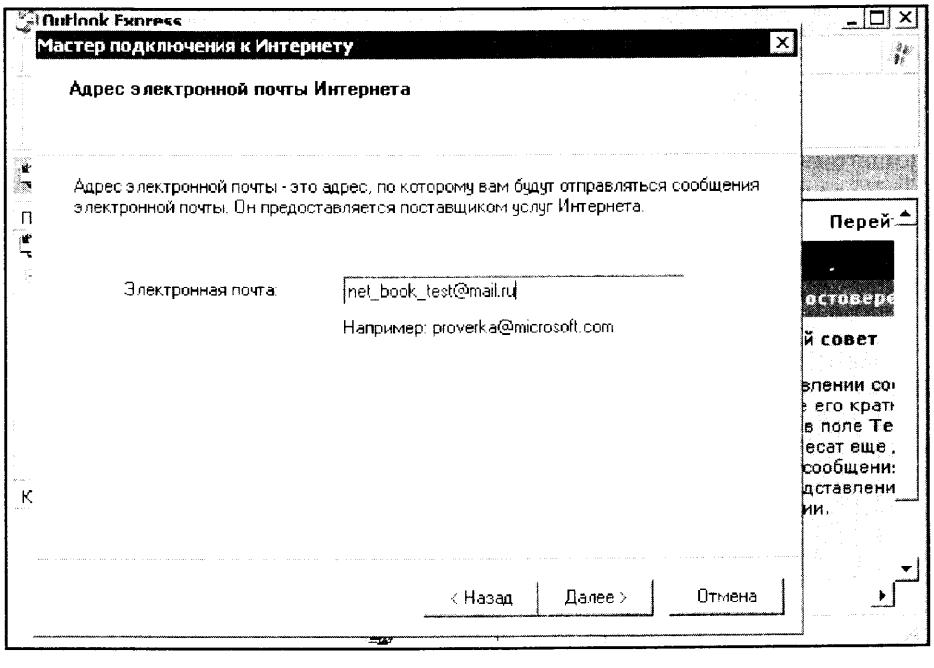


Рис. 8.25. Ввод адреса электронной почты

гурируют. Эти адреса надо «выуживать» из справочного раздела почтового сервера. Некоторые почтовые серверы выдают эту информацию сразу после того, как вы завершили регистрацию. Если e-mail выдан вам провайдером, то он предоставит и адреса серверов.

Посмотрите на рис. 8.26. Здесь вы видите то самое окно, которое вызывает больше всего проблем.

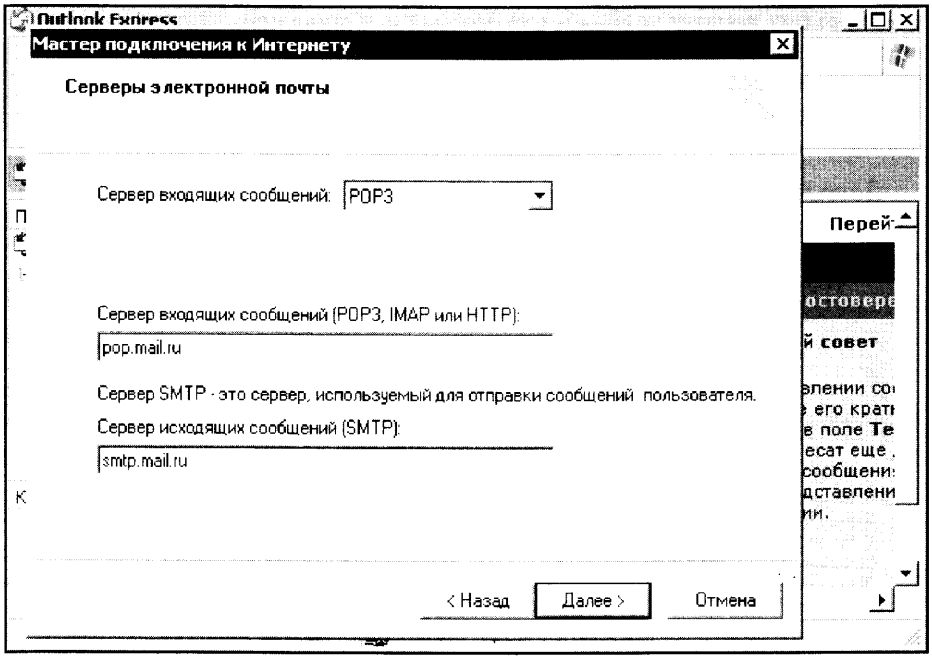


Рис. 8.26. Настройка серверов

Из справочной системы сервера Mail.ru известно, что почтовые ящики, доменным именем которых (то есть тем, что идет после значка @) является Mail.ru, работают с серверами pop.mail.ru в качестве сервера входящих сообщений и smtp.mail.ru в качестве сервера исходящих сообщений.

Обратите внимание на то, что никаких значков @ в именах этих серверов нет — только латинские символы и точки.

Если вы регистрируете адрес, скажем, на сервере вашего провайдера, то имена серверов входящей и исходящей почты могут совпадать.

Ну а дальше остается нажать **Далее**, ввести в следующем окне имя и пароль, которые мы задавали, когда регистрировали почтовый ящик, и почитать поздравления Мастера, который помог нам установить электронную почту.

В случае с сервером Mail.ru почта, которая настроена таким образом, не будет работать правильно: дело в том, что этот сервер в целях борьбы со спамом, то есть с нежелательными массовыми отправлениями почты, ввел дополнительную аутентификацию пользователей.

Обычно аутентификация требуется, чтобы можно было забрать почту, а сервер исходящих сообщений принимает исходящие сообщения без лишних условностей. Но сегодня спам принял совершенно нежелательные масштабы, и в целях борьбы с этой «чумой Интернета» Mail.ru реализовал систему защиты. Она-то и требует дополнительной настройки SMTP-сервера.

Дополнительная настройка SMTP-сервера для почты Mail.ru заключается в следующем. Выберите меню Outlook Express **Сервис ▸ Подключения**, после чего появится окно управления подключениями (рис. 8.27).

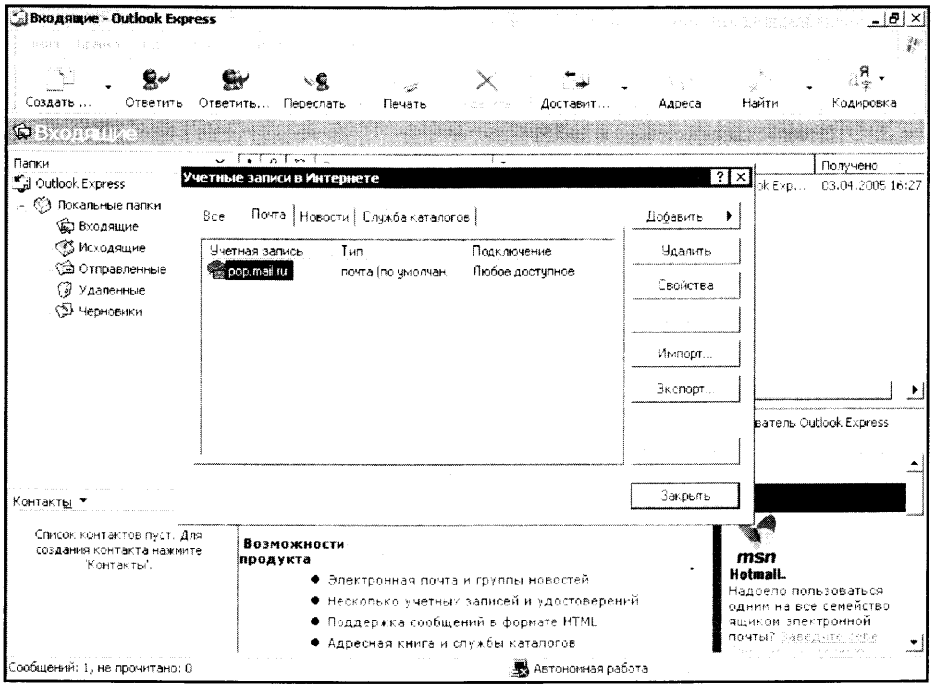


Рис. 8.27. Настройка учетных записей

Выбрав нужную учетную запись, нажмите кнопку **Свойства**. Многие вкладки этого окна повторяют логику вышеописанной настройки почтового клиента, а вот кое на какие вещи я хочу обратить ваше внимание.

Посмотрите на рис. 8.28. Здесь изображено окно настройки серверов. Сервер входящей почты уже настроен — его настройка по умолчанию

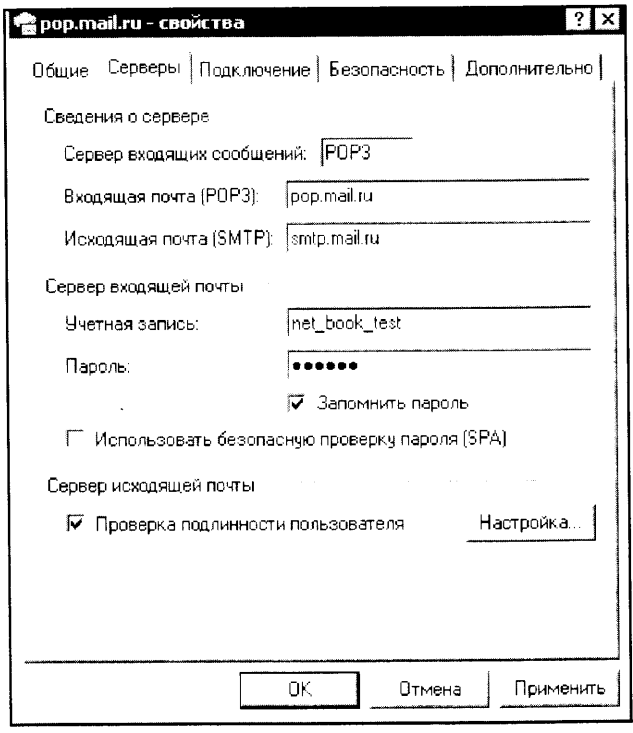


Рис. 8.28. Настройка сервера входящей почты

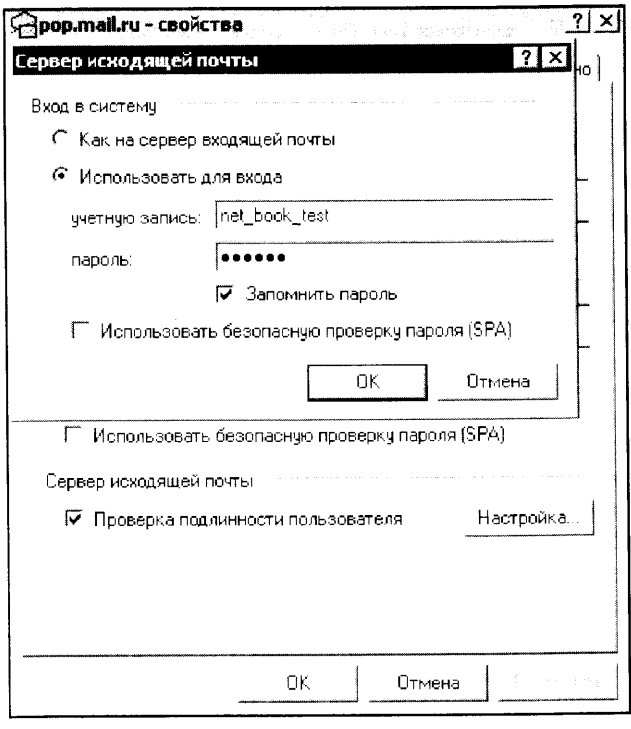


Рис. 8.29. Настройка сервера исходящей почты

подходит для большинства пользователей. А вот сервер исходящей почты требует дополнительной настройки. Для начала поставьте галочку **Проверка подлинности пользователя**, а потом нажмите на кнопку **Настройка** (рис. 8.29).

Здесь надо действовать очень внимательно и ввести в поля ввода имя почтовой записи, пароль, а затем поставить галочку **Запомнить пароль**.

Учтите, что к тому времени, когда вы будете это читать формат аутентификационных данных может измениться. Очень может быть, что в качестве имени учетной записи начнут использовать полное имя учетной записи почты и понадобится установить галочку **Использовать безопасную проверку пароля (SPA)**. По крайней мере, в одном из случаев из моей практики все заработало именно при такой настройке почтового ящика.

Теперь рассмотрим вкладку окна настройки соединения, которая называется **Дополнительно** (рис. 8.30). Она содержит очень полезный параметр, который отвечает за хранение на сервере копий отправленных писем.

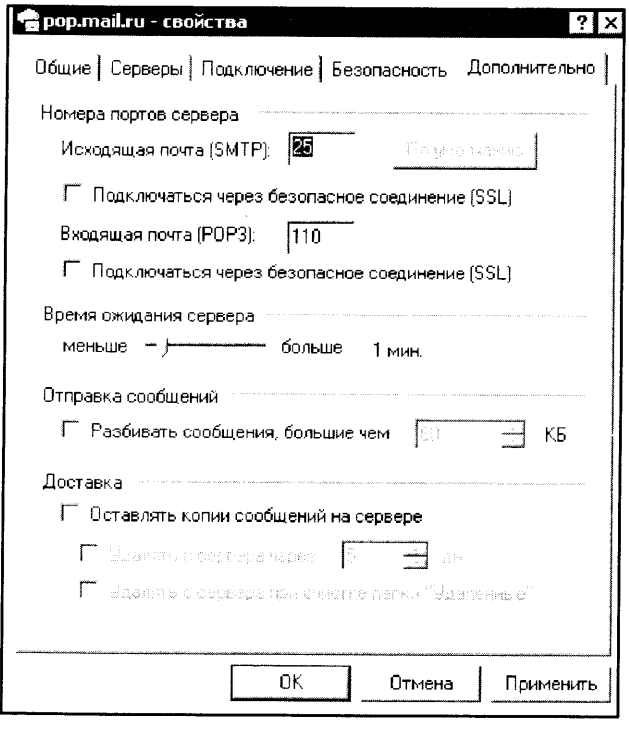


Рис. 8.30. Настройка дополнительных параметров

Поставив галочку **Оставлять копии сообщений на сервере**, вы создадите таким образом две параллельные базы собственных писем — на вашем локальном ПК и в Сети, то есть сможете получить доступ к вашей исходящей корреспонденции из любого места, где есть доступ в Интернет.

После настройки почтового клиента нужно его протестировать (рис. 8.31). Для этого достаточно написать письмо самому себе. Таким образом будет проверена правильность настройки всей нашей почтовой системы и ее возможностей по отправке и получению почты.

Для создания письма нажмите кнопку **Создать** на панели инструментов Outlook Express, в поле **Кому** нового письма напишите свой адрес (в нашем случае net_book_test@mail.ru), в тело письма введите любой текст. Нажмите кнопку **Отправить** и, если вы еще не вошли в Сеть, произведите подключение. Затем программа отправит письмо. Если все прошло без сообщений об ошибках, значит, в части сервера исходящей почты мы все сделали правильно.

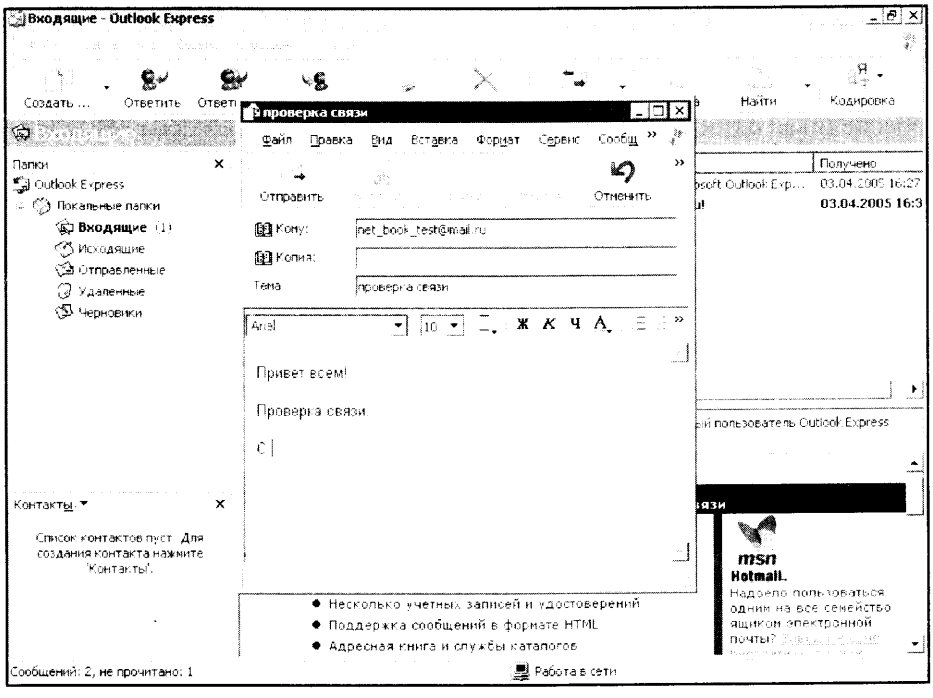


Рис. 8.31. Проверка настроек почтового клиента

А теперь, не отключаясь от Интернета, нажмите кнопку **Доставить**. Программа проверит ваш почтовый ящик, и, если все было сделано правильно, вы получите письмо, которое только что создали.

Если все так и произошло, знайте: почтовый клиент настроен правильно и теперь вы можете пользоваться его возможностями. Ну а коли вы справились с настройкой учетной записи и почтового клиента, то с остальными вопросами очень быстро разберетесь самостоятельно.

ГЛАВА 9
НАСТРОЙКА ЛОКАЛЬНОЙ СЕТИ

Займемся локальной сетью, которая уже заждалась нас. Локальная сеть, проводная или беспроводная, работает примерно на одних и тех же принципах. Правда, настройка этих сетей в части конкретных технологий уникальна для каждого ее вида. Проводные и беспроводные сети, обеспечивая одни и те же функции, настраиваются по-разному. Высокоуровневые параметры, например TCP/IP, настраиваются сходно, а все остальное требует от настройщика специальных знаний.

9.1. НАСТРОЙКА ETHERNET-СЕТИ

Сетевые адаптеры подключены к компьютеру, драйверы установлены. Теперь настало время соединить эти адаптеры с хабом при помощи кабелей. Затем включить хаб, компьютеры и начать установку локальной сети.

Локальная сеть в Windows XP может быть установлена в почти автоматическом режиме: вам придется лишь отвечать на вопросы соответствующего Мастера.

Для запуска Мастера установки локальных сетей нужно войти в панель управления, перейти к сетевым подключениям и запустить там из списка типичных задач **Мастер настройки сети** (рис. 9.1).

Этот Мастер проведет вас через все этапы установки локальной сети. Однако и здесь есть некоторые тонкости, которые мы сейчас разберем.

Сеть в Windows XP можно настроить и вручную. В учебных целях мы разберем этот процесс ниже. Существование средств автоматической настройки локальной сети не означает, что не нужно знакомиться с ручными настройками: ведь случается, что сеть, установленная автоматически, по каким-нибудь причинам не работает. В таком случае знание способов ручной настройки сети, некоторых способов проверки ее функционирования и еще кое-каких секретов позволит вам диагностировать проблему и, устранив ее, пользоваться локальной сетью.

После появления окна **Мастера** будем нажимать кнопку **Далее** до тех пор, пока не появится первое окно, требующее осмысленного решения (рис. 9.2).

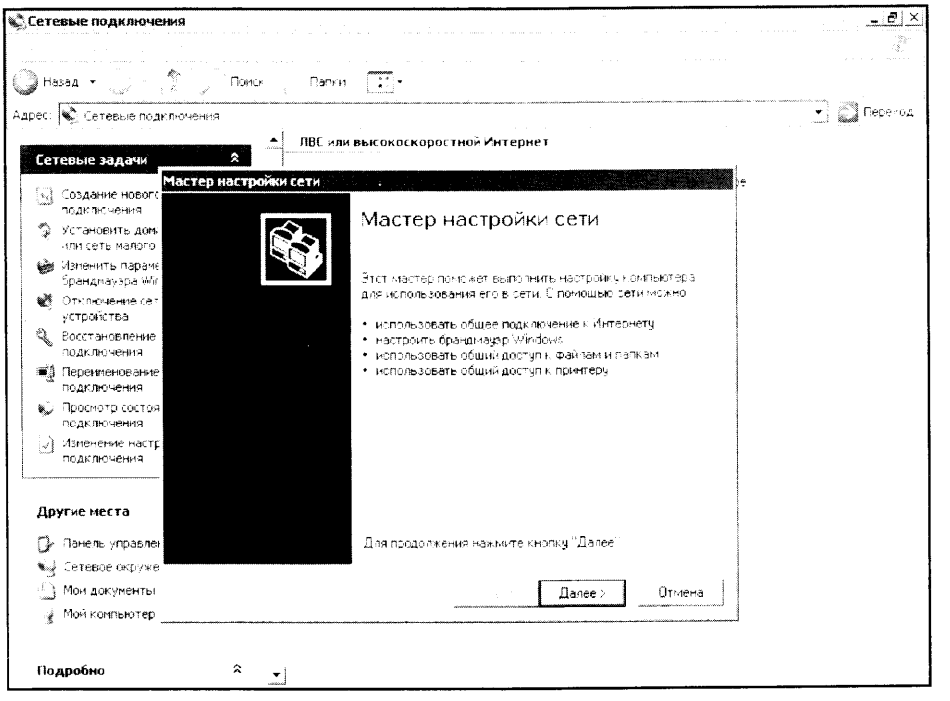


Рис. 9.1. Запуск Мастера настройки сети

Это окно позволяет настроить общий доступ в Интернет. Наш компьютер имеет выход в Сеть, поэтому выбираем первый параметр. Но при

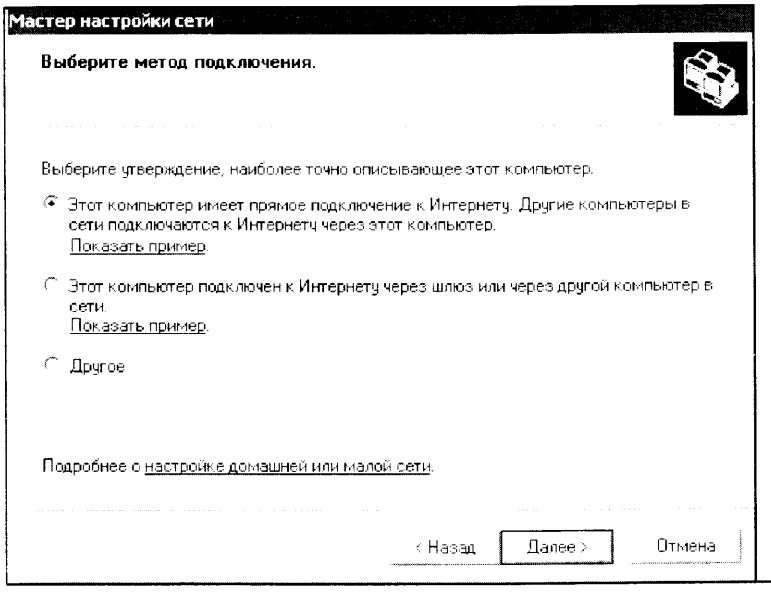


Рис. 9.2. Метод подключения компьютера сети к ...тернету

прохождении этого этапа на других компьютерах сети следует выбрать второй пункт, чтобы они могли подключаться к Интернету через компьютер, который предоставляет им свои ресурсы по подключению.

При такой настройке IP-адрес компьютера, предоставляющего доступ к интернет-подключению другим машинам, автоматически настраивается на 192.168.0.1 (о подробностях, касающихся этого IP-адреса, разговор будет ниже). В одной сети не может быть двух ПК с одинаковыми IP-адресами. Значит, остальные компьютеры вашей сети надо настроить, выбрав второй параметр.

Однако, если даже другой компьютер сети настроен на использование общего соединения, он может иметь собственный модем и выходить в Интернет независимо от других компьютеров сети. Если, например, после установки такой сети вы провели вторую телефонную линию, то второй компьютер сможет, оставаясь в локальной сети, выходить в Интернет через собственный модем.

Если вы установили локальную сеть методом, который сейчас описывается, сделать этого будет нельзя: ведь запрос на подключение к Интернету будет передаваться компьютеру с IP-адресом 192.168.0.1, который будет использовать собственный модем, чтобы дать вам доступ к Сети.

Чтобы этого избежать, надо изменить настройку IE, касающуюся использования подключения к Интернету по умолчанию. На рис. 9.3 изображена вкладка **Подключения** окна **Свойства обозревателя**. Так она выглядит после того, как сеть настроена при помощи **Мастера настройки сети**.

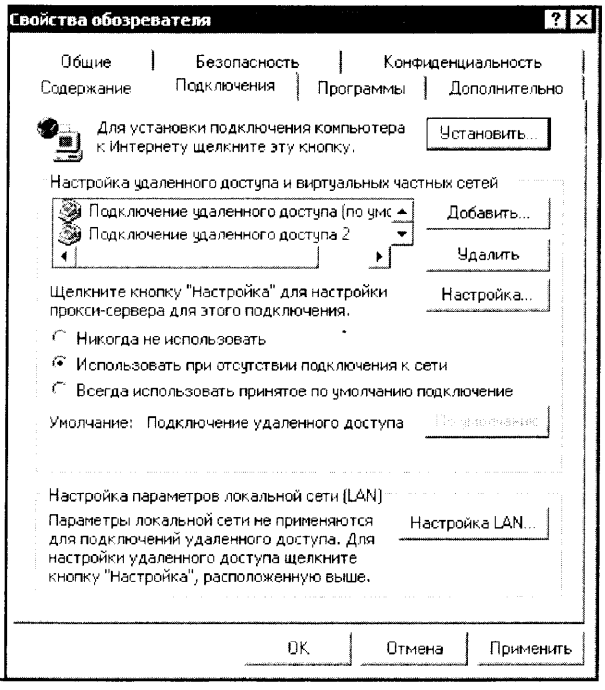


Рис. 9.3. Настройка подключений к Интернету

Чтобы компьютер, находясь в локальной сети, мог подключаться к Интернету через собственный модем, надо сделать активным параметр **Всегда использовать принятое по умолчанию подключение**. А чтобы при необходимости снова вернуться на доступ к Интернету через центральный компьютер, достаточно выбрать пункт **Использовать при отсутствии подключения к сети**.

Вернемся к настройке локальной сети на компьютере, предоставляющем свое интернет-подключение для других компьютеров сети. Посмотрите на рис. 9.4. Система просит вас указать, через какое соединение осуществляется выход в Интернет.

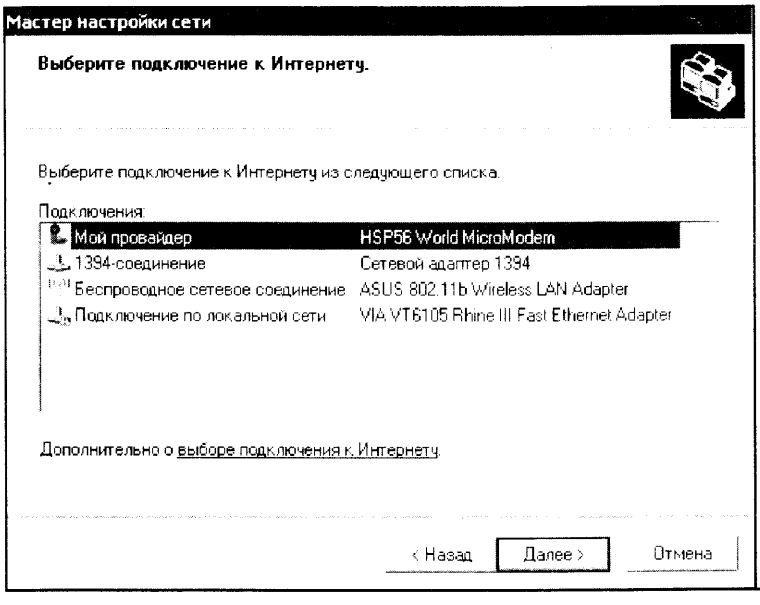


Рис. 9.4. Выбор подключения к Интернету

В предыдущей главе мы настроили модемное подключение с именем **Мой провайдер**. Его и выберем для продолжения установки.

Следующий этап работы **Мастера** — выбор подключения локальной сети. Здесь можно выбрать несколько подключений, и тогда система объединит их мостом, но об этом речь будет позже, а пока что выберем лишь одно подключение, обеспечиваемое сетевой картой.

В следующее окно (рис. 9.5) надо ввести имя и описание компьютера. При назначении имени компьютера русских символов лучше не использовать.

После задания имени компьютера в следующем окне вас попросят указать имя рабочей группы, к которой принадлежит этот компьютер. Учтите, что компьютеры, объединенные в локальную сеть, должны иметь разные имена, но имя их рабочей группы должно совпадать. В данном случае я оставил имя рабочей группы, заданное по умолчанию, это MSHOME.

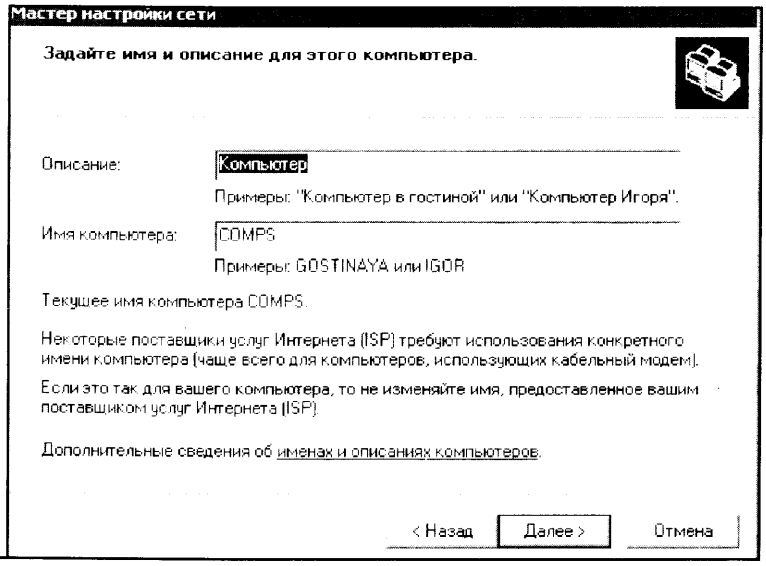


Рис. 9.5. Задание имени и описания компьютера

Следующий этап работы **Мастера** — установка разрешений на общий доступ к принтеру и особой папке данного компьютера (рис. 9.6).

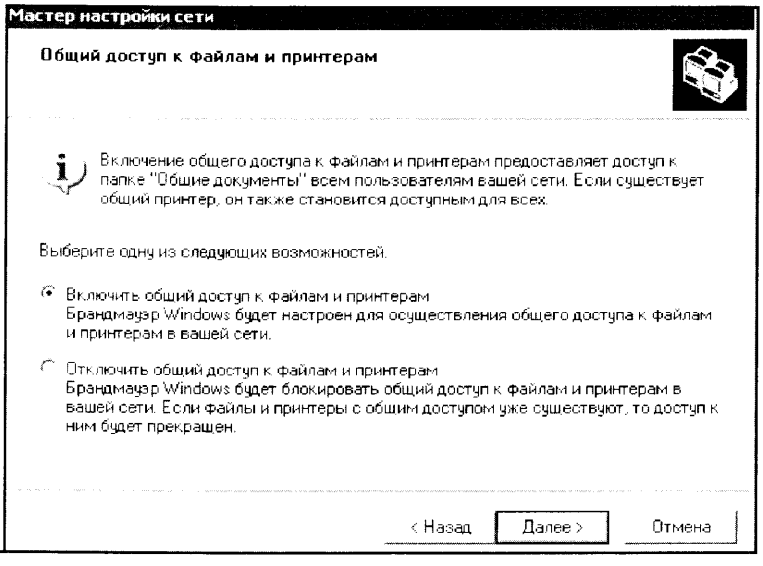


Рис. 9.6. Установка разрешений на доступ к общим ресурсам компьютера

Вот и весь процесс настройки локальной сети. Нажав еще раз кнопку **Далее**, вы попадаете на финальную страницу установки локальной сети. Теперь нужно запустить **Мастер настройки сети на других компьютерах**, которые вы хотите объединить в локальную сеть, не забыв при этом указать разные имена компьютеров, а также одинаковое имя рабочей группы.

Если вы все сделали правильно, через десяток-другой минут после начала установки локальная сеть должна заработать. Откройте на любом из компьютеров папку **Сетевое окружение.** Если все в порядке, вы увидите там общие ресурсы объединенных в сеть компьютеров. В нашем случае это всего пара машин, и поэтому **Сетевое окружение** выглядит так, как изображено на рис. 9.7.

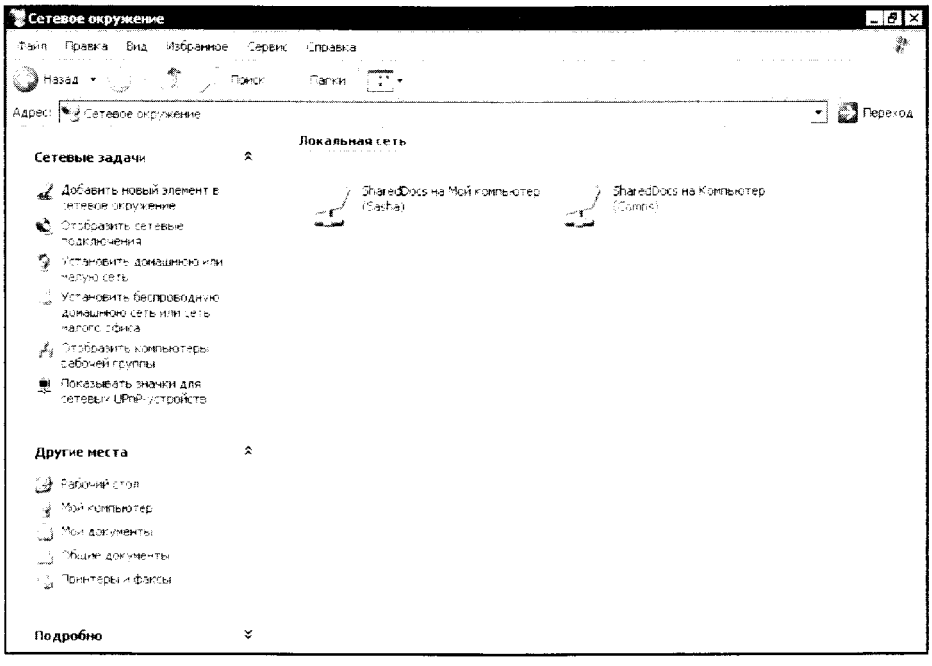


Рис. 9.7. Сетевое окружение

Для чистоты эксперимента попробуйте перейти в сетевую папку какого-нибудь из подключенных компьютеров. Если все получилось, значит, сеть настроена правильно. Теперь вы можете переписывать файлы с компьютера на компьютер, просто копируя их в общую папку, и выходить в Интернет с любого из компьютеров сети.

Стандартная установка локальной сети в большинстве случаев срабатывает безотказно. Однако бывают случаи, когда все устанавливается, а потом начинаются странности.

Прежде чем разбирать возможные проблемы установки сети, настроим локальную сеть вручную, не используя программу-Мастер.

Мы настроим протокол IP на паре объединенных компьютеров, затем попытаемся «выпустить» один компьютер в Интернет и посмотрим, что получится. Когда все трудности будут преодолены, останется лишь настроить принтер для работы в сети, открыть общий доступ к какой-нибудь папке и разобрать некоторые тонкости этого процесса.

9.2. РУЧНАЯ УСТАНОВКА ЛОКАЛЬНОЙ СЕТИ

Для ручной установки локальной сети нужно выполнить по меньшей мере два действия. Первое заключается в настройке IP-адресов сетевых адаптеров, а второе — в создании новой рабочей группы для компьютеров, объединенных в сеть. В общем случае можно назначить компьютерам локальной сети практически любой IP-адрес, но лучше, если он будет лежать в пределах от 192.168.0.1 до 192.168.0.254. Сеть, настроенная с использованием других IP-адресов, будет работать, но для установки общего подключения к Интернету IP-адреса потребуют особой настройки.

Для настройки IP-адресов сетевых адаптеров надо в папке **Сетевые подключения** найти нужное подключение по локальной сети. Далее выберите его свойства и, найдя в **Свойствах подключения** на вкладке **Общие** строку **Протокол Интернета (TCP/IP)**, выделить его и нажать на кнопку **Свойства** (рис. 9.8).

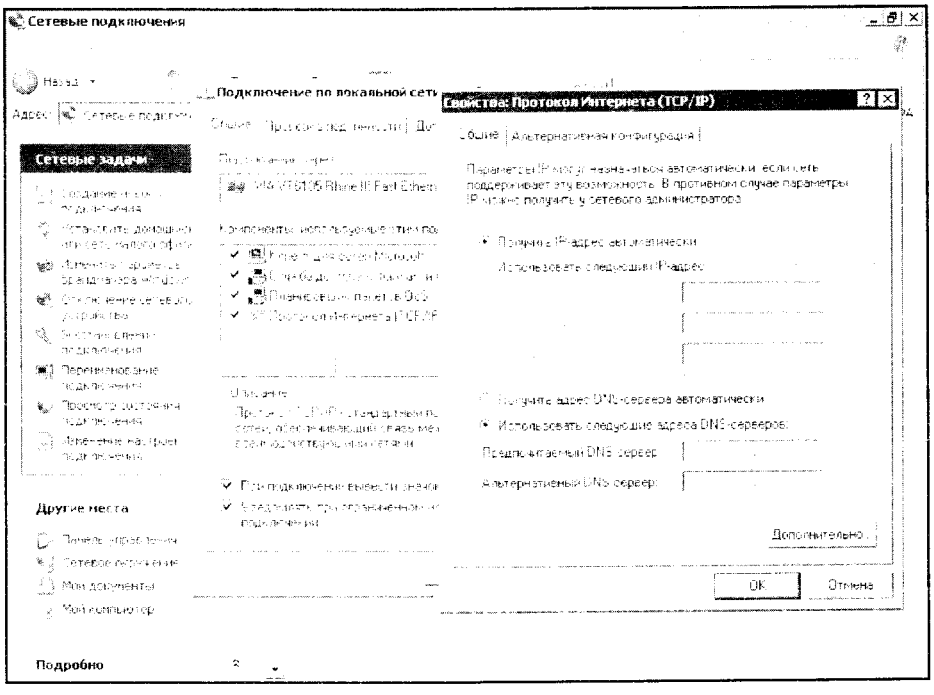


Рис. 9.8. Настройка IP-адресов

В этом окне настроено автоматическое получение IP-адреса. Но мы хотим ввести собственный IP-адрес. Для этого активируем переключатель **Использовать следующий IP-адрес**. Например, пусть это будет IP-адрес 192.168.50.100. Введите этот адрес в поле **IP-адрес**. При этом **Маска подсети** автоматически устанавливается в значение 255.255.255.0.

Теперь, нажимая **OK**, закройте все окна и перейдите к значку **Мой компьютер**. Щелчком правой кнопкой мыши вызовите контекстное меню, выберите из него **Свойства**, а в свойствах найдите вкладку **Имя компьютера** (рис. 9.9).

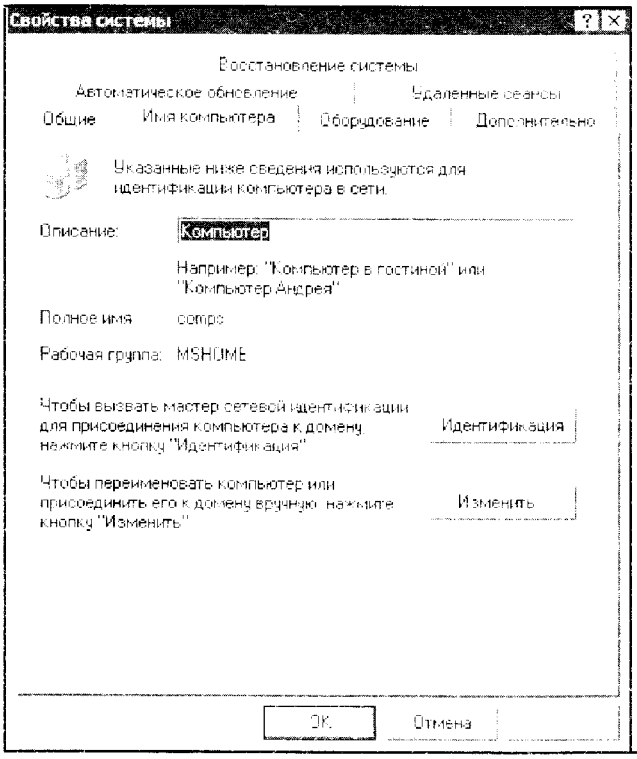


Рис. 9.9. Настройка имени и рабочей группы компьютера

В появившемся окне надо нажмите кнопку **Изменить**. Появится окно для настройки имени и рабочей группы компьютера (рис. 9.10). Напомню, что имя рабочей группы у всех компьютеров одной и той же локальной сети должно совпадать, а имена компьютеров должны различаться. В данном случае в качестве имени рабочей группы выбрано MY_WORK.

После того как вы изменили принадлежность компьютера к рабочей группе, Windows запросит разрешение на перезагрузку. Ответьте ей **OK** и, пока компьютер перезагружается, займитесь настройкой других машин.

Настройка других компьютеров сети осуществляется аналогично.

- Вначале следует настроить IP-адрес. При этом помните, что, раз вы выбрали адрес вида 192.168.50.100, имеющий маску подсети 255.255.255.0, то и все другие компьютеры в нашей сети должны иметь адреса вида 192.168.50.x. При этом в сети не может быть двух одинаковых IP-адресов. Я, к примеру, следующему компьютеру сети задал IP-адрес 192.168.50.101.

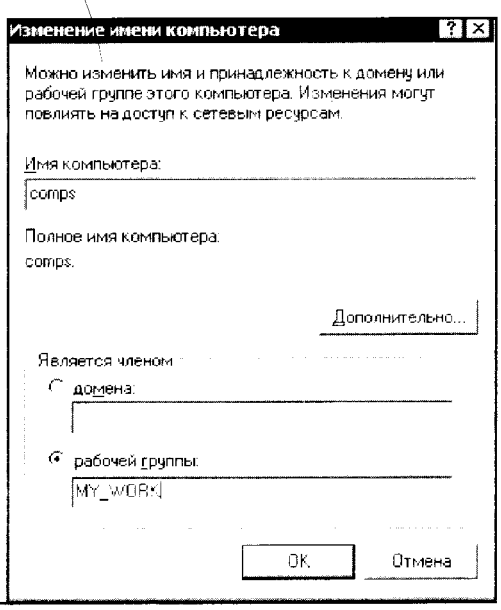


Рис. 9.10. Изменение имени компьютера

- Затем включите другие компьютеры в ту же рабочую группу, к которой принадлежит первый, аналогичным образом изменив имя их рабочей группы (рис. 9.9, 9.10). Другие компьютеры тоже надо будет перезагрузить.

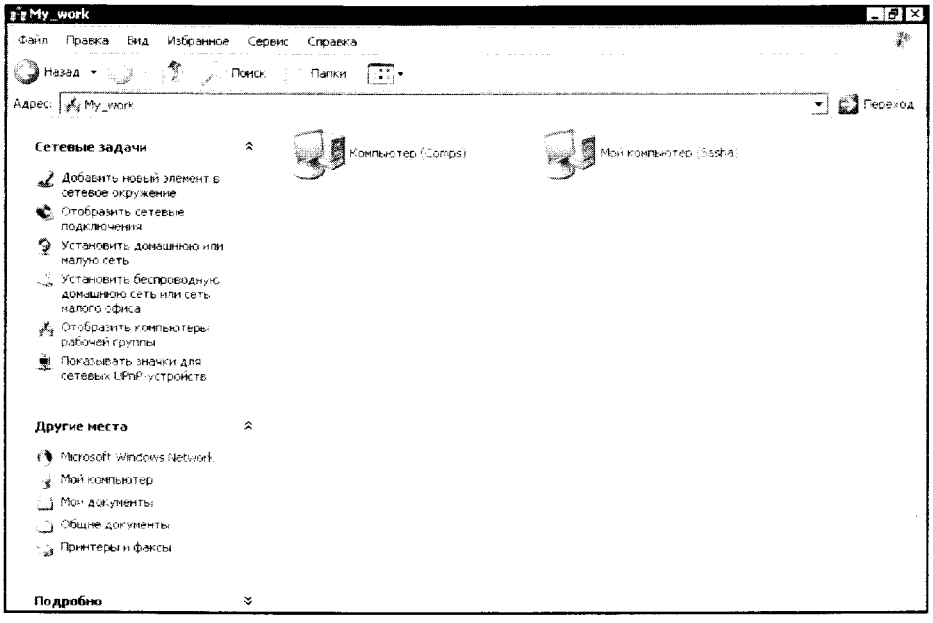


Рис. 9.11. Состав новой рабочей группы

Теперь, если все сделано верно, локальная сеть заработает. Для проверки ее работоспособности достаточно войти в папку **Мое сетевое окружение** и щелкнуть по ссылке **Отобразить компьютеры рабочей группы** (рис. 9.11).

Если компьютеры рабочей группы отобразятся в окне и если удастся открыть для просмотра общие ресурсы компьютеров, значит сеть настроена правильно и ее можно использовать, по крайней мере, для передачи файлов с одного компьютера на другой.

Но сеть — это гораздо больше, чем передача файлов. Например, один из компьютеров, объединенных в сеть, имеет принтер. При автоматической установке сети принтер, скорее всего, будет тоже установлен автоматически, причем вам ничего не придется менять. (Windows XP SP2 устанавливает принтер автоматически.)

Но иногда принтер бывает нужно установить вручную. Так бывает, если вы подключили к системе принтер уже после установки локальной сети.

Разберем процесс ручной установки принтера. Установкой драйверов мы уже занимались, поэтому сразу перейдем к настройке свойств конкретного принтера.

Для разрешения общего доступа к принтеру достаточно войти в **Панель управления**, выбрать пункт **Принтеры и факсы**, после чего, увидев в этом окне нужный принтер, щелкнуть по нему правой кнопкой мыши, выбрать **Свойства**. В **Свойствах** принтера найдите вкладку **Доступ** и установите параметр **Общий доступ к данному принтеру**, если он еще не установлен (рис. 9.12).

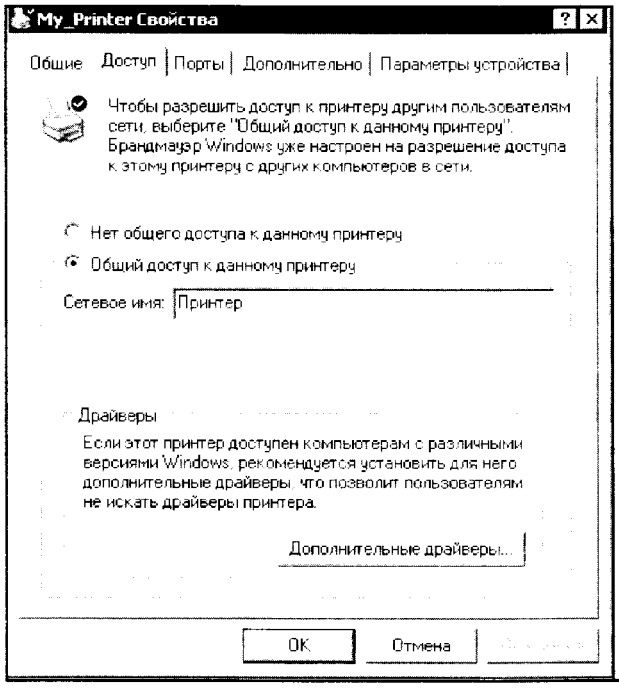


Рис. 9.12. Открытие общего доступа к принтеру

Иконка принтера, к которому разрешен общий доступ, снабжается характерным значком с изображением руки. Точно так же маркируются и другие общие ресурсы, например папки.

После того как локальный принтер стал общим, пришло время его установки на других компьютерах сети. Для этого надо точно так же, как и на том компьютере, который содержит принтер, перейти в папку **Принтеры и факсы** и, выбрав там ссылку **Установка принтера**, запустить **Мастер установки принтеров**.

Мастер задаст вам несколько вопросов. На вопросе о типе устанавливаемого принтера следует выбрать **Сетевой принтер**, а в появившемся после этого окне Мастера выбрать пункт **Обзор принтеров**. А вот в следующем окне (рис. 9.13) вам придется найти нужный принтер в вашей локальной сети и выбрать его.

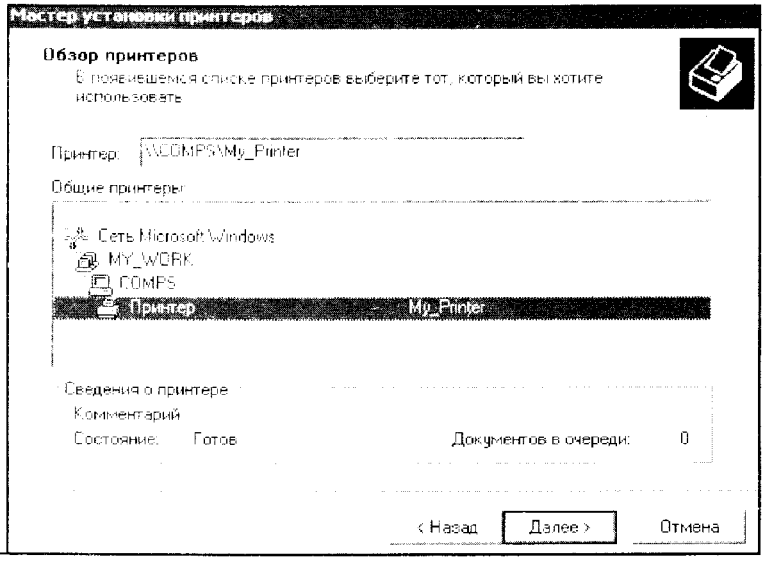


Рис. 9.13. Выбор нужного принтера

Выбрав принтер, остается нажать на **Далее** и ответить еще на несколько вопросов Мастера, ответы на которые, кстати, лучше всего оставить теми, что заданы по умолчанию.

Такую установку принтера следует провести на всех компьютерах сети. В результате вы получите сетевой принтер, на котором можно печатать с любого компьютера сети.

Помимо принтеров и стандартных папок, которые по умолчанию в Windows сделаны общими, вы можете самостоятельно задавать общие ресурсы сети, вплоть до общих жестких дисков. Но учтите: давая общий доступ к своему жесткому диску, вы «дарите» доступ к вашим данным всем, кто будет работать за любым компьютером локальной сети. Это справедливо для сети на Windows XP Home. В версии Professional можно гибко настраивать доступ разных пользователей к общим ресурсам.

Чтобы открыть общий доступ к папке или жесткому диску, следует щелкнуть правой кнопкой мыши по папке и в появившемся меню выбрать пункт **Свойства**. В окне свойств папки выберите вкладку **Доступ** (рис. 9.14).

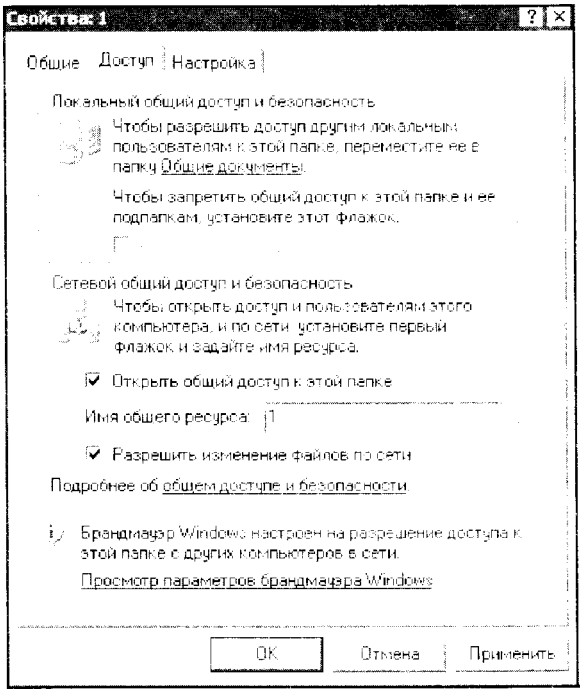


Рис. 9.14. Открытие общего доступа к папке

Напротив пункта **Открыть общий доступ к этой папке** поставьте галочку. Теперь другие пользователи сети смогут читать файлы, находящиеся в этой папке. Но записывать в нее они ничего не смогут. Не смогут они и удалять файлы из этой папки. А вот если вы установите еще и галочку **Разрешить изменение файлов по сети**, то вы дадите всем пользователям полную власть над файлами, находящимися в этой папке.

Вот, кажется и все. Сеть настроена, принтер печатает, файлами обмениваться можно. А как же общий доступ к Интернету? Этот вопрос вопросов. Выше я сознательно назначил сетевым адаптерам «неправильные» IP-адреса, чтобы мы на практике разобрались с некоторыми проблемами, которые могут возникать при ручной настройке общего подключения к Интернету.

9.3. РУЧНАЯ НАСТРОЙКА ОБЩЕГО ДОСТУПА К ИНТЕРНЕТУ

Общий доступ к Интернету в Windows XP осуществляется при помощи системы ICS, то есть Internet Connection Sharing. Использование ICS налагает некоторые ограничения на доступный диапазон IP-адресов сетевых адаптеров.

Выше я уже говорил о диапазоне IP-адресов 192.168.0.1–192.168.0.254 с маской подсети 255.255.255.0. Это диапазон, адреса из которого получают компьютеры, сконфигурированные для общего доступа к интернет-соединению с использованием ICS. При этом компьютеру, который имеет интернет-подключение, разделяемое между другими компьютерами, присваивается статический внутренний IP-адрес 192.168.0.1, а адреса других компьютеров могут быть сконфигурированы как автоматически, так и вручную.

Смысл настройки этих других компьютеров заключается в том, чтобы дать им неповторяющиеся IP-адреса из вышеуказанного диапазона. В качестве так называемого шлюза по умолчанию у них устанавливается 192.168.0.1. Если окажется, что ресурс, к которому нужно обратиться, лежит за пределами локальной сети, то запрос передается шлюзу по умолчанию, который «выводит» этот запрос в Интернет.

Для начала настроим компьютер, подключение которого мы хотим сделать общим. Для этого можно поступить так: войти в **Панель управления**, выбрать там значок **Сетевые подключения** и среди подключений выбрать то, общий доступ к которому вы хотите открыть.

Открыв окно его свойств в **Свойствах подключения**, выберите вкладку **Дополнительно**.

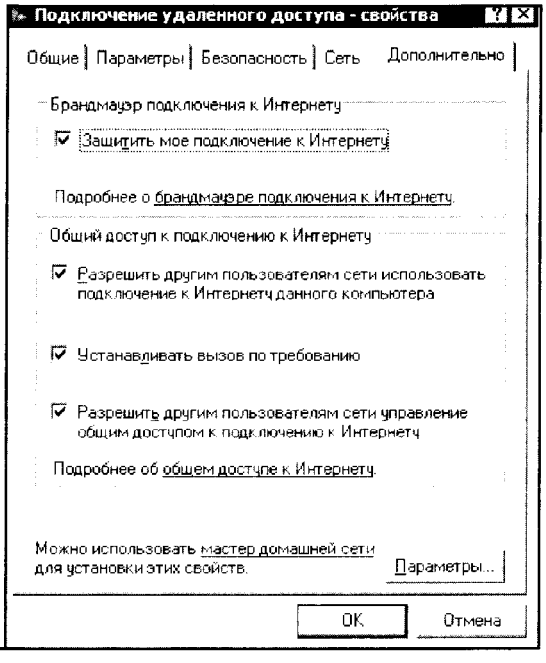


Рис. 9.15. Настройка подключения к Интернету

Обратите внимание на рис. 9.15. Экранная копия окна сделана с компьютера с установленной на нем Windows XP без SP2. В этом окне нужно отметить галочками все пункты и тем самым запустить ICS. Система

выдаст предупреждение о том, что компьютеру будет присвоен статический IP-адрес, а другие компьютеры надо сконфигурировать заново (рис. 9.16). При этом система утверждает, что их надо сконфигурировать автоматически.

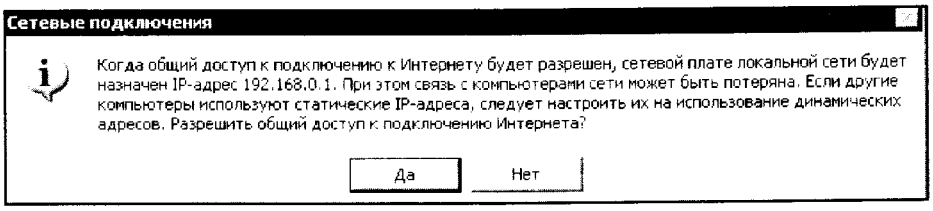


Рис. 9.16. Разрешение общего доступа к Интернету

Для автоматической конфигурации рабочих станций используется DHCP — *Dynamic Host Configuration Protocol*. У вас достаточно знаний, чтобы сконфигурировать клиентские компьютеры вручную, но лучше сэкономить собственный труд и предоставить это автоматике. К тому же автоматическая настройка ICS, особенно в достаточно большой сети, позволит избежать человеческих ошибок.

После того как дан утвердительный ответ на вопрос, заданный системой в окне на рис. 9.16, работа настроенной вручную сети будет нарушена. Помните, что за IP-адреса мы назначали ее компьютерам? У компьютеров, использующих ICS, адреса должны быть другими.

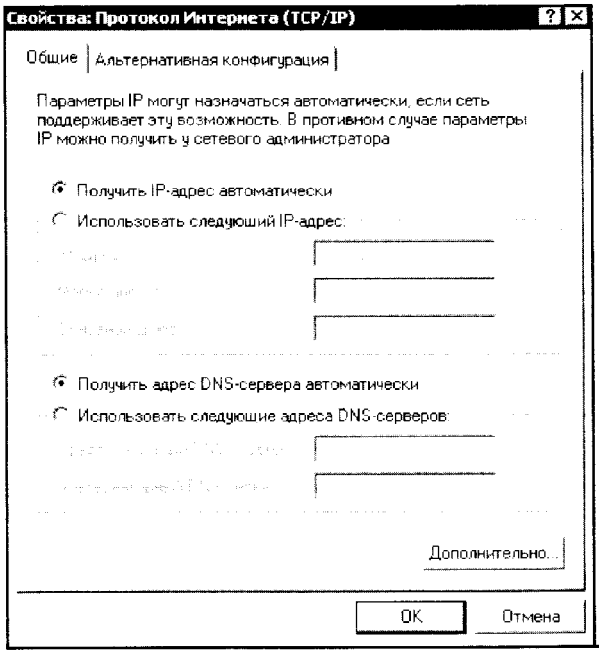


Рис. 9.17. Автоматическая настройка TCP/IP

Поэтому начнем настройку подключения на других компьютерах сети.

Перейдите в **Панель управления**, выберите **Сетевые подключения**, найдите среди сетевых подключений ваше подключение по локальной сети. Выбрав его свойства и найдя там свойства TCP/IP, установите автоматическое получение IP-адреса. Посмотрите на рис. 9.17: здесь изображено окно свойств TCP/IP после настройки.

Как уже было сказано, параметры TCP/IP можно настроить вручную. В качестве IP-адреса можно использовать любой адрес из диапазона 192.168.0.2–192.168.0.254, маска подсети будет 255.255.255.0, а в качестве шлюза по умолчанию 192.168.0.1. Но пусть за вас поработает автоматика.

После ручной или автоматической настройки TCP/IP сеть снова заработает. Но если попытаться подключиться к Интернету, ничего не получится! Для этого нужно настроить подключение к Интернету через локальную сеть. Сделать это просто.

Войдите в **Панель управления**, найдите **Свойства обозревателя** и откройте их. В появившемся окне выберите вкладку **Подключения** и нажмите кнопку **Установить**. После этого появится знакомое окно **Мастера подключения к Интернету**. Мы уже рассматривали работу этого Мастера весьма подробно, поэтому остановимся лишь на ключевых моментах процесса.

В окне **Тип сетевого подключения** оставьте переключатель в положении **Подключение к Интернету**. В следующем окне Мастера надо выбрать **Установить подключение вручную**, а дальше на вопрос о том, каким образом подключиться к Интернету, выберите пункт **Через постоянное высокоскоростное подключение** (рис. 9.18).

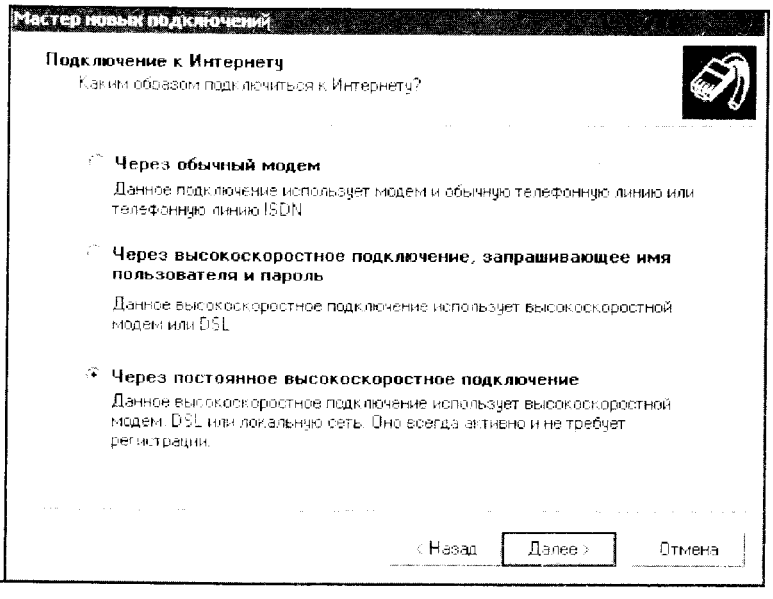


Рис. 9.18. Выбор способа подключения к Интернету

После этого никаких важных вопросов уже не будет, и в конце концов вы попадете на финальную страничку Мастера, а общее подключение к Интернету будет сконфигурировано автоматически.

Сравним конфигурацию сетевых адаптеров главного компьютера, предоставляющего свое подключение другим компьютерам, и компьютера, который пользуется этим подключением. Посмотрите на рис. 9.19. Здесь изображено окно свойств подключения по локальной сети главного компьютера (это компьютер без установленного SP2).

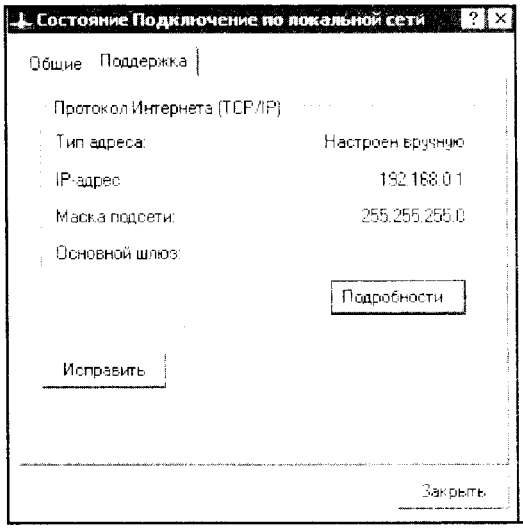


Рис. 9.19. Окно состояния подключения главного компьютера

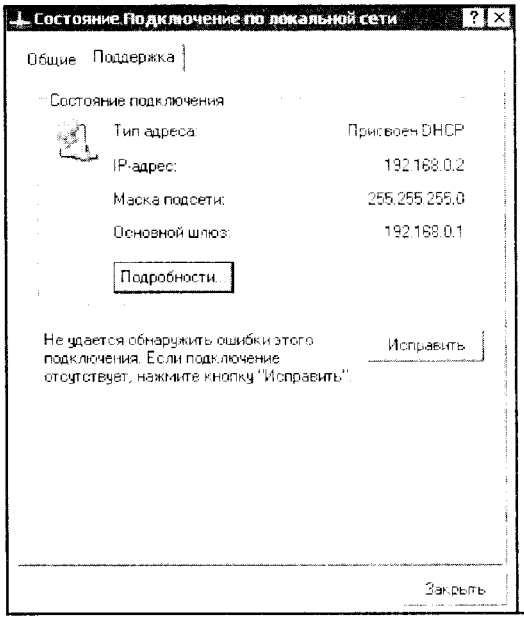


Рис. 9.20. Состояние подключения на компьютере сети

А вот (рис. 9.20) окно состояния подключения одного из других компьютеров сети.

Думаю, комментарии здесь излишни. Все настроено так, как и нужно.

Но не всегда и не все проходит гладко. Поэтому дальше мы займемся рассмотрением, диагностикой и устранением некоторых характерных проблем, возникающих в локальной сети.

Начнем с рассмотрения компонентов ICS, которые применяются для установки подключения к Интернету в Windows XP. Ведь, проверяя общее подключение к Интернету, мы таким образом проверим практически все, что имеет отношение к нашей проводной локальной сети.

9.4. ПРОБЛЕМЫ И РЕШЕНИЯ

В работе ICS участвует часть системы, которая отвечает за соединение с Интернетом на главном компьютере. Если выход в Интернет с других компьютеров сети невозможен, проверьте главный компьютер, и если с него не удается выйти в Интернет, то первый подозреваемый — это подключение к Интернету.

Перечислю некоторые типичные проблемы, связанные с нарушениями подключения к Интернету. В первую очередь интернет-подключение зависит от модема. С него мы и начнем — вернее, с проверки физического соединения модема и телефонной линии.

ПРОВЕРКА РАБОТЫ МОДЕМА

Если на локальном компьютере нет интернет-соединения, обратите внимание на системные сообщения, которые выдаются в процессе попытки подключения.

Вот последовательность ваших действий по проверке соединения.

1. Убедитесь, что телефонный провод надежно соединен с модемом вашего компьютера и с телефонной розеткой. Попробуйте вытащить и снова вставить кабель, соединяющий модем и телефонную розетку. Лучше сделать это с обоими концами кабеля: «дребезжание» контактов телефонной розетки — явление редкое, но реальное.

2. Если вы используете параллельное подключение телефона и модема, убедитесь, что в момент подключения трубка параллельного телефона не снята. Кстати, параллельное подключение телефона к модемной линии крайне нежелательно: характеристики такой линии хуже, и к тому же, если кто-нибудь поднимет трубку в момент, когда вы будете в Сети, соединение может разорваться или нарушиться. Такой телефон лучше всего подключать к линии через соответствующий разъем на модеме.

3. Если физическое подключение в порядке, а соединения все равно нет (например, при подключении выдается сообщение о том, что в линии отсутствует гудок), проверьте, есть ли гудок. Редко, но бывает, что связи нет по какой-то внешней причине — от обрыва провода до ремонтных работ на вашей телефонной линии.

4. Гудок есть, линия исправна, никто не пытается разговаривать по телефону, а соединение все равно установить не удается. Проверьте, работает ли модем. Проверку работы модема мы уже обсуждали, но напомню ваши основные действия: найдите модем в **Диспетчере устройств**, откройте его **Свойства** и, перейдя во вкладку, посвященную **Диагностике**, опросите модем. Если опрос прошел успешно, значит, система, по крайней мере, видит модем и может с ним общаться. Что же происходит? По всей видимости, на модем приходит вызов, а потом начинаются странности. Значит, проблему надо искать в настройках соединения.

5. Модем звонит провайдеру, а соединения не происходит. Для начала проверьте номер телефона, набираемого модемом. Очень может быть, что, указывая телефон провайдера, вы что-нибудь напутали или забыли убрать код страны или города. Если все в порядке, то проверьте, а лучше внимательно введите заново ваше имя и пароль доступа к провайдеру. Возможно, мешает случайная ошибка, допущенная при их вводе.

Если вы внимательно проверили все, что описано выше, и если дело не в проблемах провайдера, то вы просто не можете не подключиться к Интернету, используя модем.

Итак, с главного компьютера выход в Интернет осуществляется, а с других компьютеров сети — нет. Что делать? Для начала проверьте локальную сеть. Если окажется, что вы не можете обращаться к общим ресурсам других компьютеров через **Сетевое окружение**, следует поискать неисправность сети аналогично поиску неисправности в модемном соединении.

1. Начните с проверки физической части сети: проверьте, не поврежден ли сетевой кабель, включен ли хаб, все ли сетевые кабели вставлены в разъемы. Как правило, на хабах и сетевых картах есть светодиоды, сигнализирующие о том, что устройства обмениваются данными. Проследите, чтобы они горели.

2. Если с физической частью сети все в порядке, попробуйте еще раз обратиться к нужному компьютеру через **Сетевое окружение**.

Приведу один пример очень странной на первый взгляд неисправности, на котором мы рассмотрим некоторые секреты сетевой диагностики. Однажды мне пришлось столкнуться с удивительной проблемой. Физическая часть сети работала нормально, компьютеры видели друг друга в **Сетевом окружении** Windows XP, один из них мог обращаться к ресурсам другого, но этот другой не мог получить доступ к ресурсам первого. Еще не понимая, в чем дело, но уже кое-что заподозрив, я решил проверить сеть при помощи утилиты `Ping`. При помощи этой ко-

манды можно проверять сетевые соединения. Чтобы воспользоваться этой командой, нужно выбрать **Пуск ▸ Выполнить**, а в появившемся окне **Запуск программы** ввести команду `cmd` (рис. 9.21).

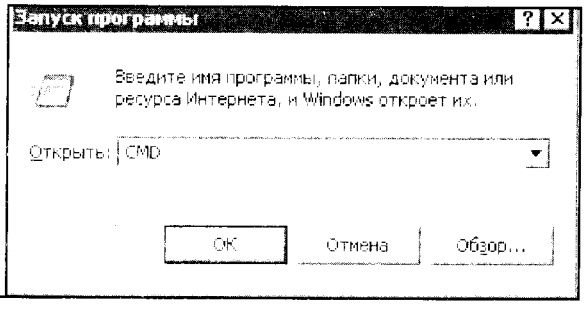


Рис. 9.21. Запуск программы

После этого появится окно командного интерпретатора, которое очень похоже на старый добрый DOS. В этом окне нужно ввести команду `Ping xxx.xxx.xxx.xxx`, где `xxx.xxx.xxx.xxx` — это IP-адрес машины, до которой вы хотите «достучаться». (То, как узнать IP-адрес, присвоенный сетевому адаптеру, мы уже обсуждали выше.)

Итак, узнав IP-адрес интересующего вас компьютера (в моем случае это был 192.168.0.2), вы вызываете эмулятор DOS и в появившемся окне пишете команду `Ping` с вашим адресом.

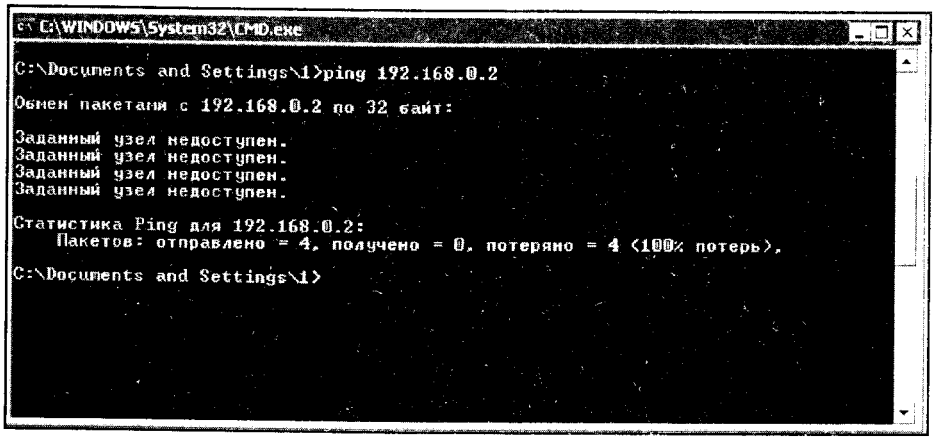


Рис. 9.22. Сообщение об ошибке обмена данными

Если вы хотите узнать о параметрах запуска `Ping` — запустите ее с параметром `/?`, то есть напечатайте такую строчку в ответ на приглашение операционной системы: `ping /?`. Вы получите объемистую справку по работе с этой командой.

После выполнения команды `ping` вы получаете сообщение об ошибке (рис. 9.22).

Такое сообщение об ошибке система выдает в случае, если ваш компьютер просто не подключен к сети. Что же, еще раз проверьте подключение. Такое же сообщение выдается, если что-то не в порядке с IP-адресами. Проверьте, принадлежат ли оба компьютера одной подсети.

А вот такое сообщение (рис. 9.23) вы получите в случае, если сеть работает, ваш компьютер к ней подключен, но что-то стряслось с компьютером, который мы пытаемся пропинговать.

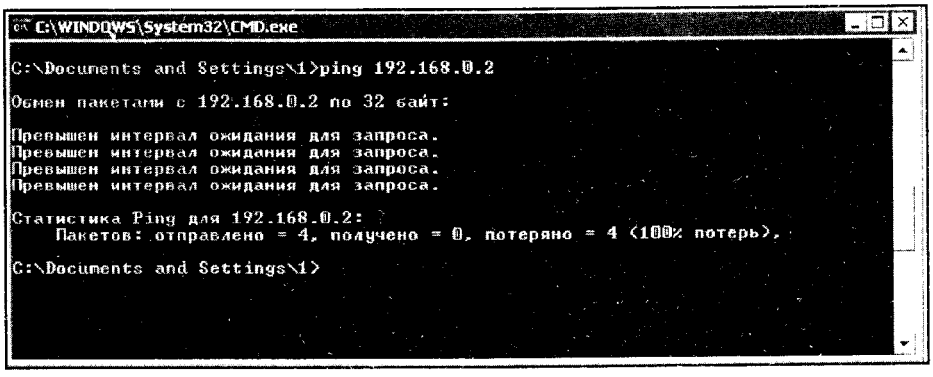


Рис. 9.23. Сообщение об ошибке обмена данными

Вернемся к моему рассказу. Самое интересное было вот что: с главного компьютера (IP 192.168.0.1) другой компьютер (IP 192.168.0.2) был недоступен, а вот с другого компьютера главный компьютер был очень даже хорошо доступен (рис. 9.24).

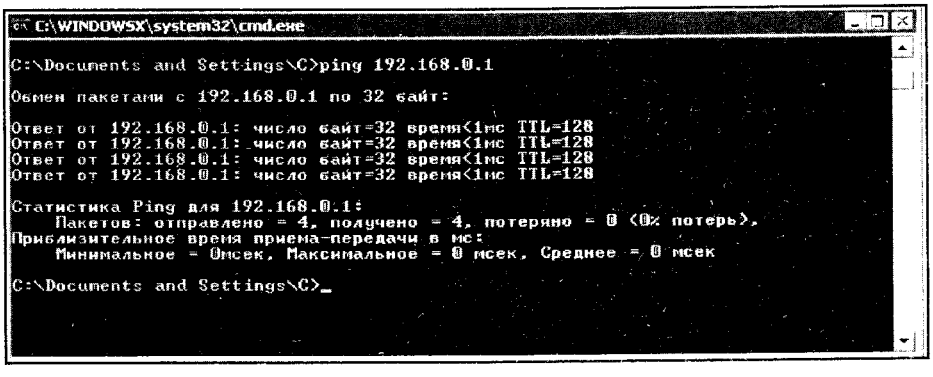


Рис. 9.24. Успешный обмен данными

Казалось, что попахивает нечистой силой, но на самом деле ситуация была вполне объяснима и предсказуема. Особенно ясна она стала после

того, как я повнимательней пригляделся к системной панели Windows. Там вольготно расположился неправильно настроенный файрволл, который позволял одному из компьютеров видеть другие, а вот данные с других компьютеров на него не пропускал.

Я не стал тратить время, просто сбросил настройки файрволла и открыл доступ системным программам. Вспомните, что в самом начале кчиги я предупреждал вас о необходимости быть осторожным с установкой файрволлов и антивирусов в сетях, чьим хозяином являетесь не вы.

Если `ping` с обеих машин вам удался, значит, по меньшей мере IP и сетевое оборудование у вас настроены правильно.

А теперь продолжим наши попытки заставить работать ICS.

3. Если физические соединения в порядке, надо проверить логику сети. Во-первых, убедитесь, что главный компьютер сети имеет адрес 192.168.0.1. Как вы помните, здесь вариантов быть не может.

4. Проверьте IP-адреса других компьютеров сети. Эти адреса должны относиться к подсети 192.168.0. Если адреса другие, то или включайте автоматическое назначение адреса, или попытайтесь назначить его вручную.

5. Если ICS все еще не хочет работать, запустите Мастер подключения к Интернету на других компьютерах сети и попробуйте подключиться к Интернету через вашу локальную сеть еще раз: возможно, в процессе установки подключения что-то пошло не так.

6. Если и после этого ваша деятельность не принесла положительных результатов, то вот мой вам совет: сделайте перерыв на несколько часов. Отойдите от компьютера, займитесь чем-нибудь посторонним, а ваше подсознание пусть анализирует собранную вами информацию. Когда информация проанализирована и разложена по полочкам, попробуйте настроить ICS еще раз. Уверен, если его вообще можно настроить на вашем компьютере, то у вас все получится.

В самых тяжелых случаях неработающий ICS и другие подобные программы легче и быстрее всего призвать к порядку при помощи чистой переустановки системы. Однако это крайняя мера, к которой следует прибегать лишь в том случае, если больше ничего не помогает. Хотя, честно говоря, лучше переустановить систему и работать «с чистого листа», чем мучиться с тем, что осталось «в наследство» от старых ошибок.

9.5. ВЫВОДЫ

С проводными сетями мы разобрались: теперь вы умеете их настраивать, диагностировать, устранять неисправности и при этом понимать, что вы делаете и зачем.

ГЛАВА 10
БЕСПРОВОДНЫЕ И НЕТРАДИЦИОННЫЕ СЕТИ

Беспроводные решения становятся все более привлекательными для создания домашних и офисных сетей. Мы уже обсуждали подробности выбора и подключения беспроводных сетевых адаптеров, устанавливали их драйверы, а теперь осталось лишь настроить беспроводную локальную сеть. В этой главе мы поговорим и о «нетрадиционных» сетях, то есть о создании локальных сетей из «подручного материала». В качестве такового выступят FireWire-адаптеры и телефонные линии.

Сети можно строить и на USB, и на параллельных и последовательных портах. По правде говоря, эти способы не кажутся нужными в современных условиях. Кстати, «народные умельцы» строят локальные сети на основе оптических средств связи — и все у них работает! Но мы не станем касаться вопросов построения таких «самодельных» сетей: для их создания нужен паяльник — и специальные знания, без которых за паяльник лучше не браться, а эта тема выходит за рамки нашей книги.

Сети эволюционируют «в беспроводную сторону». Очень возможно, что скоро начнется массовая замена проводов, которые соединяют наши компьютеры с периферийными устройствами, на невидимые и неосязаемые радиоволны. Если на рабочем столе прочно поселился спутанный клубок проводов и кабелей, то вряд ли вам нужно объяснять выгоды беспроводных технологий.

10.1. НОВШЕСТВА WINDOWS XP SP2

В операционной системе Windows XP SP2 есть особое средство для конфигурирования беспроводных сетей. Но оно не предназначено для настройки сетей между компьютерами, не использующими точку доступа. Этим полезность нового средства Windows XP для настройки локальных беспроводных сетей вовсе не уменьшается. И все же, несмотря на нововведение, которое называется Мастер беспроводных сетей, простую сеть между парой-тройкой компьютеров нам все равно придется настраивать вручную. Это довольно просто, если вы точно знаете, что и как делать, и очень сложно, если вы не дочитали предыдущих глав.

Я вспоминаю свое знакомство с настройкой беспроводных локальных сетей. Привыкнув к проводам, я не чувствовал (вернее, не хотел чувствовать) различия в настройке проводных и беспроводных сетей. И, попытавшись «навскидку» настроить беспроводную сеть между парой машин, обнаружил кучу новых параметров, окошек, настроек, всяких SSID и подобных штук. С первого раза у меня ничего не получилось! Обеспокоенный таким поворотом дел, я решил подучить теорию, и в результате сеть настроилась быстро и просто.

Настройка Wi-Fi на КПК — это простая, даже предельно простая процедура. Но и тут не обойтись без знания некоторых специфических понятий.

К технологиям, которые могут помочь в организации беспроводной сети, можно отнести Bluetooth. Правда, пока эта технология распространена куда меньше, чем Wi-Fi.

Начнем наш рассказ с описания работы того самого нового средства SP2, которое называется Мастер беспроводной сети, а продолжим ручной настройкой простой сети, не использующей точки доступа.

10.2. АВТОМАТИЧЕСКАЯ НАСТРОЙКА БЕСПРОВОДНОЙ СЕТИ

Мастер беспроводной сети можно запустить из **Панели управления**, отыскав его значок в списке типичных задач папки **Сетевое окружение**. Напомню, что этот мастер предназначен лишь для настройки сетей, исполь-

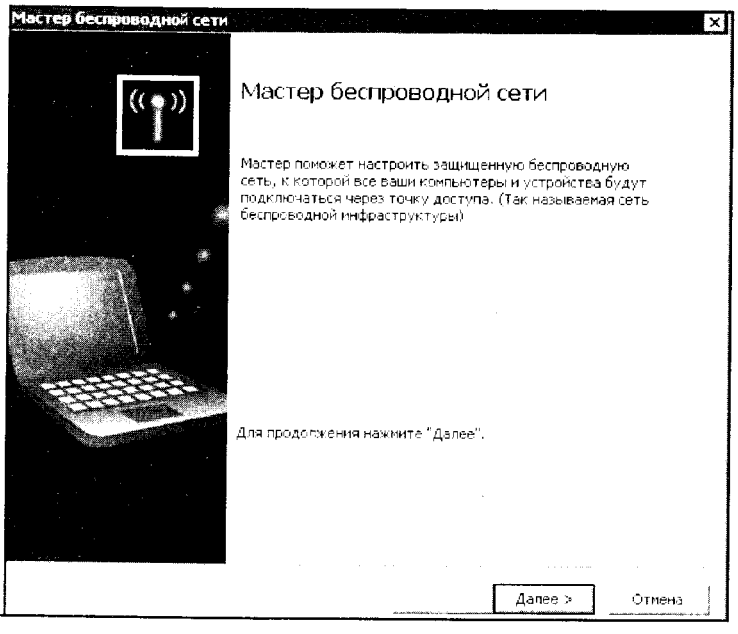


Рис. 10.1. Мастер беспроводной сети

зующих точку доступа. Посмотрите на рис. 10.1: так выглядит первое окно Мастера.

Нажав знакомую кнопку **Далее**, мы попадаем в окошко, не имеющее аналогов в настройке проводного подключения.

В этом окне (рис. 10.2) надо назначить так называемый SSID — это идентификатор беспроводной сети, используя который, к вашей сети будут подключаться другие компьютеры.

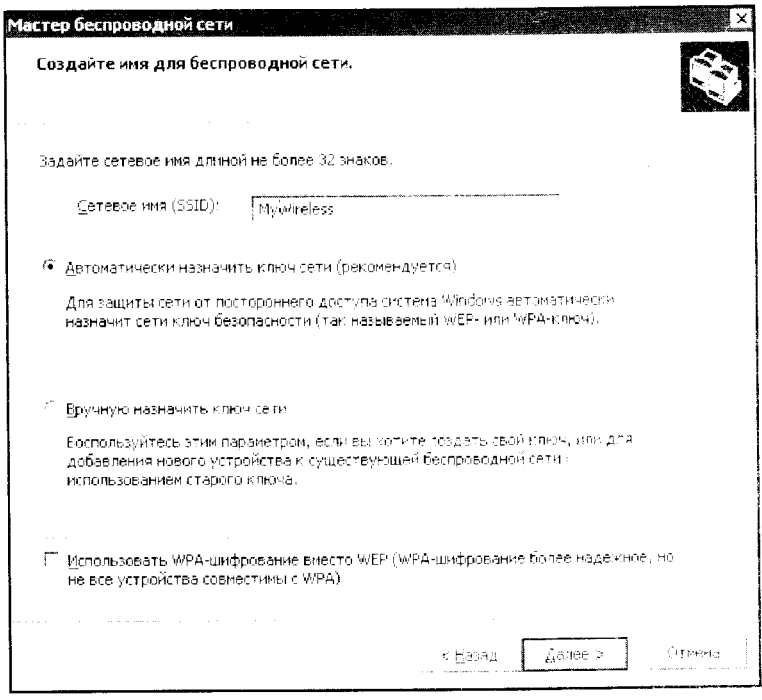


Рис. 10.2. Настройка параметров беспроводной сети

В данном случае в качестве имени соединения я назначил **MyWireless**.

В этом же окне следует выбрать способ задания ключа сети. Ключ сети — это нечто вроде пароля для доступа сети, а SSID по функциям очень похож на «имя пользователя». Желательно оставить значение этого параметра по умолчанию, то есть предоставить системе самой выбирать ключ сети. Уж она-то постарается, выберет отличный ключ.

В самом низу окна настройки параметров сети можно увидеть место для галочки, с помощью которой можно включить WPA-шифрование, которое надежнее, чем WEP-шифрование, применяемое по умолчанию.

С шифрованием WPA совместимы не все устройства.

Вопрос шифрования информации в сетях Wi-Fi — не то чтобы открытый, но в известной степени противоречивый. Дело в том, что применение шифрования снижает пропускную способность и без того не самой быстрой на сегодняшний день технологии передачи данных. Правда, нельзя назвать шифрование проблемой: с одной стороны, если вам нужны скорости повыше, чем те, что обеспечивает стандарт 802.11b (11 Мбит/с), то это повод задуматься над переходом на оборудование 802.11g (52 Мбит/с), благо, цена на него не слишком высока. А можно и вообще отказаться от беспроводных технологий и перевести свои компьютеры на 100 Мбит/с Ethernet-сеть на основе кабелей.

Но вернемся к нашему ключу сети. Если вы не хотите, чтобы система назначала его сама, выберите пункт **Вручную назначить ключ сети**. Тогда, нажав кнопку **Далее**, вы попадете на окно ввода ключа. Не скупитесь на длину этого ключа и не делайте его слишком простым. Почему-то практически все пользователи ПК считают, что их информация никому не нужна, а если им начинаешь рассказывать о хакерах и вирусах, они лишь усмехаются и говорят: «У меня красть нечего». На деле же у всех есть «чего красть», поэтому надо не уменьшать уровень защиты своей системы, а повышать его.

После того как вы ввели свой ключ сети, наступает финальная стадия настройки беспроводной сети на вашем компьютере. Она тоже предусматривает некоторые варианты выбора дальнейших действий. Заключаются эти варианты в том, каким образом будут настроены другие компьютеры сети.

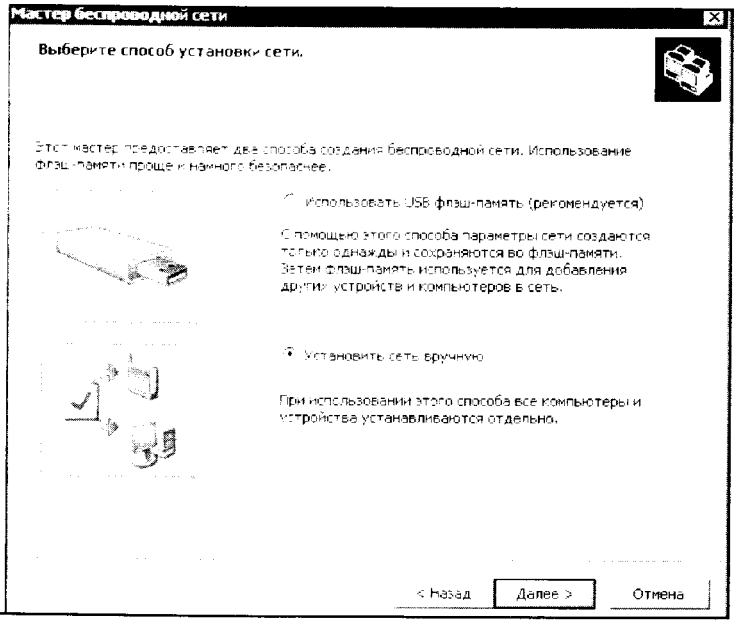


Рис. 10.3. Продолжение настройки беспроводной сети

На рис. 10.3 изображено окно с вариантами настройки.

Первый метод наиболее удобен и предпочтителен. Он заключается в том, что к USB-порту компьютера, на котором запущен Мастер, вы подключаете USB-flash-брелок, а затем идете с этим брелоком к точке доступа.

Если точка доступа не поддерживает ввод информации с подобного носителя, вам придется конфигурировать ее вручную.

После настройки точки доступа вы должны обойти с этим брелоком все компьютеры, которые хотите подключить к сети, а потом вернуться к тому компьютеру, на котором вы начинали установку. Там вы снова подключите брелок к USB-порту этого компьютера, после чего для надежности можно удалить информацию с брелка и распечатать конфигурационную информацию. Учтите, что, если эта информация попадет в чужие руки, безопасность вашей сети окажется под угрозой.

Но если выбрать в окне, которое изображено на рис. 10.3, ручную установку, некоторые параметры в компьютеры придется вводить вручную. На рис. 10.4 изображено окно, которое появляется после выбора ручной установки параметров сети.

Обратите внимание на кнопку **Напечатать параметры сети**. Без этих параметров вы просто не справитесь с установкой, поэтому обязательно нажмите на эту кнопку. У вас получится распечатка, похожая на ту, что приведена в листинге 10.1. В соответствии с этой распечаткой вы сможете настроить остальные компьютеры сети.

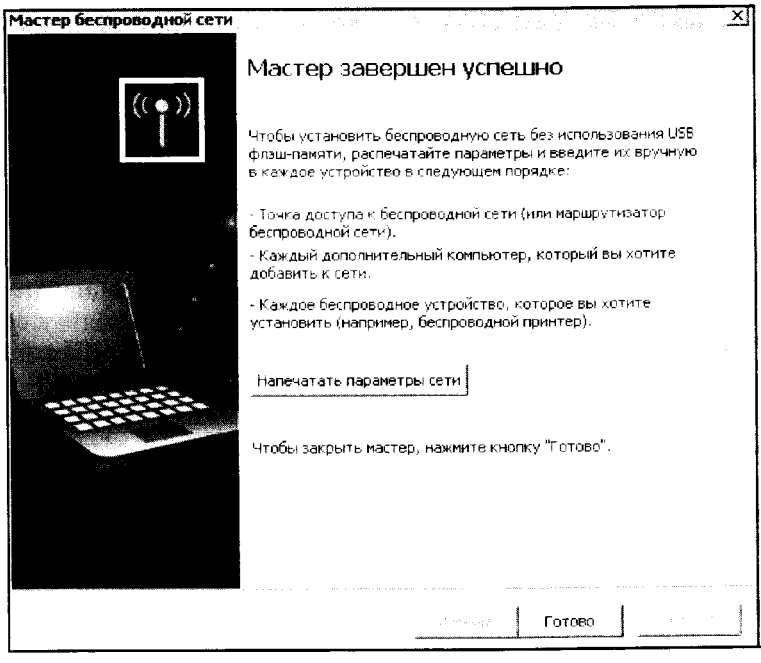


Рис. 10.4. Ручная установка параметров сети

```
Параметры беспроводной сети
Распечатайте этот документ и сохраните его в надежном месте для использования в будущем. Эти параметры могут понадобиться при добавлении дополнительных компьютеров и устройств к сети.
Параметры беспроводной сети
Сетевое имя (SSID): MyWireless
Ключ сети (WEP/WPA-ключ): 2f6cf34f73dd42d5a6add992d2
Автоматически предоставленный ключ (802.1x): 0
Тип проверки подлинности сети: open
Тип шифрования данных: WEP
Тип подключения: ESS
Индекс ключа:
Чтобы включить общий доступ к файлам и принтерам на этом компьютере, запустите мастер настройки сети.
Чтобы настроить подключение к Интернету, следуйте указаниям поставщика услуг Интернета (ISP).
```

Листинг 10.1. Параметры беспроводной сети

В этом тексте есть несколько ключевых строчек. Важнее всего пара параметров **Сетевое имя (SSID)** и **Ключ сети (WEP/WPA ключ)**. Также обратите внимание на **Тип проверки подлинности сети**, **Тип шифрования** и **Тип подключения**. Эти параметры надо будет ввести при настройке каждого из компьютеров и точки доступа.

10.3. НАСТРОЙКА БЕСПРОВОДНОЙ СЕТИ AD HOC

Перед началом рассказа об установке простой беспроводной сети напомню, что в качестве сетевого оборудования в наших примерах используются беспроводной адаптер ASUS WL-161, работающий в стандарте 802.11b и подключенный к настольному компьютеру, а также ноутбук со встроенной беспроводной сетевой картой Agere Wireless Mini PCI card стандарта 802.11b.

Здесь мы рассмотрим процесс создания беспроводной сети. Здесь же будет рассказано о подключении ноутбука к Интернету через общее соединение с Интернетом, предоставляемое настольным компьютером и выполненное с помощью уже знакомого вам ICS.

Для начала нужно создать беспроводную сеть. Для ее создания войдите в **Панель управления**, найдите значок **Сетевые подключения** и щелкните по нему дважды. Затем найдите в открывшемся списке соединений беспроводное соединение и, щелкнув по нему правой кноп-

кой мыши, выберите **Свойства**. В появившемся окне свойств выберите вкладку **Беспроводные сети**, после чего нажмите кнопку **Добавить**. Появится окно создания новой беспроводной сети (рис. 10.5).

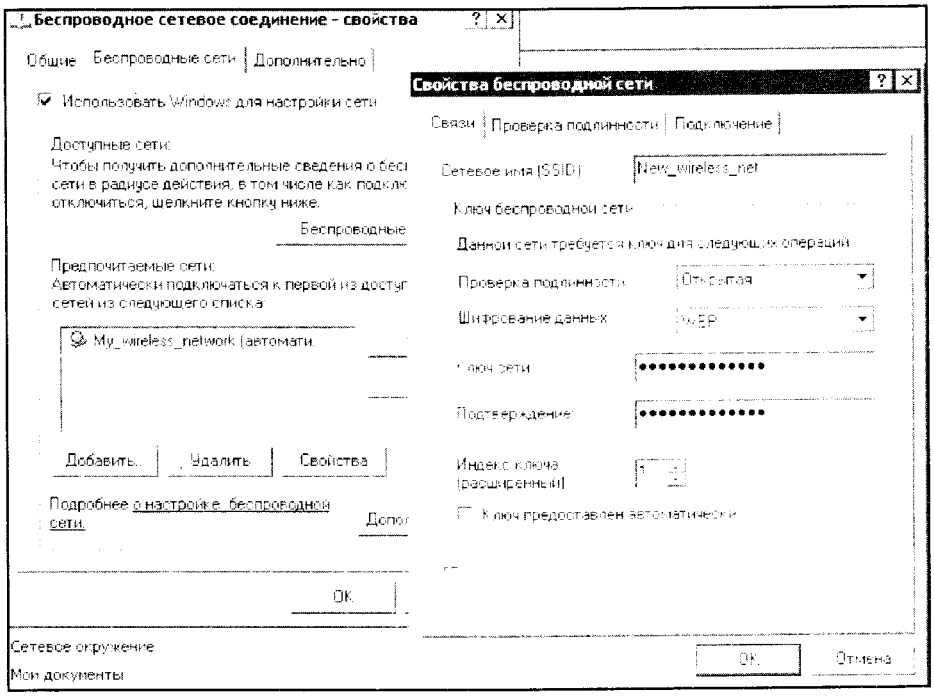


Рис. 10.5. Создание новой беспроводной сети

В это окно нужно ввести идентификатор сети SSID. При этом крайне желательно использовать при его создании лишь латинские символы. Также желательно убрать галочку напротив пункта **Ключ предоставлен автоматически**, после чего в поле **Ключ сети** ввести собственный ключ. Ключ, как вы понимаете, — это нечто вроде пароля для подключения к сети. Существуют определенные ограничения на его длину. **Рекомендуется делать ключи длиной в 5 или 13 символов.** Именно 5 или 13 — иначе система выдаст сообщение об ошибке. В нашем случае я использовал 13 — символьный ключ сети.

Иногда можно слышать разговоры о том, что WEP-шифрование для домашней сети — это ненужная роскошь. А порой даже предлагают отказаться не только от шифрования, но и от пароля, сделав подключение новых компьютеров к вашей сети предельно простым. Используя шифрование, мы действительно снижаем полезную пропускную способность сети, но от паролей нельзя отказываться ни при каких условиях. Я не рекомендую убирать флажок **Шифрование данных (WEP)**: если это сделать, ваша сеть окажется практически незащищенной.

Продолжая первоначальную настройку Wi-Fi, на вкладке **Беспроводные сети** окна свойств сетевого адаптера нажмите кнопку **Дополнительно** (рис. 10.6) и выберите в появившемся окошке пункт **Сеть компьютер — компьютер только (произв)**. Так вы сможете создавать сети, которые соединяют отдельные компьютеры без использования точки доступа.

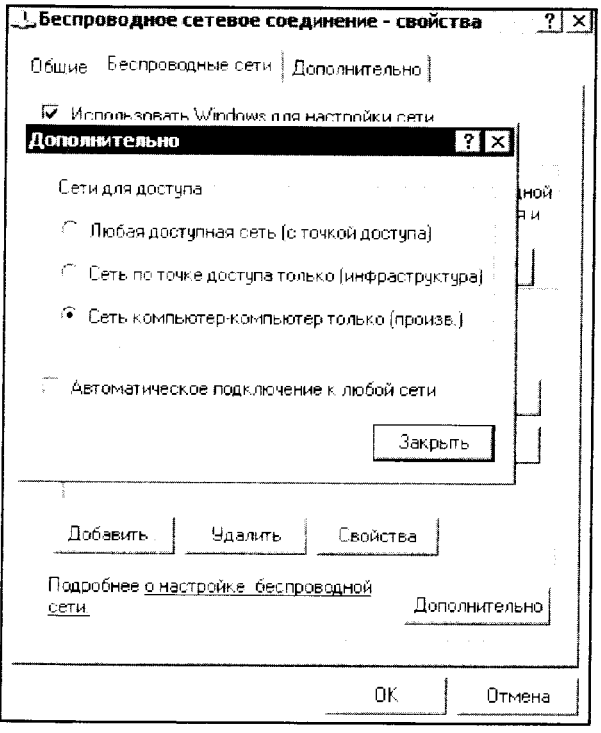


Рис. 10.6. Настройка дополнительных свойств беспроводных сетей

Теперь следует сделать то же самое на других компьютерах сети: для этого мы просто включаем опцию **Сеть компьютер — компьютер только (произв.)**.

Теперь, когда этот параметр настроен, нужно подключить компьютеры к беспроводной сети, созданной на одном из них.

В нашем случае беспроводная сеть New_wireless_net была создана на настольном компьютере. Значит, на ноутбуке нужно сделать щелчок правой кнопкой мыши по значку беспроводного соединения в системной панели Windows и выбрать там пункт **Просмотр доступных беспроводных сетей**. В появившемся окне будет видна сеть, которую вы только что создали. Если вы ее не видите сразу, нажмите на кнопку **Обновить список сети** в левой части окна.

Увидев наименование сети и информацию о нужной сети, нажмите на кнопку **Подключить**, которая находится в нижней части окна. Тут же появится запрос на ввод ключа сети (рис. 10.7). Введите ключ. После этого система подключит вас к беспроводной сети.

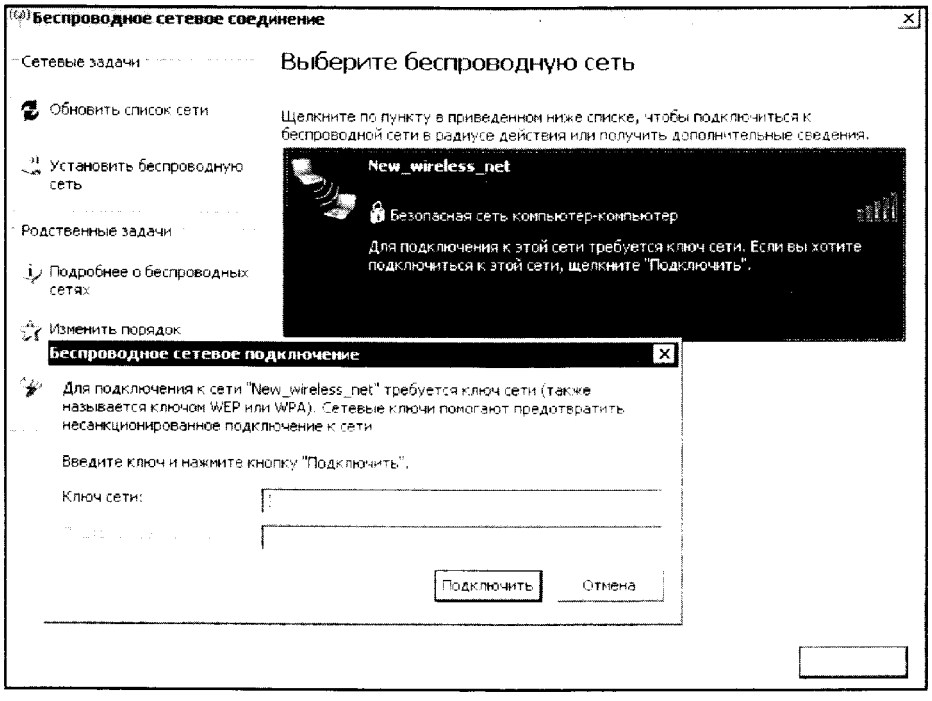


Рис. 10.7. Подключение к беспроводной сети

На всякий случай проверьте, подключен ли к ней компьютер, с которого создавалась эта сеть. Однажды сеть, которую я создавал, отказывалась работать, пока я не нажал на кнопку **Подключить** в окне управления подключениями к беспроводным сетям. Это особенно важно для Windows XP SP1. В операционной системе Windows XP SP2 подключение к собственной сети происходит автоматически, но на всякий случай лучше проверить это.

Теперь настало время запустить программу Мастер настройки сети на настольном ПК, то есть на том компьютере, через который вы собираетесь выводить в Интернет другие машины. Отвечайте на его вопросы нажатием кнопки **Далее**, пока он не спросит вас о способе подключения к Интернету. Это принципиально важный момент установки сети (рис. 10.8): здесь надо выбрать пункт **Этот компьютер имеет прямое подключение к Интернету**.

Затем Мастер спросит о том, через какое соединение осуществляется выход в Интернет. Среди предложенных соединений выберите **Интернет-соединение** (в нашем случае это модем). Дальше Мастер задаст вопрос о сетевых подключениях — здесь нужно выбрать адаптер беспроводной сети. На вопрос об именах компьютеров и об имени рабочей группы можете ответить нажатием кнопки **Далее** — установок по умолчанию достаточно, чтобы сеть заработала. Напомню, что компьютеры

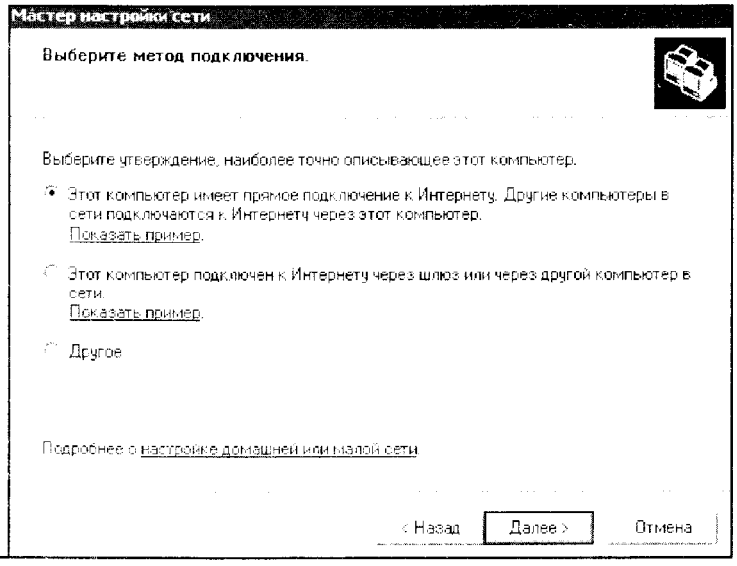


Рис. 10.8. Работа с Мастером настройки сети — компьютер, подключенный к Интернету

одной и той же сети должны иметь одинаковое имя рабочей группы и разные имена.

Закончив с этим этапом настройки сети на настольном ПК, переходим к ноутбуку.

На ноутбуке точно так же, как и на настольном ПК, запустите Мастер настройки сети. Там, где Мастер спросит нас о подключении к Интернету (рис. 10.9), выберите пункт **Этот компьютер подключен к Интернету через другой компьютер сети или шлюз**, а все остальное оставьте по умолчанию.

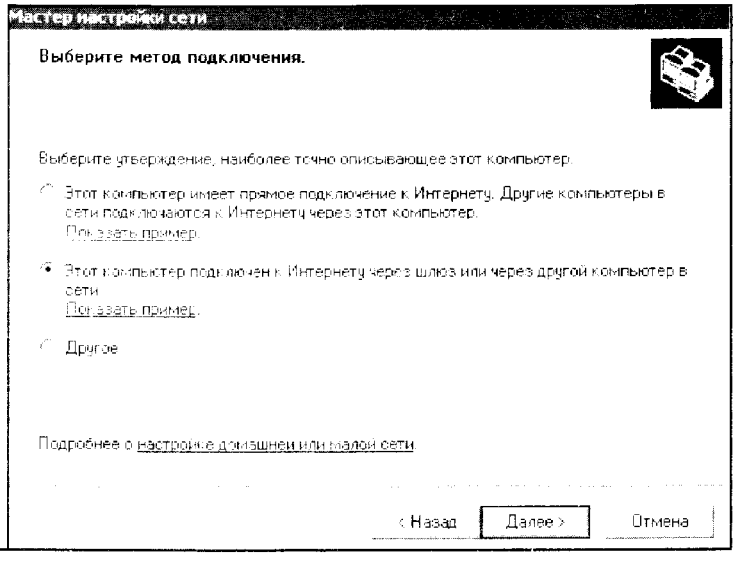


Рис. 10.9. Работа с Мастером настройки сети: компьютер, не подключенный к Интернету

Вот и все. На всякий случай можно проконтролировать настройку общего доступа к интернет-соединению на настольном ПК и на ноутбуке. Как это сделать, описано в одной из предыдущих глав.

Что, если ваша сеть не заработает? Прежде всего проверьте настройку TCP/IP. Напомню, что все компьютеры сети должны принадлежать одной и той же подсети, но иметь разные адреса в пределах этой сети.

Теперь запустите на ноутбуке Internet Explorer и введите любой URL, наблюдая при этом за поведением настольного компьютера. Если все сделано правильно, настольный ПК начнет набирать номер провайдера и «выпустит» ваш ноутбук в Сеть.

Теперь, когда Wi-Fi сеть установлена и работает, пришло время поговорить о безопасности беспроводных сетей. Это очень, очень важный вопрос.

10.4. WI-FI СЕТИ — ЗАЩИТА И ИССЛЕДОВАНИЯ

Что или кто может угрожать вашей Wi-Fi сети? Что вам грозит, если ваша локальная сеть охватывает вашу квартиру, квартиры соседей и большую часть близлежащей улицы? Если в радиусе охвата вашей сети нет тех, кто возомнил себя хакером, то, строго говоря, ничего. Ну а если есть, то такой «хакер» может перехватить передаваемые по сети данные, узнать ключ сети и, воспользовавшись специальным софтом, скрытно к ней подключиться, пользоваться вашим доступом в Интернет, почитать вашу переписку, удалить что-нибудь с вашего жесткого диска или, потихоньку скопировав все, что нужно, попытаться вас скомпрометировать.

Конечно, вышеперечисленный список включает все возможные варианты нападения на вашу беспроводную сеть. Бывает всякое. Лучше заранее узнать побольше о том, как оценить физическую безопасность своей сети, и постараться повысить эту самую безопасность. Иначе рано или поздно придется раскаяться в своей беззаботности.

Для начала запасемся программным обеспечением, которое поможет этому делу. Это самое что ни на есть хакерское ПО, с помощью которого злоумышленники (или просто любопытные) могут попытаться атаковать вашу локальную беспроводную сеть. Такое программное обеспечение делится на несколько видов. Деление это довольно условное, но, однако же, позволяет получить довольно полное представление о том, что технически оснащенный «любопытный» может сделать с чужими сетями.

Для начала рассмотрим всяческие варианты так называемых снифферов. Русское слово «сниффер» — это прямая транскрипция английского «*sniffer*». Это слово переводится примерно как «нюхач», «любитель вынюхивать». Сниффер — это программа, которая занимается перехватом всех пакетов данных, проходящих через сетевую карту компьютера,

на котором она запущена. Такие снифферы существуют как для проводных, так и для беспроводных сетей.

Как бы вы ни шифровали трафик беспроводной сети, он все равно будет передаваться (хоть и в зашифрованном виде) на приличное расстояние от местонахождения своего физического адресата. Ведь физический уровень беспроводной сети остается одним и тем же. А это значит, что перехват пакетов, пусть зашифрованных, вполне реален.

Я понимаю, что когда разговор заходит о хакерах, перехватах пакетов из радиосети и прочих подобных вещах, у вас возникают очень несерьезные ассоциации с какой-нибудь «Матрицей». Поверьте, хакеры не имеют отношения к вооруженным до зубов людям в черном, которые входят в ваш дом через парадную дверь и начинают эффектно взламывать ваши беспроводные сети. Те, кто называет себя «хакерами», внешне не отличаются от обычных людей, но последствия их действий могут быть куда внушительней, чем самая «взрывная» сцена любого боевика. Фильмы про хакеров вы смотрите по телевизору, а вот результаты вторжения в вашу сеть будут касаться вас лично.

Вернемся к перехвату пакетов. Существует схема взлома WEP-шифрования, при которой программа-сниффер перехватывает большое количество пакетов, ничем себя не выдавая. Программа анализирует пакеты и собирает данные о SSID, о ключе сети, о некоторых других вещах, которые позволяют злоумышленнику (или просто любопытному гражданину) подключиться к вашей сети. Существует ПО, которое позволяет организовывать особые виды атак на беспроводные сети, например атаки типа DOS (*Denial Of Service* — отказ в обслуживании). Такая атака может быть реализована по схеме, в соответствии с которой компьютеры, входящие в сеть, будут постоянно от нее отключаться, подключаться снова и так далее. В результате нормальная работа сети окажется невозможной.

Кстати, возвращаясь к теме хакеров. Знаете, как может выглядеть хакер, занимающийся взломом вашей сети? Да очень просто и неприметно: ходит себе некто с простеньким кейсом по улице и, поглядывая на часы, ждет кого-то. Или сидит в близлежащем кафе, или в автомобиле, или этажом выше, ниже и так далее. А ноутбук, спрятанный в кейсе, занимается сбором информации о вашей сети.

Да что там ноутбук! Определенную информацию о том, где «ловится» ваша беспроводная сеть, может дать даже КПК, на котором установлена соответствующая программа. Такую программу мы рассмотрим ниже.

Но что за прок вам в подобных программах, если вы не собираетесь никого «ломать»? Прок есть, да еще какой: вооружившись снифферром, вы можете попытаться взломать собственную сеть, проверив ее таким образом на прочность. Если получится, значит, нужно всерьез задуматься о безопасности.

10.5. СЕТЬ НА FIREWIRE

ХАРАКТЕРИСТИКИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ

FireWire в переводе означает «огненный провод». Это название компания Apple использует для обозначения технологии IEEE 1394. С легкой руки Apple термин прижился, и теперь IEEE 1394 и FireWire используются как синонимы.

IEEE 1394 стандартизирована в 1995 году и с тех пор применяется преимущественно в цифровой видеотехнике. Нас же интересует применение шины FireWire для связи двух компьютеров между собой.

FireWire — это последовательная шина. Последовательные архитектуры вообще характерны для современных интерфейсов. Применение последовательной логики передачи данных позволяет значительно сократить число проводников, которое требуется подводить к устройству, упростить процесс подключения и достичь более высоких скоростей передачи данных, чем при использовании параллельных архитектур.

На первый взгляд может показаться, что параллельные шины способны на большее, но когда скорости передачи данных вырастают до определенных значений, параллельные шины оказывается гораздо сложнее заставить работать, чем шины последовательные. Поэтому многие технологии двигаются в последовательном направлении.

В середине 90-х годов IEEE 1394 была уникальным стандартом. Она была очень похожа на USB, но отличалась гораздо большей пропускной способностью (до 400 Мбит/с). К тому же имелась возможность подводить по шине большую мощность для питания устройств. Но сходство с USB этим не заканчивается: FireWire поддерживает «горячее» подключение, то есть подключать и отключать устройства можно при включенном компьютере.

Стандарт IEEE 1394 разрабатывался для высокоскоростного подключения периферийных устройств к компьютеру. Собственно говоря, для этого FireWire и используется. Но особенности ее архитектуры позволяют создавать FireWire-сети: ведь шина может работать в режиме «точка-точка». А от этой возможности до локальной сети всего один шаг. Так, если соединить подходящим FireWire-кабелем пару компьютеров, то получится та самая «точка-точка», а если разыскать FireWire-хаб, то появляется возможность создания сети звездообразной топологии.

При этом в такую сеть естественным и сравнительно недорогим образом интегрируются самые разные устройства, поддерживающие IEEE 1394. Например, к хабу можно подключить компьютеры, какой-нибудь FireWire-дисковод и другие устройства. Это решение особенно интересно для домашней сети: ведь DVD-дисководы и жесткие диски с поддержкой FireWire можно найти едва ли не в каждом уважающем себя компьютерном магазине, торгующем «домашней» техникой.

Однако не стоит думать, что шина FireWire в существующем варианте способна послужить полноценной заменой тому же Ethernet 100BaseT. В соответствии со спецификациями длина кабеля FireWire ограничена 4,5 метра. Существуют и более длинные кабели, не соответствующие стандарту. С их использованием возможны проблемы. Хотя не исключено, что именно в вашем случае все будет нормально.

Получается, что сети FireWire пригодны для соединения компьютеров и другой подходящей техники кабельными отрезками длиной до 10 метров, а лучше — до 4,5 метра. Такое решение подходит лишь для объединения устройств в пределах комнаты средних размеров. Но если «концентрация» компьютеров и других устройств в вашей квартире достаточно высока и некоторые из них (преимущественно речь идет о компьютерах) имеют FireWire-адаптеры, у вас появляется достаточно простая возможность объединить их в сеть. При этом скорость передачи данных по такой сети будет значительно выше скорости, на которую способен 100-мегабитный Ethernet.

Цены Ethernet-адаптера и IEEE 1394-адаптера различаются весьма незначительно, поэтому выбор той или иной технологии зависит только от вашего желания и расположения компьютеров в вашей квартире. Однако Ethernet-сети — это фактический стандарт, которым пользуются буквально все, а сеть на FireWire придется хорошенько поискать. Ограниченность стандарта не позволяет использовать его для создания полноценных (хотя бы по параметру дальности связи) локальных сетей. Но все остальное у FireWire есть, поэтому будем ждать развития этой технологии в сторону увеличения дальности связи и, возможно, скорости передачи данных. Собственно говоря, так и случилось: ведь наряду со стандартом IEEE 1394/1394a существует стандарт IEEE 1394b. Этот стандарт поддерживает скорость работы до 800 Мбит/с и использует 9-контактный разъем. К тому же в стандарте IEEE 1394b появились новые кабели: если прежде FireWire не признавал ничего, кроме экранированного кабеля, то новый стандарт (его называют GigaWire) может работать как с привычными кабелями, так и на обычном UTP-кабеле и на оптоволокне.

В случае с UTP шина FireWire поддерживает дальность связи до 100 метров. Вот только скорость оказывается до боли знакомой: все те же 100 Мбит/с. Получается, что GigaWire — это потенциальный конкурент Ethernet 100BaseT, но пока конкуренция этих стандартов не слишком заметна. FireWire-адаптеры встраивают уже в очень многие материнские платы, и для связи по нему пары компьютеров нужен лишь подходящий кабель, да и стоимость FireWire-карты практически равна стоимости сетевой карты Ethernet. Но адаптер GigaWire стоит около $ 50–100, а это многовато для построения непопулярной локальной сети. С другой стороны, если в сети нужны участки с высокой пропускной способностью, то скорость 800 Мбит/с даже скептика заставит задуматься. Но здесь стартует спор IEEE 1394 с Gigabit Ethernet, и можно

предположить, что в обозримом будущем локальные сети на FireWire или GigaWire так и останутся экзотикой.

Обсудив теоретические положения, касающиеся FireWire, перейдем к практическим вопросам.

ОБОРУДОВАНИЕ FIREWIRE

Существуют две модификации IEEE 1394-разъемов. Одна из них (рис. 10.10) — это четырехконтактный разъем.

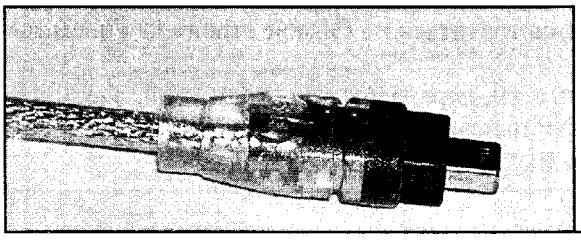


Рис. 10.10. Четырехконтактный разъем FireWire

Розетки, к которым он подходит, обычно устанавливаются в различных мобильных устройствах: в ноутбуках, принтерах, цифровых камерах.

Вторая модификация — шестиконтактный разъем (рис. 10.11). Такой разъем подходит для розеток, которыми оснащаются стационарные FireWire-адаптеры.

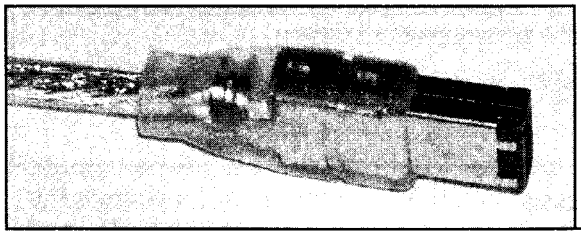


Рис. 10.11. Шестиконтактный разъем FireWire

Существует несколько типов кабелей FireWire. Есть кабели с 6-контактным разъемом на одном конце и 4-контактным на другом. Такие кабели предназначены для связи между компьютерами и различными устройствами, оснащенными 4-контактным разъемом. Есть кабели, которые имеют два 4-контактных разъема, они нужны, например, для связи между парой цифровых видеокамер. Кабели, оснащенные двумя 6-контактными разъемами, подходят для организации IEEE 1394-сети.

FireWire-сеть имеет довольно узкую сферу применения: если не учитывать возможность использования FireWire-хаба, то сеть FireWire обычно состоит из пары компьютеров, оснащенных IEEE 1394-адаптерами. При этом компьютеры должны находиться на расстоянии до 10 метров друг от друга. Это не решение для офиса, так как офисные сети

обычно строятся на Ethernet или на Wi-Fi. Скорее, FireWire сеть нужно строить там, где она сама «просится» быть построенной. Ее можно рассматривать как своего рода запасной вариант создания сети. Если говорить о стоимости соединения пары компьютеров, оснащенных FireWire-адаптерами, то окажется, что она равна стоимости кабеля, то есть примерно $ 3–5 или чуть больше.

Полагаю, что не стоит покупать FireWire-адаптеры специально для того, чтобы организовать FireWire-сеть. Лучше взять обычные Ethernet-карты и хаб в придачу. Но если вам нужна более высокая производительность сети, чем та, которую может обеспечить 100-мегабитный Ethernet, если расстояние между соединяемыми компьютерами вряд ли превысит 10 метров и если вам не хочется тратиться на Gigabit Ethernet — посмотрите в сторону FireWire.

Обсудив аппаратную часть сети, переходим к программной. Здесь все предельно просто. Windows XP изначально считает FireWire-адаптер сетевым устройством (рис. 10.12).

Надо сказать, что не во всех версиях Windows предусмотрена установка сети FireWire. Например, в Windows 98 такой возможности нет.

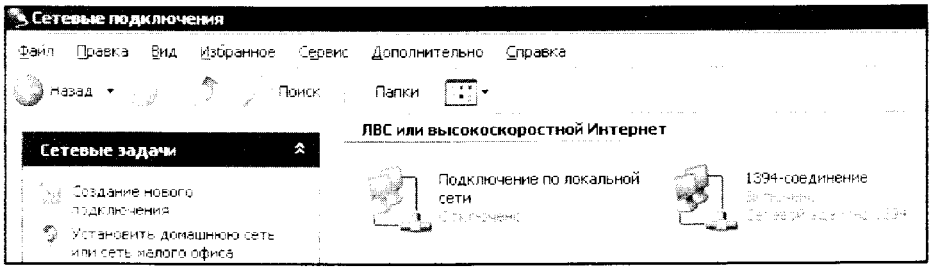


Рис. 10.12. Windows XP и FireWire-адаптер

Что касается программного обеспечения, при помощи которого можно настроить FireWire-соединение, то здесь все так же просто, как и в случае с Ethernet-соединением: нужно установить и настроить соответствующие протоколы в окне настройки свойств соединения (рис. 10.13). Выше мы весьма подробно обсуждали вопросы настройки соединения, и потому здесь на этом останавливаться не будем.

Отмечу, что использование FireWire в качестве сетевого интерфейса создает достаточно сильную нагрузку на центральный процессор. Если у вас слабый компьютер (скажем, на каком-нибудь гигагерцовом Celeron'e), то может случиться, что производительность системы сильно упадет. Поэтому владельцам таких компьютеров стоит присмотреться к традиционным Ethernet-сетям.

Обсудив особенности создания локальных сетей на FireWire, переходим к созданию «телефонной» сети.

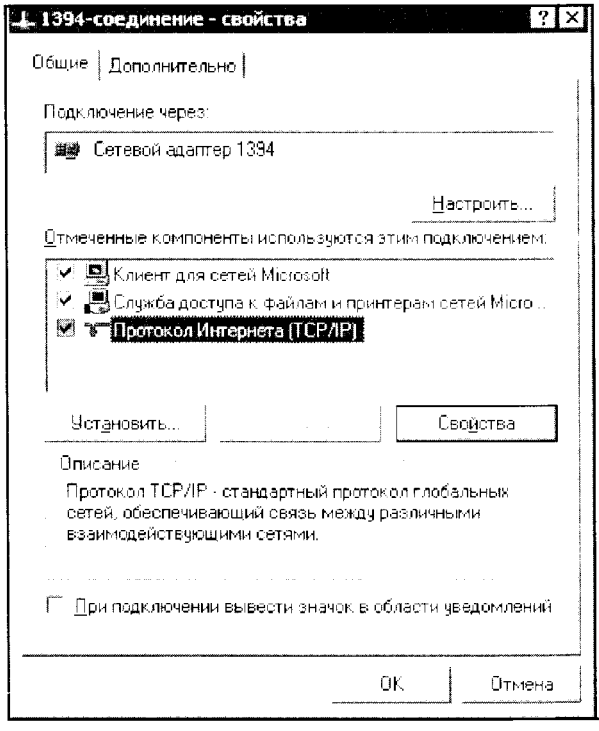


Рис. 10.13. Окно настройки свойств IEEE 1394-соединения

10.6. СЕТЬ ИЗ МОДЕМОВ

Модемное соединение, которым мы пользуемся для организации dial-up-доступа в Интернет, подходит для создания полноценной локальной сети. Правда, скорость связи в такой сети будет низкой, но этот недостаток компенсируется легкостью установки и отсутствием необходимости дополнительного программного и аппаратного обеспечения. Все, что необходимо для такой сети, это пара модемов и телефонные линии.

В начале книги мы обсуждали особенности связи пары компьютеров с использованием технологии Hyper Terminal. Соединение получается, но его возможности очень уж примитивны. Передача файлов да довольно «кривой» обмен сообщениями — вот и все, на что способен Hyper Terminal. И все же Hyper Terminal позволяет установить связь между компьютерами буквально в считанные минуты, да еще и без предварительной подготовки. А в процессе наладки компьютерной сети между парой машин немало времени занимает их настройка.

Для начала немного теории. При помощи модемов можно соединить лишь два компьютера. При этом один из них будет сервером, а второй — клиентом. (Если у вас есть огромное желание, два модема и две телефонные линии, можно попытаться создать двухмодемный сервер и подключить к нему пару компьютеров, но это уже чистая экзотика.)

Итак, один из компьютеров становится сервером, его модем ждет звонков. Второй компьютер — клиент — готов к дозвону на сервер. После того как происходит дозвон, компьютеры оказываются объединенными локальной сетью. При этом трудно классифицировать такую сеть как локальную, особенно если компьютеры разделены десятком-другим километров.

Скорость связи по такой сети очень сильно зависит от качества телефонных линий. В лучшем случае это будет что-то в районе 45,3 Кбит/с, но практика показывает, что обычно скорость более или менее равна 36,6 Кбит/с. Но, чтобы поиграть в простые сетевые игры или обменяться файлами, этого достаточно.

Переходя к практике настройки телефонной сети, для начала разберемся с сервером. Переходим в окно **Панели управления**, содержащее информацию о сетевых подключениях (**Пуск ▶ Панель управления ▶ Сетевые подключения**). В этом окне выполняем команду меню **Файл ▶ Новое подключение**. В ответ на эту команду появляется окно Мастера новых подключений (рис. 10.14).

Здесь нужно выбрать опцию **Установить прямое подключение к другому компьютеру**. Кстати, как видно из разъяснений, помещенных рядом с этим пунктом, его можно использовать для настройки прямых подключений при помощи различных коммуникационных интерфейсов.

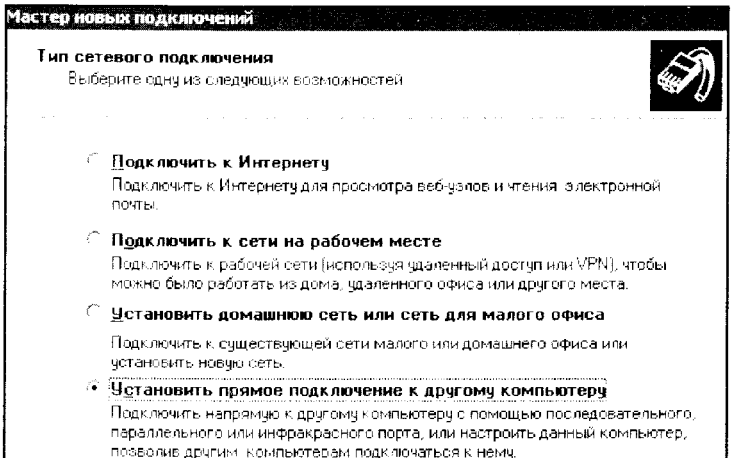


Рис. 10.14. Выбор типа создаваемого сетевого подключения

Нажав кнопку **Далее**, переходим к следующему окну Мастера настройки новых подключений. Здесь нужно выбрать опцию **Принимать входящие подключения**.

Следующее окно отвечает за устройства, с помощью которых осуществляется прием входящих подключений: вам нужно будет установить галочку напротив наименования вашего модема (рис. 10.15).

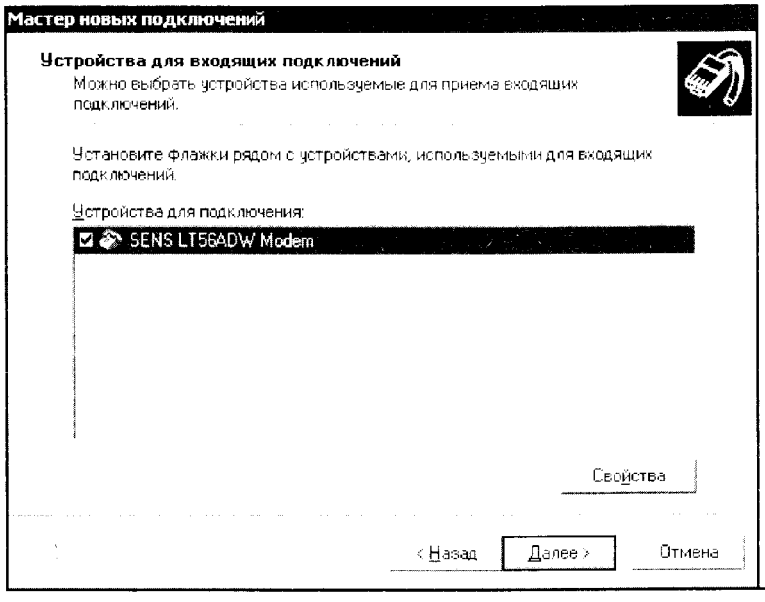


Рис. 10.15. Устройства для приема входящих подключений

В следующем окне вам будет задан вопрос, разрешить или нет VPN-подключения. Установите переключатель в позицию **Разрешить виртуальные частные подключения**.

Дальнейший этап настройки касается настроек разрешений для пользователей. В окне разрешений нажмите на кнопку **Добавить**, а в появившемся окне (рис. 10.16) введите учетные данные, которые будет применять пользователь на другом конце провода для доступа к вашему компьютеру.

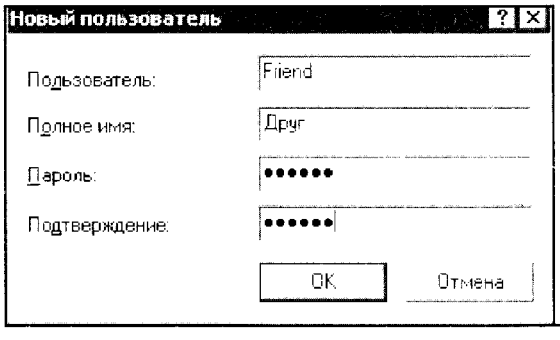


Рис. 10.16. Добавление нового пользователя

Постарайтесь запомнить, а лучше запишите введенные вами данные, то есть содержимое полей **Пользователь** и **Пароль**. Они понадобятся вам (или вашему другу) для настройки параметров второго компьютера нашей телефонной сети.

После добавления нового пользователя и назначения ему разрешения в окне управления пользователями появится новый пользователь (рис. 10.17).

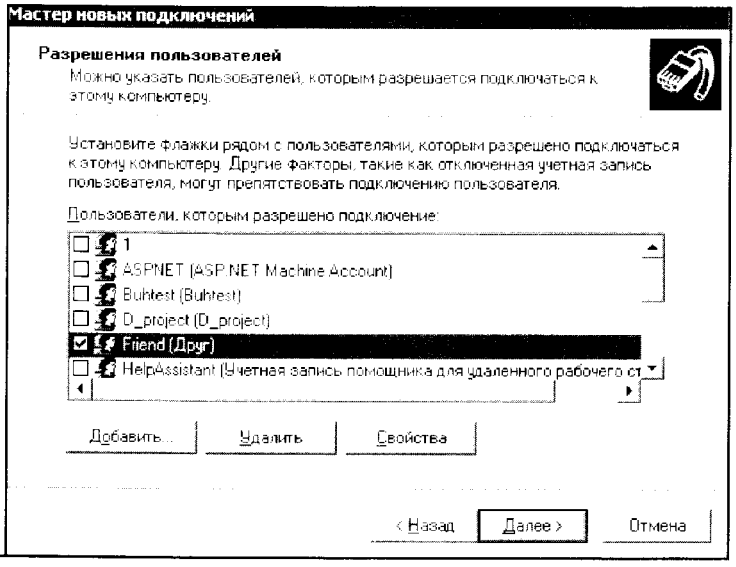


Рис. 10.17. Новый пользователь

Следующее окно Мастера посвящено настройке сетевых протоколов: вам нужно проконтролировать наличие TCP/IP, IPX/SPX, NetBios, Службы доступа к файлам и принтерам сетей Microsoft, клиента для сетей Microsoft.

Вот и все. Теперь ваш компьютер настроен как сервер. Пришло время настраивать второй компьютер.

Для настройки компьютера вашего друга понадобится создать на нем новое подключение к Интернету, но в качестве номера провайдера нужно будет ввести ваш номер, в качестве имени пользователя и пароля — те, которые вы задали при настройке сервера. Когда и эта часть работы будет сделана, ваш друг сможет позвонить вам, через несколько секунд произойдет соединение, и вы сможете пользоваться возможностями сети.

Хочу обратить ваше внимание на одно следствие настройки компьютера в качестве сервера. Очень часто там, где в Интернет выходят через dial-up-подключение, на одной телефонной линии находятся обычный телефон и модем. Так вот, когда вы настроите компьютер в качестве dial-up-сервера, он будет отвечать на все входящие звонки. И если вам позвонят, ваш модем «снимет трубку» и начнет отвечать звонящему на своем языке. Будьте готовы к этому и, настраивая подобное соединение, деактивируйте его на то время, когда оно не используется. Иначе никто не сможет к вам дозвониться.

Чтобы ваша телефонная сеть заработала, нужно выполнять все требования, предъявляемые к обычным компьютерным сетям касательно IP-адресов входящих в нее компьютеров, имен компьютеров и рабочих групп, в которые они входят. Напомню, что для успешной работы в сети Microsoft компьютеры должны иметь одно и то же имя рабочей группы и разные имена компьютеров, а IP-адреса компьютеров должны принадлежать к одной и той же подсети, но быть разными.

10.7. ВЫВОДЫ

Теперь вы без проблем сможете установить проводную и беспроводную сеть, подключить ее к Интернету и устранить возможные неисправности. Вы также справитесь с настройкой «телефонной» сети и сети на основе FireWire.

Но это далеко не все, что вам нужно знать и уметь для эффективной работы с локальными сетями. Вопросы безопасности, кажется, никогда не были так актуальны, как сейчас. Поэтому следующая наша глава целиком будет посвящена обеспечению безопасности при работе в сети.

ГЛАВА 11
СЕТЕВАЯ БЕЗОПАСНОСТЬ

В прошлой главе мы обсуждали возможные опасности, грозящие пользователям беспроводных сетей, а здесь поговорим об общесетевых угрозах и о том, как защититься от неведомого врага. Самый лучший способ поднять уровень безопасности вашего компьютера на небывалую высоту — это вовсе не включать его в розетку, а еще лучше — не становиться владельцем компьютера. Но тем, кто хочет надежно защитить работающую систему от вторжения, этот путь не подходит.

Чтобы эффективно защищаться от врага, нужно его знать как можно лучше: оружие, методы нападения, тактику борьбы и так далее. Так вы сможете эффективно спланировать собственную систему обороны. Кстати, лозунг «лучшая защита — это нападение» в компьютерном мире теряет смысл. Если речь идет о компьютерах, то лучшая защита — это осведомленность и профилактика. Этим мы и займемся.

11.1. КЛАССИФИКАЦИЯ СЕТЕВЫХ УГРОЗ

Что же угрожает обычному пользователю сети? Для автономной локальной сети, которая не подключена к Интернету, угрозы извне не страшны. Эта оговорка не касается беспроводных сетей, исправно транслирующих данные пользователя, пусть зашифрованные, на большие расстояния.

Автономной сети страшны лишь физические (или «почти физические») способы вторжения да вирусы, которые могут быть занесены с дискет, компакт-дисков или других носителей информации. А вот сеть или компьютер, подключенные к Интернету, подвергаются гораздо большему количеству опасностей. Попытаемся классифицировать эти угрозы, чтобы вы представляли, от чего защищаться, чем и зачем.

На рис. 11.1 классификация угроз представлена графически.

Обратите внимание на верхнюю часть рисунка. Неосторожное поведение пользователя — это тоже угроза системе. Хакеры и их программы — это вполне традиционная угроза. Вирусы, троянцы и черви тоже, думаю, известны всем.

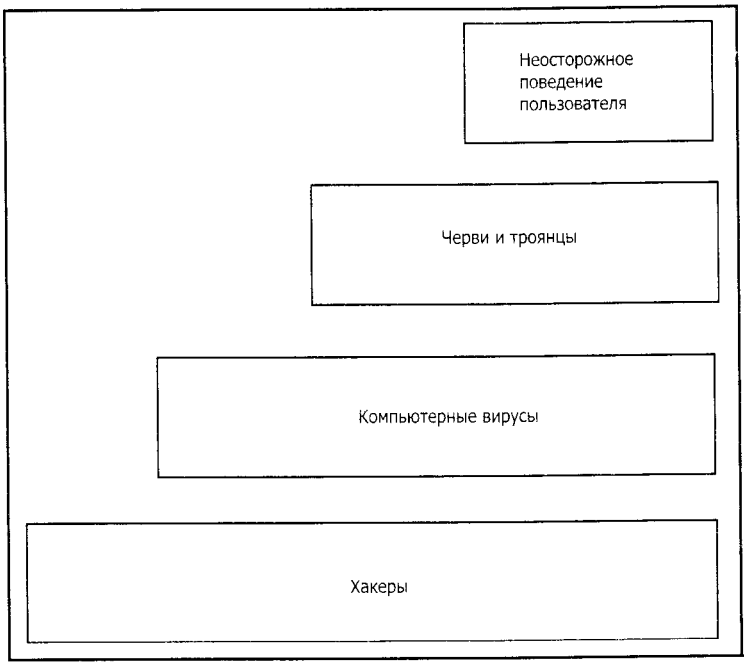


Рис. 11.1. Классификация сетевых угроз

Начнем со знакомых многим хакеров. В прошлой главе я уже занимался «превращением» хакеров из героев фантастических боевиков в обычных людей и продолжу эту тему здесь.

Понаблюдав некоторое время за статистикой атак на мой компьютер из Интернета, я пришел к выводу о том, кто чаще всего пытается атаковать мою систему. Мои данные о злоумышленниках не содержат ничего кроме IP-адресов «умников», которые при наличии очень сильного желания можно было бы превратить в конкретные адреса, имена и фамилии. Но я не задавался целью устраивать охоту, а просто уточнял, что за люди пытаются меня атаковать. Итак, вот мой ответ: большинство этих людей подключены к Интернету через того же провайдера, что и я. Уверен: их интересовала как минимум моя учетная информация. О том, как узнать, кто вас атакует, мы поговорим в разделе о защите информации, а пока продолжим разговор о сетевых угрозах.

Итак, предположим, вы — обычный пользователь Интернета. Выходите в Сеть через *dial-up*, держите дома маленькую беспроводную сеть из настольного компьютера и ноутбука. Чем вы можете заинтересовать среднестатистического хакера? Начнем с вашего *dial-up*-пароля. А точнее, имени пользователя и пароля для доступа в Интернет. Этот вопрос потенциально интересен любому хакеру. Или не любому, но все равно интересен. Перехватив ваши регистрационные данные, злоумышленник сможет пользоваться Интернетом за ваш счет.

Если вы пользуетесь какой-нибудь онлайновой платежной системой, например, WebMoney, то злоумышленник постарается узнать ваш пароль и скачать с вашего компьютера файл с ключами для доступа к WM-аккаунту.

А как насчет вашей почты? Может быть, некто хочет ее почитать или отправить кому-нибудь письмо от вашего имени? А может, вы храните на своем жестком диске в незашифрованном виде данные к вашей кредитке, по которой иногда что-то покупаете в интернет-магазинах?

Следующая после хакеров угроза — сетевые черви и вирусы. Это вредоносные программы. Бывают вирусы, распространяющиеся по сети, и те, что размножаются, инфицируя другие программы.

Вирус (почтовый червь) можно получить по почте в виде вложения. Также вирус (даже не вирус, а интернет-червь) может проникнуть в ваш компьютер прямо из Сети.

Почтовые черви очень изобретательны. Вы можете получить благопристойное с виду письмо, содержащее компьютерный вирус. Такое письмо может быть маркировано как чей-то ответ на ваше сообщение или как сообщение об ошибке, поступившее с почтового сервера. В письме может быть текст, предлагающий вам открыть вложение, которое выглядит как файл картинки с расширением JPG. На самом деле это не картинка, а вредоносная программа. Черви, равно как и хакеры, широко применяют методы социальной инженерии, прикидываясь полезными, интересными и нужными.

Например, если к вам пришло письмо, где вас срочно просят сменить пароль к вашему почтовому аккаунту, отнеситесь к этой просьбе с настороженностью. Если у вас есть сомнения в том, что письмо от вашей почтовой системы, но на всякий случай вы хотите сменить этот пароль, войдите на сервер обычным способом, не трогая ссылок в пришедшем подозрительном письме, и поменяйте пароль так, как обычно его меняете. Очень может быть, что ссылка из письма заведет вас на сайт, внешне очень похожий на сайт вашего почтового сервера. Но на самом деле это будет фальшивая страничка, созданная с целью обмана.

О вирусах придется поговорить особо. Не нужно быть квалифицированным программистом, чтобы, модифицировав написанный кем-то вирус, превратить его из сравнительно безобидной программы в разрушительное оружие. Особенно это верно для макровирусов, текст которых лежит буквально «на поверхности» и может быть модифицирован кем угодно. Вирус может сделать с вашим компьютером почти все, что угодно: испортить или вовсе стереть данные, замедлить работу, что-нибудь украсть и так далее. Поэтому заявляю вам со всей ответственностью: опасайтесь вирусов. Их можно даже бояться, но впадать в панику при мысли о том, что ваш компьютер заражен, не стоит. Хуже, если вы относитесь к вирусам пренебрежительно. Как правило, такое отношение к ним сохраняется лишь до первой крупной неприятности.

Сетевые черви в последнее время занимаются не похищением информации (хотя такое тоже случается), а превращением компьютеров в «зомби». Такие компьютеры могут использоваться злоумышленниками, например, для рассылки спама и для организации масштабных компьютерных атак на определенные ресурсы.

А теперь подробнее остановимся на классификации компьютерных угроз в соответствии с моделью OSI.

СЕТЕВЫЕ УГРОЗЫ И НЕКОТОРЫЕ УРОВНИ OSI

Начнем с физического уровня. Так как этот уровень OSI отвечает за физическую передачу сигналов в среде передачи данных, очевидной является возможность атак, направленных на ухудшение рабочих характеристик среды: например, для беспроводных сетей это может быть постановка помех, которые «забивают» полезный сигнал. Это вариант DOS-атаки.

Далее рассмотрим канальный уровень. Как вы помните, на этом уровне работают протоколы канального уровня, например известный вам Ethernet. Доступ к среде передачи данных осуществляется способом под названием CSMA/CD. Сетевые адаптеры постоянно «слушают» друг друга, передают данные в определенное время, не имеют права затягивать передачу на большее время, нежели это позволено стандартом, и так далее. А что будет, если какой-нибудь сетевой адаптер вдруг начнет передавать данные в произвольном порядке, никого не слушая? Получится вариант DOS-атаки, который работает на канальном уровне OSI.

На сетевом уровне, где действует протокол IP, возможны атаки, связанные с неправильной маршрутизацией IP-пакетов.

Транспортный уровень тоже уязвим: протоколы TCP и UDP в терминологии стека протоколов TCP/IP также могут быть атакованы. В основном это атаки, в основе которых лежит возможность IP заниматься сегментацией пакетов, чтобы они могли передаваться по сетям с разным максимальным размером пакета. Как вы помните, в результате получается, что одно сообщение оказывается разбитым на множество пакетов, которые путешествуют по сети автономно, а потом из них собирается исходное сообщение на компьютере-приемнике. Что будет, если компьютер-отправитель начнет слать в сеть пакеты некого сообщения, сделанные как положено, но некоторые из пакетов так и не будут отправлены в сеть? Это тоже вариант DOS-атаки: система должна хранить принятые пакеты в ожидании продолжения, которого не будет.

Для сеансового уровня (на котором, кстати, находится все тот же TCP) характерна операция установления соединения компьютеров, передающих и принимающих информацию. Компьютеры, прежде чем начать обмен данными, договариваются о параметрах связи, обмениваясь служебными сообщениями. Так, известен вариант DOS-атаки, называю-

щийся *SYN-Flood*. Он использует особенность установления соединения между двумя компьютерами, а название это пошло от названия служебного бита, используемого при создании запроса на соединение. Когда сервер получает такой запрос, он отправляет ответ на него и начинает ждать подтверждения приема своего ответа, после чего может начаться обмен данными. А если подтверждения нет, сервер вынужден ждать его достаточно долго — до нескольких секунд. Если злоумышленник сгенерирует несколько тысяч неправильных пакетов с запросом на соединение, то он сможет парализовать на некоторое время работу среднего сервера. Ну а если это не один злоумышленник, а сеть компьютеров-зомби, которые «бомбят» даже очень крупный сервер специально подготовленными пакетами, то у сервера просто не останется времени для обработки запросов настоящих пользователей.

В этих запросах на соединение могут указываться произвольные IP-адреса — например, злоумышленник отправляет серверу запрос с указанием реального адреса, но, естественно, не своего. Сервер, ничего не подозревая, отправляет по обратному адресу, который находится в сообщении, ответ. А система, которая имеет адрес, указанный в качестве обратного, получает странный ответ от сервера неизвестно на какое сообщение. Это сообщение будет проигнорировано, но сервер будет ожидать ответа. А если таких безнадежных адресатов оказывается много, то получается вариант DOS-атаки для сеансового уровня.

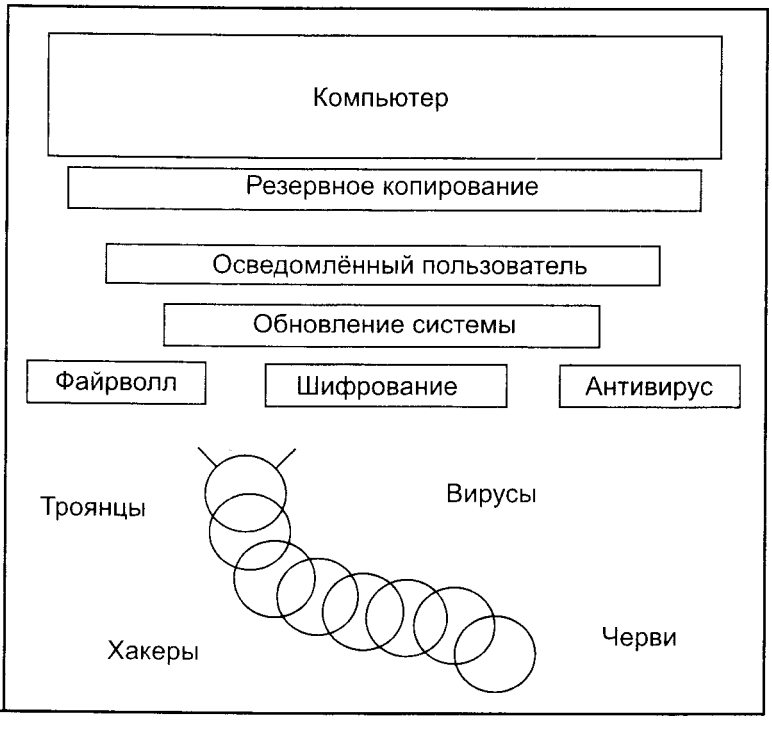


Рис. 11.2. Структура защитной системы компьютера

Атаки на более высоких уровнях OSI могут проводиться, например, с использованием уязвимостей протоколов и программного обеспечения.

Все эти сетевые угрозы означают, что вы должны уметь защищаться. Компьютерная, сетевая защита состоит из нескольких важных вещей (рис. 11.2).

Во-первых, это файрволл, или, как его еще называют, брандмауэр. Второй ступенью защиты является антивирус. Третьей — шифрование данных. А четвертой, хотя, скорее, не четвертой, а все-таки первый — вы сами. Осведомленный пользователь — это лучшая защита для любого компьютера.

Традиционно в состав Windows не входят антивирусы, однако в случае с файрволлами дело идет в сторону интеграции их в ОС. А начнем мы наш рассказ о ПО именно с файрволлов, — а именно с описания возможностей файрволлов и видов атак. Потом поговорим о встроенном в Windows файрволле и рассмотрим несколько продуктов сторонних производителей.

11.2. ФАЙРВОЛЛЫ: ПРИНЦИПЫ РАБОТЫ

У слова «файрволл» нет русского аналога. Оно происходит от английского *Firewall*, что переводится как брандмауэр (защитная стена от огня). Файрволл — это программный комплекс, который занимается контролем передачи данных между вашим компьютером и сетью. Вначале рассмотрим теоретические основы работы файрволла, а потом приступим к практическим примерам.

Итак, чем занимается файрволл в системе? Для начала он составляет список программ, которым нужен доступ к локальной сети и Интернету. Обычно файрволлы задают пользователю вопросы, касающиеся программ, которые можно или нельзя «выпускать» в сеть. Отвечать на вопросы файрволла надо очень осторожно и обдуманно.

Например, доступ к Интернету нужен системным службам. Если вы ненароком откажете в доступе к Интернету чему-то важному, то с вашим доступом к Интернету может начаться такой кошмар, о котором лучше не говорить. В то же время, выпустив в Интернет какой-нибудь Microsoft Word (и ему подобные программки), которому, по моему глубокому убеждению, совершенно нечего там делать, вы лишь нагрузите свое интернет-соединение лишним трафиком.

Помимо контроля над программами, файрволлы фильтруют входящий трафик. Ведь ваш компьютер, подключенный к Интернету, постоянно подвергается атакам.

Я проводил эксперимент, пытаясь засечь, сколько раз мой компьютер, подключенный к Интернету в общей сложности часа два, будет атакован. В качестве «измерителя атак» был использован файрволл Zone Alarm, о котором мы подробно поговорим ниже. Так вот, за это время

было зафиксировано две сотни попыток несанкционированного доступа к системе, которые в большинстве своем были расценены файрволлом как опасности среднего уровня. Например, больше всего было попыток подключиться к 445-му порту на моем компьютере. Скорее всего, это были попытки поиска общих ресурсов сети.

Интересно, что большая часть этих среднеуровневых атак (или не атак) велась клиентами провайдера, услугами которого пользуюсь я сам. Было несколько таких же атак от клиентуры нескольких российских провайдеров, да еще каким-то ветром сюда занесло клиента французского провайдера, деятеля из Арабских Эмиратов, кого-то из Финляндии и с Украины.

Среди этих двух сотен атак была одна, о которой файрволл известил меня особо. Решив разузнать подробнее о том, что случилось, я воспользовался средствами файрволла по «расследованию» происшествия и узнал следующее. Во-первых, некто пытался подключиться к 21 TCP-порту, который обычно используется FTP-сервером. FTP — это протокол, позволяющий принимать и передавать файлы. Он популярен у хакеров так как позволяет манипулировать с файлами на незащищенной машине. Видимо, хакер занимался сканированием портов и попался моему файрволлу. Продолжая исследование этого инцидента, я обнаружил, что угроза исходит из городка недалеко от Амстердама.

Правда, нормальной для хакеров практикой является скрытие своего реального IP-адреса. Для этого они пользуются прокси-серверами. На незащищенный компьютер они могут установить особые программы, позволяющие управлять этим компьютером. Но для атаки, которой подвергся мой компьютер, не нужно никакого сложного программного обеспечения. Все, что нужно, это обычный сканер портов и уйма свободного времени. Своего или чужого. Так, атака на 21-й порт, которую я разбирал немного выше, вполне могла исходить от какого-то местного хакера (местного — в смысле пользующегося услугами того же провайдера, что и я), который, устроив себе «базу» в Европе, запустил там сканер, изучающий компьютеры, принадлежащие к подсети этого самого хакера. Если ему удастся (и даже не «если» — обязательно удастся) найти незащищенную систему, то у этого хакера найдется, что «залить» по FTP, а уж что искать в папках открытого для атаки компьютера, он прекрасно знает и сам.

Ниже, в описании файрволла Zone Alarm, я приведу подробный иллюстрированный пример «расследования» атаки с пояснением некоторых подробностей.

Вернемся к функциям файрволла. Эта программа фильтрует трафик, который исходит из компьютера и входит в компьютер. Она также занимается предотвращением несанкционированного доступа к компьютеру из Интернета. Пример попытки такого доступа был описан выше.

Напомню, что программы, работающие с сетью, используют TCP и UDP-порты, каждый из который имеет определенный номер. Данные передаются с использованием какого-нибудь протокола для передачи

данных. Среди них можно отметить HTTP, FTP, POP и так далее. Так вот, файрволл занимается контролем портов и слежением за использованием протоколов. Например, файрволлы умеют «прятать» порты для того, чтобы сделать компьютер невидимым в прямом смысле слова.

Хочу пояснить, что означает «видимость» в понятиях Интернета и локальных сетей. Допустим, один компьютер отправляет другому компьютеру какой-то запрос, как сделал в вышеприведенном примере хакер из-под Амстердама. Если бы компьютер был незащищен и если бы на нем работал FTP-сервер, хакер получил бы то, что ему нужно. Но для этого он должен бы был получить как минимум ответ от моего компьютера. Этот ответ и определяет видимость моего компьютера для компьютера хакера. А так получилось, что он отправил мне запрос, но этот запрос перехватил файрволл и, проанализировав его, понял, что тут что-то нечисто. Поэтому файрволл решил не отвечать подозрительному отправителю запроса, вывел предупреждающее сообщение и занес запись в журнал.

А если компьютера не видно, если он не отвечает на провокационные вопросы, задаваемые ему сканерами портов и прочим подобным софтом, то его нельзя будет и атаковать. На расстоянии можно узнать о компьютере пользователя очень многое, даже не «вламываясь» в него.

По некоторым данным известно, что многие атаки проводятся не снаружи, а изнутри компьютера. Например, вам могут установить шпионскую программку, которая будет собирать информацию и отправлять ее куда-нибудь. Когда файрволл работает, он отслеживает и такие программы.

Помимо контроля за трафиком, файрволл может контролировать использование различных веб-компонентов. Например, он может блокировать файлы *cookies*. Эти файлы содержат информацию о том, когда вы были на каком-то сайте, что там делали, под каким именем и паролем входили и так далее. Эти данные могут использоваться серверами для автоматической аутентификации, для запоминания каких-то действий, которые вы выполняли. Но эти безобидное на первый взгляд *cookies* вызывают массу споров и разногласий. Главная их проблема заключается в том, что они нагло вмешиваются в частную жизнь пользователя, рассылая информацию о нем чуть ли не всем желающим.

Конечно, все желающие не получат ваших *cookies*, но с их помощью проводится сбор информации о вас как о посетителе того или иного сайта, к тому же генерируется лишний сетевой трафик. Файрволлы умеют блокировать эти файлы.

Далее, даже обычные веб-страницы могут содержать опасные элементы. Это элементы управления ActiveX, Java-апплеты и так далее. Их использование тоже можно ограничить и даже не ограничить, а просто сделать безопаснее с помощью файрволла.

Интернет-странички могут содержать кучу рекламы и разного рода баннеров, которые подгружаются на эти странички с других серверов.

Получается, что интернет-трафик тратится непроизводительно: вам приходится дольше ждать загрузки нужной вам странички, наблюдая, как вместе с важными данными загружается ненужная рекламная графика и анимация. Конечно, можно пойти на крайнюю меру и отключить в браузере графику. Но, хотя графические элементы на интернет-сайтах должны иметь текстовые подписи, гулять по интернету без графики — сомнительное удовольствие.

Файрволлы, кроме всего прочего, могут наблюдать за вашим почтовым клиентом, отслеживая возможные атаки червей, противостоять потоку спама и так далее. Некоторые файрволлы обладают встроенным антивирусом. Заметим, что в системе не рекомендуется использовать больше одного антивируса. Но все же главная роль файрволла заключается в контроле сетевого трафика.

Резюмируя, отмечу здесь основные преимущества, которые вы получаете, используя файрволл.

1. Используя файрволл, вы защищаете компьютер от внешних атак. Также файрволл защищает вас от атак внутренних: например, «троянский конь», внедренный в вашу систему, может попытаться украсть и передать по Интернету какие-то данные, которые будут перехвачены файрволлом.

2. Вы получаете возможность контролировать программы, которые пытаются получить доступ к Интернету в своих собственных целях. Если вы не желаете, чтобы какая-нибудь программа самостоятельно работала с Сетью, расходуя таким образом ваше время и деньги, можно закрыть ей доступ к Интернету. Так вы получаете возможность более рационально использовать пропускную способность вашего интернет-канала.

3. Вы можете контролировать загрузку ненужного рекламного контента на просматриваемые вами веб-странички и блокировать передачу вашей персональной информации.

А теперь поговорим об антивирусах.

11.3. АНТИВИРУСЫ: ПРИНЦИПЫ РАБОТЫ

Антивирус — это программа для борьбы с компьютерными вирусами. Компьютерные вирусы — это программы, умеющие распространяться, например, внедряя свой код в другие программы, рассылая себя по электронной почте или «расползаясь» по незащищенным компьютерам. Классический вирус никого не трогает — он просто живет и распространяется. Это не значит, что вирус, не содержащий разрушительных функций, безвреден. Все вирусы вредны, так как они загружают линии передачи данных ненужным трафиком, занимают системные ресурсы, замедляя работу компьютера, и так далее. Для борьбы с ними и существуют антивирусы.

Типичный антивирус работает следующим образом: он следит за системными событиями, проверяет файлы, с которыми вы совершаете какие-либо действия, и в случае обнаружения в проверяемом файле сигнатуры (характерной последовательности байтов) вируса начинает бить тревогу. Антивирус выводит сообщение о том, что такой-то файл инфицирован, и, как правило, предлагает вам на выбор несколько вариантов действий, которые он может выполнить с этим файлом. Так, файл может быть вылечен (в английской терминологии — *Cure*) — вирус будет из него удален, а антивирус восстановит оригинальную структуру файла, чтобы с ним можно было продолжать работу. Неизлечимый файл может быть либо «очищен» (wipe), либо помещен на карантин (Carantine), он может быть просто удален (Delete) или переименован (Rename). В свете растущего количества почтовых вирусов антивирусы весьма внимательно относятся к почтовым клиентам, проверяя входящую, а довольно часто и исходящую корреспонденцию.

Общей проблемой антивирусов и файрволлов является то, что они при всей полезности существенно замедляют работу системы. Но на современных, достаточно быстрых компьютерах это не очень заметно.

Еще антивирусы занимаются проверкой оперативной памяти в поисках резидентных вирусов. Они также проверяют загрузочные сектора жестких дисков в поиске загрузочных вирусов, сканируют офисные документы в поиске макровирусов. Работы у антивируса хватает.

Антивирусы умеют обнаруживать не только вирусы, сигнатуры которых хранятся в их антивирусных базах. Они имеют механизм, называющийся эвристическим анализатором. Это особая программная конструкция, которая помогает антивирусу оценить опасность той или иной программы. Эвристические анализаторы не дают стопроцентной гарантии обнаружения вируса, и далеко не все новые вирусы могут быть найдены с помощью эвристического анализатора, но уровень защиты использование такого анализатора все же повышает.

Очень важным этапом в работе с антивирусом является его своевременное обновление. Строго говоря, антивирус желательно обновлять несколько раз в день, но это слишком жесткий режим, почти недоступный обычным пользователям по причине достаточно больших затрат времени на обновление. Поэтому общепринятой является практика обновления антивирусных баз хотя бы раз в неделю.

Антивирусом следует проверять все, что вы получаете из не слишком надежных источников. Желательно проверять им все, что поступает к вам на дискетах, и все, что вы скачиваете из Интернета. Информация на компакт-дисках обычно более надежна, но и ей нельзя полностью доверять без проверки. Как правило, вышеприведенные рекомендации касаются не команд антивирусу, которые должны давать вы сами. Нет, он сам все сделает, самое главное — не отключайте антивирус и позвольте ему сделать его работу.

Ниже перечислены преимущества использования антивируса.

Антивирус защищает вас от вирусов, которые могут уничтожить вашу информацию, украсть ее или испортить. Это главное преимущество, которое дает использование антивируса. Запомните: главное, чем вы можете помочь антивирусу, не мешать ему.

Если вы не уверены в настройках, которые можно изменить, настраивая антивирус, не трогайте параметры, назначенные по умолчанию. Будьте осторожны с параметрами настроек, например эвристического анализа. Некоторые процедуры, которые выполняет анализатор, могут вызывать большие затраты системных ресурсов при выборе максимальных уровней. Например, тот же эвристический анализатор, если его настройки «выкрутить» на максимум, может серьезно затормозить работу вашего компьютера. Придется решать, что важнее: потенциально высокий процент обнаружения неизвестных вирусов или более быстрая работа системы.

Некоторые пользователи пытаются обходиться и вовсе без антивируса, не желая занимать этой программой жесткие диски, память и системные ресурсы своего компьютера. В принципе, можно понять раздражение пользователя тормозящим систему антивирусом, если его суперкомпьютер используется исключительно как машина для игр, самый ценный ресурс которой — производительность. В этом я солидарен с геймерами: к чему терять часть производительности на борьбу с вирусами, которых может и не быть. Ведь в погоне за производительностью некоторые (или даже не некоторые) геймеры идут на сознательный риск, разгоняя свои процессоры и видеокарты. В других же случаях антивирус просто обязателен.

Если хранящаяся на вашем компьютере информация представляет для вас ценность, обязательно пользуйтесь антивирусом. Если у вас нет возможности скачать из Интернета свежую версию бесплатного антивируса или обновить ваш антивирус, пользуйтесь устаревшим, но не отключайте его вовсе.

Некоторые системные администраторы, то ли в погоне за производительностью, то ли просто не желая возиться с этой «ерундой», оставляют свои сети без антивирусной защиты. Глупость, конечно, но так случается. Бывают офисы (мне таких довелось повидать немало), где уделяют внимание всему, чему угодно, только не антивирусной безопасности.

Наблюдая за поведением офисных работников до проблем, вызванных вирусом, и после, я сделал вывод. Не сталкиваясь с вирусной проблемой, они либо не знают о существовании вирусов, либо относятся к ним с пренебрежением. Но когда вирус наносит удар, отношение к проблеме мгновенно меняется, и те, чья работа была уничтожена вирусом, начинают панически бояться заразы. Они ходят за системным администратором и просят его поставить свежий антивирус, а некоторые на свой страх и риск ставят этот софт сами. И знаете что? Они правы. Если системный администратор не в состоянии защитить ваши

данные, защищайте их сами. Антивирус не влияет на работу локальной сети, поэтому ставить его на свой рабочий компьютер можно гораздо смелее, чем файрволл.

А сейчас мы перейдем к следующей ступени защиты системы — к ее обновлению и настройке.

11.4. ОБНОВЛЕНИЕ И НАСТРОЙКА СИСТЕМЫ

Обновление системы — это еще одна важная часть ее безопасности. Windows XP — это сложнейший программный продукт. Часто можно слышать нелицеприятные слова в адрес этой операционной системы, и читать или слушать это просто неприятно.

Большинство из тех, кто ругает Windows, работают на ней сами, и это при том, что у Windows есть альтернативы вроде Unix, Linux и MacOS. Об удобстве в сравнении с той же MacOS судить не могу, так как не имею опыта работы с последней, а работа с Unix требует более высокой квалификации, нежели с Windows.

Что бы ни говорили, а Windows — это результат труда множества людей, и эта система, равно как и корпорация Microsoft, достойна уважения. Но Windows XP, как и все, что нас окружает, несовершенна. Если вы пробовали писать программы (или пишете их профессионально), вы непременно сталкивались с неправильной работой очевидных, казалось бы, операций. Написано вроде бы элементарное A+B, а программа выдает ошибку. В случае с этими A и B все обычно очень просто: переменные, скажем, объявлены латиницей, а вы случайно написали их кириллицей. А представляете, какие тексты лежат в основе той же XP? Это миллионы строк, которые нужно отладить и проверить. Но ошибки встречаются везде.

Кроме этого, совокупность программ, которые называются Windows XP, функционируют в тесном взаимодействии друг с другом. В среде Windows работают программы сторонних производителей, драйверы устройств, сетевые службы, вышеописанные файрволлы и антивирусы и еще неописуемое количество других вещей. Здесь просто не обойтись без ошибок. И все же этот гигант умудряется работать достаточно стабильно. Поэтому я испытываю глубокое уважение к Microsoft и ее операционным системам. Но ошибки все же надо исправлять, чем и занимается вышеупомянутая Microsoft, регулярно выпуская заплатки (патчи — от английского *patch*, что так и переводится — заплатка) для своей операционной системы. Как правило, они касаются исправления различных проблем безопасности, реже встречаются поправки других частей. Например, заплатки могут касаться устранения проблемы взаимодействия ОС с какими-либо устройствами.

Нужны ли пользователю эти заплатки? Нужны. К тому же Windows XP может загружать и устанавливать их автоматически. Некоторые поль-

зователи не любят, когда что-то там лезет в Интернет без их ведома, поэтому Windows может выполнять обновления, каждый раз спрашивая вас разрешения на загрузку. Поверьте: обновления стоят вашего времени, даже если вы сидите на плохоньком *dial-up*-подключении.

Другая проблема заключается в неправильной настройке самой ОС. Особенно это касается нерациональной настройки сетевых соединений. Если вы в чем-то не уверены — лучше ничего не трогайте. Хотя иногда правильная настройка системных параметров может повысить защищенность вашей системы.

Следующим пунктом нашего введения в защиту данных является шифрование.

11.5. ШИФРОВАНИЕ И ПАРОЛИ

Шифрование — один из весьма эффективных способов защиты информации. Даже обычный пароль на архиве формата RAR может стать неодолимой преградой на пути злоумышленников.

Если вы работаете с ценной конфиденциальной информацией, для повышения уровня защиты не поленитесь шифровать ее. Конечно, шифрование надо применять вместе с другими способами защиты информации, но оно может быть полезно и само по себе. Например, если ваша почта должна быть секретной, воспользуйтесь специальной системой шифрования почтовых сообщений.

Широко распространены так называемые системы шифрования с открытым ключом. Сейчас мы вкратце рассмотрим основу их функционирования.

У такой системы есть два ключа — два пароля, если хотите. Один ключ используется для шифрования информации, а второй — для ее дешифровки. Ключи эти разные. Открытый ключ вы можете раздавать всем желающим, а закрытый будете знать только вы сами, и расшифровать сообщение, которое отправлено вам, сможете только вы.

Ключи, как и все на свете, могут быть взломаны, но для взлома хорошего ключа требуются годы машинного времени. Это делает взлом ключей нерациональным занятием, особенно если учесть, что информация, до которой хотят докопаться взломщики, ценна только в течение определенного времени.

Возьмем архиватор RAR. Его особенностью является то, что пароль для доступа к закрытому архиву проверяется не перед началом его распаковки, а после. Таким образом прямой перебор паролей для достаточно больших архивов превращается в никчемное занятие. Если вы подозреваете, что вашу почту кто-то читает, а заниматься установкой и настройкой специальных программ для шифрования некогда, можно упаковать сообщение в закрытый архив RAR, а с получателем конфиденциальной информации договориться о пароле, не используя электронные средства связи.

Пароли лучше не хранить в электронном виде. Самые ценные пароли лучше всего хранить записанными на бумаге. Не забывайте и о сложности паролей: чем он длиннее и чем «запутаннее», тем лучше. Обратите внимание на физическую безопасность паролей, которые вы храните. Некоторые пользователи вешают листочки с паролями на видное место. Мне приходилось видеть умилительную картину почтового пароля, написанного крупными буквами на бумажке, приклеенной на стене, где ее мог видеть любой. Электронная почта имела в той фирме не первостепенную важность, поэтому такое поведение можно объяснить, но все же с паролями так обращаться нельзя.

11.6. АРХИВИРОВАНИЕ И РЕЗЕРВНОЕ КОПИРОВАНИЕ

Средства защиты информации, которые описываются в этом разделе, наиболее эффективны. Если ваша рабочая информация будет записана и сохранена в надежном месте, то можно не задумываться о ее сохранности. Резервное копирование спасло и спасет еще очень многих. Современная компьютерная техника довольно надежна, но где гарантия, что вы сами не сотрете случайно результаты вашей работы или что мигнувший некстати свет не сделает то же самое с трудами целого дня?

Мне известен случай предотвращения катастрофы в одном учреждении, системный администратор которого разумно настроил систему автоматического архивирования данных. Поверьте: если с вами случится что-нибудь подобное, вы тут же поймете всю необходимость резервного копирования.

Мы много говорили об угрозах вашей информационной безопасности, рассматривали теоретические основы защиты, но не упомянули пока о главном. А главное — разумный баланс между уровнем защиты вашей системы, ценностью информации, которую вы защищаете, и затратами на эту защиту. Защита должна быть рациональной. Слишком много защиты не бывает, но если вам что-нибудь кажется излишеством, то, возможно, так оно и есть.

А дальше мы немного подробнее поговорим о таком способе атаки на вашу информацию, как социальная инженерия.

11.7. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Социальная инженерия — это искусство убеждать и получать от людей то, что вам нужно. Люди, владеющие этими технологиями и использующие их, способны разузнать многое. Так, у вас могут «увести» какой-нибудь пароль, секретную корпоративную информацию и так далее. Сродни методам социальной инженерии цыганский гипноз. Вас хватают за руки, начинают в чем-то убеждать, запутывая вас и подчиняя таким об-

разом своим целям. И в обоих случаях главным оружием против «злоумышленников» является здоровый скептицизм.

Не заговаривайте с уличными гипнотизерами, отвлекитесь от их разговоров, не смотрите им в глаза и задавайте им глупые вопросы. Точно так же можно поступить в том случае, если вы подозреваете, что вас хотят использовать как источник информации. Например, классической схемой, используемой социальной инженерией, является запугивание. Не прямое запугивание, а попытка вызвать у человека страх. Если злоумышленнику удалось заставить вас чего-то бояться, он таким образом притупил ваше чувство осторожности и воспользуется этим, чтобы выведать нужные ему сведения.

11.8. ВЫВОДЫ

Теоретические основы защиты информации — большая и интересная тема. То, что вы узнали, позволит вам эффективно воспринимать материал следующей главы, которая полностью посвящена вопросам защиты информации в сети.

Сеть — это компьютер, как справедливо заметили в свое время в SUN Microsystems, поэтому защита информации в сети тесно связана с защитой информации на отдельно взятом компьютере. Итак, в следующих главах мы подробно рассмотрим настройку и использование нескольких популярных файрволлов и антивирусов, познакомимся с несколькими программами для шифрования данных, архивирования и восстановления информации, а также рассмотрим некоторые неочевидные вопросы создания архивов почтовых баз Outlook Express.

ГЛАВА 12
ЗАЩИТА КОМПЬЮТЕРА: ФАЙРВОЛЛЫ

В этой главе вы ближе познакомитесь с программами для защиты информации. Это файрволлы, антивирусы, программы для шифрования и архиваторы.

Существует множество программ для защиты информации. На первый взгляд все они удобны, функциональны и вообще достойны всяческого внимания. Но практика показывает, что у каждого пользователя, осознавшего важность средств информационной защиты, появляются собственные предпочтения в отношении программ. Это и понятно: мне самому случалось, установив популярную программу с самыми хорошими рекомендациями, через некоторое время осознавать, что мы с ней «не сходимся характерами». Но бывает и по-другому: установив программу, срастаешься с нею душой (я не шучу!) и хранишь ей верность долгие годы.

Но, чтобы найти свою любовь, ее нужно по меньшей мере искать. Этим мы и займемся. Я представлю вашему вниманию по нескольку разных программ из каждого «семейства» защитных средств, а вы будете решать, что вам подходит, а что нет.

Начнем со стандартного брандмауэра, который появился в Windows XP с пакетом обновлений SP2.

12.1. БРАНДМАУЭР WINDOWS

При установке операционной системы Windows XP SP2 файрволл, в отличие от старого (ICF) Internet Connection Firewall, включается по умолчанию и начинает защищать систему сразу после ее установки. Старый ICF нужно было настраивать для каждого соединения отдельно, устанавливая флажок на вкладке **Дополнительно** окна свойств соединения, а управление новым файрволлом ведется централизованно. К тому же у «новичка» имеется развитый интерфейс настройки. И еще одно новшество: брандмауэр Windows XP SP2 поддерживает протокол IP v.6.

Настройку Windows Firewall начнем с **Панели управления** (рис. 12.1).

Зайдя в **Панель управления**, достаточно щелкнуть по иконке **Брандмауэр Windows**. Откроются настройки его свойств. Но можно поступить по-другому.

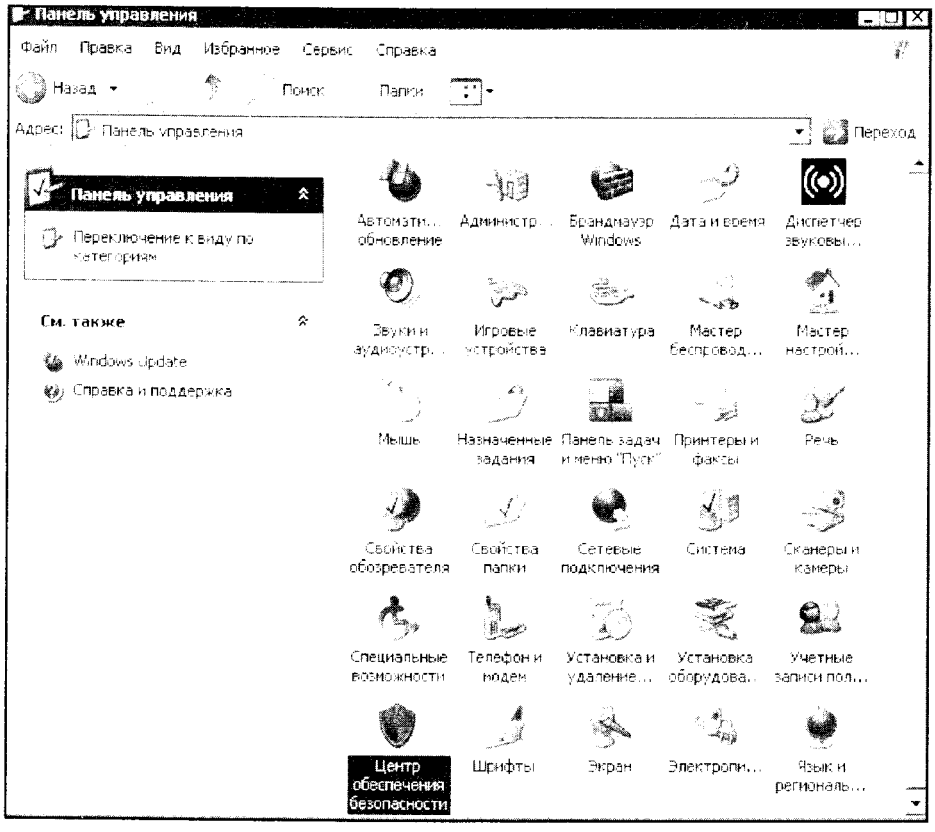


Рис. 12.1. Панель управления

На рис. 12.1 выделен значок **Центра обеспечения безопасности раздела Панель управления**. Это тоже одно из нововведений SP2. **Центр обеспечения безопасности** объединяет информацию о файрволле, антивирусе и обновлении системы. Открыв окно **Центра** (рис. 12.2), можно оперативно оценить состояние этих параметров системы и настроить их.

Правда, **Центр обеспечения безопасности** иногда неаккуратно работает с антивирусами. Посмотрите: на рис. 12.3 он предупреждает, что антивирус необходимо обновить. Но обновление состоялось всего за несколько минут до запуска **Центра**! Так что даже такому удобному и полезному новшеству, как Центр обеспечения, не стоит доверяться вслепую, особенно в том, что касается программных продуктов сторонних производителей. Если вы уверены, что базы вашего антивируса дышат свежестью и новизной, просто не обращайте внимания на заявления **Центра**.

Теперь запустим окно свойств брандмауэра. Сделать это можно или прямо из окна **Центра**, или из **Панели управления**. В этом окне есть вкладка **Общие**, где можно настроить основные параметры брандмауэра.

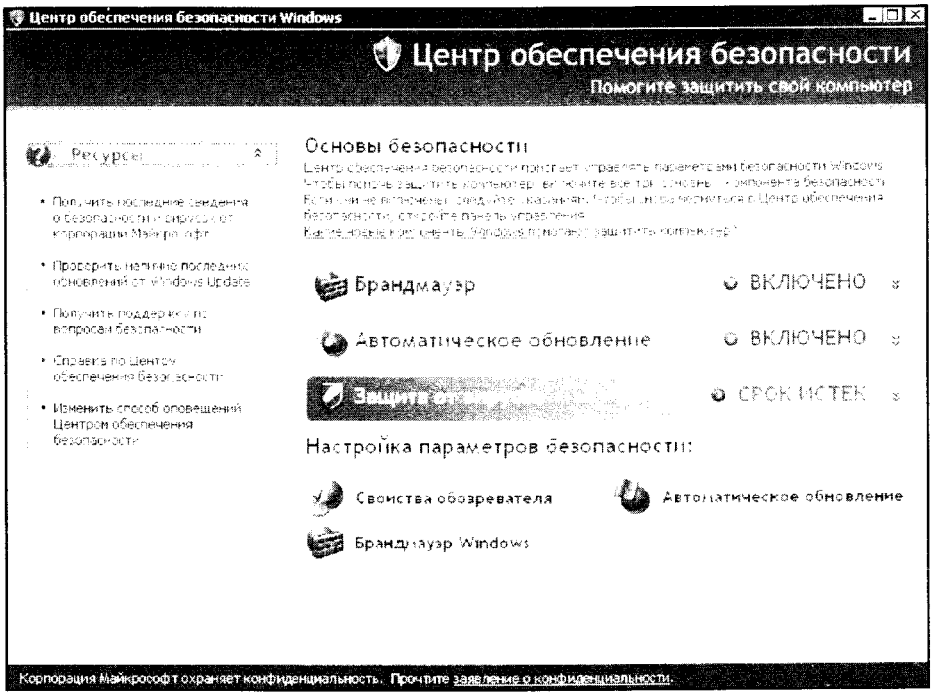


Рис. 12.2. Центр обеспечения безопасности

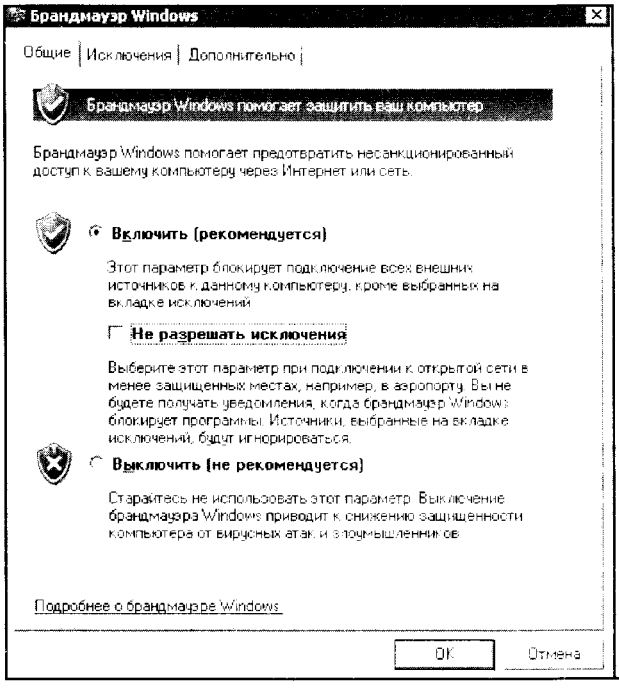


Рис. 12.3. Вкладка Общие окна настройки брандмауэра

Здесь можно включать и выключать файрволл, используя соответствующие переключатели. Если с этими параметрами все понятно, то рассмотрим подробнее параметр **Не разрешать исключения**.

Исключения — это особые правила, которые назначаются программам, нуждающимся в работе с Сетью. Если установить флажок **Не разрешать исключения** и тем самым запретить эти самые исключения, то ни одна программа, кроме веб-браузера и почтового клиента, не получит доступа в сеть, а вас не будут беспокоить их назойливые запросы доступа. Но для программ, которым действительно нужен Интернет, можно настроить исключения из этого правила. Для этого в окне есть специальная вкладка с одноименным названием (рис. 12.4).

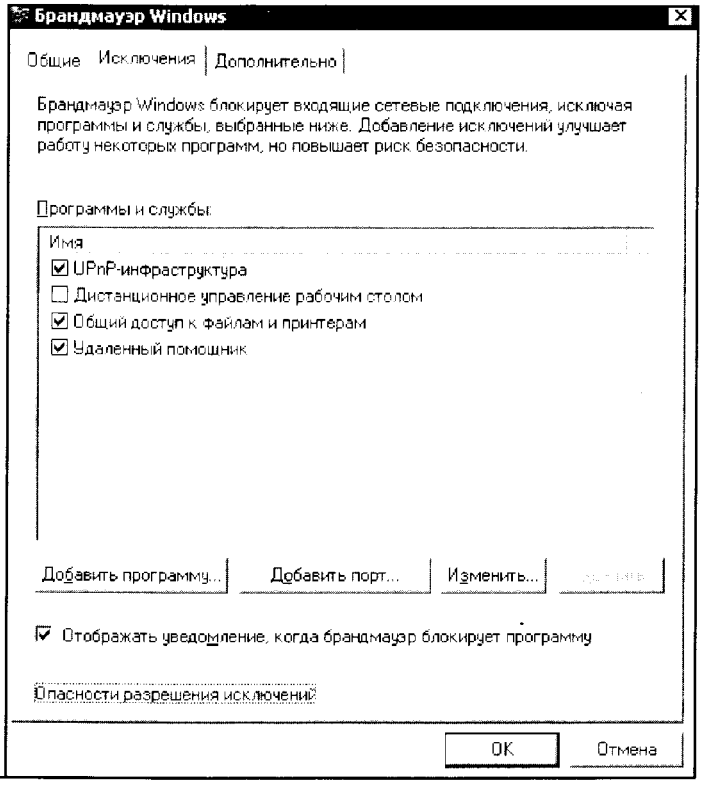


Рис. 12.4. Настройка исключений

Здесь вы самостоятельно можете добавить в список исключений нужные программы. При этом помните: добавляя программы и порты в список исключений, вы разрешаете программам свободный доступ в Интернет и открываете добавленные порты.

Но обычно нет необходимости добавлять программы вручную и назначать для них исключения: при установке или первом запуске любой программы Windows сама предложит вам создать для нее исключение (рис. 12.5).

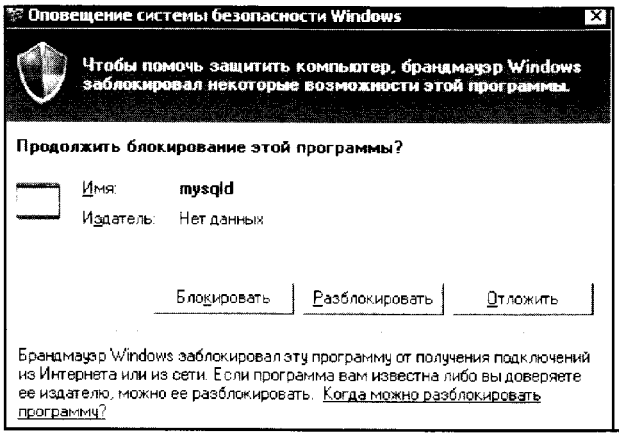


Рис. 12.5. Настройка исключения

Все очень просто: если вы хотите создать исключение — нажмите кнопку **Разблокировать**, ну а если хотите запретить программе прием входящих подключений из Интернета или из локальной сети, нажмите **Блокировать**.

В соединении с Интернетом или с локальной сетью нуждаются немногие программы, и вряд ли вы будете часто видеть эти окна. Ну а если вы не пользуетесь ничем, кроме электронной почты и браузера, то исключения вам и вовсе не потребуются.

Брандмауэр Windows защищает систему от несанкционированных внешних подключений, пропуская только те данные, которые пришли в ответ на запрос с вашего компьютера или предназначены для соответствующего соединения.

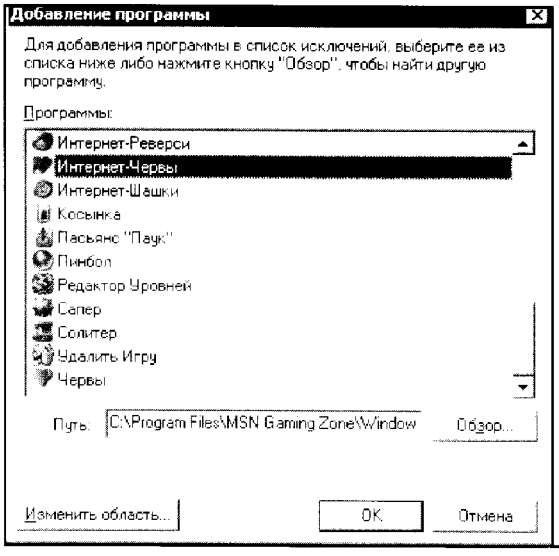


Рис. 12.6. Добавление программы к списку исключений

Программы в окно исключений можно добавлять и вручную. Чтобы добавить программу в список исключений, нажмите на кнопку **Добавить программу** вкладки **Исключения** (рис. 12.6).

В окне **Добавление программы** можно при необходимости задать область, из которой добавленной программе будет разрешено принимать подключения (рис. 12.7).

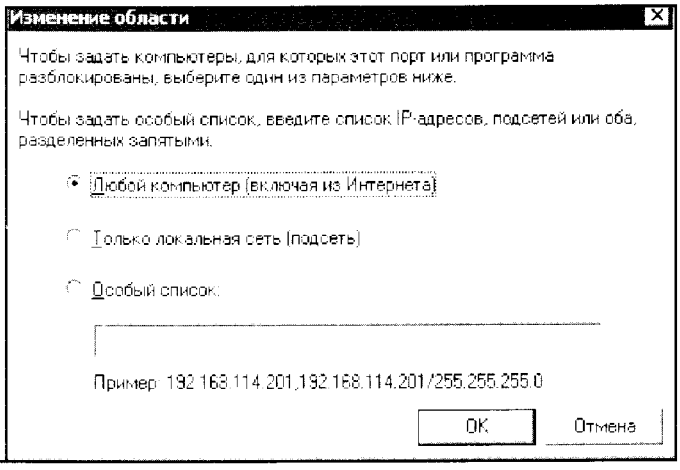


Рис. 12.7. Изменение области

Помимо общих установок, открывающих доступ к подключению с любого компьютера или из локальной сети, здесь доступны особые установки IP-адресов, с которых разрешено принимать входящие подключения для программы.

На той же вкладке **Исключения** можно добавлять порты, по которым ваш компьютер сможет принимать входящие подключения (рис. 12.8). Если ваш компьютер обычная пользовательская рабочая станция, лучше не открывать никаких портов: это может серьезно повредить безопасности вашего компьютера.

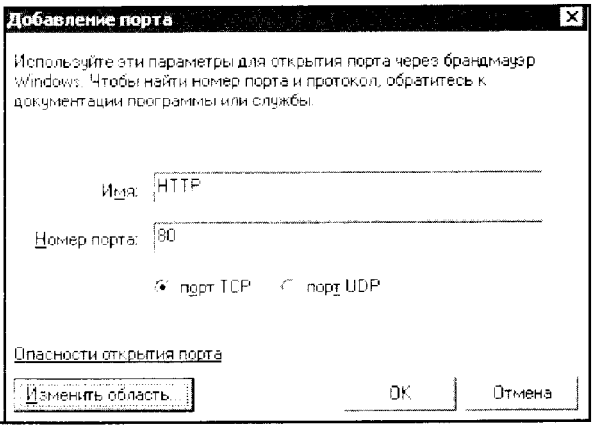


Рис. 12.8. Открытие порта

Но раз так, спросите вы, зачем же операционная система предусматривает возможность произвольного открытия портов? Открытие портов требуется для функционирования серверов. Если бы у вас на компьютере функционировал, к примеру, HTTP-сервер, то, чтобы сервер мог принимать входящие подключения, пришлось бы открыть 80-й порт. Но в остальных случаях — никаких открытых портов! Если вам в точности известно, какой порт использует та или иная программа, можно просто добавить этот самый порт, не добавляя программу в список исключений, или поступить наоборот, то есть сделать программу исключением, не добавляя портов. Результат будет один и тот же.

Обратите внимание на список исключений вкладки **Исключения** (рис. 12.4). Что же за программы стали исключениями по умолчанию? Посмотрите: в списке есть пункт **Общий доступ к файлам и принтерам**. Сбрасывание этой установки приведет к проблемам с доступом к вашим ресурсам по локальной сети, но они настроены так, что из Интернета получить доступ к ним нельзя.

Посмотрите на рис. 12.9. Здесь изображена следующая вкладка окна настройки свойств брандмауэра Windows, которая называется **Дополнительно**.

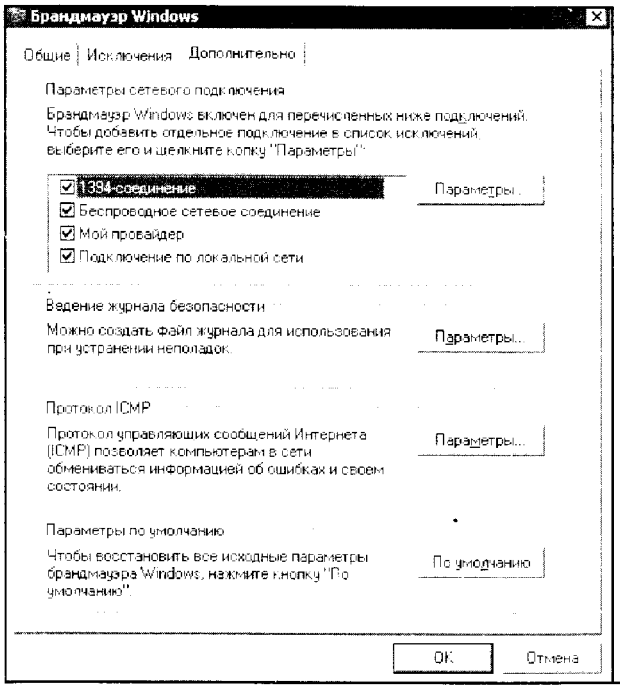


Рис. 12.9. Настройка дополнительных параметров брандмауэра

Здесь перечисляются сетевые подключения, с которыми работает **Брандмауэр Windows**. Их, кстати, можно настроить. Для этого нужно выделить подключение и нажать на кнопку **Параметры**: при этом появится окно для настройки дополнительных параметров этого подключения (рис. 12.10).

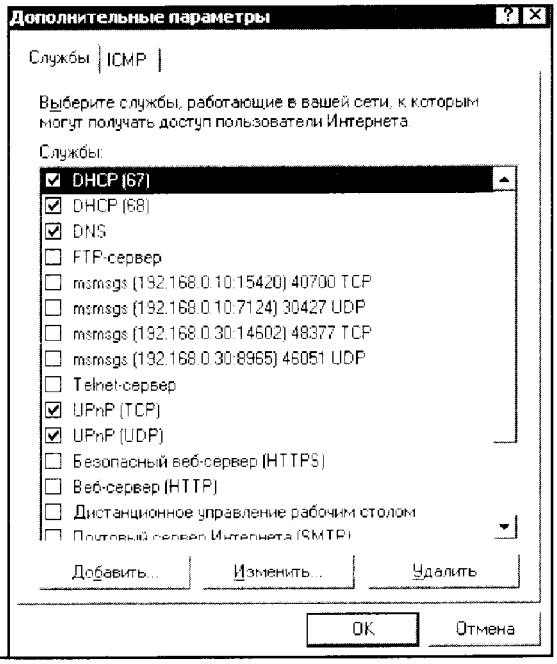


Рис. 12.10. Настройка дополнительных параметров соединения

Вкладка **Службы** позволяет настроить доступ пользователей Интернета к службам вашей локальной сети. К этой вкладке мы вернемся, когда займемся настройками собственного веб-сервера, а также почтового

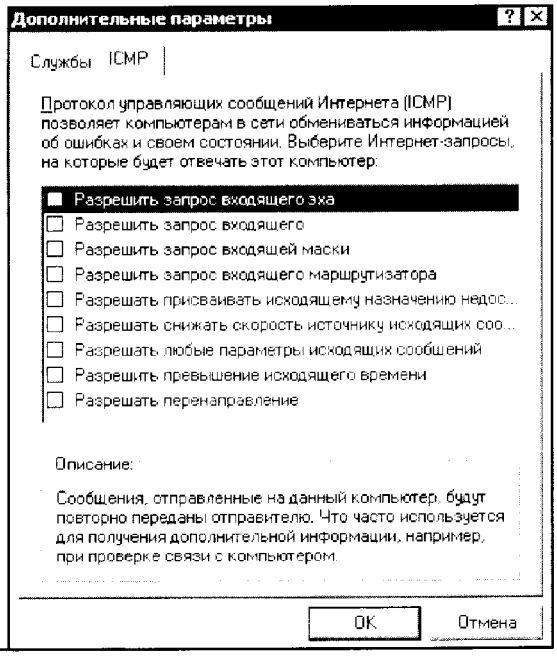


Рис. 12.11. Настройка ICMP

и FTP-серверов. Пока же замечу: чтобы, например, пользователи локальной сети могли использовать ваш HTTP-сервер, нужно убрать 80-й порт из списка исключений, разрешив при этом работу сервиса (веб-сервер HTTP) при настройке свойств подключения.

Вторая вкладка окна **Дополнительные параметры** называется ICMP (рис. 12.11).

Здесь нужно установить галочку напротив параметра **Разрешить запрос входящего эха**. Иначе вы не сможете проверять работу сети средствами команды `ping`.

Вернемся на вкладку **Дополнительно** окна настройки **Брандмауэра Windows**. В нем есть еще несколько кнопок, которые позволяют настраивать дополнительные опции.

Кнопка **Параметры** рамки **Ведение журнала безопасности** позволяет установить параметры такого журнала (рис. 12.12).

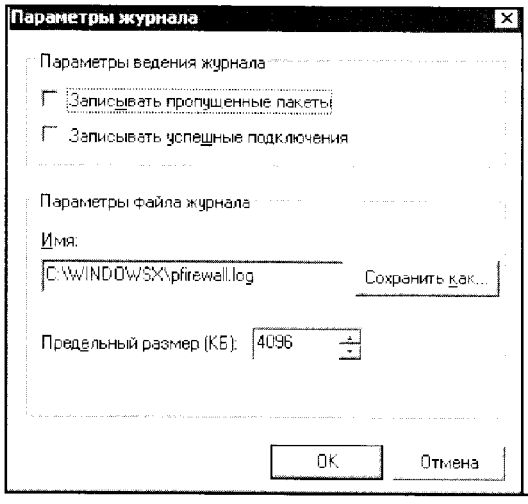


Рис. 12.12.
Настройка параметров журнала

Вести журнал нужно, чтобы следить за работой брандмауэра и анализировать ее. Если вы подозреваете, что с сетевой безопасностью вашей системы не все в порядке, можно включить протоколирование, а потом проанализировать записи журнала. Возможно, с непривычки вам сложно будет разобраться в них, но после прочтения этой главы вам многое станет понятно.

О журналах мы еще поговорим — по той причине, что другие файрволлы, о которых пойдет речь в этой главе, содержат более развитые и информативные средства для работы с журналами и протоколируют куда больше интересных вещей, чем стандартный файрволл Windows.

На вкладке **Дополнительно** в рамке настройки протокола ICMP есть кнопка **Дополнительно**. Она позволяет настроить ICMP для всех сетевых соединений. Внешний вид окна настроек ICMP очень похож на рис. 12.11. Также как и в случае с конкретными соединениями, здесь ре-

комендуется устанавливать флажок напротив параметра **Разрешить запрос входящего эха**.

Для сброса дополнительных параметров по умолчанию можно нажать кнопку **По умолчанию** на той же вкладке.

12.2. ZONE ALARM

Если говорить об улучшениях встроенного программного обеспечения Windows, то файрволл Windows — серьезный шаг вперед. Но этот файрволл «в одиночку» не может обеспечить достаточный уровень контроля над системой. Дело в том, что он не содержит средства для управления исходящими соединениями, то есть по умолчанию он «считает», что содержимое вашего компьютера достойно доверия. При этом вы не получаете даже простейших средств для контроля за программами, установленными на вашем ПК.

И все же не стоит увлекаться файрволлом Windows: к примеру, если вы только что купили компьютер и не настроили все необходимые программы, ваша система вовсе не беззащитна. Но потом все же лучше обзавестись более продвинутым файрволлом. Их много, но мы остановимся на нескольких из них.

Начнем с известного и заслуженно популярного файрволла Zone Alarm. Он хорош, кроме прочего, еще и тем, что в придачу к платной имеет и официальную бесплатную версию. В этом разделе мы рассмотрим полнофункциональную версию файрволла: скачав и установив ее, вы можете в течение некоторого времени ею пользоваться, попутно изучая возможности этой программы. Ну а когда закончится испытательный (*trial*) период, можно решить, стоит ли этот файрволл своей цены или вам хватит его упрощенной бесплатной версии.

Упрощения Zone Alarm коснулись в основном возможности настроек программы и дополнительных возможностей, а ядро программы — файрволл — одно и то же и в платной версии, и в бесплатной. Однако уровень защиты бесплатной версии ниже, чем уровень «платной» защиты». Так что если Zone Alarm вам понравится, обратите внимание именно на полнофункциональную его версию.

Начиная рассказ о Zone Alarm, хочу уточнить, что мы будем рассматривать не только файрволл Zone Alarm, но и всю систему безопасности ZoneAlarm Security Suite. С сайта компании можно скачать пробную 15-дневную версию этого продукта. Вы также можете найти бесплатную копию установочного пакета на компакт-диске, приложенном к этой книге.

Перечислим основные возможности ZoneAlarm Security Suite. Для начала — файрволл, то есть центральная часть программы. Особенностью Zone Alarm является простой и дружественный интерфейс. На первый взгляд его крупные кнопки, яркие надписи и стрелки кажут-

ся легкомысленными или даже «игрушечными», но это впечатление быстро проходит, а «легкомысленный» дизайн делает работу с ZoneAlarm легкой и приятной.

Файрволл ZoneAlarm поддерживает как защиту от внешних вторжений, по которым он ведет подробную статистику, так и пристальный контроль за всеми программами, которые пытаются получить доступ к Интернету с вашего компьютера.

Также в пакет ZoneAlarm Security Suite входит антивирус. Этот антивирус построен по тем же принципам, что и файрволл, то есть он прост, понятен и обладает высокими качествами.

Кроме файрволла и антивируса, пакет ZoneAlarm Security Suite включает средства для защиты ваших персональных данных: блокировщик *cookies* и блокировщик всплывающих окон. Помимо этого, программа пристально наблюдает и сканирует содержимое входящей и исходящей электронной почты. А еще ZoneAlarm умеет блокировать спам и фильтрует доступ к определенным веб-сайтам.

Установка программы представляет собой стандартную процедуру. Вам зададут несколько обычных вопросов, на которые вы ответите нажатием кнопки **Next**, заполните простую анкету (рис. 12.13), и первый этап установки на этом завершится.

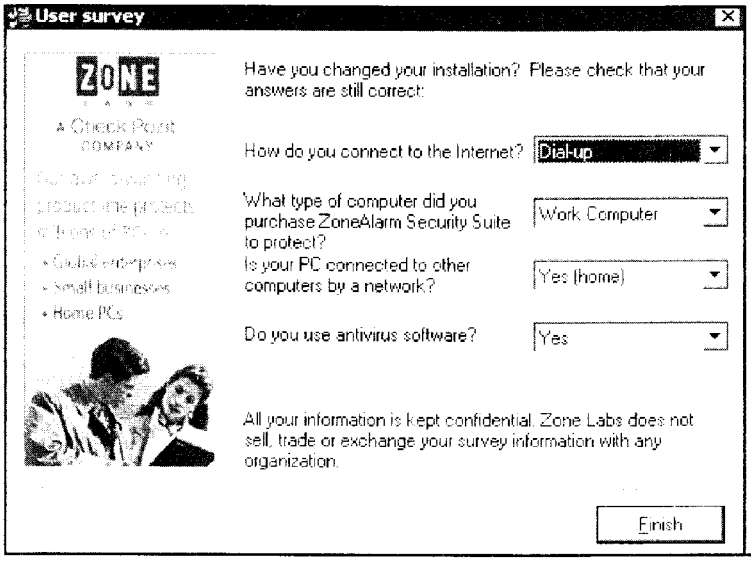


Рис. 12.13. Установка ZoneAlarm Security Suite

После первого запуска программы вы увидите окошко (рис. 12.14), приглашающее вас просмотреть и при необходимости исправить первоначальные установки, а также пройти курс обучения работы с программой. Текста в «обучалке» немного, и, вооружившись англо-русским словарем, даже несведущий в языках пользователь быстро научится работать с программным пакетом ZoneAlarm Security Suite.

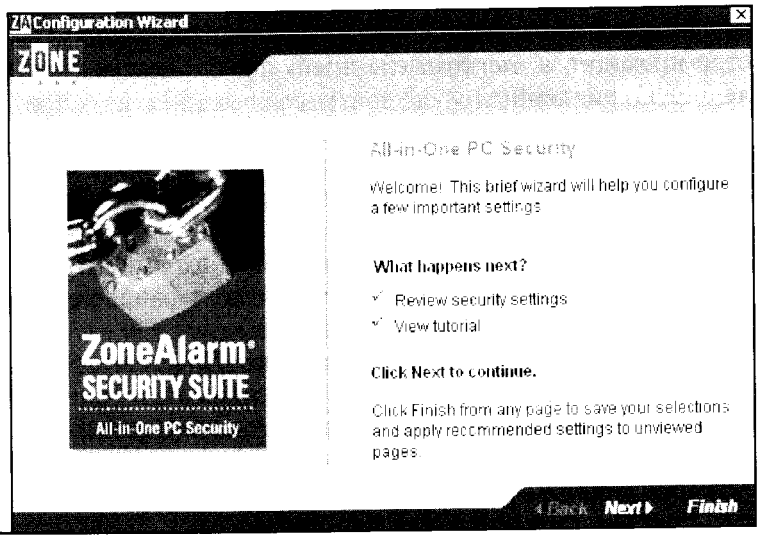


Рис. 12.14. Первоначальная настройка программы

Нажав кнопку **Next**, вы попадете в окно, где программа спрашивает вас о том, позволяете ли вы отослать ваши настройки на ее сайт, чтобы специалисты компании проанализировали их и применили полученный опыт в создании новых версий программы. Вы можете ответить либо **Yes, anonymously share my setting**, согласившись с ее предложением, либо **No, thanks**. И тот и другой ответы подходят для продолжения первоначальной настройки программы, но я бы рекомендовал ответить согласием — хотя бы из благодарности разработчикам.

Следующее окошко содержит вопрос об установках так называемого **Alert Advisor'a** — это сообщения, которые выдает программа в случае атак на ваш компьютер. Здесь будет разумным выбрать пункт **Automatic**, чтобы программа автоматически настроила эту свою возможность.

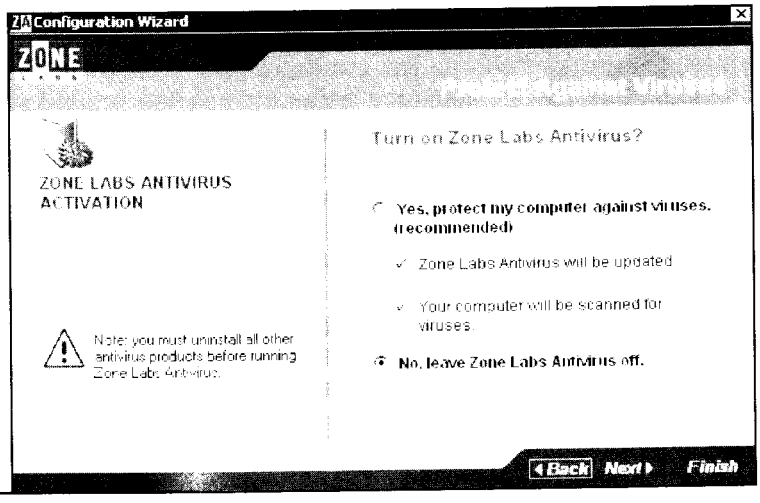


Рис. 12.15. Включение или выключение антивируса

Дальше предстоит сделать серьезный выбор, касающийся включения или отключения антивируса, встроенного в пакет (рис. 12.15). У нас уже есть антивирус (какой — скажу позже), поэтому сейчас мы отключим антивирус ZoneAlarm, выбрав соответствующий пункт.

Но если вы не пользуетесь другими антивирусными программами, лучше включить антивирус ZoneAlarm, который все же неплох.

Следующее окно посвящено настройке блокировки спама. Эту опцию лучше выключить: в России блокировка спама этой программе не удается.

Если вы активно пользуетесь ICQ или другим интернет-пейджером, обратите внимание на возможность защиты систем обмена сообщениями (рис. 12.16).

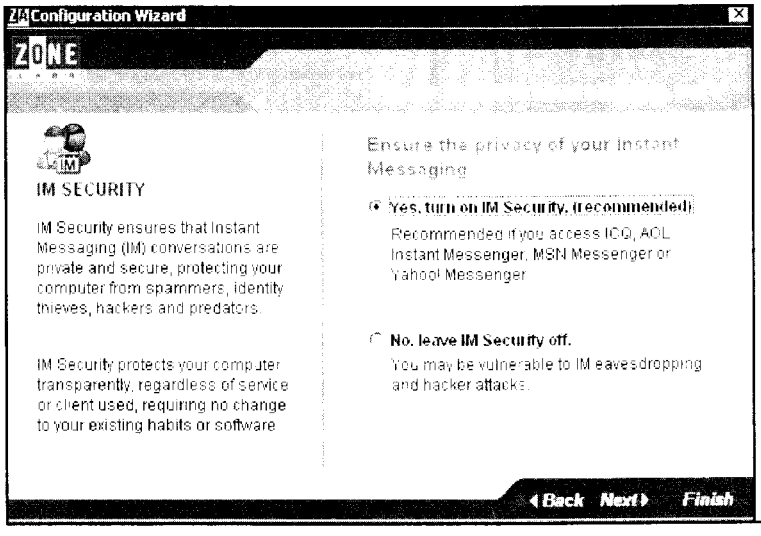


Рис. 12.16. Настройка защиты систем обмена сообщениями

Следующее окно, которое позволяет настроить веб-фильтрацию, по умолчанию отключает эту возможность. Если вам нужно будет что-нибудь фильтровать, отсекая ненужные или вредные сайты, вы сможете вернуться к настройке этого параметра позднее. (Да и вообще ко всем настройкам, которых мы касаемся на начальном этапе, можно вернуться позже, уже после того, как программа заработает.)

Дальше программа предложит вам включить настройки по защите вашей персональной информации (рис. 12.17).

Включив эти настройки, вы сможете увеличить эффективную пропускную способность вашего интернет-канала за счет блокирования загрузки всплывающих окон, рекламных баннеров, фильтрации *cookies*. Помимо экономии пропускной способности канала, все это делает информацию о ваших перемещениях в Сети недоступной для тех, кто захочет проследить за вами. Речь тут идет, скорее, о статистике, собираемой различными серверами, как утверждается, в мирных целях, но установки с рис. 12.17 все же лучше включить.

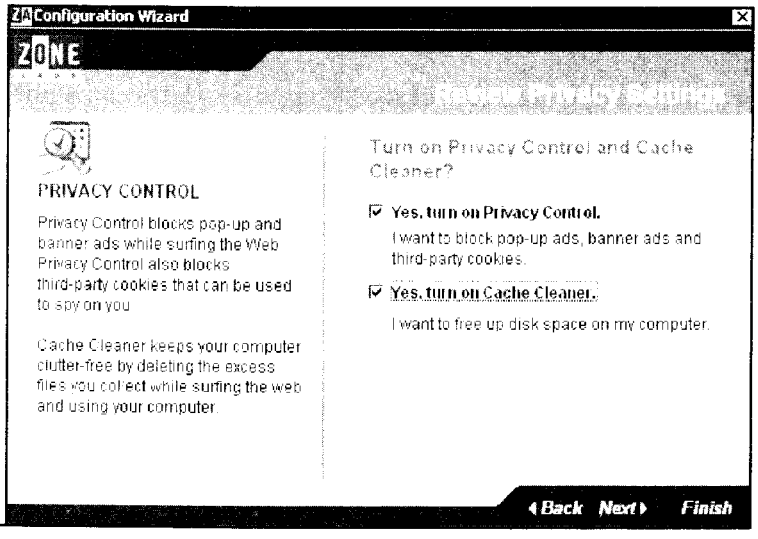


Рис. 12.17. Настройка персональной информации

Если сравнить ощущения от работы без файрволла и с файрволлом, то во втором случае скорость загрузки страничек заметно возрастает. Еще бы: блокируются всплывающие окна и рекламные баннеры, «съедающие» ощутимую часть пропускной способности вашего канала доступа.

Когда вы выполните все эти действия, вам предложат перезагрузиться, после чего начнется учебный курс ZoneAlarm (рис. 12.18). Он состоит из 10 уроков, и я очень советую вам просмотреть этот курс: в простой и доходчивой форме он рассказывает о том, как пользоваться основными возможностями программы.

Когда вы просмотрите учебный курс или просто нажмете на кнопку **Finish**, файрволл заработает. И тут же завалит вас кучей вопросов, касающихся предоставления доступа в Интернет различным программам.

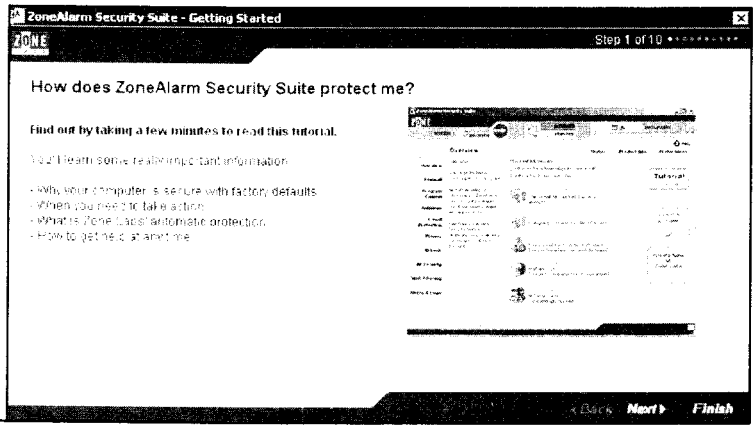


Рис. 12.18. Учебный курс программы

Посмотрите на рис. 12.19. Здесь изображена немного нетипичная ситуация. Программа ActiveSynk, которая нужна для подключения к компьютеру КПК, хочет действовать в качестве сервера. Это правильно, и такое действие ей надо разрешить.

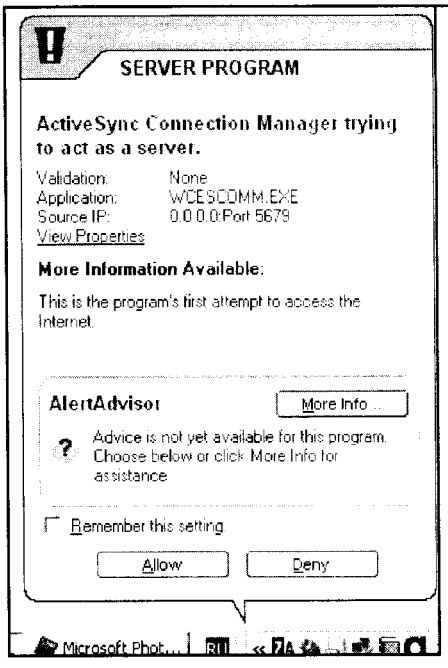


Рис. 12.19. Запрос на предоставление программе разрешения для работы в качестве сервера

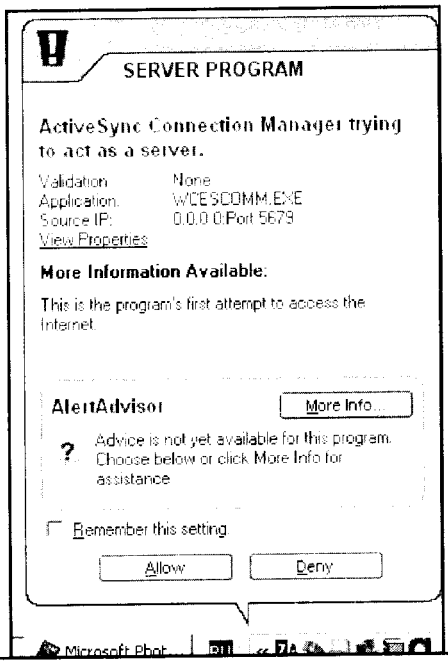


Рис. 12.20. Включение разрешения для программы

Для этого нажмите на кнопку **Allow (Разрешить)**, предварительно установив флажок **Remember this setting (Запомнить настройки)**. Если такой флажок не установить, то, если этой программе снова что-нибудь понадобится сделать, файрволл будет спрашивать вашего позволения снова и снова.

Программа ZoneAlarm «разговорчива» и сообщений выдает много. Она, к примеру, станет спрашивать вашего разрешения на доступ в Интернет для каждой программы, которая захочет туда попасть. Например, на рис. 12.20 изображен запрос, который файрволл выдает в ответ на попытку Outlook Express проверить почту.

Ну а если вы работаете в Интернете, то программа будет постоянно бомбить вас сообщениями о заблокированных атаках и попытках несанкционированного доступа к вашим ресурсам (рис. 12.21). Вот тут-то вы по-настоящему поймете необходимость мер безопасности в сети!

Это еще довольно мирные сообщения, но есть у ZoneAlarm и сообщения менее приятные, связанные с атаками разного уровня (рис. 12.22).

Рис. 12.21. Сообщение системы безопасности

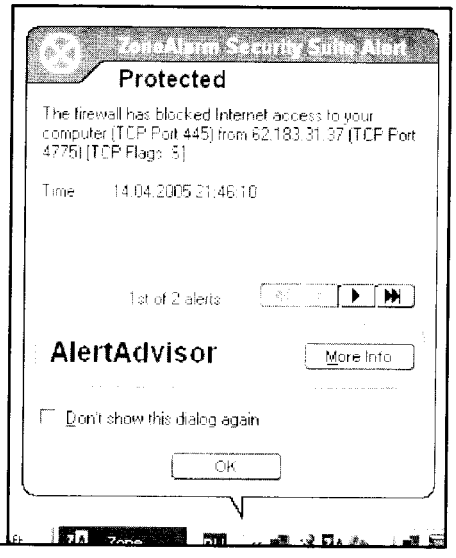


Рис. 12.22. Информация о предотвращенной атаке

Ну а если сообщения ZoneAlarm будут мешать работе, их можно отключить, поставив галочку перед параметром **Turn off Privacy Advisor (Отключить сообщения о попытках вторжения)**.

Всеми возможностями программы можно управлять через ее главное окно. Его можно открыть, сделав двойной щелчок по значку файрволла в системной панели. Если закрыть главное окно программы, она от этого не остановится, а лишь «спрячется», превратившись в крохотный значок на системной панели.

Окно Zone Alarm состоит из множества разделов, каждый из которых поделен на вкладки. Посмотрите на рис. 12.23. Здесь вы можете видеть главное окно программы, Overview, где находится общая статистика деятельности файрволла. Здесь же можно найти несколько вкладок.

В верхней правой части окна есть большая красная кнопка **Stop** и пиктограмма, изображающая незапертый замок. Если вы хотите мгновенно запретить подозрительную сетевую активность, щелкните по этой кнопке или по замку. При этом замок закроется и нехорошая интернет-активность будет остановлена.

На вкладке **Status (Статус)** раздела **Overview (Обзор)** можно найти общую информацию о файрволле и о предотвращенных им атаках. Вкладка **Product Info (О программе)** содержит информацию о версиях установленных продуктов, причем с помощью этой вкладки можно купить

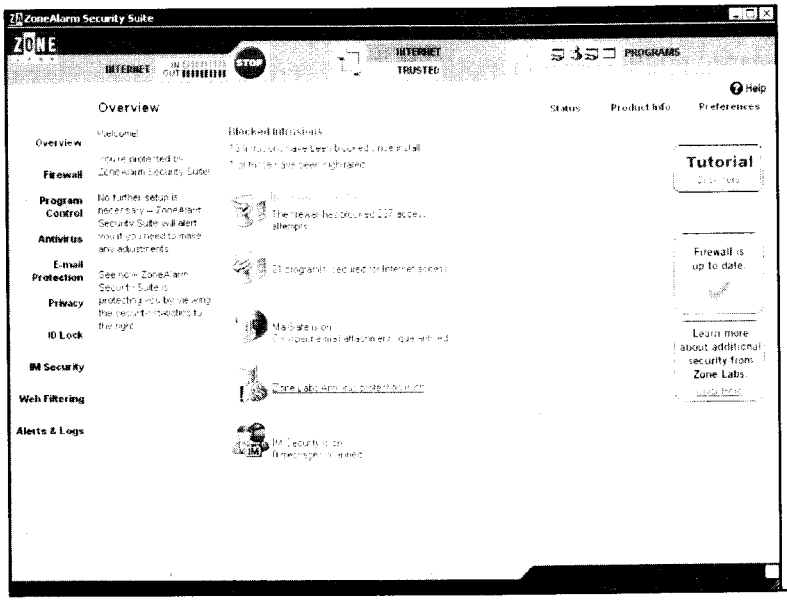


Рис. 12.23. Раздел Overview, вкладка Status

полнофункциональную версию продукта. На вкладке **Preferences (Предпочтения)**, что на рис. 12.24, можно установить пароль, настроить порядок загрузки ZoneAlarm и порядок работы с вашим IP-адресом во время взаимодействия с Zone Labs.

Установка **Hide the last octet of my IP address when applicable (Скрыть последние 8 бит моего IP-адреса)** позволит скрывать последний байт вашего IP-адреса при контактах программы с компанией-разработчи-

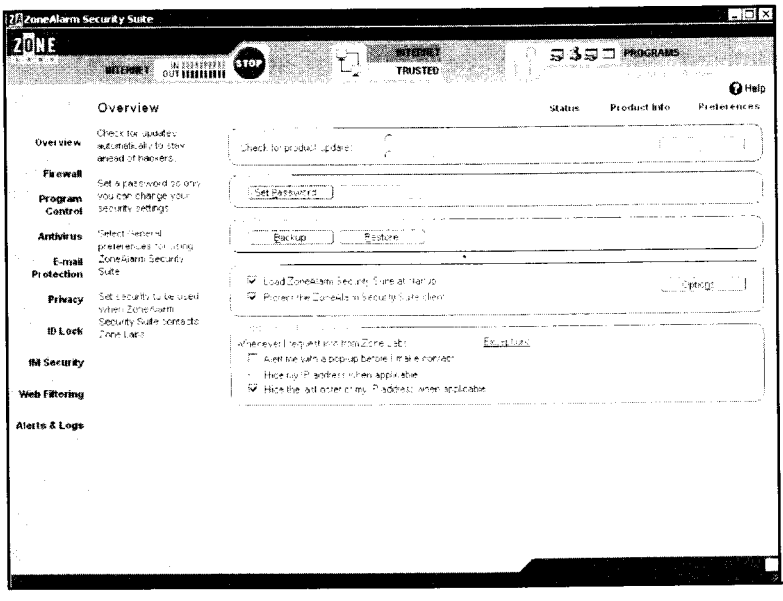


Рис. 12.24. Раздел Overview, вкладка Preferences

ком. Ну а установка **Hide my IP address when applicable** позволяет скрывать ваш IP-адрес полностью.

Следующий раздел окна Zone Alarm называется Firewall и служит, ясное дело, для настройки файрволла (рис. 12.25).

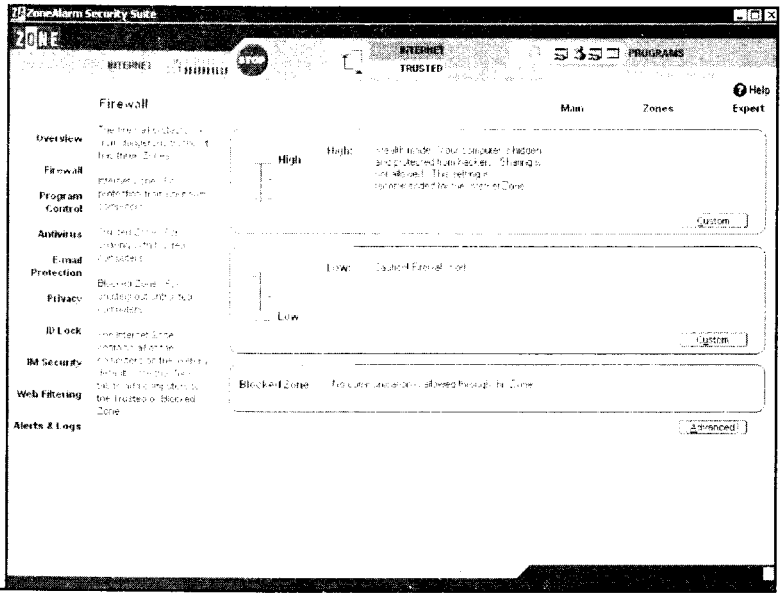


Рис. 12.25. Раздел Firewall, вкладка Main

Настраивая файрволл, ходить дальше вкладки **Main (Главная)** нет смысла, да и ручными установками, доступными при нажатии кнопок **Custom (Пользовательский выбор)**, лучше тоже не заниматься, особенно если ваш компьютер — обычная рабочая станция. Передвиньте бегунок в рамке **Internet Zone Security (Безопасность зоны Интернета)** в положение **High (Высокая)**, и ваша система безопасности заработает во всю мощь. А вот кнопка **Advanced (Дополнительно)** может оказаться полезной: она позволяет настроить параметры работы с ICS или NAT.

Если вы организовали в сети разделяемый доступ к Интернету, то эти параметры придется настраивать вручную. На рис. 12.26 вы можете видеть окно, появляющееся после нажатия на кнопку **Advanced (Дополнительно)**.

В группе параметров **Internet Connection Sharing (Разделяемый интернет-доступ)** можно выбрать роль компьютера в сети, использующей ICS или NAT. К примеру, установка **This computer is not on an ICS/NAT network (Этот компьютер работает в сети, не использующей ICS/NAT)** включена по умолчанию.

Установка **This computer is a client of an ICS/NAT gateway**... нужна для компьютеров, которые выходят в Интернет, используя другой компьютер, то есть ICS-шлюз. И третья установка **This computer is an ICS/NAT gateway** нужна для ICS-шлюзов. Здесь же нужно настроить IP-адрес шлюза.

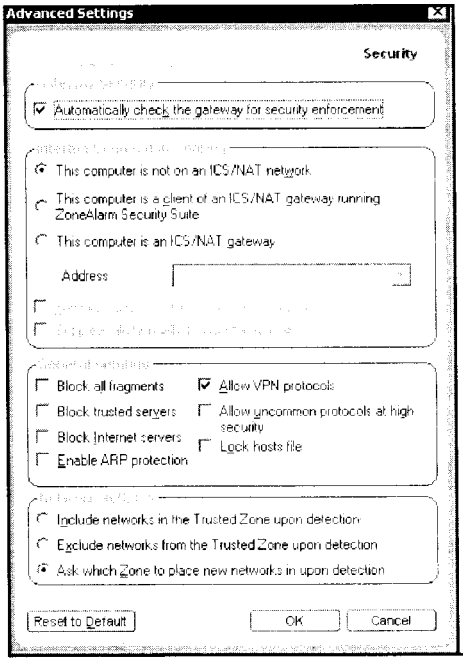


Рис. 12.26. Окно Advanced Settings

Если вы используете ICS, тогда адресом шлюза будет 192.168.0.1, ну а в других случаях за вас это сделает системный администратор вашей сети — NAT. Это довольно сложная система (схожая с ICS, но более продвинутая), которая в небольших домашних сетях практически не встречается.

Следующее окно (рис. 12.27) предназначено для настройки доступа к Интернету программ, установленных на вашем компьютере.

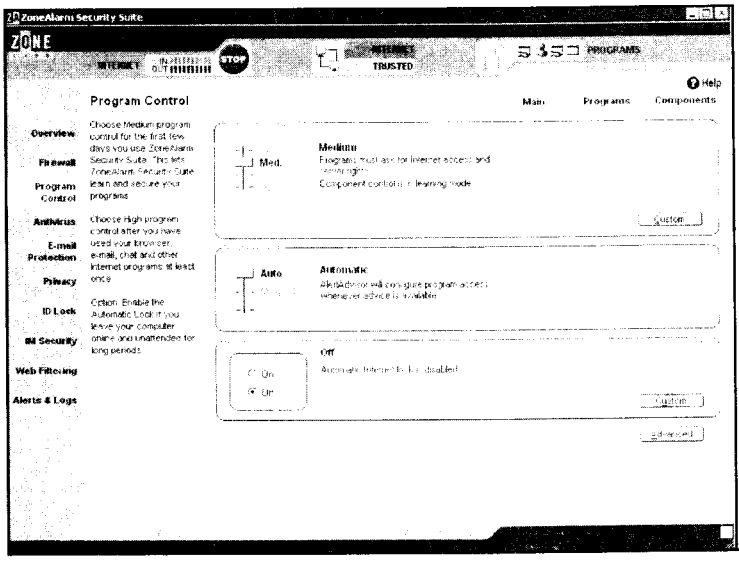


Рис. 12.27. Раздел Program control, вкладка Main

Эта вкладка похожа на вкладку настройки файрволла, только здесь вы настраиваете доступ программ к ресурсам Интернета. По умолчанию в рамке **Programm Control (Программный контроль)** установлен средний уровень контроля. Компонент **Component control** находится в режиме обучения, самостоятельно конфигурируя параметры доступа для новых компонентов.

Обратите внимание на группу параметров **Automatic Lock (Автоматическая блокировка)**. Эти настройки позволяют управлять параметрами автоматической блокировки интернет-активности в случае, если вы подключены к Интернету по высокоскоростному постоянному соединению. Если нажать на кнопку **Custom (Выбор пользователя)**, вы сможете настраивать параметры автоматической блокировки соединения самостоятельно (рис. 12.28).

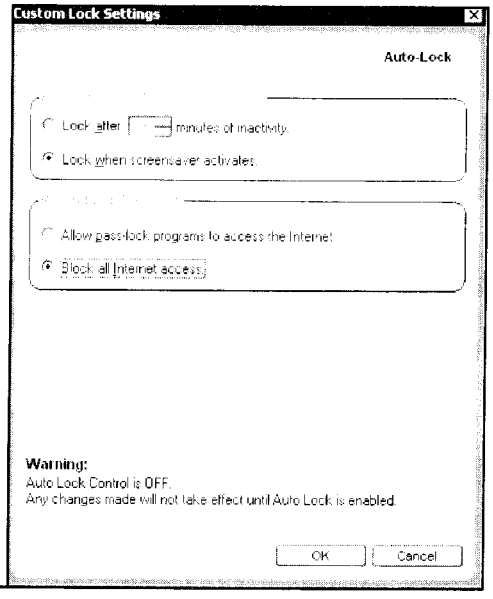


Рис. 12.28. Ручная настройка параметров автоматической блокировки соединения

Установка **Lock after screensaver activates (Блокировать после активации скринсейвера)** включает автоблокировку, если запускается хранитель экрана. Этот параметр можно установить на блокировку соединения по прошествии определенного времени. Если вы хотите, чтобы блокировка была полной, установите параметр **Block all internet access (Блокировать интернет-доступ)**. Так вы перекроете доступ в Интернет для всех программ. Эта установка полезна, если вы не хотите, чтобы программы соединялись с Интернетом без вашего ведома. В случае с *dial-up*-соединением эта проблема решается обычным разрывом связи, а если вы подключены к Сети иным способом, да еще и платите не за время соединения, а за трафик, эта установка позволяет вам лучше контролировать расход трафика.

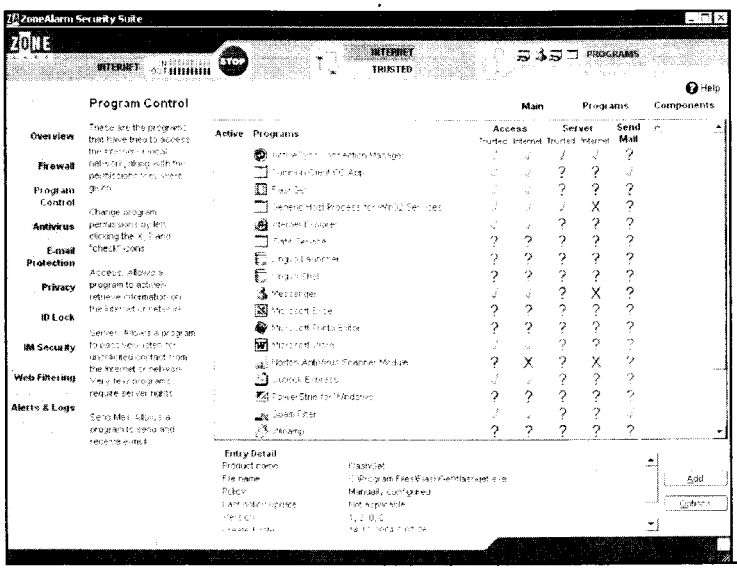


Рис. 12.29. Раздел Program control, вкладка Programs

Раздел **Program control** имеет вкладку, называющуюся Programs (рис. 12.29).

Здесь можно видеть список программ, для которых настроены права доступа к Интернету, а также добавлять программы, модифицировать их установки и так далее.

Первая колонка таблицы, в которой собраны программы, называется **Active**. Она служит для индикации интернет-активности программы. Вторая колонка — **Programs** — содержит список программ, для которых созданы правила. Третья колонка **Access** разбита на две — **Trusted** и **Internet**. Зона **Trusted** — это ваша локальная сеть, а вот **Internet** — это Интернет. Колонка **Access** определяет возможность доступа конкретной программы к ресурсам в Интернете или вашей локальной сети, видны значки, определяющие действия файрволла по отношению к данной программе.

Зеленая галочка означает наличие разрешения на доступ к ресурсам. Красный значок X определяет запрет доступа, а синий вопросительный знак означает, что действие не определено и что файрволл сам спросит вас о том, как ему поступить, если программа запросит доступ в Интернет.

Аналогично колонке **Access** устроена и колонка **Server**. Только здесь определяется возможность программ предоставлять серверные услуги в локальной сети или в Интернете.

Четвертая колонка позволяет (или не позволяет) программам отправлять электронную почту.

Последняя колонка таблицы, где изображен замок, разрешает «выпускать» в Интернет некоторые приложения даже тогда, когда доступ для всех остальных приложений закрыт. Для настройки разрешений достаточно щелкнуть левой кнопкой мыши по иконке нужной программы и по конкретной зоне доступа (рис 12.30).

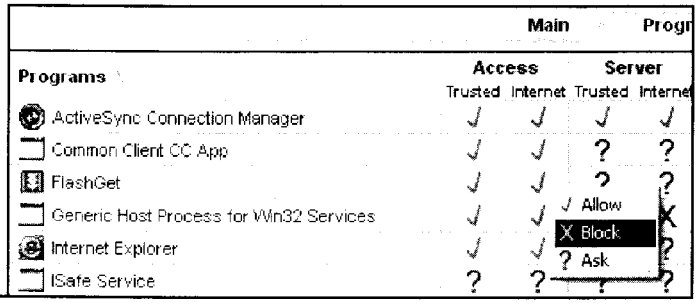


Рис. 12.30. Назначение разрешения для FlashGet

В окне на рис. 12.30 мы пытаемся настроить менеджер закачек FlashGet для доступа в Интернет. Выбрав параметр **Block**, мы попросту запретим доступ. Выбрав параметр **Allow** (который уже выбран для него), мы разрешим программе доступ к ресурсам Интернета, а выбором параметра **Ask** заставим файрволл задавать нам вопрос о разрешении или запрете доступа в Интернет для этой программы.

Ручная настройка разрешений особенно полезна, если вы случайно закрыли доступ в Интернет программе, которой он нужен. Для более продвинутых настроек программ в нижней части вкладки **Programs** есть кнопка **Options**. Выделив программу и нажав на эту кнопку, вы увидите окно, изображенное на рис. 12.31.

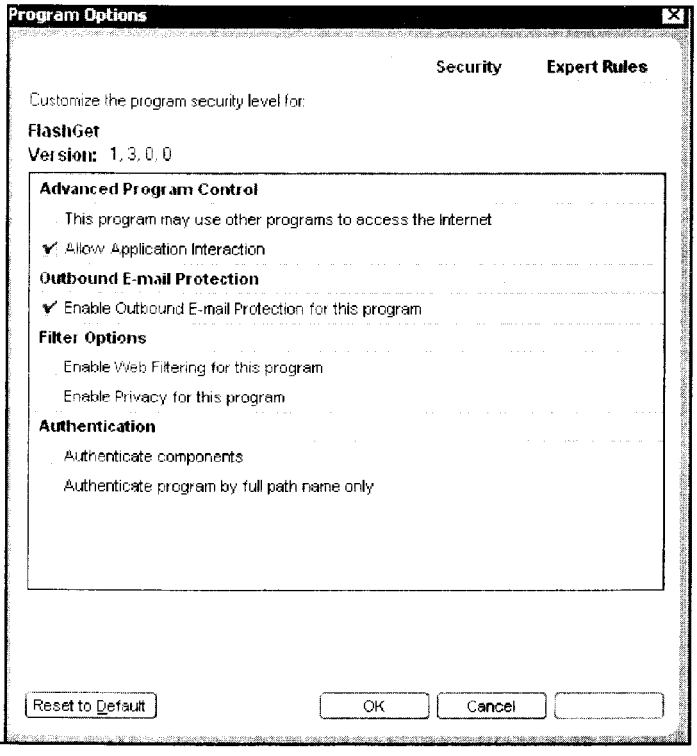


Рис. 12.31. Ручное управление параметрами программы

Как правило, здесь можно оставить установки, заданные по умолчанию. Взглянуть на них бывает полезно, если вы видите, что что-то работает не так. Например, параметры веб-фильтрации (**Enable Web Filtering for this program**) и контроля приватности (**Enable Privacy for this program**) касаются программ-браузеров. И если в случае с IE они настраиваются автоматически, то при использовании другого браузера не обойтись без дополнительных установок, если вы хотите блокировать всплывающие окна и рекламные баннеры.

Следующий раздел окна программы называется **Antivirus**. Его средствами осуществляется управление встроенным антивирусом.

Теперь настало время рассказа о защите электронной почты (рис. 12.32).

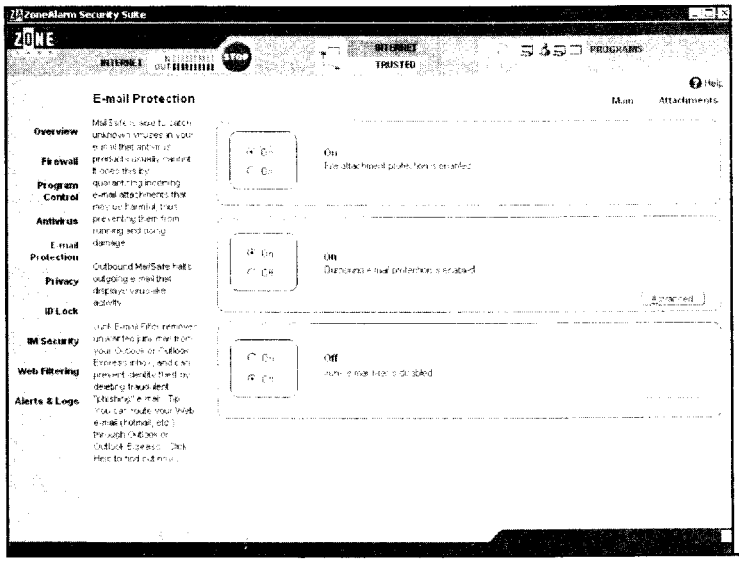


Рис. 12.32. Раздел E-mail Protection, вкладка Main

Вкладка **Main (Главная)** раздела **E-mail Protection (Защита электронной почты)** служит для общих настроек безопасности почтового клиента. Здесь есть полезные параметры **Inbound MailSafe Protection** и **Outbound MailSafe protection**. Первая установка предназначена для включения сканирования входящих писем, а вторая — для проверки исходящей почты.

Современным программам по защите электронной почты присущ комплексный подход, который предусматривает не только защиту локального пользователя от опасных вложений, но и защиту внешних пользователей от возможных проблем, вызванных локальным компьютером. Ведь файрволл или антивирус не в состоянии отследить всех червей, троянцев, программ-шпионов, которые уже могут быть установлены на ваш компьютер. А такие программы любят размножаться, рассылая самих себя по электронной почте. На рис. 12.33. изображено окно,

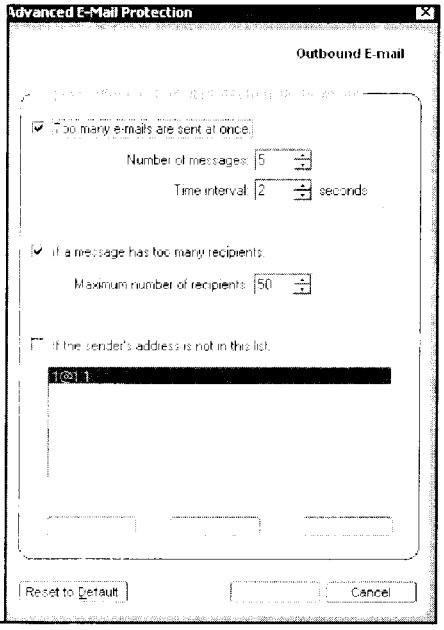


Рис. 12.33. Дополнительные параметры Outbound MailSafe protection

которое появляется при нажатии на кнопку **Advanced (Дополнительно)** группы параметров **Outbound MailSafe protection (Проверка безопасности исходящей почты)**.

Эти параметры нуждаются в дополнительной настройке, особенно в том случае, если вы активно работаете с электронной почтой и не желаете видеть периодические сообщения файрволла о возможных неприятностях.

Параметр **Too many e-mails are sent at once** предназначен для того, чтобы файрволл мог контролировать подозрительно большие количества писем, рассылаемых с малым интервалом. По умолчанию подозрительными считаются больше чем пять писем, рассылаемых с интервалом в две секунды. Если эти показатели превысят установленные по умолчанию значения, файрволл выдаст предупреждение. Если вы интенсивно работаете с электронной почтой и получаете сообщения об угрозе вашей безопасности, попробуйте увеличить значение **Number of messages (Число сообщений)** и уменьшить **Time interval (Временной интервал)**.

Еще один параметр, который стоит рассмотреть, называется **If the message have too many recipients (Если сообщение имеет слишком много получателей)**. По умолчанию слово «много» означает, что письмо отправлено больше чем пятидесяти получателям. Это в самом деле много, и защита от спама на почтовых серверах может сработать задолго до того, как число получателей письма достигнет пятидесяти. Поэтому для дополнительного контроля за исходящими сообщениями этот параметр лучше уменьшить хотя бы до 20: ведь большее число получателей встречается очень редко.

И, наконец, параметр **If the sender's address is not in this list (Если адрес отправителя не из этого списка)** обращает внимание файрволла на письма, отправленные с вашего компьютера, но имеющие адреса отправителя, которые вы не внесли в список.

Теперь перейдем ко второй вкладке раздела **E-mail protection**. Она называется **Attachment (Вложения)** и служит для настройки типов вложений, на которые файрволл должен обращать особое внимание. Лучше всего не редактировать этот список, оставив все как есть.

Следующий раздел, на который стоит обратить внимание, называется **Privacy (Приватность)**. Его вы видите на рис. 12.34.

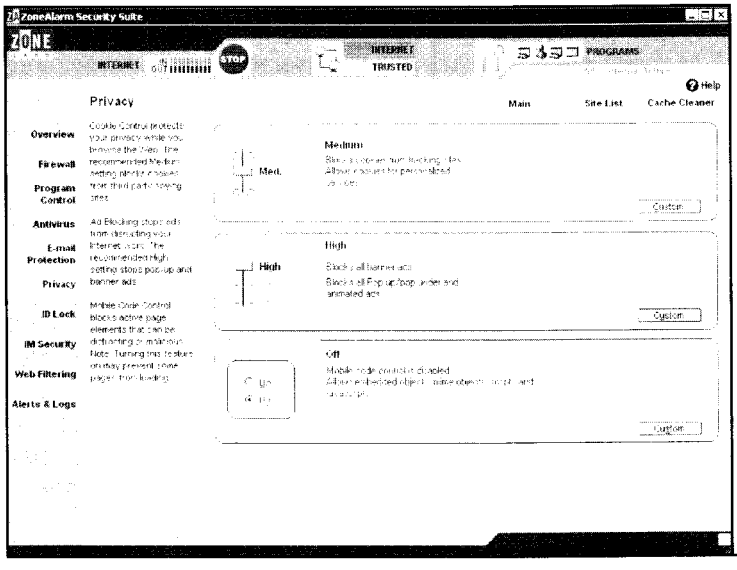


Рис. 12.34. Раздел Privacy, вкладка Main

Группа параметров **Cookie Control** предназначена для управления блокированием файлов *cookies*. Как и в других разделах программы, основные установки этих параметров можно провести, двигая бегунки. Но для более тонких настроек придется нажать на кнопку **Custom (Пользовательские настройки)**. Прежде чем нажать эту кнопку, отметим, что группа параметров **Ad Blocking** служит для настройки блокирования баннеров, всплывающих окон и прочего, а группа **Mobile Code Control** нужна для включения блокировки внедренных в веб-страницы объектов и скриптов, которые выполняются на стороне пользователя. Если вы хотите включить блокирование этих скриптов и объектов, то часть веб-страниц может потерять немалую долю функциональности.

К примеру, для организации интерфейса пользователя — различных меню, систем навигации по сайтам — весьма популярен Java Script. Если вы включите блокировку, то вы не сможете работать с некоторыми сайтами. Зато эта блокировка повышает уровень защиты.

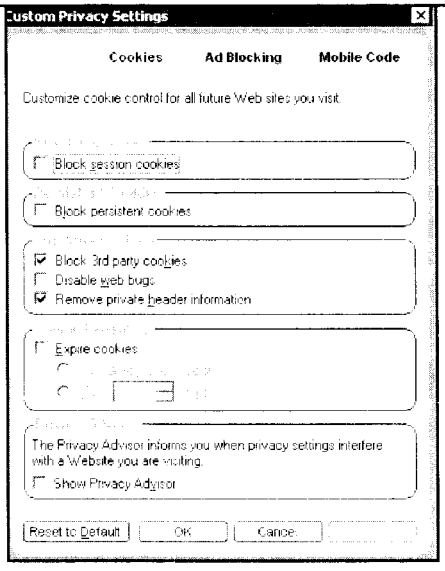


Рис. 12.35. Управление cookies

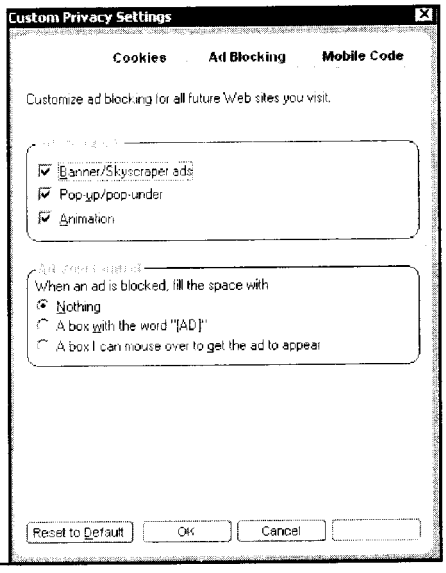


Рис. 12.36. Управление Ad blocking

Теперь обратимся к окну на рис. 12.35. Здесь можно настроить свойства блокировки *cookies*.

Чтобы установить максимальный уровень приватности, отметьте все пункты этого окна галочками. В разделе **Cookie Expiration** тоже поставьте галочку и установите параметр на **Immediately after receipt (Немедленно после приема)**. И, разумеется, включите блокировку *Web bugs* (их еще называют *Web beacons*) — маленьких невидимых картинок, которые используются для сбора информации о пользователе. Принцип их работы заключается в том, что для загрузки этой картинки браузер вынужден обратиться к веб-серверу даже в том случае, если открываемая страничка загружена не из Интернета, а например, была сохранена на жесткий диск и только после этого загружена.

Но можно и ограничиться установками по умолчанию. Ну а если вы хотите видеть сообщения ZoneAlarm о заблокированных им *cookies*, *Private Header*'ах и тому подобных вещах, поставьте галочку **Show Privacy Advisor**.

Теперь научимся блокировать рекламу и прочий мусор. На рис. 12.36 вы видите окно настройки **Ad blocking**.

По умолчанию здесь заблокировано все, что можно: рекламные баннеры (**Banner/Skyscraper ads**), всплывающие окна (**Pop-up/pop-under**) и анимационные вставки (**Animation**). Этот раздел настройки файрволла увеличивает эффективную скорость работы с Интернетом за счет блокирования загрузки ненужного рекламного контента.

Группа настроек **Ad Void Control** позволяет задать параметры замены заблокированного контента. К примеру, если установлен параметр **Nothing**,

вместо «вырезанного» баннера вы увидите фон веб-страницы или белый прямоугольник. Если установить этот параметр в **A box with the word «[AD]»**, то на месте «вырезанного» баннера появится слово AD. А если установить этот параметр в положение **A box I can mouse over to get the ad to appear**, то легким движением мыши вы сможете включать отображение баннеров: ведь некоторым Интернет без баннеров кажется скучным и бедным.

В правом верхнем углу окна есть еще одна вкладка (рис. 12.37), которая служит для настройки параметров **Mobile Code**. Эти параметры лучше не включать. Без рекламных баннеров работать можно, а вот без меню, написанного на языке JS, некоторые сайты просто перестанут отображаться или потеряют функциональность.

Вкладка **Site List** раздела **Privacy** содержит список сайтов, которые подверглись веб-фильтрации. Вкладка **Cashe Cleaner** служит для настройки параметров очистки кэша браузера и для удаления *cookies*. Этот раздел можно не трогать, так как его настройки по умолчанию вполне подходят для повседневного использования.

Разделы **IM Lock** и **ID Security** тоже можно оставить настроенными по умолчанию, а вот на разделе **Web filtering** остановимся подробнее.

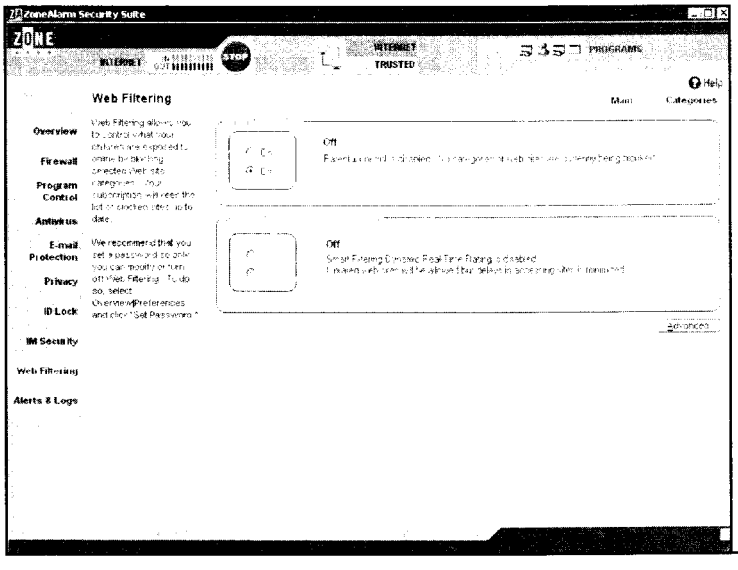


Рис. 12.37. Раздел Web Filtering, вкладка Main

Этот раздел, скорее, дань моде, чем полезная функция. Говоря теоретически, если включить блокирование веб-сайтов, то вы сможете не допустить посещения вашими детьми или подчиненными сайтов, список категорий которых содержится на вкладке **Categories**.

Но стандартизированной системы оценки контента сайтов пока нет, поэтому абсолютно надежной блокировки не получится. Лучшая «блокировка» — правильное воспитание детей и здоровые отношения в коллективе, но это к теме нашего разговора не относится.

Переходим к последнему разделу настройки ZoneAlarm Security Suite, который называется **Оповещения и данные журнала**, или **Alerts & Logs** (рис. 12.38). Здесь можно просмотреть журналы, которые ведет файрволл, и провести их настройку.

Если параметр **Program Logging** установить в значение **High**, то будут протоколироваться все события, генерируемые программами.

Параметр **Alert Events Shown** позволяет включать и отключать сообщения об атаках. Если вы хотите видеть все атаки на ваш компьютер

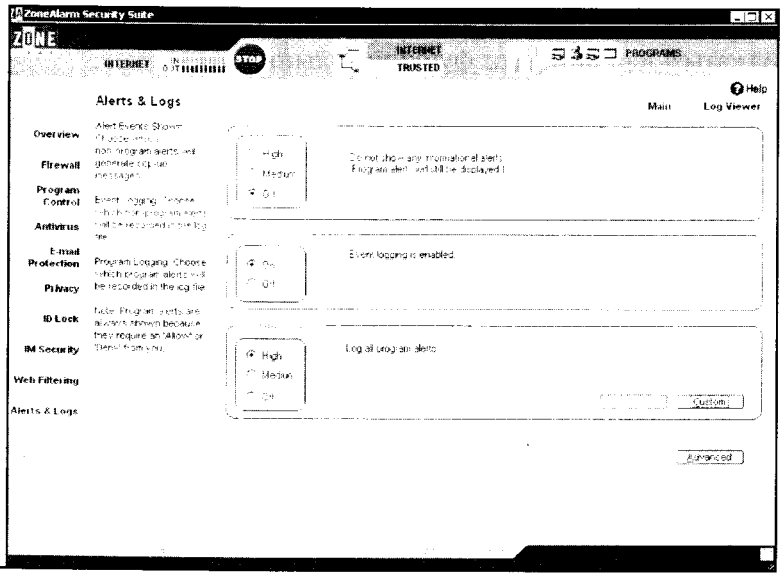


Рис. 12.38. Раздел Alerts & Logs, вкладка Main

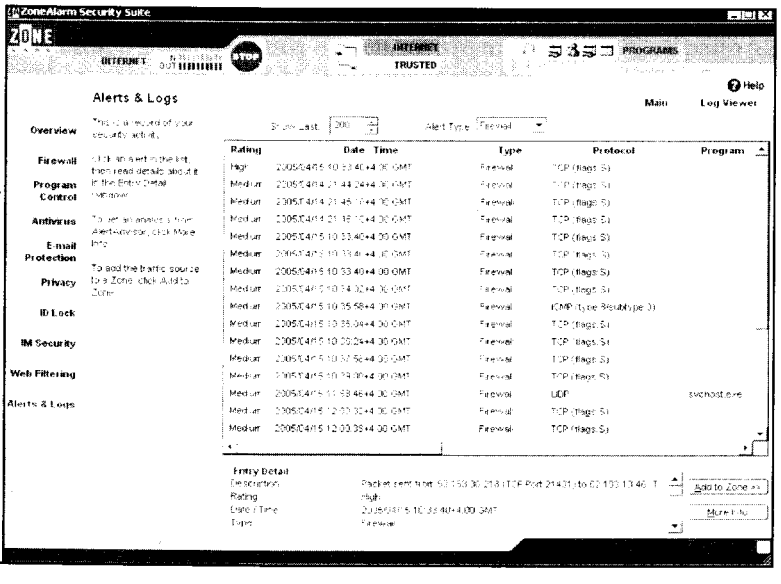


Рис. 12.39. Раздел Alerts & Logs, вкладка Log Viewer

(обычно это не такие уж и атаки), ставьте его в значение **High**, если вас интересуют только самые опасные из них — в значение **Medium**, а если вам надоело наблюдать бурную деятельность файрволла по защите от вторжений, эти оповещения можно отключить. И, наконец, включив параметр **Event Logging is enabled**, вы заставите программу протоколировать все события, касающиеся вопросов безопасности.

Для анализа происходящих атак полезна вкладка **Log Viewer** (рис. 12.39).

Эта вкладка позволяет просматривать журналы безопасности, выбирая их виды в окошке **Alert type**. Количество выводимых записей регулируется параметром **Show last (Показывать последние...)**, который позволяет показывать определенное число событий, начиная с последнего происшедшего.

В таблице, которая занимает большую часть этой вкладки, каждое событие расписано очень подробно. Ниже, в табл. 12.1, дан аннотированный список столбцов этой таблицы. Анализ таблицы полезен для «расследования» атак и принятия соответствующих мер. Например, если вас часто пытаются атаковать с какого-то IP-адреса, вы можете обратиться с жалобой на атакующего к администратору организации, выдавшей этот адрес.

Название столбца в Log Viewer	Описание параметра
Rating	Это так называемый рейтинг события. В этой колонке вы можете встретить значения Medium, то есть события средней важности, средней степени риска, и High — это опасные события. Если вы хотите проанализировать безопасность вашего компьютера, обращайте внимание на события, отмеченные как High, это, с высокой долей вероятности, реальные попытки атак на компьютер. События средней тяжести могут быть вызваны другими причинами
Date / Time	Дата и время события
Type	Тип события Firewall — это события, генерируемые файрволлом. В журнале программ можно увидеть другие типы событий
Protocol	Протокол, на уровне которого было зафиксировано событие. Например, это может быть TCP, UDP, ICMP
Program	Программа, вызвавшая событие. При попытках вторжения извне это поле останется пустым, а вот если какая-нибудь программа попытается установить несанкционированное соединение с внешним источником, ее название ищите здесь
Source IP	IP-адрес источника атаки
Destination IP	IP-адрес целевого назначения атаки. Здесь будет обозначен ваш IP-адрес, обычно снабженный номером порта, по которому вас пытались атаковать
Direction	Направление атаки. Incoming — атака извне, Outgoing — изнутри
Action taken	Предпринятое действие. Как правило, файрволл реагирует блокировкой опасности (Blocked)
Count	Количество событий
Source DNS	DNS источника атаки
Destination DNS	DNS цели атаки

Таблица 12.1. Структура протокола

Но даже эта объемистая и интересная таблица — далеко не все, что может предоставить ZoneAlarm любопытному пользователю.

Выделив интересующее вас событие и нажав кнопку **More Info** в нижней части программы, вы попадете на сайт компании, где ваш случай будет подробно проанализирован с рассказом о том, кто или что могло его вызвать. Вы даже сможете узнать примерное местоположение атакующего и координаты его провайдера. Возможно, это будет полезно, если кто-то атакует вас слишком настойчиво. Проведя небольшое расследование, ход которого будет описан ниже, вы сможете локализовать источник атаки и попытаться воздействовать на него. Перед началом разбора атаки вооружитесь англо-русским словарем или переводчиком, если вы неуверенно читаете английские тексты.

Разберем атаку, похожую на ту, что мы анализировали в прошлой главе. Для исследования я выбрал атаку, отмеченную рейтингом High, то есть потенциально реальную попытку нападения на компьютер. Выделив ее, я нажал на кнопку **More Info**, после чего загрузилась интернет-страничка сайта компании с общей информацией об этой атаке (рис. 12.40).

При этом ZoneAlarm сообщает, что на компьютер была проведена атака, выражающаяся в сканировании портов на предмет обнаружения троянской программы (скорее это был бы *backdoor*-клиент), которая

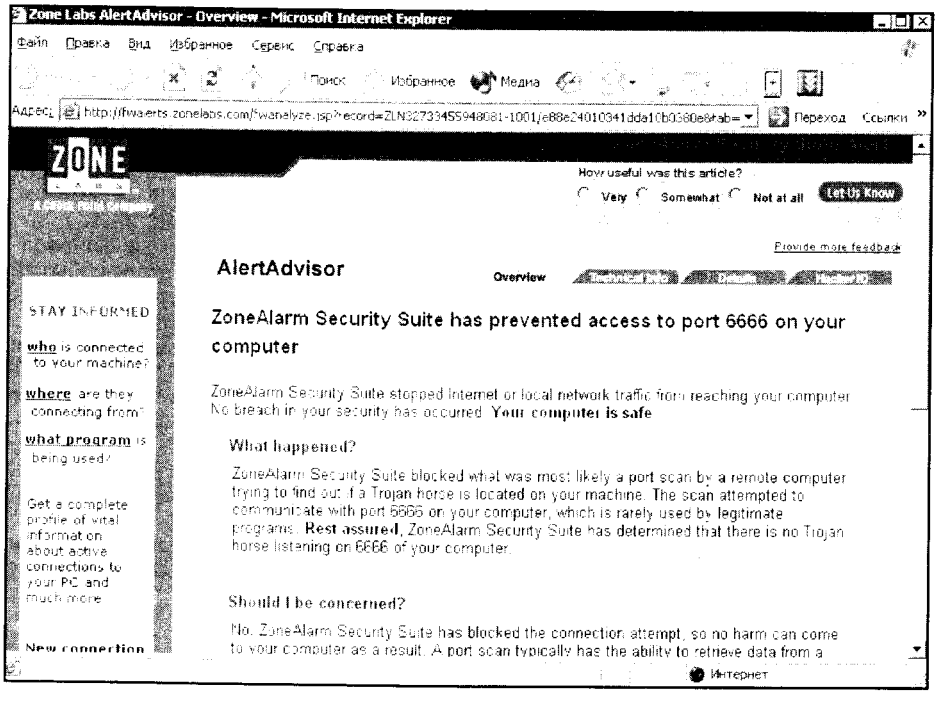


Рис. 12.40. Анализ атаки: общие сведения

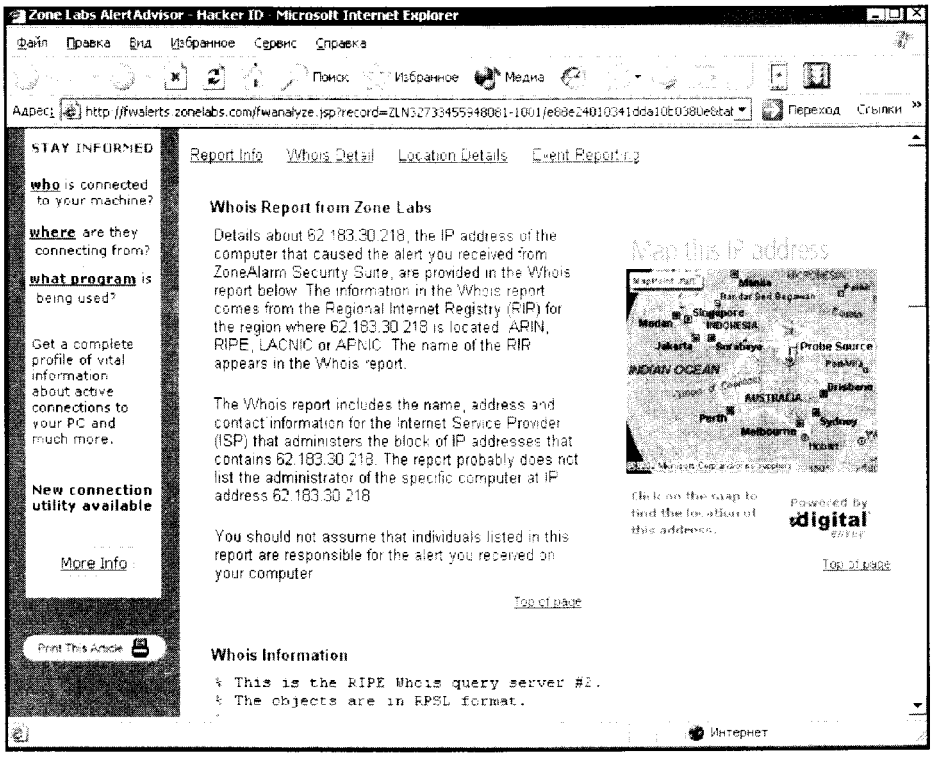


Рис. 12.41. Анализ атаки: техническая информация

«сидит» на 6666 порту. ZoneAlarm не обнаружил на этом порту троянца, но факт остается фактом: была проведена атака.

Разбираемся дальше. На страничке есть ссылка **Technical Info**, которая вызывает страничку с технической информацией об атаке (рис. 12.41).

Здесь нет ничего принципиально нового: почти та же самая информация может быть найдена в стандартном журнале безопасности и без выхода в Интернет. Куда больший интерес представляет вкладка **Details** с подробной информацией об атаке. Здесь можно почитать о том, что такое сканирование портов (мы с вами займемся этими вопросами в одной из следующих глав), и посмотреть советы по обеспечению безопасности компьютера в сети.

Самое интересное начинается на вкладке **Hacker ID** (рис. 12.42). Здесь мы подходим к цели нашего расследования: система выдает информацию об организации, выдавшей IP-адрес, с которого велась атака. Такой организацией может быть провайдер, который подключает своих клиентов по *dial-up*-соединению, выдавая им динамические IP-адреса. Для «ручного» определения этих данных существуют специальные программы, работающие с сервисом Whois, здесь же система сделала это са-

ма: она не только определила IP-адрес злоумышленника (или зараженного компьютера, который используется хакерами для поиска незащищенных машин), но и получила данные, используя которые, можно сообщить об этом провайдеру.

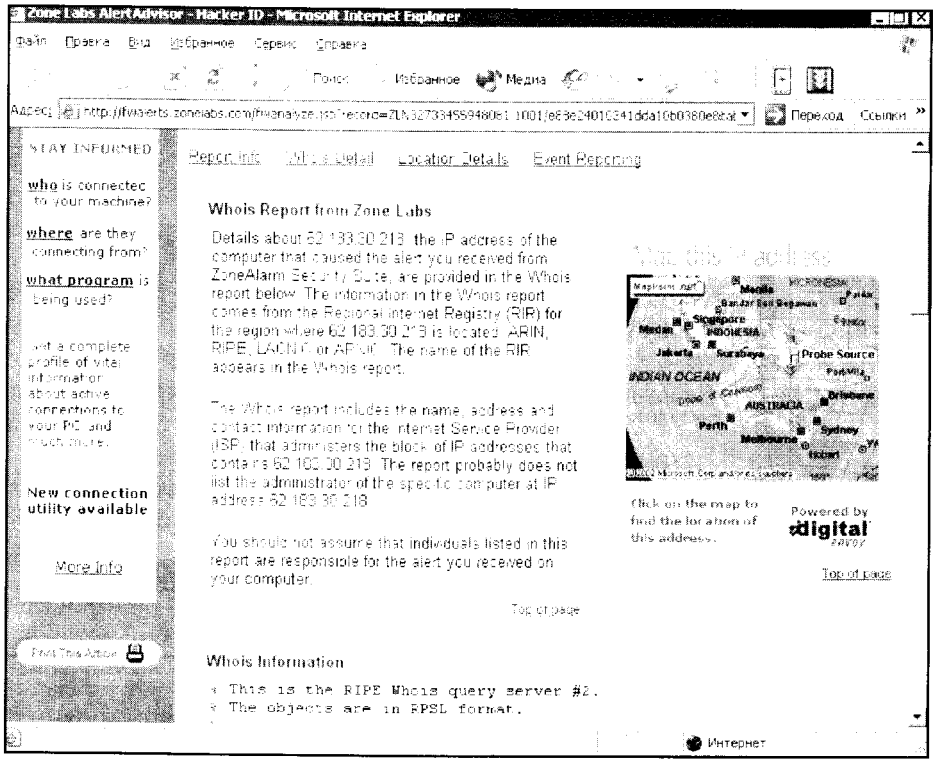


Рис. 12.42. Определение информации о провайдере, выдавшем IP-адрес атакующей машине

В нижней части окошка видны подробные данные провайдера, выдавшего IP-адрес. Для совсем уж любопытных исследователей на этой страничке есть картинка с изображением карты. Если щелкнуть по ней мышью, то появится новая страница, содержащая фрагмент карты с приблизительным местоположением атакующего компьютера. Практической ценности она не имеет, но смотрится (рис. 12.43) весьма эффектно. Прямо как в фильмах про хакеров и про тех, кто за ними охотится.

Наш рассказ был бы не полным без описания одной продвинутой возможности ZoneAlarm по настройке разрешений доступа к программам.

Как вы заметили, ZoneAlarm имеет многоуровневую систему настроек. Первый, самый простой уровень — те самые бегунки, которые можно ставить в несколько положений. Второй — **Advanced Settings**, и третий — так называемые **Expert Rules (Правила эксперта)**, то есть правила,

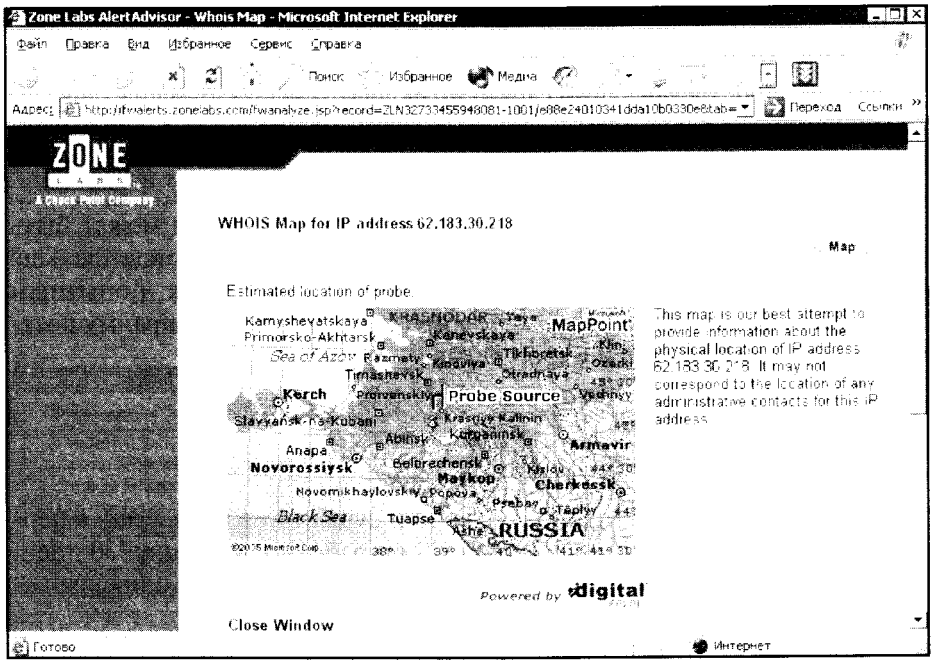


Рис. 12.43. Определение географического местоположения атакующего компьютера

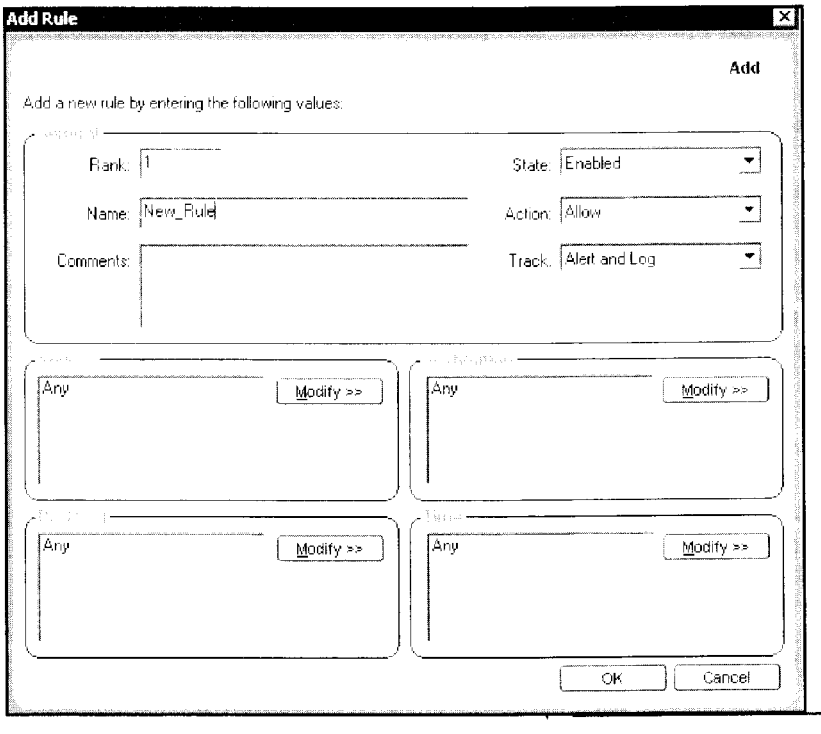


Рис. 12.44. Создание нового правила

которые продвинутые пользователи могут назначать для управления теми или иными аспектами работы программы.

Эти правила чрезвычайно гибки, позволяют учитывать массу параметров и настраивать каждую мелочь. Посмотрите на рис. 12.44. Так выглядит окно для настройки экспертных правил. Но если вы не системный администратор, то эти тонкости вам вряд ли пригодятся.

Подведем итоги. ZoneAlarm — это файрволл, который может быть использован как новичком, который, настраивая его, не пойдет дальше бегунков, определяющих уровень защиты компьютера, так и опытным системным администратором, которому будут интересны преимущественно **Advanced Options** и **Expert Rules**.

12.3. LOOK'N'STOP

Файрволл Look'n'Stop появился недавно и существует пока лишь в персональной версии. Демоверсия Look'n'Stop работает в течение 30 дней, после чего вы должны принять решение о его покупке или о прекращении использования этой программы.

По результатам независимых тестов, Look'n'Stop занимает одно из первых мест по надежности и эффективности работы. Забегая вперед, скажу, что главным минусом этого файрволла является непродуманная русификация.

Дистрибутив программы, который можно скачать на сайте компании (*http://www.soft4ever.com/LooknStop/En/looknstop.htm*), «весит» всего 600 с лишним килобайт. Это радует. Радует и то, что на сайте есть ссылка для загрузки этого файрволла в русском варианте. Установка (рис. 12.45) очень проста.

Не задавая лишних вопросов, программа устанавливается на компьютер, просит перезагрузки, а потом начинается самое интересное. Устанавливал-то я, как казалось, русскую версию, а программа выдала мне престранное сообщение, гласящее (рис. 12.46), что у меня нет какого-то там языкового файла. Я понял, что во всем «виноват» новоустановленный файрволл.

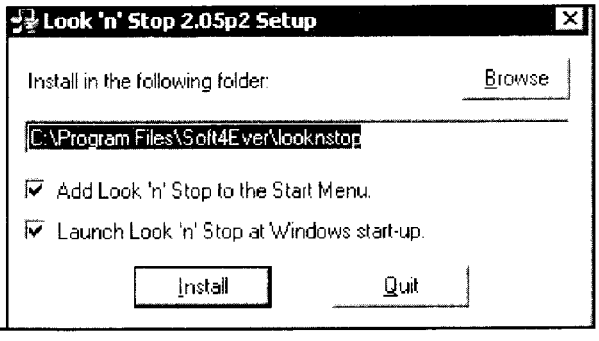


Рис. 12.45. Установка Look'n'Stop

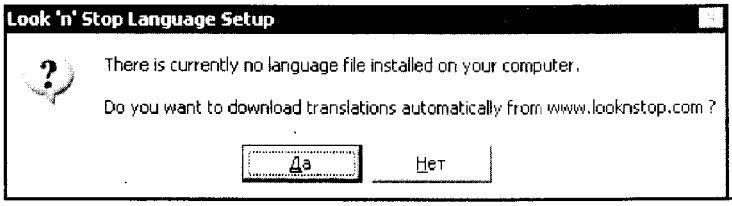


Рис. 12.46. Загрузка языкового файла

Загружать этот самый файл нужно было с сайта компании. Долго ли, коротко ли, но все же я добрался до списка языковых файлов на сайте компании-разработчика (рис. 12.47).

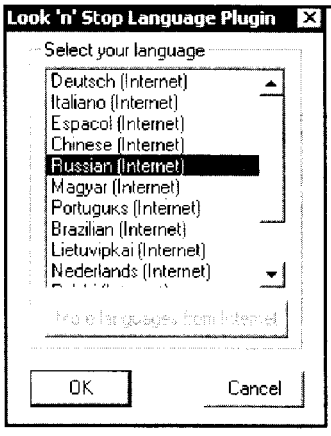


Рис. 12.47. Выбор языка

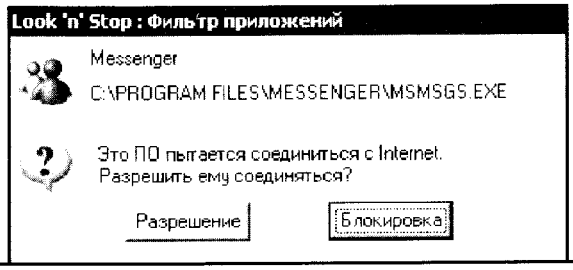


Рис. 12.48. Назначение разрешений для программ

Но перейдем к работе с программой. Нажав кнопку **OK** в окошке на рис. 12.48, мы, как ни странно, никуда больше не попадаем. В системной же панели поселяется новый значок — компьютер, бушующий огонь и разделяющая их «огнезащитная стена», то есть *firewall*. И тут Look'n'Stop начинает планомерно «бомбить» пользователя запросами о программах, которым что-то понадобилось в Интернете (рис. 12.48).

Я бы с опаской рекомендовал этот файрволл начинающим из-за одной его неприятной особенности. Дело в том, что программа задает вопросы не только о пользовательских приложениях и всяческих компонентах других программ, но и о системных модулях, без которых работа в Интернете станет невозможной. А если случайно или по незнанию запретить доступ к Интернету какому-нибудь **Generic Host Process for Win32 Services**, вы затем будете долго искать отошедший кабель вашего модема — и не найдете до тех пор, пока не выпустите вышеупомянутый компонент в Интернет.

Generic Host Process for Win32 Services — противоречивый компонент: с его помощью в Сеть могут выйти не только полезные программы, но и троянцы. Но если перекрыть ему доступ в Сеть, тогда проблемы будут как раз таки у полезного софта, который использует этот процесс.

Главное окно программы выполнено в стиле окон свойств различных компонентов Windows и вызывается двойным щелчком по значку файрволла в системной панели (рис. 12.49).

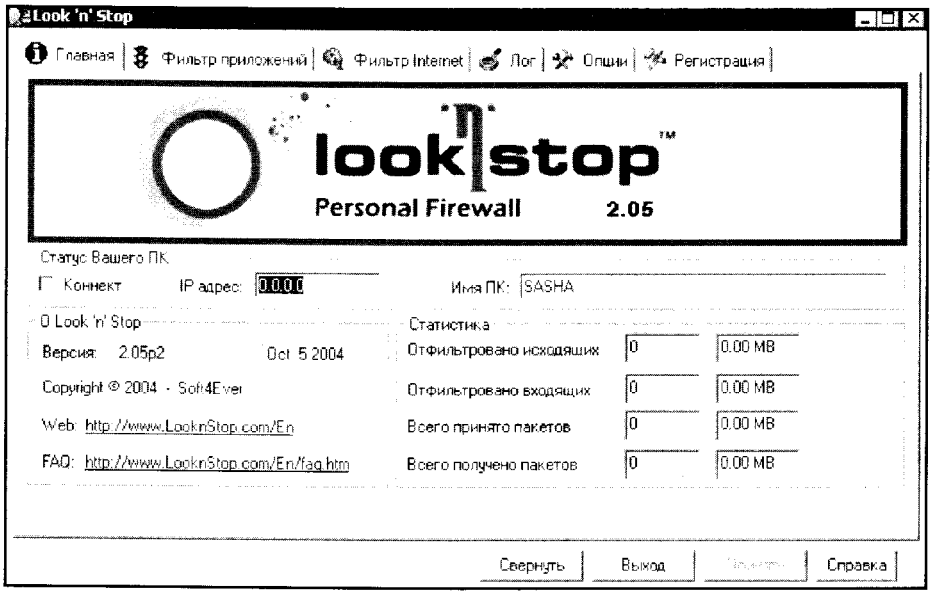


Рис. 12.49. Главное окно Look'n'Stop

Обычное главное окно, ничего особенного здесь обнаружить не удается. Да, еще файрволл довольно честно попытался «заблокировать сам себя», выдав запрос на попытку получить обновление с сайта компании (рис. 12.50).

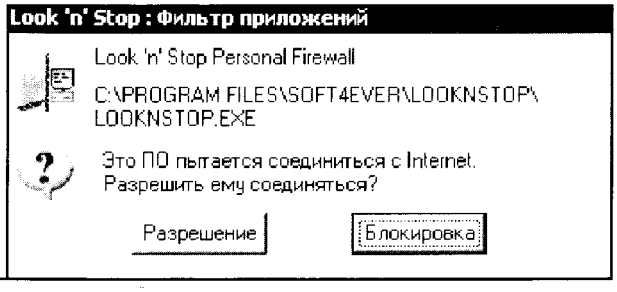


Рис. 12.50. Блокировка самого себя

Разработчики программы перечисляют следующие полезные свойства Look'n'Stop, которые должны, по их мнению, стать для вас ключевыми в выборе файрволла.

Программа Look'n'Stop поддерживает ICS. Для тех, кто прочел предыдущие главы, это должно стать важным аргументом.

Если ваш файрволл не поддерживает ICS, то, даже проверив все установки, вы можете так и не установить общий доступ к Сети.

Look'n'Stop умеет «резать» баннеры и другую рекламу, поддерживает защиту конфигурации паролем, возможность удаленного администрирования и возможность ограничения доступа к определенным ресурсам Интернета. Файрволл, по словам разработчиков, полностью совместим с Windows XP SP2 и нормально опознается встроенной системой безопасности. По их же словам, этот файрволл не будет слишком сильно загружать систему.

В работе русская версия Look'n'Stop производит впечатление недоработанности и непрезентабельности внешнего вида, хотя внешность не так уж и важна. А вот внутреннее содержание настолько сложно и продвинуто, что наводит на мысль о квалифицированных системных администраторах. На рис. 12.51 вы видите окно файрволла, в нем настраивается фильтрация приложений. Стандартный файрволл Windows лишен этой возможности, а здесь она есть. Это еще один довод за то, что дополнительный файрволл для пользователей Windows просто необходим.

В левой части окна фильтрации приложений находится список активных программ, то есть тех, которые в данный момент пользуются до-

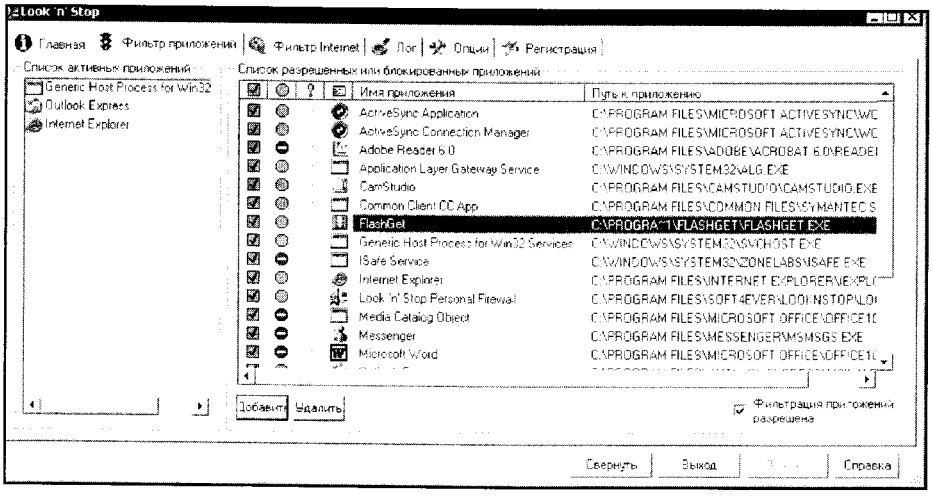


Рис. 12.51. Окно настройки фильтрации приложений

ступом к Интернету. В правой части расположена таблица с наименованиями и характеристиками программ, которым нужен доступ к Интернету, и с разрешениями, назначенными этим программам.

Если файрволл встречает новую программу, которой нужен доступ к Сети, он спрашивает разрешения пользователя. Здесь также можно настраивать разрешения вручную.

Первая колонка списка разрешенных или блокированных приложений содержит флажок, который может быть либо снят, либо установлен. Если флажок установлен (то есть в первой колонке против названия приложения стоит галочка), то файрволл применит к приложению фильтр, который настроен в его свойствах, не задавая вам дополнительных вопросов. А если этот флажок снять, то попытка этого приложения получить доступ к Сети будет воспринят файрволлом как первая, и вы сможете самостоятельно решить, давать доступ или нет.

Вторая колонка, в которой видны красные значки **Stop** или зеленые кружки, отвечает за предоставление доступа соответствующей программе к Интернету. Смысл этих значков понятен: пустить или не пустить.

Третья колонка, отмеченная восклицательным знаком, позволяет настраивать ведение лог-файлов по каждой из программ. К примеру, если установить для программы значок из одного восклицательного знака, то записываться будут лишь события, вызванные блокированием доступа данного приложения к Сети. Если «восклицаний» будет два, то протоколироваться будут все попытки доступа программы к Интернету. Ну а смысл колонок **Имя приложения** и **Путь к приложению** понятен без дополнительных пояснений.

Программы можно добавлять в список разрешенных или блокированных приложений в автоматическом и в ручном режимах. В автома-

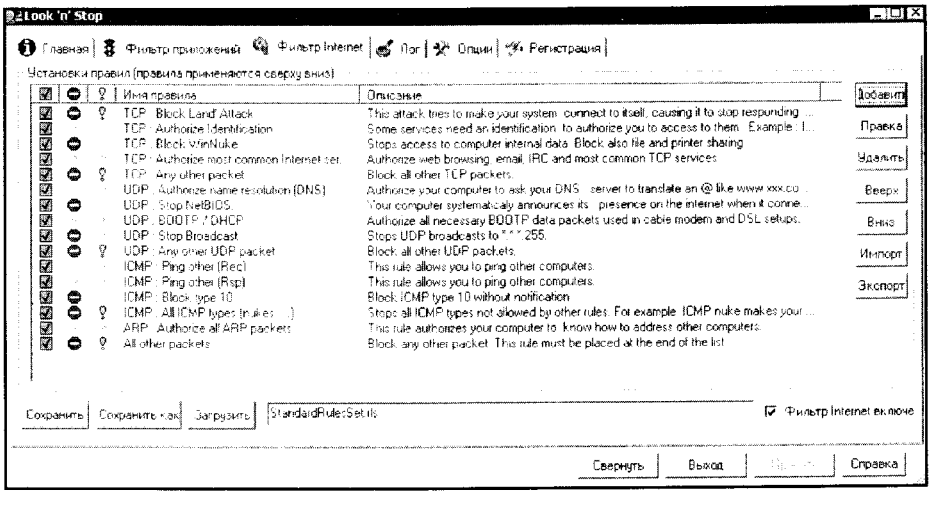


Рис. 12.52. Фильтр Internet

тическом режиме это происходит в момент вашего ответа на вопрос файрволла о предоставлении доступа к Сети той или иной программе. Инструмент ручного режима — кнопка **Удалить** в окне **Фильтр приложений файрволла**.

Следующее окно называется **Фильтр Internet** (рис. 12.52).

До сих пор мы рассматривали уровень процессов и приложений. В окне **Фильтр Internet** можно настраивать правила фильтрации сетевого уровня, то есть здесь мы можем управлять доступом на сетевом уровне.

Управление доступом на сетевом уровне предусматривает фильтрацию пакетов. В стандартном режиме файрволл придерживается правил, которые подходят для большинства случаев. Но мощь Look'n'Stop заключается в том, что эти правила можно настраивать. Это довольно сложно, и такой настройкой можно заниматься, лишь ознакомившись с соответствующей литературой. Чтобы лучше познакомиться с настройкой подобных параметров, я рекомендую документы, которые можно найти на сайте http://rfc.net — RFC 894, который рассматривает особенности инкапсуляции IP-пакетов в кадры Ethernet, RFC 791, посвященный описанию протокола IP, RFC 792, который рассказывает об ICMP, RFC 793, посвященный TCP, и RFC 768, где речь идет об UDP. Воспользовавшись этими источниками, вы сможете самостоятельно заниматься изучением правил.

Изучим окно **Фильтр Internet** в подробностях.

В правой части окна есть несколько кнопок. Кнопка **Добавить** предназначена для добавления нового правила. При ее нажатии появляется окно (рис. 12.53), содержащее поля, заполнив которые, вы создадите новое правило.

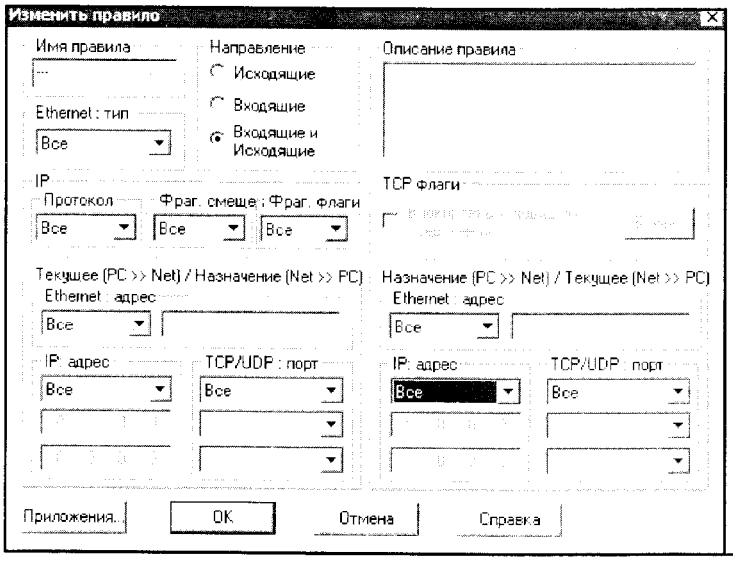


Рис. 12.53. Добавление нового правила

Настройка правил выходит за рамки этой книги: чтобы описать особенности этих настроек, понадобится еще одна книга, ориентированная на профессиональных системных администраторов.

Следующая кнопка — **Правка**. Она позволяет править выделенное правило.

Кнопка **Удалить** удаляет его, кнопки **Вверх** и **Вниз** перемещают выделенную строку с правилом выше или ниже в списке правил. Положение каждой строки имеет значение: правила применяются «сверху вниз», то есть верхнее правило важнее и приоритетней нижнего. Кнопки **Импорт** и **Экспорт** служат для импорта и экспорта правил, то есть каждое правило можно записать в отдельный файл.

В нижней части окна расположены еще несколько кнопок. Кнопка **Сохранить** предназначена для сохранения модификаций, которые вы внесли в текущий набор правил, кнопка **Сохранить как** позволяет сохранить набор правил в отдельный файл, а кнопка **Загрузить** позволяет загрузить набор правил из файла. Такие файлы можно найти на сайте файрволла.

В таблице со списком правил есть несколько столбцов. Их назначение аналогично таким же столбцам в списке фильтруемых приложений. Так же как и в случае с приложениями, вы можете отключить фильтрование пакетов.

Следующее окно этого файрволла называется **Лог** (рис. 12.54) и содержит результаты протоколирования событий.

Протокол организован в виде списка.

Колонка этого списка, которая называется **U/D#**, говорит о направлении отфильтрованных пакетов. Буква **U** обозначает отфильтрованный пакет, направлявшийся из компьютера в Интернет, а **D** — наоборот. Эта колонка содержит порядковый номер отфильтрованного пакета. Колонка **Дата** содержит дату и время события. В колонке **Правило** содержится описание правила, на основании которого был отфильтрован пакет. Ко-

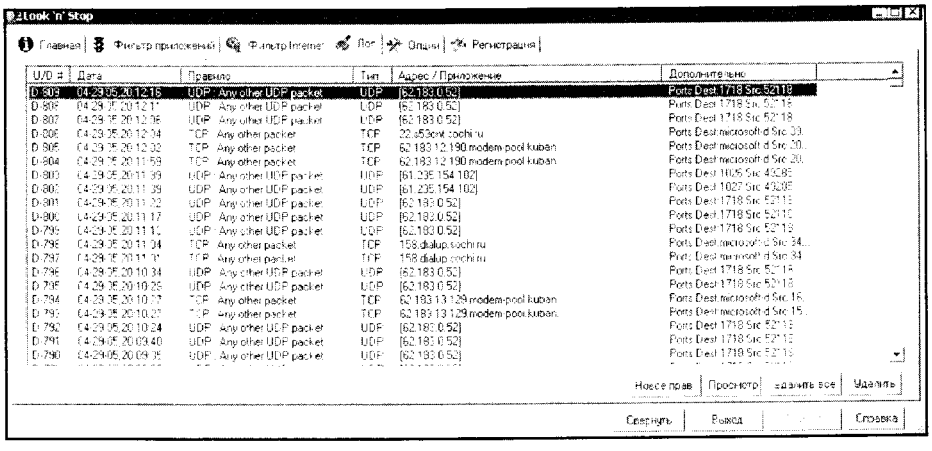


Рис. 12.54. Окно протокола

лонка **Тип** определяет тип отфильтрованного пакета (TCP или UDP). В строке **Адрес/приложение** можно увидеть IP-адрес или приложение, к которым относится данный пакет.

Если выделить какую-нибудь строку списка протокола и нажать на кнопку **Просмотр**, появится окно, содержащее подробную информацию об отфильтрованном пакете (рис. 12.55).

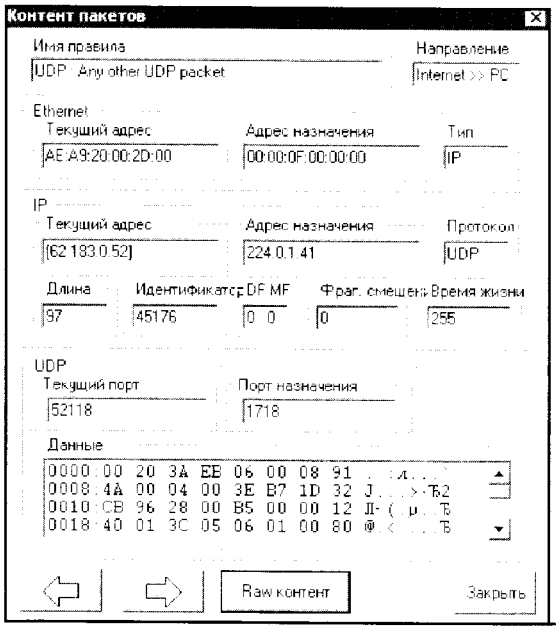


Рис. 12.55. Изучение подробностей, касающихся отфильтрованного пакета

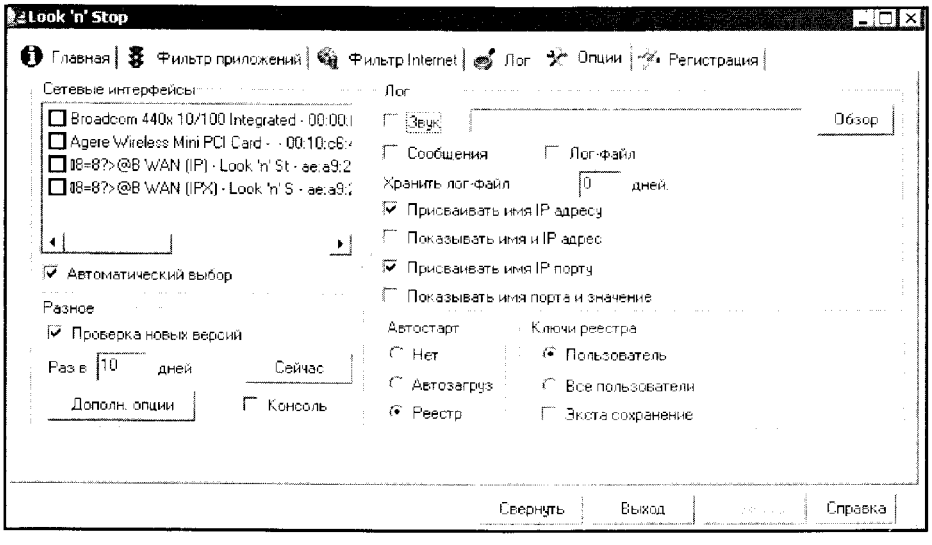


Рис. 12.56. Общие настройки файрволла

Теперь рассмотрим окно, касающееся общих настроек файрволла (рис. 12.56).

В рамке **Сетевые интерфейсы** можно поставить галочку против пункта **Автоматический выбор**. А вот группа параметров **Лог** нуждается в более тонкой настройке.

По умолчанию файрволл не сохраняет протокол событий в файле. Ежедневно он обнуляет записи и начинает их снова.

Если установить галочку против пункта **Лог-файл** и установить период хранения лог-файла больше, чем 0 дней, то в вашем распоряжении окажется протокол событий за любое число дней. Такой протокол может быть полезен для анализа.

Остальные галочки против пунктов **Показывать имя и IP-адрес** и **Показывать имя IP-порта и значение** тоже можно установить, чтобы файл протокола был более полным.

Обратите внимание на, как кажется, совершенно неважный пункт под названием Звук. По умолчанию он отмечен галочкой, и всякий раз, когда файрволл отфильтровывает пакет и заносит запись в лог-файл, раздается предупреждающий звук. При этом больше никаких действий не производится, и о том, отчего файрволл вдруг расшумелся, пользователь догадывается не сразу. Но записи в лог-файлы заносятся довольно часто, и эти звуки начинают надоедать. Конечно, такая музыка должна доказать рвение файрволла в деле фильтрации пакетов, но больше получаса слушать все это довольно тяжело, и я очень рекомендую сразу же сбросить галочку против пункта Звук.

Группа параметров **Автостарт** определяет порядок автоматического запуска файрволла. Если этот параметр установить в положение **Нет**, файрволл не будет стартовать автоматически, а если выбрать **Автозагрузка**, он начинает работу из меню автозагрузки. Ну а если выбрать **Реестр**, то старт программы будет произведен посредством ключа в реестре.

Теперь рассмотрим группу параметров **Разное**. Параметр **Проверка новых версий** отвечает за загрузку из Интернета обновлений файрволла.

Если установить галочку против пункта **Консоль**, появится консоль файрволла (рис. 12.57), которой можно воспользоваться для просмотра различных событий.

Консоль позволяет просматривать протоколы соединения к Интернету и некоторые другие вещи, связанные, например, с библиотеками DLL.

Если нажать на кнопку **Дополнительные опции** группы параметров **Разное**, появится окно, которое позволит заняться тонкой настройкой сетевых интерфейсов, задавать пароль для доступа к функциям программы и так далее.

И, наконец, на вкладке **Регистрация** вы можете зарегистрировать вашу копию файрволла, введя в соответствующее поле серийный номер, полученный при покупке продукта на сайте разработчиков.

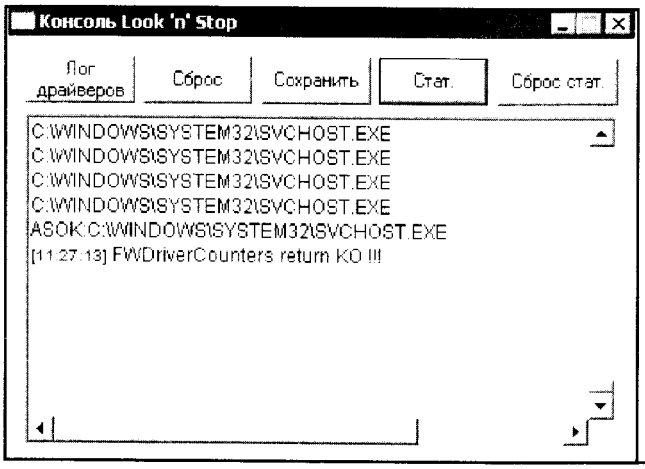


Рис. 12.57. Консоль Look'n'Stop

Подведем итоги разговору о файрволле Look'n'Stop. Его плюсы — высокие оценки независимых тестеров, стабильность работы и сравнительно небольшой размер дистрибутива. А немного запутанные настройки и кривоватая русификация — это, наверное, удел всех сравнительно молодых продуктов, разработкой которых занимается группа энтузиастов.

Но наш разговор о файрволлах еще не закончен.

12.4. AGNITUM OUTPOST FIREWALL PRO

Agnitum Outpost Firewall Pro — это файрволл, обладающий богатыми возможностями настройки, качественно русифицированный и удобный. Его установка стандартна, за исключением того, что вы должны будете выбрать язык интерфейса (рис. 12.58).

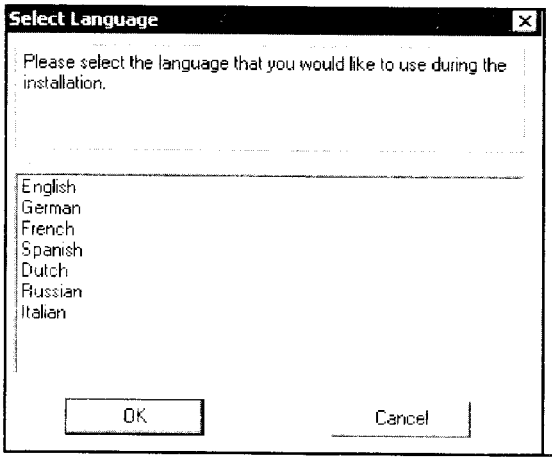


Рис. 12.58. Выбор языка

После того как из предложенного списка языков выбран Russian, дальнейший процесс установки идет на русском языке.

Перед установкой Outpost Firewall следует деинсталлировать ранее установленные на вашем компьютере файрволлы: соседство нескольких таких программ может привести к проблемам. Эти проблемы могут выглядеть как внезапные перезагрузки системы, сбои, нестабильность работы. Конечно, вы можете попробовать поработать с несколькими файрволлами одновременно, но лучше так не делать.

На одном из последних этапов установки файрволла вы увидите окно (рис. 12.59), где установщик предложит вам автоматически создать правила для приложений и сетевых интерфейсов.

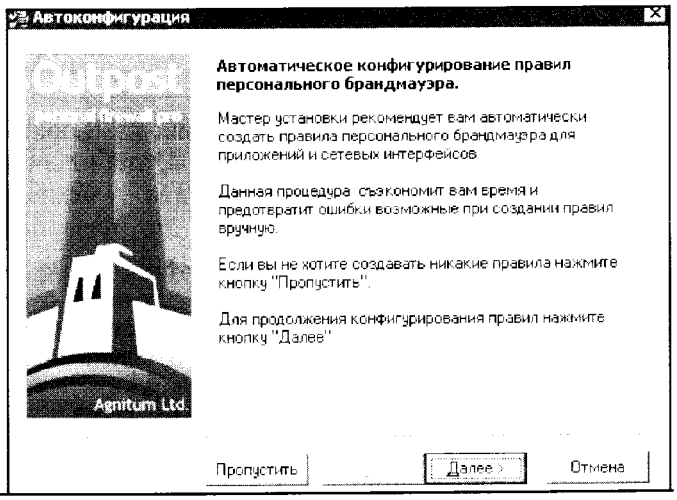


Рис. 12.59. Автоконфигурация

Этот шаг установки можно пропустить, нажав соответствующую кнопку. Дело в том, что автоматическое создание правил добавит в списки приложений, которым разрешен доступ к Интернету, такие программы, как Microsoft Word, Adobe Acrobat Reader и так далее. Они начнут «проситься» в Интернет за обновлениями, загружая таким образом канал связи ненужной информацией. Поэтому лучше нажать кнопку **Пропустить**, а в процессе работы с файрволлом настроить эти правила самостоятельно. Это, кстати, не слишком сложно.

После окончания установки и перезагрузки компьютера ваш брандмауэр готов к работе. В системной панели Windows появляется иконка программы в виде знака вопроса на синем поле. По умолчанию файрволл настроен на автоматический запуск во время загрузки Windows.

После перезагрузки, которая следует за установкой, файрволл запустится, и вы увидите его главное окно (рис. 12.60). Оно служит для контроля за работой файрволла, для настроек параметров фильтрации и просмотра лог-файлов. Если закрыть это окно, файрволл не прекратит работу, а просто «уйдет» в системную панель.

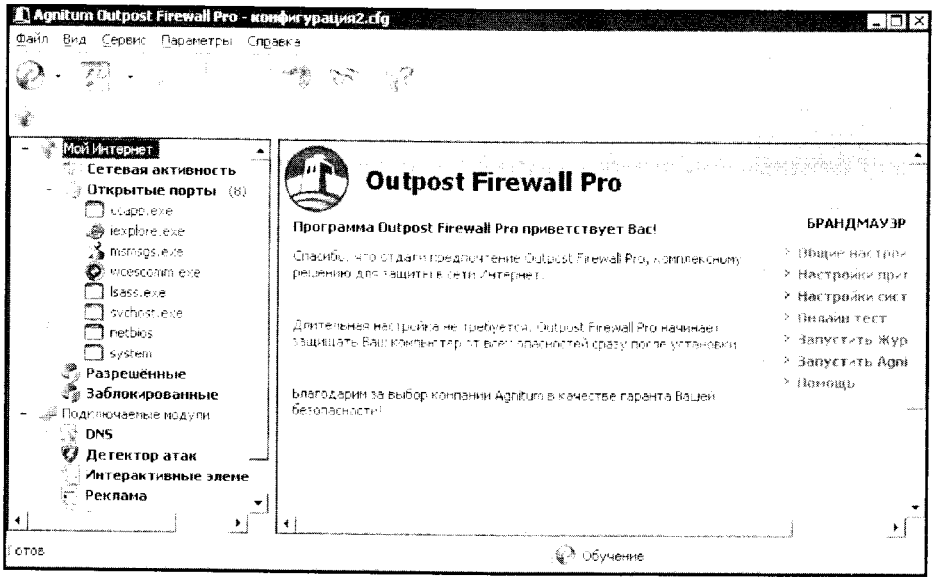


Рис. 12.60. Главное окно Outpost Firewall Pro

Главное окно программы разделено на две части. Слева расположена панель представлений, а справа — информационная панель. Остановимся на них подробнее.

- Список **Мой Интернет** содержит различные элементы, которые позволяют осуществлять настройку сетевых функций файрволла.
- Подраздел **Сетевая активность** позволяет отслеживать приложения, которые в данный момент соединены с сетью.
- Подраздел **Открытые порты** содержит список открытых портов.
- Подраздел **Разрешенные** содержит статистику о работе разрешенных приложений и позволяет просматривать лог-файл по разрешенным приложениям.
- В подразделе **Заблокированные** можно узнать о запрещенных файрволлом попытках сетевой активности.
- В списке **Подключаемые модули** содержится перечень компонентов, расширяющих функциональность программы. По желанию можно подключать к Outpost Firewall Pro дополнительные модули.

По умолчанию включены следующие компоненты.

- DNS содержит журнал событий модуля DNS. Этот модуль предназначен для кэширования DNS-запросов и ведения протокола запросов DNS-адресов.
- **Детектор атак** отслеживает возможные атаки, ведет лог атак и предупреждает пользователя о возможных вторжениях в его систему.
- Модуль **Интерактивные элементы** предназначен для контроля за интерактивными элементами (среди них ActiveX-элементы,

Java-приложения, скрипты Visual Basic, *cookies*, всплывающие окна, скрытые фреймы, анимированные GIF, Flash-анимация и так далее).

- **Внешние объекты на веб-страницах**. Эти элементы потенциально опасны, поэтому в целях обеспечения максимального уровня защиты их отключают. Но не следует забывать о том, что отключение этих элементов может привести к неполной функциональности некоторых веб-страничек.
- Модуль **Реклама** предназначен для блокировки рекламы.
- Модуль **Содержимое** предназначен для блокировки отображения определенных веб-сайтов на основании текстов, расположенных на этих сайтах, либо на основании их адресов.
- Модуль **Фильтрация почтовых вложений** служит для управления почтовыми вложениями: как вам известно, множество почтовых червей распространяется именно с помощью вложений.

Outpost Firewall может работать в нескольких режимах. О том, в каком режиме работает файрволл, сигнализируют внешний вид его иконки в системной панели и сообщение в нижней части главного окна.

Сразу после установки файрволл работает в режиме обучения: если произойдет некое новое для файрволла событие, программа спросит вас о том, какие действия ей следует предпринять. Таким образом, через несколько дней после установки Outpost практически все программы, которым нужен Интернет, запросят разрешения на доступ, и вы за это время сформируете правила для ваших программ.

Когда происходит событие, для которого файрволл еще не имеет готового правила, он задает вопрос.

В окне на рис. 12.61 мы видим, что приложение Internet Explorer запрашивает исходящее соединение через порт 80 по протоколу HTTP и по адресу *www.softforum.ru*. Это нормальное явление, и разрешение нужно дать.

Если приложение, которое запрашивает соединение, знакомо файрволлу (как в примере на рис. 12.61), он предлагает вам создать стандарт-

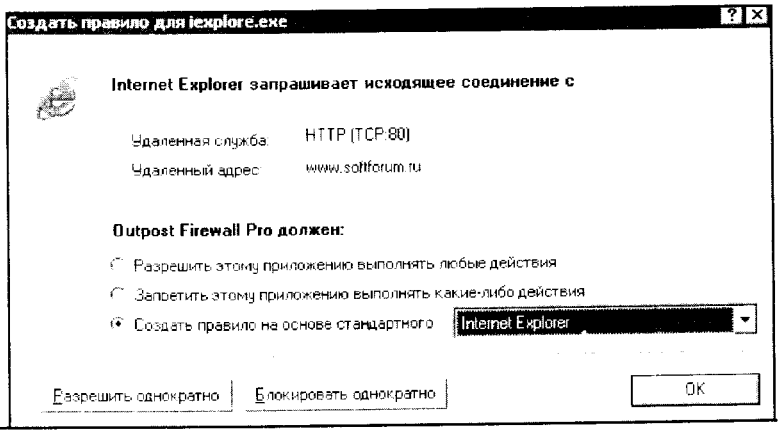


Рис. 12.61. Создание правила

ное правило, и, чтобы дать этому приложению доступ в Интернет, вы просто нажимаете **OK**.

Если вам точно известно, что приложению в Сети делать нечего или что от такой его активности пользы не будет, можно выбрать пункт **Запретить этому приложению выполнять какие-либо действия**. Такой пункт, к примеру, можно выбрать для Microsoft Word.

Аналогично, если вы точно знаете, что приложению необходим доступ в Интернет, а стандартного правила для него не предусмотрено, вы можете выбрать пункт **Разрешить этому приложению выполнять любые действия** и нажать **OK**.

Что делать, если вы не уверены в том, нужен ли приложению, которое просится в Интернет, доступ? Так, когда в Сеть просится нечто вроде **Common Client CC App**, вы можете и не знать, для чего этому приложению нужен доступ. К тому же при виде любого странного или незнакомого названия вы вправе задуматься: возможно, это троянец или другая вредоносная программа. Но если запретить нужной службе доступ к Сети, то не смогут работать важные приложения. Для таких случаев в Outpost Firewall есть кнопки **Разрешить однократно** и **Блокировать однократно**. Если вы один раз блокировали подозрительную программу и после этого спокойно сделали в Интернете все, что нужно (посмотрели какие-нибудь веб-странички, проверили почту при помощи почтового клиента, скачали что-нибудь с помощью менеджера закачек), то при повторном запросе подозрительной программы на соединение можно спокойно запретить ее активность. Ну а если, заблокировав программу, вы обнаружили, что странички в IE отказываются открываться, а почтовый клиент не может подключиться к почтовому серверу, значит, увидев запрос файрволла на разрешение доступа этого приложения, в следующий раз нужно разрешить сетевую активность.

После того как вы определились с программами, которым нужен доступ в Интернет, файрволл из режима обучения можно переключить в режим блокировки. Это можно сделать, щелкнув правой кнопкой мышки по значку файрволла в системной панели и выбрав в появившемся меню пункт **Политики**.

Сущность работы файрволла в режиме **Политики ▸ Режим блокировки** заключается в блокировке всех явно не разрешенных соединений. Такую политику можно изложить словами «Запрещено все, что не разрешено». При установке новых программ вам, возможно, придется переключиться обратно в режим обучения, чтобы установить для них разрешения.

Если выбрать пункт меню **Политики ▸ Режим разрешения**, то файрволл заработает в режиме «Разрешено все, что не запрещено». Это довольно опасный режим, и лучше его не использовать.

Пункт меню **Политики ▸ Блокировать все** мгновенно останавливает любую активность любых приложений. Это полезно в случае, если вы подозреваете, что кто-то собирается атаковать ваш компьютер или уже атакует, например, выкачивая с него какой-то ценный файл.

Пункт меню **Политики ▸ Режим бездействия** переводит файрволл в пассивный режим, когда разрешена любая сетевая активность.

Рассмотрим некоторые настройки Outpost Firewall. Чтобы вызвать на экран его главное окно, дважды щелкните по иконке файрволла в системной панели. В открывшемся окне выберите пункт меню **Параметры ▸ Общие**. Вы увидите окно настройки основных параметров файрволла (рис. 12.62).

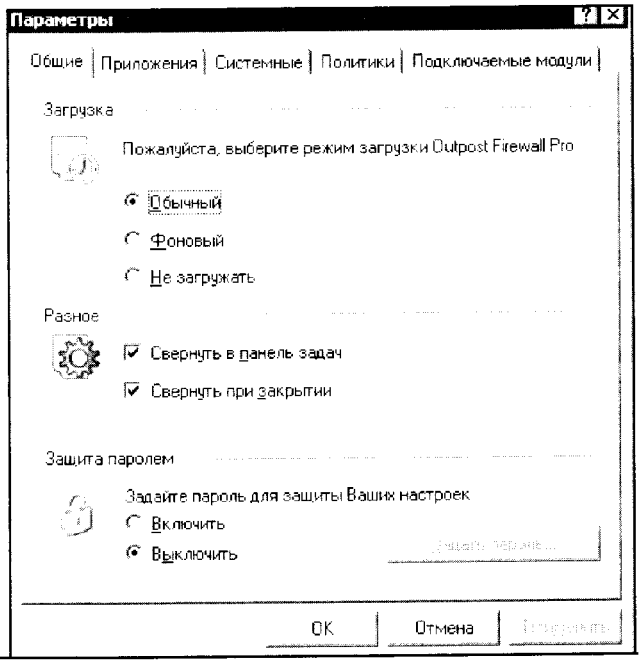


Рис. 12.62. Общие параметры настройки файрволла

Здесь, воспользовавшись группой параметров **Загрузка**, можно настроить параметры запуска Outpost Firewall, а также защиту параметров настройки файрволла паролем.

Вкладка **Приложения** окна **Параметры** (рис. 12.63) позволяет настраивать разрешения для приложений. После того как вы настроили то или иное разрешение для конкретного приложения, его можно изменить именно здесь. Это окно пригодится, если вы случайно задали не то разрешение.

Приложения здесь разбиты на три группы.

- **Запрещенным приложениям** запрещена сетевая активность.
- **Пользовательский уровень** — это приложения, для которых созданы правила доступа. Как правило, это стандартные правила, которые файрволл предлагает при назначении разрешения для того или иного приложения.
- **Доверенные приложения** — это группа программ, которым разрешены все сетевые подключения.

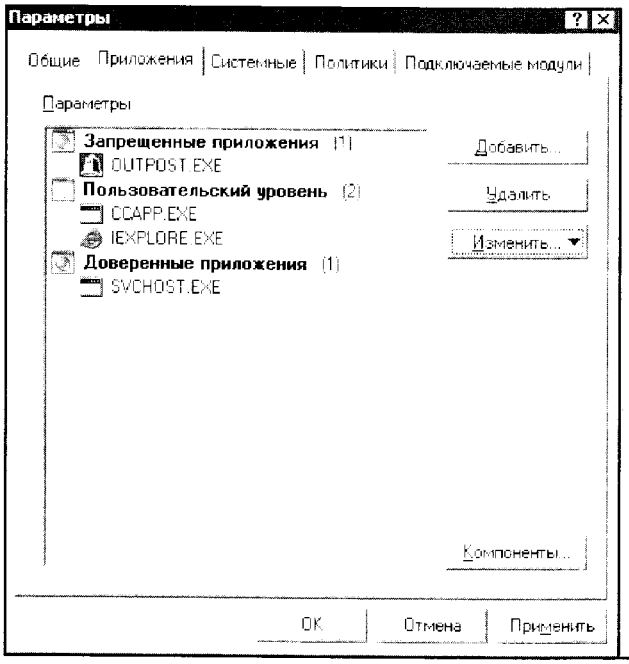


Рис. 12.63. Параметры настройки приложений

Программы можно перемещать из группы в группу при помощи мыши. Если переместить программу в группу **Пользовательский уровень**, файрволл предложит вам создать правило для этого приложения. При перетаскивании программы в одну из других групп правила созда-

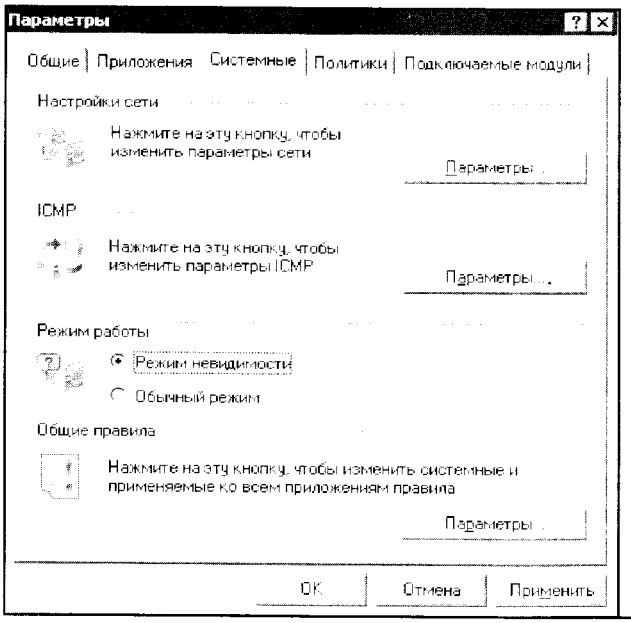


Рис. 12.64. Параметры системы

вать не требуется. Изменить принадлежность программы можно путем ее выделения и щелчка по кнопке **Изменить**.

Вкладка **Системные** окна **Параметры** предназначена для настройки некоторых системных параметров (рис. 12.64).

Нажимая на кнопки **Параметры** этого окна, можно настраивать различные параметры файрволла. Обычно для нормальной работы вполне достаточно умолчаний. Проследите за тем, чтобы был включен параметр **Режим невидимости**: в ином случае степень защиты компьютера значительно снижается.

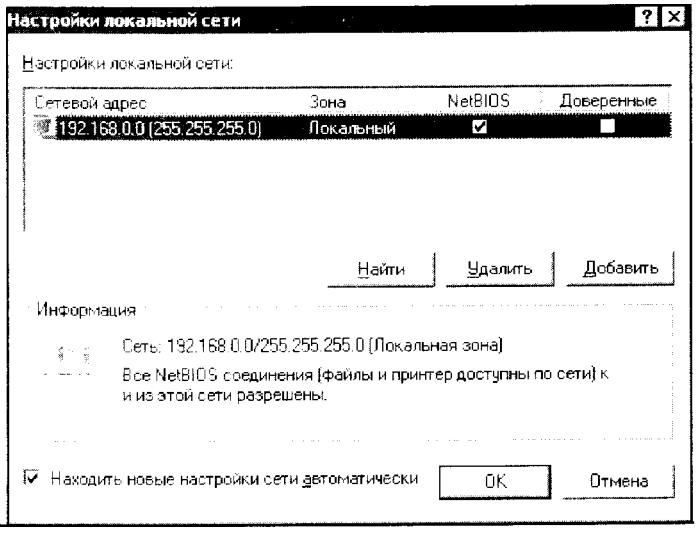


Рис. 12.65. Настройки локальной сети

Обратите внимание на группу параметров **Настройки сети** (рис. 12.65). Здесь можно настраивать взаимоотношения вашего компьютера с локальной сетью, в которую он входит.

Если вы хотите разрешить любые взаимодействия с выбранной локальной сетью, поставьте галочку в поле **Доверенные**. Ну а если хотите предотвратить любую активность, уберите все галочки для данной сети.

На вкладке **Политики** можно переключаться между режимами разрешения, обучения, блокировки, запрещения и отключения. Эти режимы и их воздействие на работу файрволла мы обсуждали выше.

Outpost Firewall построен по модульному принципу. Вкладка **Подключаемые модули** позволяет управлять модулями, подключаемыми к файрволлу (рис. 12.66).

Здесь можно добавлять новые модули, удалять существующие, запускать и останавливать работу модулей и настраивать их параметры. На параметрах подключаемых модулей мы остановимся подробнее.

Файлы модулей имеют расширение `.ofp`. Они реализуют дополнительную функциональность файрволла. Начнем рассмотрение их настроек с модуля **Attack Detection** (рис. 12.67).

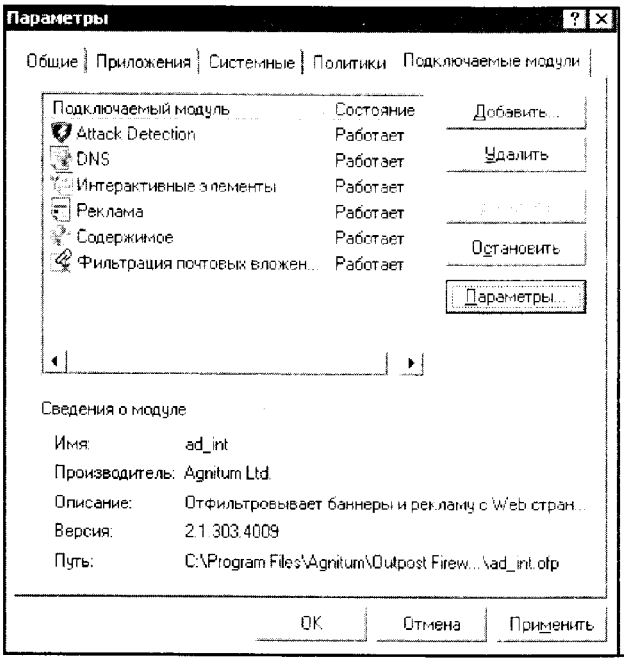


Рис. 12.66. Подключаемые модули

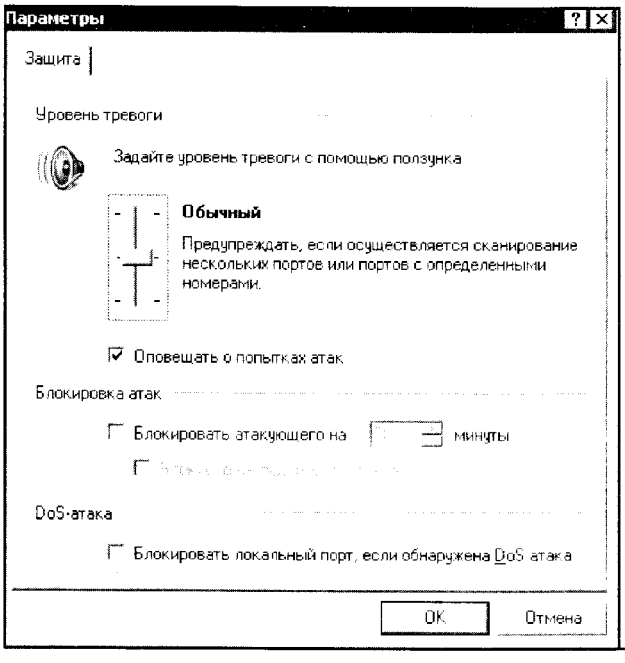


Рис. 12.67. Параметры Attack Detection

Уровень тревоги позволяет настраивать появление предупреждений об атаках. Обычный уровень предусматривает появление сообщения об атаке при попытке сканирования нескольких портов вашего компью-

тера или только определенных портов, которые чаще всего подвергаются атакам злоумышленников. Если передвинуть ползунок вверх, вы будете получать сообщения обо всех атаках и даже о попытках сканирования отдельно взятого порта. Ну а передвинув ползунок вниз, вы получите сообщения только о зарегистрированных и распознанных файрволлом атаках.

Если вы не желаете, чтобы файрволл сообщал вам об атаках, — пусть он делает свою работу, а вы будете заниматься своей! — то можно снять галочку около параметра **Оповещать о попытках атак**. Параметры блокировки атак вы можете оставить выключенными.

Теперь рассмотрим подробности настройки компонента DNS.

Этот компонент (рис. 12.68) предназначен для кэширования DNS-записей.

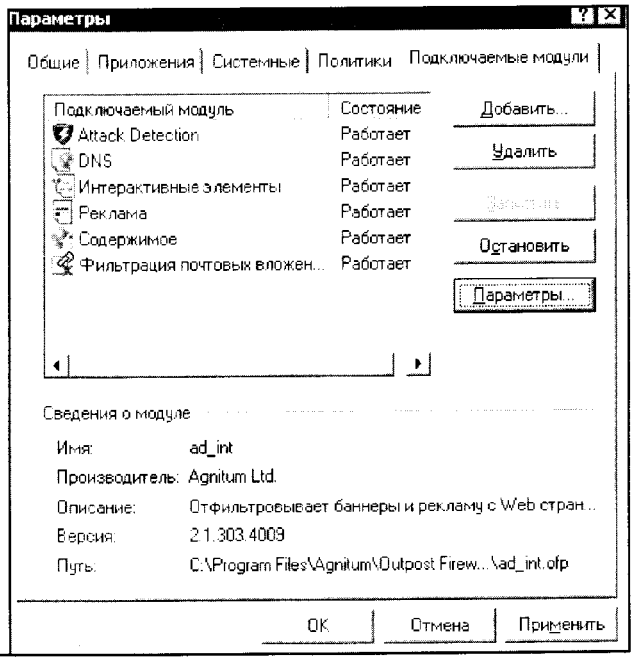


Рис. 12.68. Параметры кэширования DNS-записей

Кэширование DNS-записей нужно для ускорения процесса обращения к интернет-ресурсам. Как вы помните, ресурсы (серверы или обычные компьютеры) могут иметь несколько имен, которые находятся на разных уровнях OSI.

Символьные, доменные имена легко воспринимаются человеком, но настоящее общение между узлами происходит с использованием IP-адресов. Когда вы набираете в строке браузера что-то вроде rambler.ru, ваш браузер обращается к DNS-серверу (а если у этого сервера нет ответа, то к другому серверу, и так до получения ответа), переводит доменное имя сайта в IP-адрес, после чего начинает обмен данными с нужным сайтом.

Это занимает не слишком много времени, но происходит далеко не мгновенно. А DNS-кэш позволяет браузеру получать нужный ему IP-адрес практически мгновенно — при условии, конечно, что нужный IP уже есть в кэше. Главная проблема кэшей — это устаревание записей. Если у сайта вдруг изменится IP-адрес при неизменном доменном имени, а в вашем кэше будет лежать старый адрес, вы, скорее всего, не сможете получить доступ к сайту. Такое происходит нечасто, поэтому лучше всего не увеличивать параметр **Записи DNS устаревают через**... Пусть там останутся установленные по умолчанию 7 дней.

Теперь рассмотрим параметры модуля **Интерактивные элементы** (рис. 12.69).

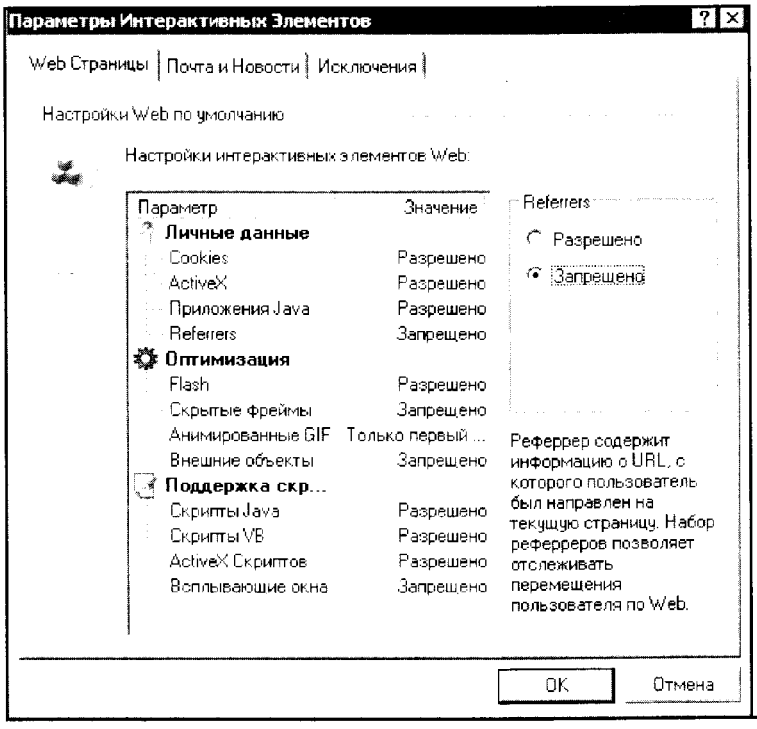


Рис. 12.69. Параметры интерактивных элементов

По умолчанию разрешены все интерактивные элементы на веб-страничках. На рис. 12.69 вы видите окно с модифицированными параметрами. Изменять эти параметры нужно, чтобы достигнуть баланса между функциональностью страничек и скоростью загрузки.

К примеру, параметр **Referrers** в группе **Личные данные** я установил в значение **Запрещено** — не потому, что он замедляет работу, а исключительно из личных предпочтений. Этот параметр позволяет определить, с какого сайта вы пришли, в чем нет ничего страшного. **Cookies** можно и запретить, но некоторые сайты при этом теряют часть функциональности, поэтому я оставил этот пункт включенным.

В группе параметров **Оптимизация** я провел серьезную работу. Flash-анимацию, довольно «тяжелую» как в загрузке, так и в выполнении, я все же оставил: иногда flash-ролики на страничках бывают важными и к тому же довольно красивыми.

Скрытые фреймы, которые занимаются своими «скрытыми» делами, я решил отключить, анимированные GIF'ы урезал до размера одного кадра, а также отключил внешние объекты.

С такими настройками, учитывая то, что в группе параметров **Поддержка скриптов** я выключил всплывающие окна, браузер начинает загружать странички заметно быстрее. Ну а если вдруг окажется, что страничкам чего-то не хватает, эти параметры всегда можно включить.

Если вы хотите просматривать полные версии сайтов, достаточно внести их веб-адреса в список, который доступен на вкладке **Исключения**. Все же некоторые сайты теряют очень много, если отключить на них анимацию, графику и прочие интересные вещи.

Параметры, касающиеся **Почты и новостей**, во многом аналогичны вышеописанным.

Далее переходим к настройкам модуля **Реклама** (рис. 12.70).

Полезность этого модуля вы начинаете видеть буквально сразу же после установки файрволла. Ведь современные веб-странички порой пере-

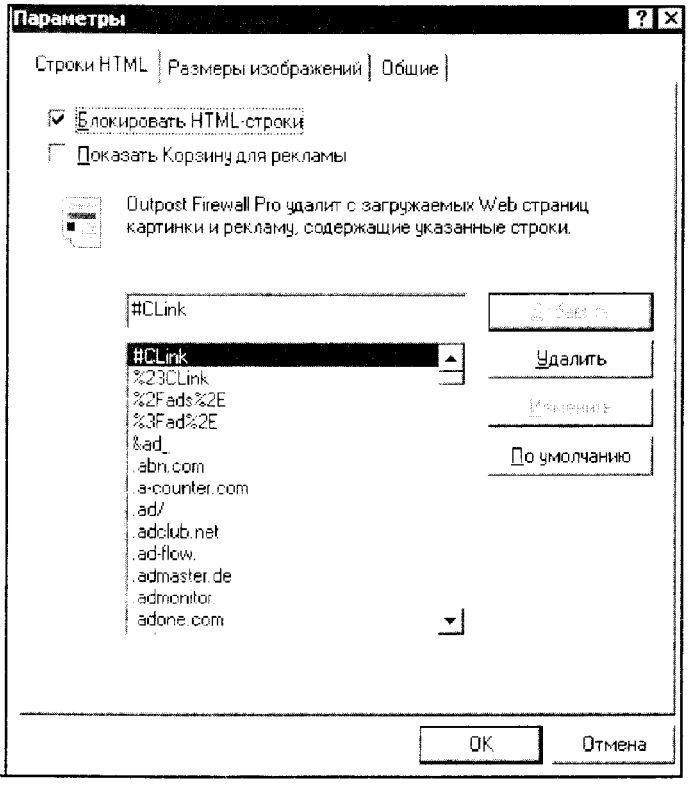


Рис. 12.70. Параметры модуля Реклама

гружены рекламой, а от этого снижается скорость их загрузки. На быстрых соединениях это незаметно, но если вы подключены по *dial-up* и/или платите за трафик, то лишние данные вам ни к чему.

Как правило, можно оставить назначенные по умолчанию параметры этого модуля. Но если вы вдруг увидели на страничке какую-нибудь потенциально интересную рекламу, можно самостоятельно настроить параметры ее блокирования, внеся характерные для нее строки в «черный список». Для этого вам нужно знать язык HTML. (В этой книге мы не будем заниматься разбором особенностей этого языка. За этим вам придется обратиться к соответствующей литературе.)

Вкладка **Размеры изображений** окна настройки параметров блокирования рекламы нужна, чтобы файрволл мог отслеживать изображения, имеющие характерные для рекламных баннеров размеры.

На вкладке **Общие** можно настроить важный параметр, касающийся доверенных сайтов, то есть сформировать список сайтов, рекламу с которых вы хотели бы видеть.

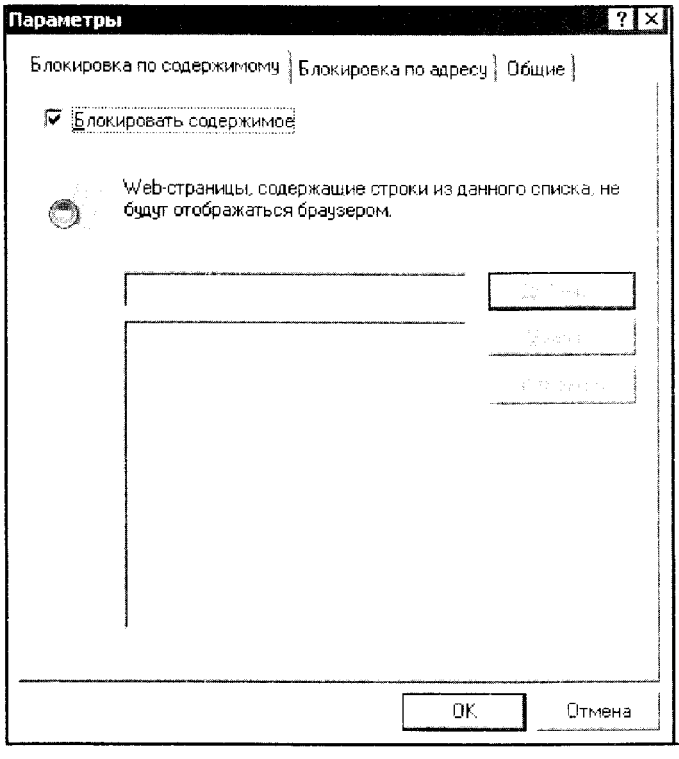


Рис. 12.71. Настройка параметров содержимого

Теперь посмотрим на настройку модуля **Содержимое** (рис. 12.71).

На вкладке **Блокировка по содержимому** можно задать список «плохих» слов, и файрволл будет блокировать странички, на которых есть эти слова.

Список этот по умолчанию пуст, и если вы хотите заблокировать какие-нибудь странички, например, чтобы ограничить доступ детей к каким-нибудь сайтам с ненормативной лексикой, то вспоминайте все нехорошие выражения и вносите в этот список. Чем больше вы знаете таких слов, тем лучше будет защита. Вот только позаботьтесь, чтобы дети не добрались до этого вашего списка, который повлияет на ваши отношения куда хуже, чем соответствующие сайты.

На вкладке **Блокировка по адресу** можно ввести адреса сайтов, которые желательно блокировать.

Параметры настройки фильтрации почтовых вложений (рис. 12.72) следует настраивать так, чтобы эти параметры не нарушали нормальной работы.

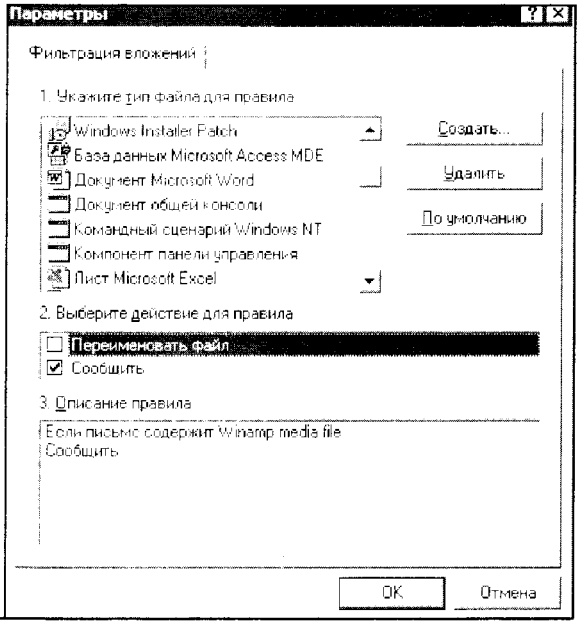


Рис. 12.72. Настройка параметров фильтрации почтовых вложений

К примеру, если программа сообщает о подозрительном почтовом вложении, я предпочитаю выбирать свои дальнейшие действия сам, чтобы не потерять из-за излишней подозрительности файрволла нужные файлы и письма.

Будьте осторожны со вложенными в письма файлами! Для почтовых вложений есть простое правило: если вы не уверены в том, что письмо, содержащее почтовое вложение, безопасно, просто удалите его. Особенно это касается странных писем, которые выглядят как сообщения почтовых серверов о невозможности доставить письмо, и писем, пришедших неизвестно от кого. Вирусы и черви могут быть замаскированы под что угодно, даже под невинный jpg-файл.

Теперь вы умеете эффективно использовать Agnitum Outpost Firewall Pro. К тому же он снабжен отличной русскоязычной справкой, к которой можно обратиться за разъяснениями. От этого файрволла у меня остались самые приятные впечатления, а скорость загрузки веб-страничек после его установки существенно возросла.

12.5. ВЫВОДЫ

Файрволлы — очень важная часть защитного программного обеспечения, которой порой уделяют незаслуженно мало внимания. Конечно, список файрволлов не ограничивается тремя вышеописанными программами и стандартным брандмауэром Windows XP SP2. На самом деле их множество, и если в результате тестирования окажется, что ни один из представленных файрволлов вас не удовлетворил, вы в конце концов найдете что-нибудь подходящее для себя. Стоит лишь поискать.

Программы ZoneAlarm или Outpost Firewall я бы смело рекомендовал всем без исключения: они отлично знают свою работу и несложны в обращении. Look'n'Stop — тоже интересный продукт, но он довольно специфичен.

Надежная защита вашего компьютера находится в сильной зависимости от тандема файрволл+антивирус (а также, разумеется, от частоты обновлений системы, вашей осторожности и осведомленности). Поэтому переходим к описанию антивирусов.

ГЛАВА 13
ЗАЩИТА: АНТИВИРУСЫ, ОБНОВЛЕНИЕ СИСТЕМЫ

Антивирусы — это важные программы, но без обновлений они быстро устаревают. Антивирус считается устаревшим, если его базам данных больше двух недель. Этот показатель может варьироваться, но общее правило таково: чем меньше срок давности базы, тем лучше. Если у вас есть возможность, можете обновлять базы вашего антивируса хоть несколько раз за день. Примерно в таком режиме работают ведущие антивирусные лаборатории. Конечно, такое частое обновление обычно излишне, но хотя бы раз в неделю антивирус желательно обновлять. Новые вирусы, модификации существующих вирусов, черви, троянские программы и другие представители программного андеграунда появляются ежедневно, поэтому чем новее ваши базы — тем лучше.

Никакой антивирус не способен обеспечить стопроцентную защиту. Поэтому я не устану это повторять: будьте осторожны.

Конечно, осторожность должна быть разумной. Если из-за боязни инфекций не пользоваться компакт-дисками, дискетами и не выходить в Интернет, не лучше ли отключить такой компьютер от электросети?

Разумная осторожность еще никому не мешала, но важно, чтобы вирусобоязнь не превращалась в навязчивую идею, которая мешает жить. А раз так — приступаем к рассмотрению некоторых популярных антивирусов.

Дам совет о практике использования антивирусов. К примеру, вы постоянно пользуетесь некой хорошей антивирусной программой, вовремя ее обновляете и полагаете, что у вас в системе все хорошо. Возможно, так и есть, но на всякий случай полезно иногда проверяться другим антивирусом, пусть даже бесплатным: вовсе не исключено, что вы найдете «хворь», которую ваш основной антивирус просто проглядел. Дело тут не в некачественной программе, а в том, что в мире вирусов и антивирусов случается и такое.

13.1. NORTON ANTIVIRUS

Norton Antivirus — это антивирусный комплекс, который рассчитан на комплексную защиту компьютера от вирусов, троянцев, вредных почтовых вложений и других вирусных угроз.

Разберем особенности управления этой программой. Она имеет английский интерфейс. Это вовсе не станет проблемой для тех, кто нетверд в английском, так как многое Norton Antivirus делает самостоятельно.

Главное окно антивируса (рис. 13.1) можно вызвать, дважды щелкнув по его значку в системной панели Windows.

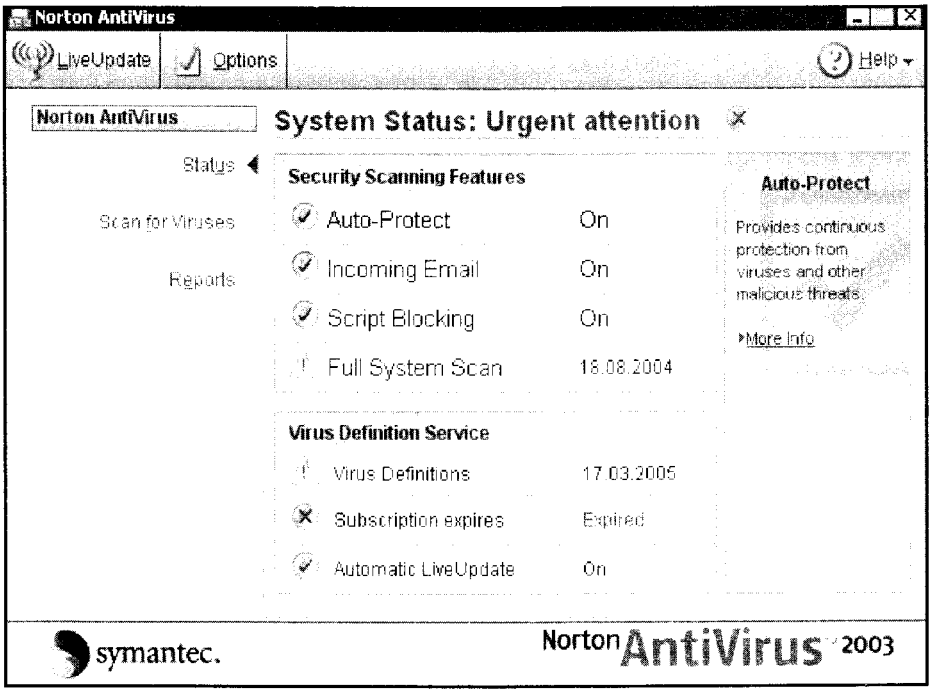


Рис. 13.1. Norton Antivirus, панель System Status

В левой части окна есть панель **Norton Antivirus**, содержащая названия трех разделов программы: **Status (Статус)**, отображающего основные показатели работы антивируса, **Scan for Viruses (Сканирование)**, который позволяет управлять сканированием системы, и **Reports (Отчеты)**, с помощью которого можно просмотреть сообщения об обнаруженных в вашей системе вирусах.

В левой части окна программы расположена панель, раскрывающая параметры показателя, выбранного в панели **Norton Antivirus**.

На панели **System Status (Состояние системы)** можно видеть основные показатели работы антивируса. На рис.13.1 видно, что включен ре-

жим **Auto-Protect**, то есть режим автоматической защиты, и производится сканирование входящей почты (**Incoming Email**).

Поле, информирующее о состоянии сканирования почты, может принимать различные значения. Так, если в нем появилась надпись **Email Scanning On**, это значит, что осуществляется сканирование входящей и исходящей почты.

В этой же строчке может быть написано **Outgoing Email On** — сканирование исходящих сообщений. Если вы попытаетесь отправить по почте файл, зараженный вирусом, то антивирус предотвратит его дальнейшее распространение. Зачем сканировать исходящую почту? В этом выражается забота не только о вашем компьютере, но и о компьютерах тех, с кем вы ведете переписку.

Сканирование почтовых сообщений можно выключить, но делать это не рекомендуется.

Дальше идет пункт, отвечающий за блокирование опасных скриптов (**Script Blocking**). Напротив пунктов, которые отражают функционирование антивируса в нормальном порядке, стоят галочки, а вот пункты, которые требуют вашего внимания, отмечены восклицательным знаком. Так, например, восклицательным знаком отмечено время полного сканирования системы (**Full System Scan**). Если вы пользуетесь Norton Antivirus, постарайтесь, чтобы таких восклицательных знаков было как можно меньше.

Случается, что заражение происходит при включенном антивирусе. Несмотря на то что программа работает в режиме антивирусного мониторинга, отслеживая все потенциально опасные системные события — к примеру, копирование файлов, — ваша система все же может содержать вирусы, о которых антивирус пока не знает.

Допустим, вам показалось, что антивирусная программа тормозит работу системы в то время, когда вы пытаетесь запустить на ней какую-нибудь новую ресурсоемкую игру, и вы отключили антивирусную программу. В это время компьютер мог заразиться — неважно каким путем. При этом ни вы, ни антивирус не знаете о том, что система инфицирована: ведь вирус, заразив какой-нибудь файл, остался тихо лежать на винчестере, поджидая своего часа.

Через пару дней после отключения антивируса вы включили его, но вирусто все еще лежит на винчестере. Если вы не будете производить с файлом, в котором он затаился, никаких действий, то вирус так и останется на жестком диске до тех пор, пока вы не запустите процедуру полного сканирования системы или не попытаетесь запустить инфицированный файл. Это один сценарий инфицирования системы при включенном антивирусе. Другой путь заражения заключается в том, что антивирус может просто не обнаружить абсолютно новый вирус в момент его первого проникновения в систему. Такое хоть и редко, но бывает. По старому сценарию вирус заражает что-нибудь и затихает, а в процессе следующего обновления антивирус получает информацию, которая нужна для обнаружения и лечения этого вируса. Затем вы запускаете процедуру полного сканирования системы, и новый вирус будет обнаружен. Поэтому не стоит пренебрегать процедурой полного сканирования. Конечно, оно может продолжаться несколько часов и занять много системных ресурсов, но безопасность дороже.

В нижней части стартового окна нашего антивируса в поле **Virus Definition** имеется служебная информация о последней дате обновления антивируса, сроке истечения подписки (поле **Subscription**) и автоматического обновления (**Live update**). Постарайтесь, чтобы и в описаниях этих полей не было бы ничего кроме зеленых галочек, сигнализирующих о том, что все в порядке.

Теперь рассмотрим панель **Scan for Viruses** (рис. 13.2).

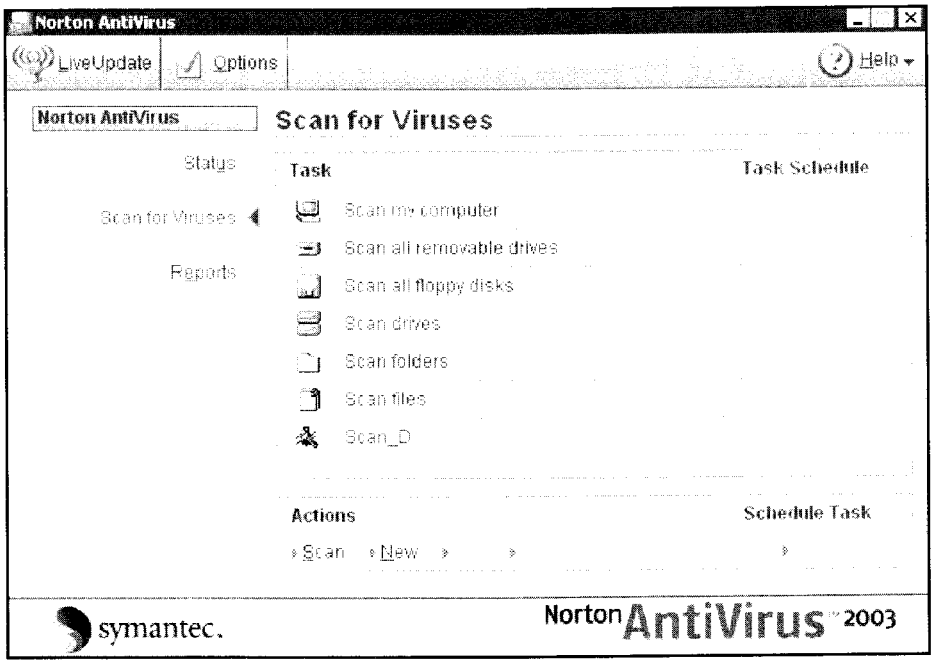


Рис. 13.2. Norton Antivirus, панель Scan for Viruses

На этой панели можно выбирать объекты для сканирования на вирусы. Вы можете выбрать:

- **Scan my computer** — сканирование всех дисков компьютера. Это глобальная проверка, обычно она длится довольно долгое время, зато позволяет как следует проверить ваш компьютер
- **Scan all removable drives** — сканирует все съемные диски: к примеру, эта команда позволяет включить сканирование CD-диска
- **Scan all floppy disks** — сканирует дискеты. На компьютерах, не имеющих дисковода для дискет, этот пункт работать не будет
- **Scan folders** — позволяет просканировать определенные папки
- **Scan files** — позволяет просканировать выбранные файлы.

Чтобы начать выполнять одну из задач, перечисленных в этом окне, достаточно дважды щелкнуть по ней (или выделить ее мышью) и нажать кнопку **Scan** в нижней части окна.

Здесь же можно настраивать автоматическое сканирование определенных объектов системы при помощи планировщика и Мастера новых заданий.

Вы можете даже создать собственную задачу, которую можно будет запускать по расписанию. Например, удобно включить в список сканируемых папок те, которые содержат постоянно обновляемые файлы: папки, где хранятся загруженные из Интернета файлы, папки с рабочими документами и так далее. Чтобы создать задание нового типа, нажмите кнопку **New** в нижней части окна **Scan for Viruses**. При этом появится окно Мастера, помогающего создать новый отчет (рис. 13.3).

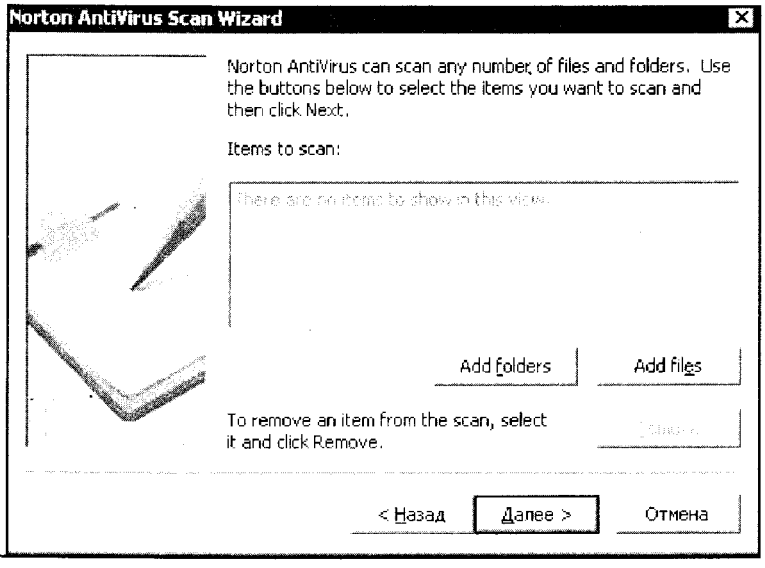


Рис. 13.3. Создание нового задания

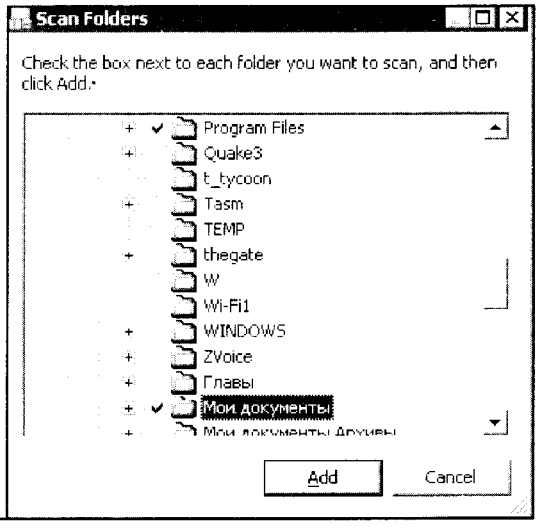


Рис. 13.4. Выбор папок для сканирования

Здесь можно добавлять папки или файлы для сканирования. Для добавления папок достаточно щелкнуть по кнопке **Add folders** и из появившегося списка папок вашего компьютера выбрать те, что вас интересуют (рис. 13.4).

После этого нажмите кнопку **Add**, и выбранные папки будут добавлены в список для сканирования. Теперь нажмите **Далее**, дайте заданию название (например, это задание я назову «Мои документы и программы») и нажмите **Готово**.

В результате в списке заданий появится новое задание (рис. 13.5), с которым можно работать дальше. Если выделить строчку с нашим заданием при помощи мышки, то активируются некоторые кнопки в нижней части окна **Scan for Viruses**, которые были до этого неактивны. Они предназначены для правки задания (**Edit**) и для его удаления (**Delete**).

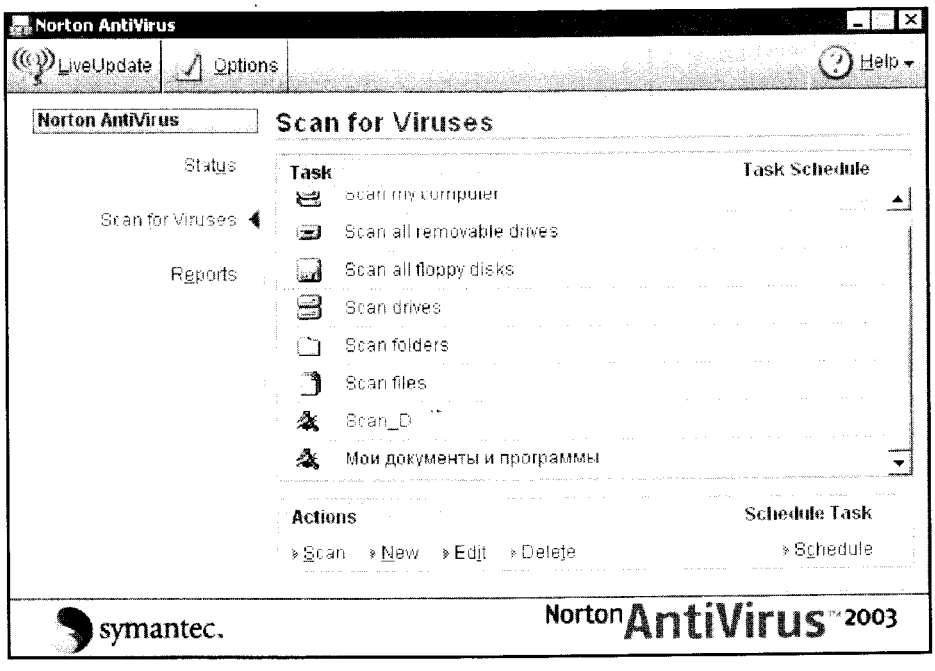


Рис. 13.5. Окно Scan for Viruses с активированным заданием

Среди этих кнопок есть еще одна, расположенная в правой части окна. Она называется **Schedule** и предназначена для создания расписания запуска вашего задания. Воспользовавшись этой кнопкой, вы запустите окно создания расписаний. В этом окне достаточно нажать кнопку **Создать** и отредактировать новое расписание (рис. 13.6).

После того как вы создадите расписание для запуска вашего задания, оно будет запускаться и выполняться с заданной периодичностью.

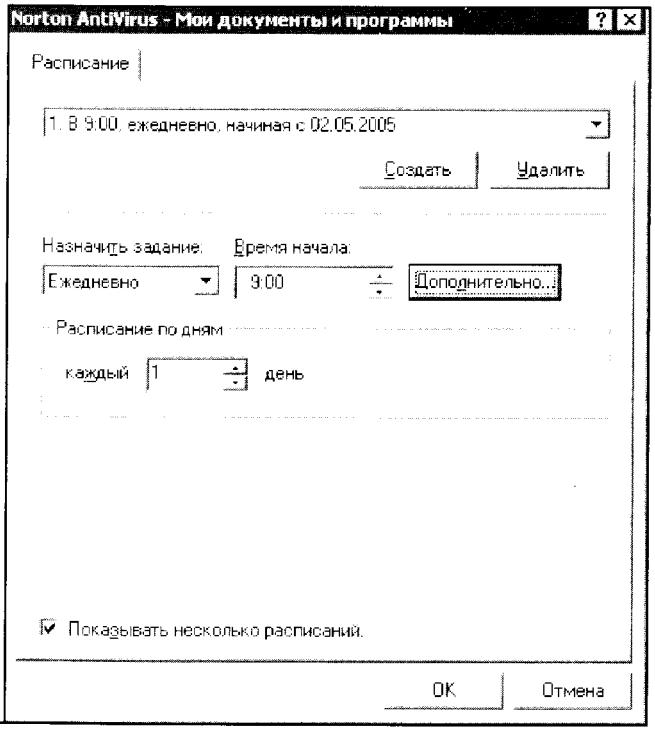


Рис. 13.6. Создание расписания

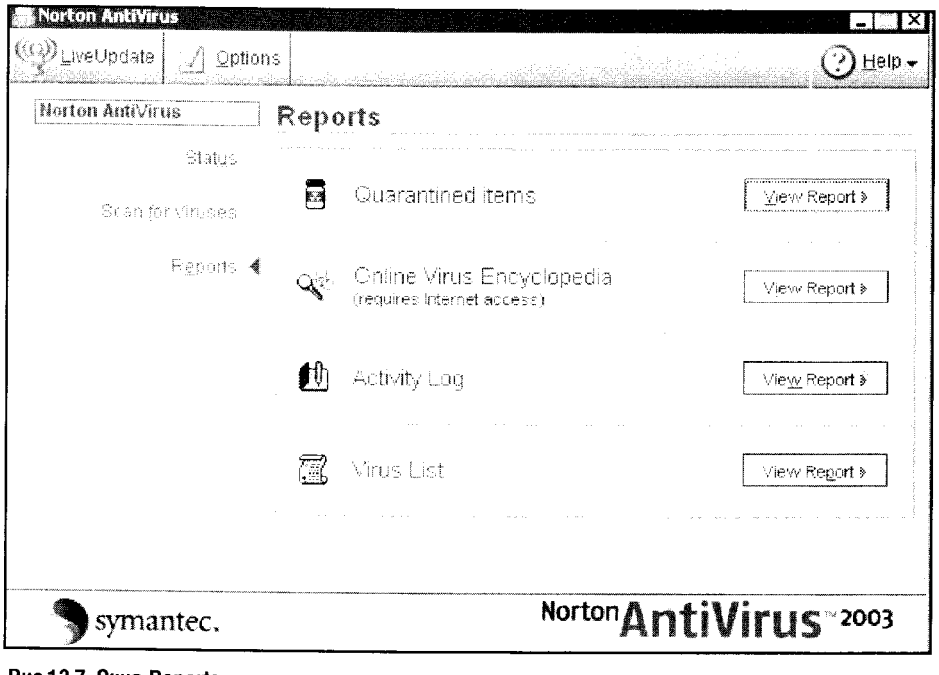


Рис.13.7. Окно Reports

Теперь перейдем к разделу **Reports**, связанному с просмотром отчетов (рис. 13.7). Здесь можно просмотреть отчеты, касающиеся файлов, помещенных в карантин (**Quarantined Items**), почитать онлайновую вирусную энциклопедию (**Online Virus Encyclopaedia**), просмотреть журнал (**Activity Log**) и ознакомиться с подробностями личной жизни вирусов, известных системе (**Virus List**).

В разделе **Quarantined Items** можно найти список файлов, помещенных в карантин. Дело в том, что антивирус не всегда может вылечить файлы, в которых он обнаружил вирус. В этом случае у программы есть два варианта действий: удалить файл или поместить в карантин. Если важный для вас файл оказался зараженным, то лучше поместить этот файл в карантин для того, чтобы позже, воспользовавшись обновленными антивирусными базами, попытаться вылечить его.

На рис. 13.8 изображено окно просмотра объектов, помещенных в карантин. Оно разделено на две части. В правой находятся группы объектов:

- **Quarantined Items** — объекты, помещенные в карантин;
- **Backup Items** — сохраненные объекты;
- **Submitted to Symantec** — объекты, отправленные в лабораторию Symantec.

В левой части окна можно видеть содержимое каждой из групп.

Если выделить один из объектов, помещенных в карантин, с ним можно проделать некоторые действия, воспользовавшись панелью ин-

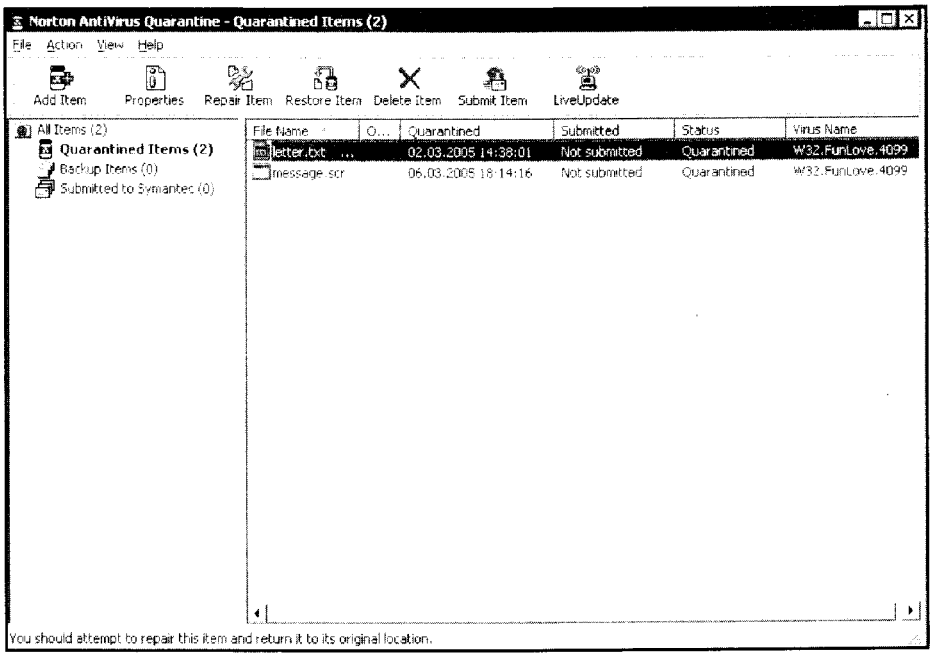


Рис. 13.8. Просмотр объектов, помещенных в карантин

струментов, которая расположена в верхней части окна. При помощи кнопки **Properties** можно вывести на экран окно свойств выделенного объекта, кнопка **Repair Item** нужна, чтобы антивирус попытался вылечить объект, кнопка **Restore Item** служит для восстановления объекта, **Delete Item** — для удаления, а **Submit Item** — для отправки его в лабораторию Symantec.

Теперь посмотрим на верхнюю часть главного окна программы, где есть несколько кнопок. Левая кнопка **Live Update** служит для запуска обновления программы. Если вы запустили обновление (как правило, антивирус делает это автоматически сам), то остается только нажимать кнопку **Далее**, ничего не меняя в предлагаемых программой вариантах его настройки.

Кнопка справа называется **Help**, и она помогает запустить справочную систему программы.

А вот на кнопке под названием **Options** мы остановимся подробнее, так как она позволяет управлять некоторыми дополнительными параметрами программы.

Посмотрите на рис. 13.9, где изображено окно свойств антивируса.

Окно это разделено на две части. В левой части находятся группы параметров, а в правой — детальные установки.

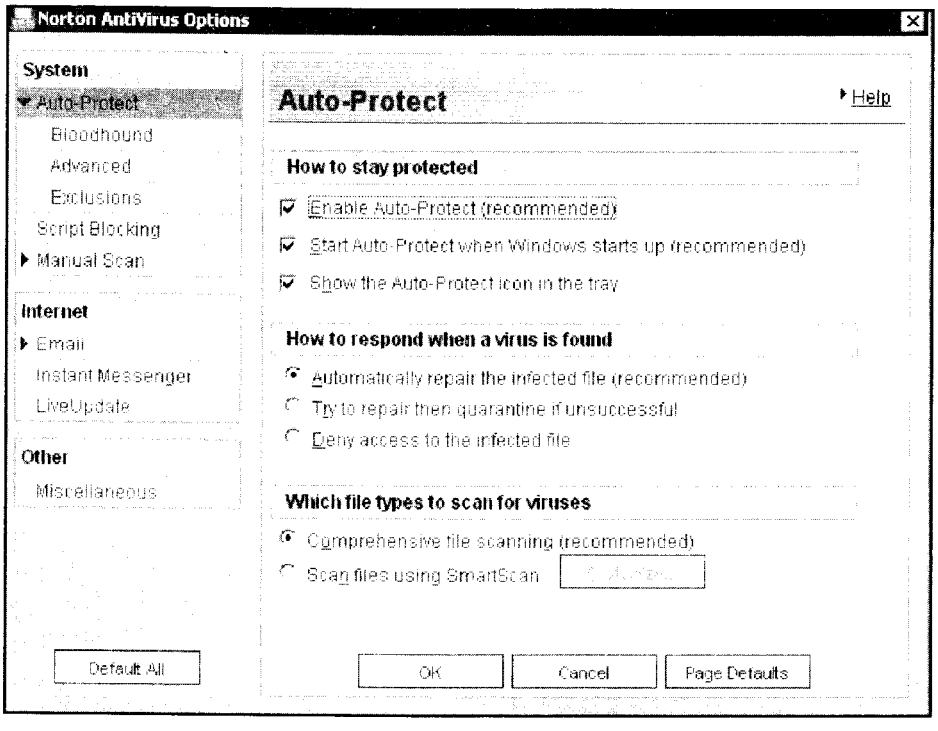


Рис. 13.9. Опции Auto-Protect

На рис. 13.9 показаны опции **Auto-Protect**, то есть установки, которые отвечают за автоматическое сканирование файлов, выявление и лечение вирусов. Группа параметров **How to stay protected (Как остаться защищенным)** отвечает:

- за включение автозащиты (параметр **Enable Auto-Protect (recommended)**);
- за старт автозащиты вместе с Windows (**Start Auto-Protect when Windows starts up (recommended)**);
- за показ значка автозащиты в системной панели (**Show the Auto-Protect icon in the tray**).

Рекомендуется включить все эти параметры, чтобы обеспечить ваш компьютер максимальной защитой, а вас — информацией о том, что защита включена.

Группа параметров **How to respond when a virus is found (Как отвечать, если вирус найден)** отвечает за поведение антивируса в момент, когда он обнаружит инфицированный файл.

- Параметр **Automatically repair the infected file (recommended)** заставит антивирус вылечить инфицированный файл автоматически.
- Параметр **Try to repair then quarantine if unsuccessfull** приказывает антивирусу поместить файл в карантин при невозможности лечения.
- Параметр **Deny access to the infected file** запрещает доступ к инфицированному файлу.

Группа параметров **Which file types to scan for viruses** определяет типы файлов, которые нужно сканировать.

- Параметр **Comprehensive file scanning (recommended)** включает сканирование всех файлов. Такой ход оправдан, так как зловредный код может быть где угодно.
- Параметр **Scan files using SmartScan** позволяет сканировать лишь файлы с определенными расширениями.

Отметим, что первый параметр, рекомендованный разработчиком, сильно повышает нагрузку на систему.

В левой части окна опций антивируса, сразу под строчкой **Auto-Protect** есть еще несколько органов управления. Строка **Bloodhound (Ищейка)** позволяет управлять эвристическим анализатором (рис. 13.10). Желательно, чтобы этот параметр был включен.

Особенности работы эвристических анализаторов нам уже знакомы из прошлой главы. Напомню, что отключение эвристического анализатора освободит некоторое количество системных ресурсов, зато его работа позволяет выявлять неизвестные антивирусу вредоносные программы — словом, отключать анализатор не рекомендуется. А если вам нужен максимальный уровень защиты, поставьте его в позицию **Highest Level of protection**, учитывая, однако, что в этом режиме нагрузка на систему резко возрастает.

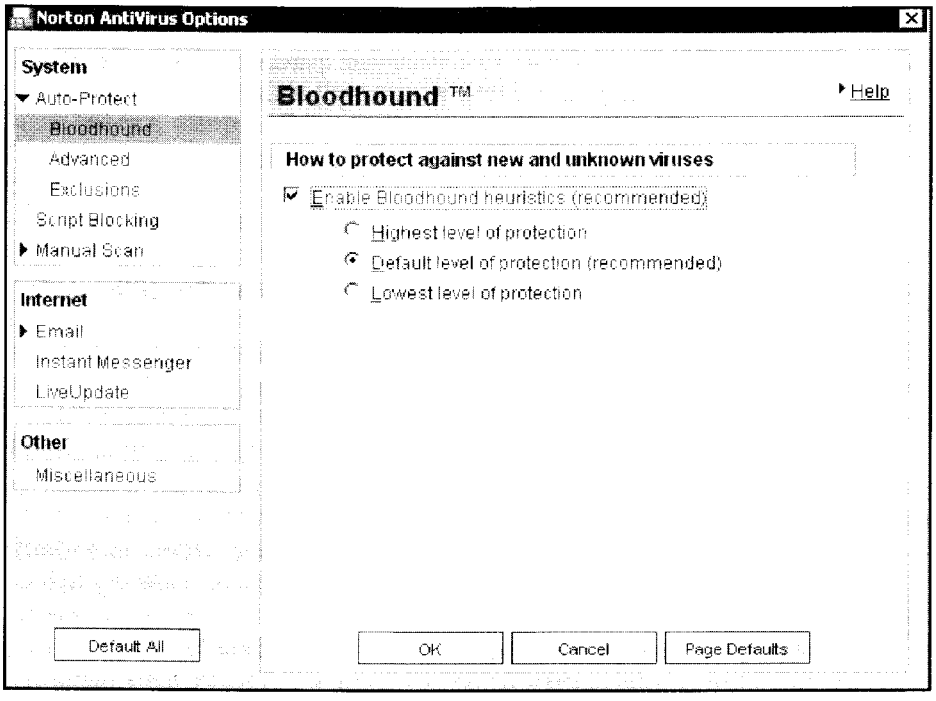


Рис. 13.10. Опции Bloodhount

Группа параметров **Advanced** из левой части окна опций антивируса предназначена для контроля активности дисковода гибких дисков. По умолчанию антивирус обыскивает дискеты на предмет загрузочных вирусов всякий раз, когда их вставляют в дисковод, и дополнительно проверяет их перед выключением компьютера.

Не рекомендуется оставлять дискеты в дисководе при перезагрузке или выключении компьютера. Эта рекомендация восходит к тем временам, когда основным носителем информации (и переносчиком вирусов) между компьютерами были дискеты. Многие загрузочные вирусы могут заражать жесткие диски компьютера именно при старте с дискеты, случайно забытой в дисководе. Сейчас таких вирусов в «диком» виде почти не осталось, и все же не стоит пренебрегать простым правилом: при выключении или перезагрузке компьютера извлеките дискету из дисковода.

Группа **Exclusions** предназначена для задания списка исключений файлов: программа позволяет указать файлы и папки, проверять которые не нужно (рис. 13.11).

На том же рис. 13.11 показано окно для ввода информации о новом исключении, которое появляется при нажатии кнопки **New** окна **Auto-Protect Exclusion List**.

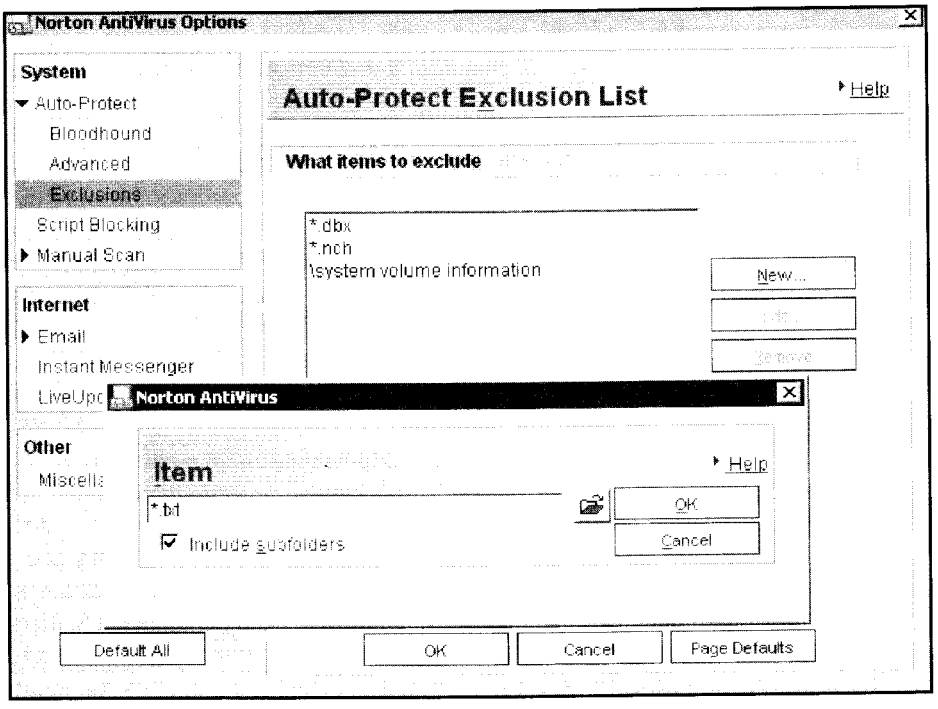


Рис. 13.11. Опции Exclusions

Исключение представляет собой имя файла или путь к папке. При задании исключений можно использовать символы «*» и «?». Традиционно символ «*» означает любое количество любых символов, а «?» — один любой символ. Например, «***.txt**» означает все файлы с расширением **.txt**.

Задавая программе исключения, помните: любое исключение снижает уровень защищенности вашей системы. Даже такое на первый взгляд безобидное, как ***.txt**.

Группа **Script Blocking** (рис. 13.12) предназначена для управления блокированием скриптов, которые могут содержать вирусы.

Скрипты (например, программы на VB Script, Java-script и еще некоторые) нельзя отключать полностью. Они могут использоваться некоторыми программными продуктами для вполне мирных целей. Но скрипты, как и другие программные продукты, таят потенциальную опасность, поэтому за ними нужен глаз да глаз. По умолчанию антивирус имеет достаточно строгую конфигурацию: параметр **Enable script blocking (recommended)** включен, то есть включен контроль за скриптами, а параметр **How to respond when a malicious script is found** установлен в значение **Ask me what to do (recommended)**. Это означает, что при обнаружении скриптовой активности антивирус спросит вас, что ему делать дальше.

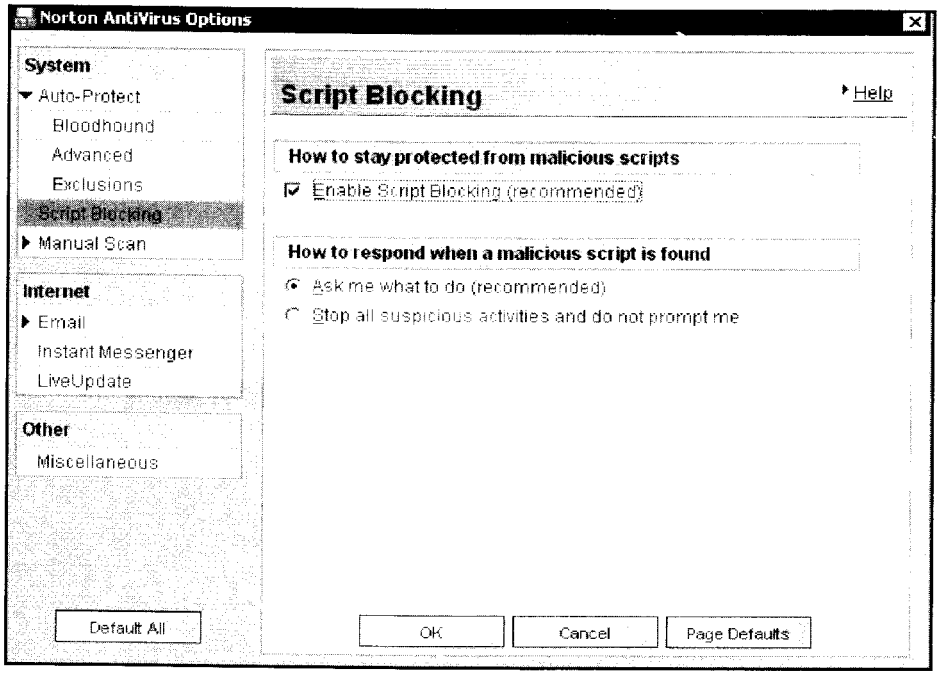


Рис. 13.12. Опции Script Blocking

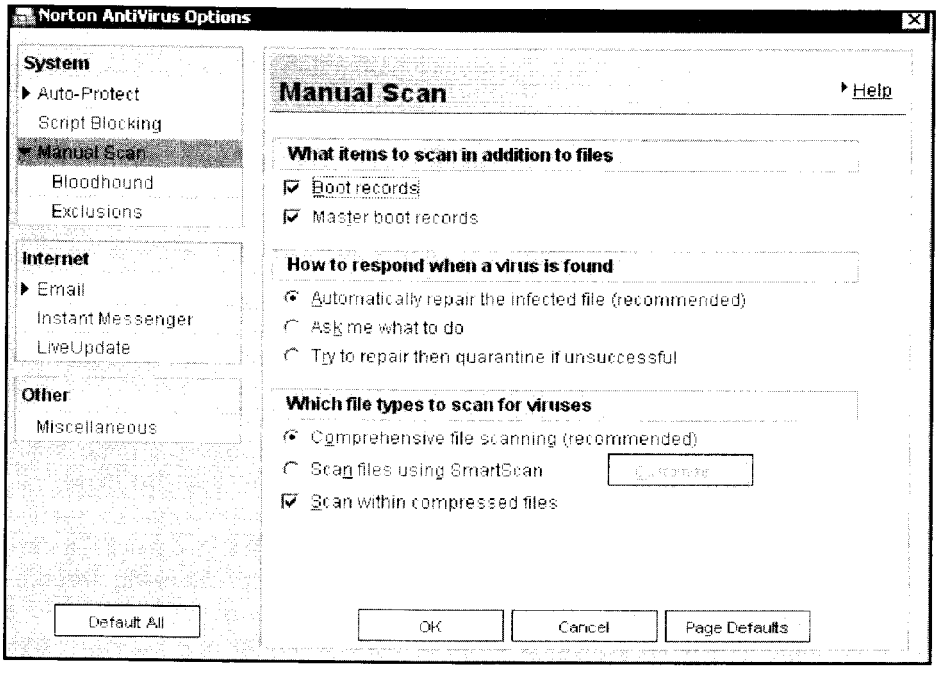


Рис. 13.13. Опции Manual Scan

Далее в левой части окна опций антивируса расположен блок регулировки ручного сканирования файлов (рис. 13.13).

Первая группа параметров в окне **Manual Scan** называется **What items to scan in addition to files**. Желательно установить галочки перед параметрами **Boot records** и **Master boot records**. Эта мера направлена против загрузочных вирусов, которые могут заражать загрузочные секторы жестких дисков.

Остальные группы параметров уже были описаны выше (см. описание рис. 13.9) — здесь они аналогичны тем же параметрам, применяемым к настройке автоматического сканирования файлов. Аналогичны вышеописанным и разделы **Bloodhound** и **Exclusions**, которые видны в левом окне программы под строчкой **Manual Scan**. Здесь функция **Bloodhound** отвечает за использование эвристического анализатора, а **Exclusions** — за исключения.

Познакомимся с параметрами сканирования электронной почты (рис. 13.14). Если вы прежде не пользовались этим Norton Antivirus, то первая попытка отправки почты с вашего почтового клиента при включенной опции проверки исходящей корреспонденции может вызвать у вас недоумение. Почтовый клиент отправит почту необыкновенно быстро, но в системной панели появится индикатор отправки почты, принадлежащий антивирусу. По сути дела почтовый клиент передает свою почту антивирусу, который сканирует ее и затем отправляет по адресу назначения.

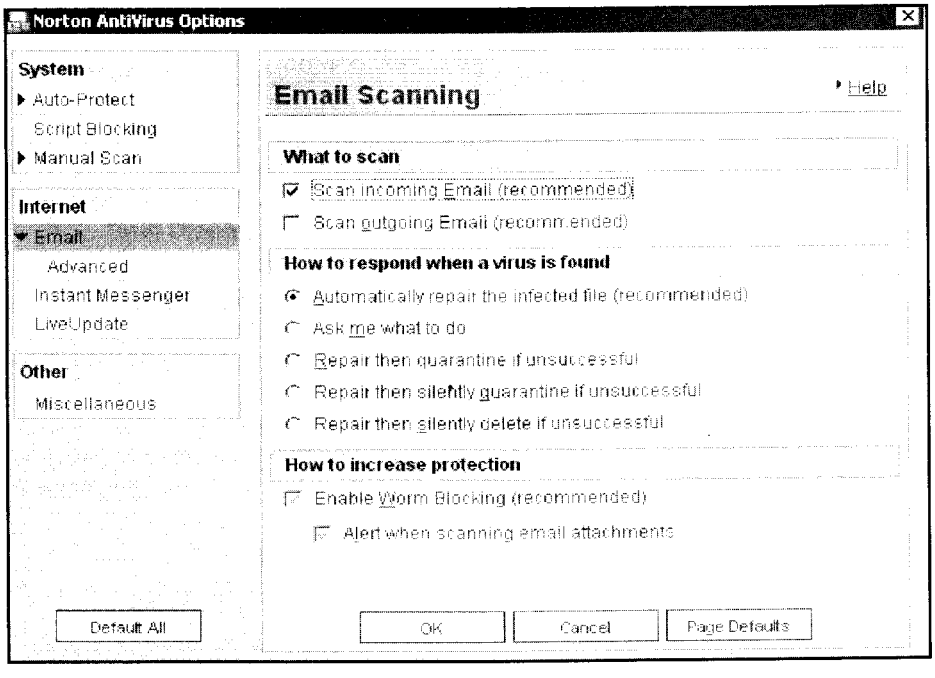


Рис. 13.14. Опции Email Scanning

При сканировании почты следует определиться, во-первых, что именно сканировать (группа параметров **What to scan**). Здесь могут быть варианты.

Рекомендуется сканировать и входящую, и исходящую почту. Сканировать исходящие сообщения следует для того, чтобы не допустить распространения вирусов с вашего компьютера на другие компьютеры Сети. Ну а необходимость сканирования входящей почты, думаю, в объяснениях не нуждается: ведь почта — это едва ли не главный путь проникновения с вашу систему современных вирусов и червей.

Во-вторых, это окно помогает определить действия антивируса при обнаружении заразы (группа параметров **How to respond when a virus is found**). Здесь по умолчанию установлена настройка **Automatically repair the infected file (recommended)**, которая приказывает антивирусу автоматически лечить инфицированный файл. Эта установка позволяет антивирусу действовать полностью самостоятельно.

Теперь рассмотрим дополнительные параметры, касающиеся настройки электронной почты (строка **Advanced** раздела **Email** в левой части окна **Options**), (рис. 13.15).

Эти опции предназначены не для защиты от вирусов, а для повышения удобства работы с антивирусом.

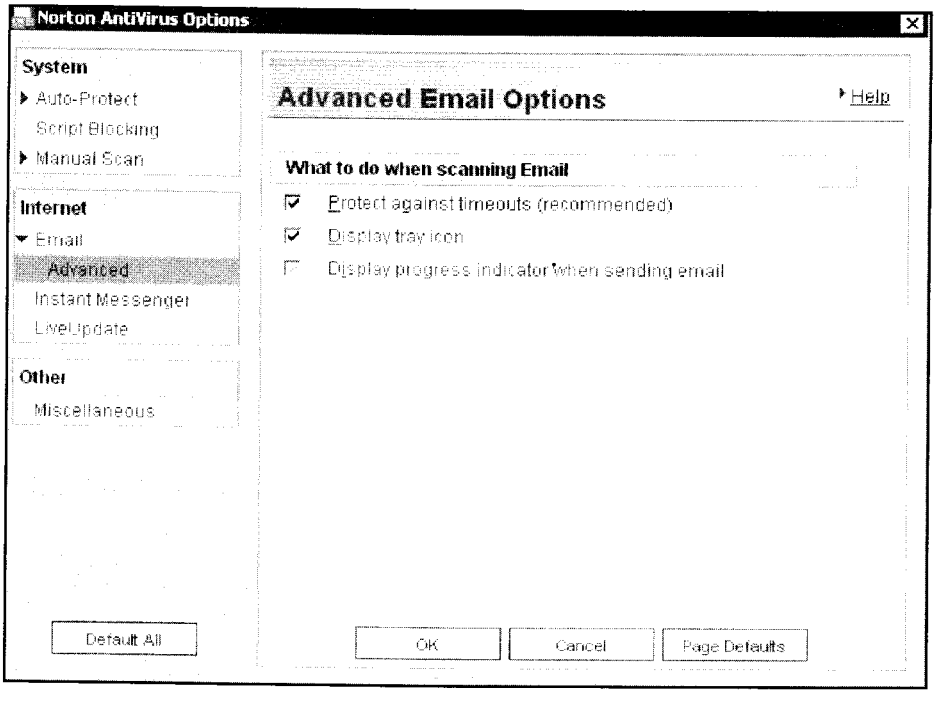


Рис. 13.15. Опции Advanced Email Options

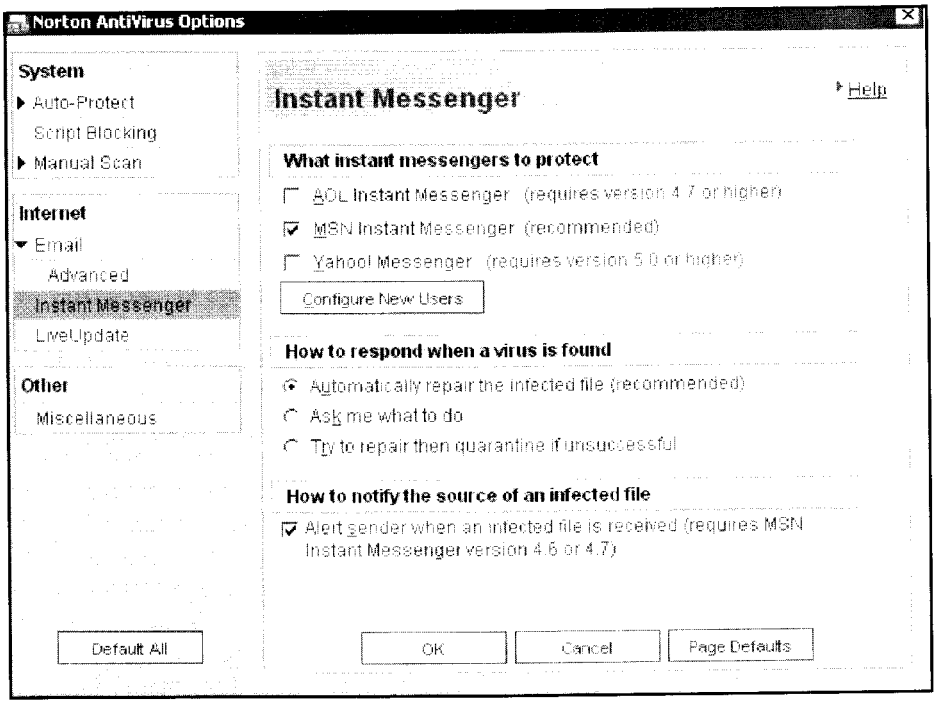


Рис. 13.16. Опции Instant Messenger

- Опция **Protect against timeouts (recommended)** нужна, чтобы почтовый клиент не выводил сообщения об ошибке, когда антивирус перехватывает письма для проверки.
- Опция **Display tray icon** выводит значок отправки почты в системную панель во время проверки отправляемой или принимаемой почты.
- Опция **Display progress indicator when sending email** позволяет показывать индикатор отправки электронной почты в процессе отправки почты.

Теперь рассмотрим параметры защиты интернет-мессенджеров (**Instant messenger**) (рис. 13.16).

Если вы пользуетесь программами для обмена мгновенными сообщениями, то вы должны знать, что и они являются источником опасности. Поэтому следует включить защиту этих программ в опциях **Instant Messenger**.

Группа параметров **What instant messenger to protect** отвечает за защиту AOL Instant Messenger, MSN Instant Messenger и Yahoo messenger. Если вы пользуетесь одной из этих программ, установите галочки против их наименований.

Группа параметров **How to respond when a virus is found** определяет поведение антивируса при обнаружении вируса. Наиболее адекватной

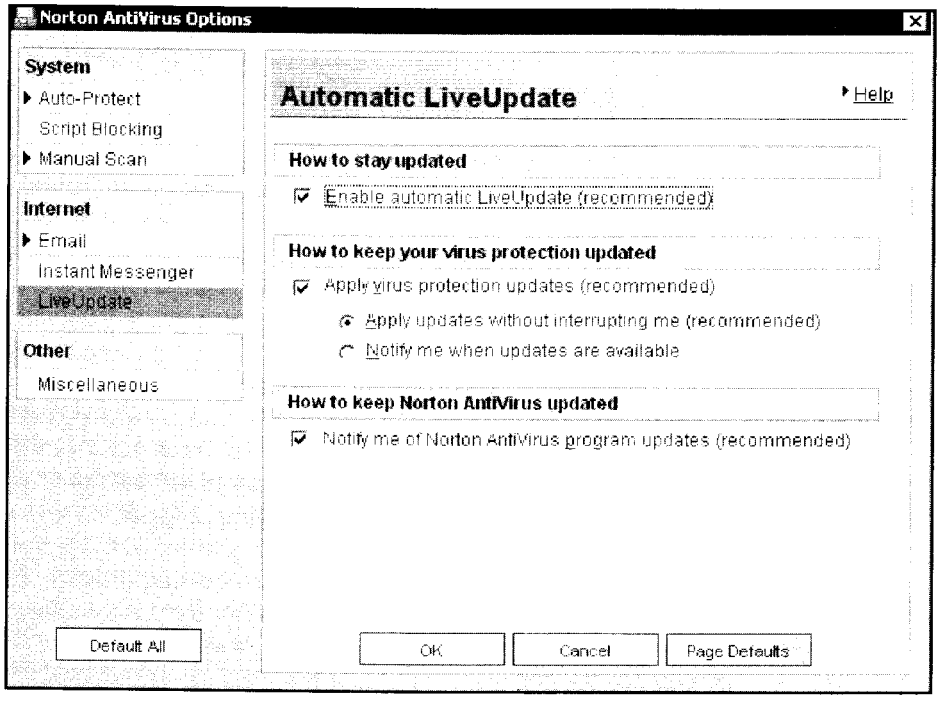


Рис. 13.17. Опции LiveUpdate

установкой для этого параметра является **Automatically repair the infected file**, то есть автоматическое лечение инфицированного файла.

Рассмотрим теперь параметры автоматического обновления (строка **LiveUpdate** в левой части окна программы), (рис. 13.17).

- Если включен параметр **Enable Automatic LiveUpdate (recommended)** группы **How to stay updated**, то программа будет автоматически обновлять свои компоненты и антивирусные базы при соединении с Интернетом.
- Если в группе параметров **How to keep you virus protection updated** установить галочку в поле **Apply virus protection updates (recommended)**, то антивирус будет инициировать процесс установки обновлений самостоятельно. При этом, если выбран подпараметр **Apply updates without interrupting me (recommended)**, антивирус сделает все сам, не потревожив вас, а если выбрать подпараметр **Notify me when updates are available**, антивирус спросит вас о том, устанавливать ли обновления.
- Если включить параметр **Notify me of Norton AntiVirus program updates (recommended)**, то программа сообщит вам о том, что доступны обновления.

Строго рекомендуется в любом случае включить автоматическое обновление, так как это повышает уровень защищенности вашего ком-

пьютера. Возможно, однако, что антивирус будет слишком часто пытаться провести обновления. Для тех, кто пользуется *dial-up*-доступом, это не слишком удобно. В этом случае вам придется либо самостоятельно обновлять его хотя бы раз в неделю, либо ждать появления сообщений об угрозе безопасности вашего компьютера, которые сам антивирус может выдавать с некоторой периодичностью.

Теперь рассмотрим параметры **Miscellaneous** (они находятся в группе **Other** левой части окна программы), (рис. 13.18).

Это важная группа опций, где собраны установки, касающиеся разных вопросов работы антивируса.

- Опция **Create backup file in Quarantine before attempting a repair** предназначена для того, чтобы программа делала архивную копию объектов перед попыткой их лечения. Ведь даже проверенный временем антивирус может так «вылечить» файл, что тот больше не сможет выполнять свои функции. Дело здесь не столько в антивирусах, сколько в новых модификациях вирусов, которые могут сделать с файлом что-то такое, о чем не знает антивирус. В результате получаются казусы. Опция **Create backup file in Quarantine before attempting a repair** нужна, чтобы обезопасить вас от возможной порчи зараженного, но ценного для вас файла.

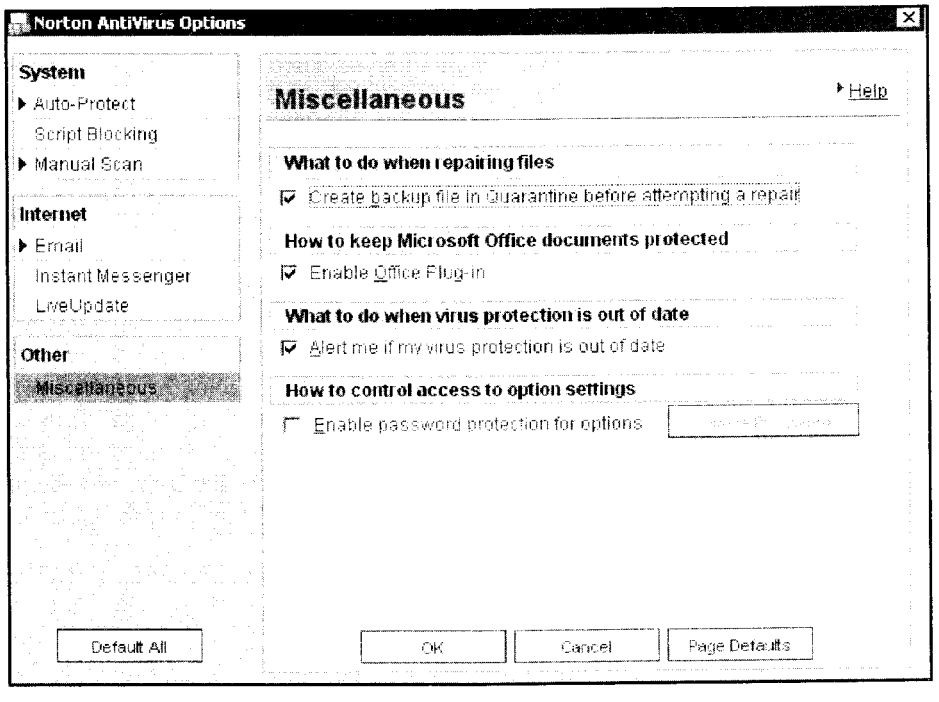


Рис. 13.18. Опции Miscellaneous

- Установка **Enable Office Plug-in** предназначена для включения защиты офисных приложений от вирусов. Макровирусы по своим возможностям ничем не уступают другим типам вирусов, поэтому повышенный уровень безопасности при использовании офисных программ (Microsoft Word, например) вам не помешает.
- Благодаря параметру **Alert me if my virus protection is out of date** антивирус сообщит вам о том, что вашу программу пора обновить. Это, кстати, и есть средство, заменяющее автоматическое обновление, о котором я говорил выше. Оно особенно полезно «диалапникам», которые не могут позволить себе ежедневные лишние полчаса работы в Сети только для того, чтобы антивирус обновил свои базы и компоненты. А этот параметр будет периодически напоминать вам о том, что пора обновляться.
- И, наконец, установка **Enable password protection for option** позволяет настроить парольную защиту для настройки опций антивируса. Включайте этот параметр и устанавливайте пароль только в том случае, если вашим компьютером пользуются другие люди, и постарайтесь не забыть пароль, так как иначе у вас могут быть сложности с его восстановлением.

13.2. NOD32

Рассмотрим следующий антивирусный продукт, который признан лучшим в деле обнаружения так называемых «диких вирусов» по состоянию на апрель 2005 года (по информации *http://www.antivirus.ru/OknoA.html#M12*). Эта оценка несколько субъективна: к примеру, замечательный и надежный Norton Antivirus, описанный выше, расположен в этом рейтинге далеко не на первом месте (что, однако, вовсе не значит, что он плохо защитит вашу систему).

Антивирус NOD32 разработан компанией Eset. Скачать его можно на сайте *http://www.nod32.com*. Вы можете загрузить полнофункциональную демо — версию антивируса и, поработав и оценив ее, купить саму программу.

Дистрибутив этого антивируса «весит» всего около 7,5 мегабайт. Для одного из лучших антивирусов это совсем немного. Разработчики разделили подробную документацию: описание продукта и описание собственно антивируса, так что если вам нужна документация, придется потратиться на ее загрузку, а если вам нужна лишь антивирусная защита, то объем закачки ограничится 7,5 мегабайтами.

Если в вашей системе были установлены другие антивирусы (особенно это касается антивирусов, имеющих резидентные антивирусные мониторы), их перед установкой NOD32 рекомендуется деинсталлировать или по меньшей мере, отключить, иначе возможны проблемы.

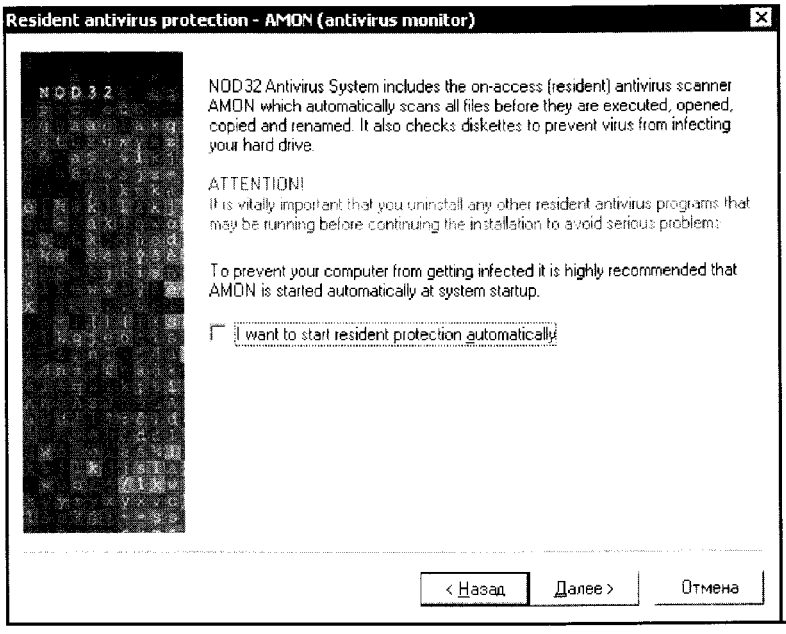


Рис. 13.19. Установка антивируса NOD32

Процесс установки антивируса полностью стандартен (рис. 13.19).

Вы ответите на несколько стандартных вопросов, прочтете лицензионное соглашение, выберете тип установки — вот и все. После установки следует обычная в таких случаях перезагрузка, и работа начинается.

Рассмотрим для начала основные возможности этого антивируса, а затем подробнее коснемся его точной настройки.

NOD32 поддерживает все современные антивирусные возможности. Он содержит антивирусный сканер, резидентный антивирусный монитор, умеет проверять входящий POP3-трафик, то есть сканирует сообщения электронной почты. Антивирус умеет находить и лечить все типы вирусов, он обладает эвристическим анализатором, который помогает ему обнаруживать ранее неизвестные вредные программы.

NOD32 управляется при помощи модуля централизованного управления. Этот модуль можно вызвать двойным щелчком по иконке антивируса в системной панели Windows. Здесь вам предоставят доступ ко всем функциям и настройкам антивируса.

Заголовки компонентов антивируса объединены по умолчанию в левой части окна модуля управления, а подробные установки появляются в правом окне программы. На рис. 13.20 изображено окно модуля управления с открытым окном свойств модуля обновления антивируса (**Update**).

Обзор функций продукта начнем с модуля обновлений. В окне **Update** сразу под информационной панелью есть параметр **Automatic update**, и, если он включен, антивирус будет проводить обновление сам. Ниже расположена кнопка **Abort (Прервать)**. Если вы хотите прервать процесс обновления, следует воспользоваться этой кнопкой.

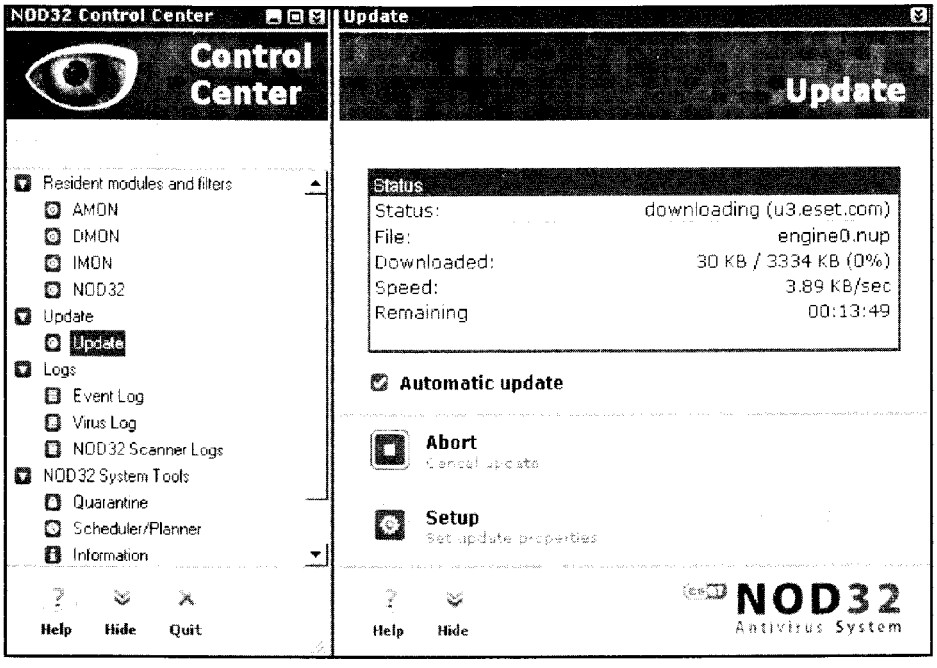


Рис. 13.20. Модуль обновления антивируса NOD32

Для запуска обновления вручную можно воспользоваться кнопкой **Update Now**, которая будет располагаться на месте кнопки **Abort**, появляющейся в процессе обновления. Еще ниже есть кнопка **Setup**, которая позволяет настраивать различные параметры обновления антивируса. Остановимся на них подробнее (рис. 13.21).

Это окно позволяет создавать различные профили обновления (группа параметров **Profiles**), выбирать сервер, с которого будет осуществляться скачивание обновлений (группа параметров **Location**). При необходимости в этой же группе параметров можно вводить имя пользователя и пароль доступа к обновлениям.

- Группа параметров **Type of update** позволяет задавать компоненты, которые нужно обновлять. Посмотрите на рис. 13.22. Здесь изображено окно, которое появляется после нажатия кнопки **Change**.

Здесь можно настраивать набор компонентов, требующих обновления.

Антивирусы имеют два типа компонентов: базы вирусных сигнатур, которые нуждаются в частом обновлении, и программные компоненты, которые можно обновлять пореже. В идеале все требует регулярного обновления, но вирусные базы важнее, чем обновления программы (правда, важнее на достаточно коротком промежутке времени, скажем недели две-три). Программные компоненты антивируса тоже нуждаются в обновлениях, так как программы постоянно улучшаются и в них исправляются ошибки, порой весьма серьезные.

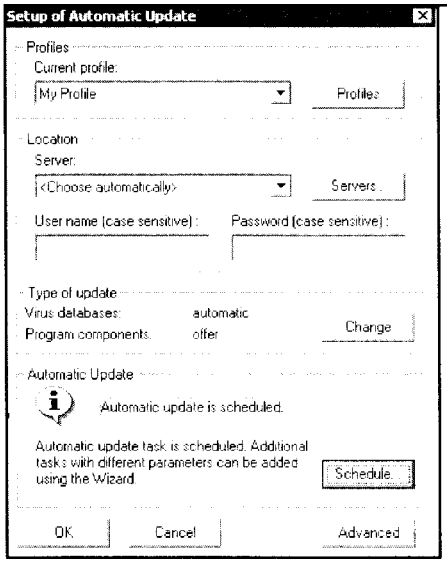


Рис. 13.21. Настройка автоматического обновления антивируса

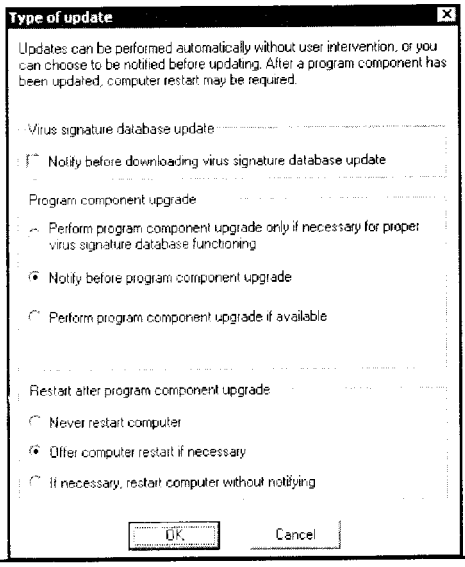


Рис. 13.22. Настройка параметров Type of update

- Группа параметров **Virus signature database update** позволяет включать режим вывода запроса о загрузке антивирусных баз. Если поставить галочку против параметра **Notify before downloading virus signature database update**, то перед загрузкой вирусных баз вы получите уведомление с вопросом о том, следует ли загружать эти базы. По умолчанию эта галочка сброшена, поэтому загрузка вирусных баз происходит без дополнительных вопросов.
- Группа параметров **Program component upgrade** позволяет настроить порядок обновления программных компонентов антивируса.
  - Параметр **Perform program component** позволяет запускать обновление программных компонентов только тогда, когда без этого обновления будет невозможно работать с вирусными базами. Это весьма экономная установка, так как подобное случается нечасто — невозможность работы с новой вирусной базой характерна для достаточно старой программной оболочки.
  - Параметр **Notify before program component upgrade** включает вывод сообщения о том, что программа хочет обновить свои компоненты, а параметр **Perform program component upgrade if available** позволяет программе обновлять компоненты автоматически.
- Группа **Restart after program component upgrade** позволяет настраивать порядок перезагрузки компьютера после обновления программных компонентов.

- **Never restart computer** — то есть никогда не перезагружать компьютер.
- **Offer computer restart if necessary** — предлагать перезагрузку, если нужно.
- **If necessary, restart computer without notifying** — если нужно, перезагружать компьютер без уведомления.

Вернемся к обсуждению настройки обновления (рис. 13.21). Последней группой параметров здесь является настройка расписания автоматического обновления — **Automatic update**. По умолчанию расписание настроено, но, если вы хотите его изменить, воспользуйтесь кнопкой **Shedule**.

В том же окне настройки обновления есть кнопка **Advanced**. Она открывает окно параметров, позволяющее настроить тип соединения с Интернетом.

Рассмотрим теперь настройки, касающиеся модулей антивируса, отвечающих непосредственно за безопасность вашей системы. Начнем с модуля AMON (рис. 13.23) — резидентного антивирусного монитора.

Этот модуль имеет такую же структуру, как и вышеописанный модуль обновления. Параметр **Resident module (AMON) enabled** показывает, включен монитор или нет, кнопка **Start** включает модуль, кнопка **Setup** служит для открытия окна установок. Информационная панель модуля доводит до нашего сведения статистическую информацию о действиях

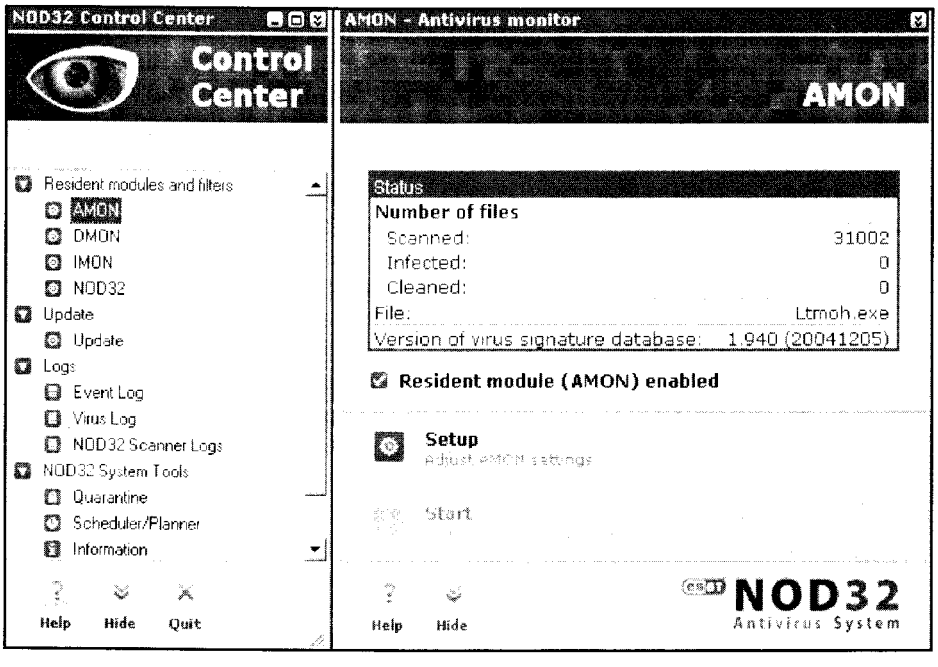


Рис. 13.23. Модуль настройки и управления резидентным монитором AMON

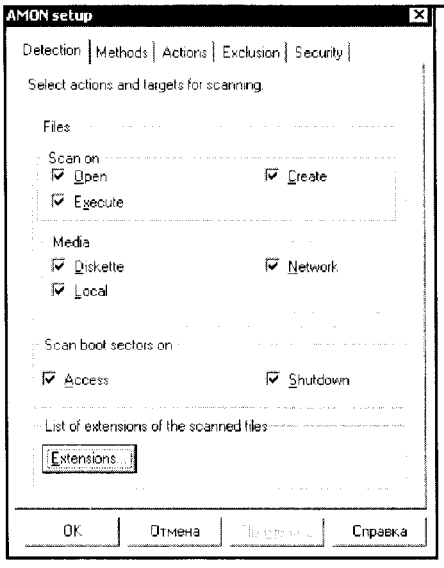


Рис. 13.24. Вкладка Detection окна настройки параметров AMON

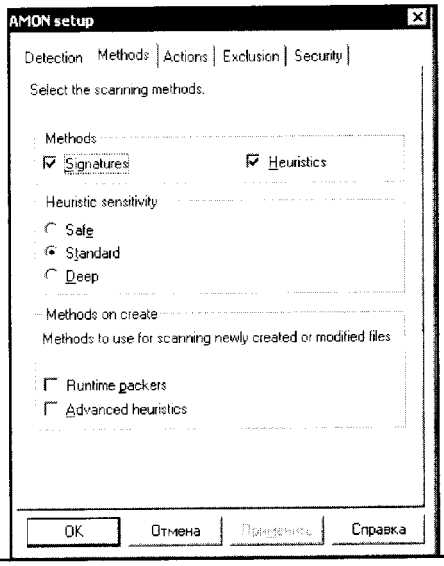


Рис. 13.25. Вкладка Methods окна настройки параметров AMON

AMON: строка **Scanned** сообщает о количестве просканированных файлов, строка **Infected** — о количестве инфицированных, а **Cleaned** — о количестве уничтоженных неизлечимых файлов.

Остановимся подробнее на настройке монитора, нажав кнопку **Setup** (рис. 13.24). Рассматривать все возможные варианты настройки мы не будем и остановимся подробно лишь на самых важных.

На вкладке **Detection** сосредоточены параметры, отвечающие за порядок сканирования файлов (группа **Files**) и загрузочных секторов (**Scan boot sectors on**). Файлы можно сканировать при открытии (**Open**), исполнении (**Execute**) и даже при создании (**Create**).

Для обеспечения максимального уровня безопасности все эти параметры должны быть включены (равно как и параметры подгруппы **Media**, отвечающие за сканирование носителей данных). Сканирование загрузочных секторов может проводиться либо при доступе к ним (**Access**), либо при выключении компьютера (**Shutdown**).

Вкладка **Methods** (рис. 13.25) отвечает за методы проведения анализа файлов.

В качестве методов обнаружения вирусов могут выступать сигнатурный (параметр **Signature** группы **Methods**) и эвристический (**Heuristics**) методы.

Эвристический метод можно настраивать, изменяя его чувствительность (**Safe, Standard, Deep**). Чем чувствительнее эвристический анализатор (наибольшую чувствительность определяет параметр **Deep**), тем

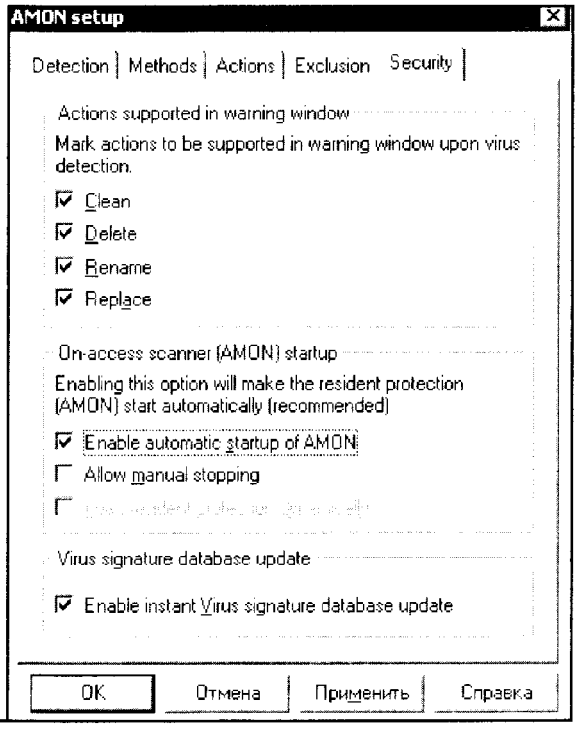


Рис. 13.26. Вкладка Security окна настройки параметров AMON

выше вероятность обнаружения неизвестного ранее вируса, но и тем больше ложных срабатываний может появиться, да и нагрузка на систему возрастет.

Особое внимание уделено методам проверки создаваемых файлов. Как ни странно, создаваемый файл — это потенциально опасный объект.

- Параметр **Runtime packers** настраивает антивирус на сканирование файлов, упакованных различными упаковщиками исполняемых файлов вроде AsPack, FSG, Petite, Neolite, ExeStealth, PECompact, Pklite, Lzexe, Diet, Exepack, CPAV и так далее.
- Параметр **Advanced heuristics** включает для таких файлов дополнительную проверку, которая нужна для выявления ранее неизвестных антивирусу вирусов, троянцев и червей.

Вкладка **Actions** позволяет определить действия антивируса при обнаружении объекта, зараженного неизвестным вирусом. Здесь нечего настраивать: по умолчанию антивирус заблокирует доступ к объекту и спросит вас о дальнейших действиях.

Вкладка **Exclusion** позволяет настраивать список исключений, то есть файлов и папок, которые не следует сканировать. Лучшее, что вы можете сделать, не включать вкладку **Exclusion** вовсе: ведь любые исключения снижают уровень безопасности.

Остановимся подробнее на вкладке **Security** (рис. 13.26). Она позволяет настраивать действия антивируса при обнаружении угрозы.

- Группа параметров **Actions supported in warning window** позволяет настроить перечень действий, которые вы сможете применить к зараженному объекту в тот момент, когда антивирус выдаст вам сообщение об этом. Вот эти действия: **Clean** — очистить (вылечить) файл, **Delete** — удалить файл, **Rename** — переименовать файл и **Replace** — переместить.
- Группа параметров **On-access scanner (AMON) startup** позволяет настроить параметры запуска и остановки AMON. Рекомендуется установить параметр **Enable automatic startup of AMON**, то есть включить автоматический старт резидентного монитора. Включив параметр **Allow manual stopping**, вы позволите останавливать сервис вручную. Параметр **Enable instant Virus signature database update** позволяет включить оперативное обновление базы вирусных сигнатур. Рекомендуется активировать этот параметр.

Перейдем к рассмотрению модуля DMON. Он предназначен для защиты от вирусов, которые могут распространяться через документы Microsoft Office и Microsoft Internet Explorer (рис. 13.27).

Структура главного окна DMON аналогична вышеописанным: параметр **MS Office document monitor (DMON) enabled** определяет, включен DMON или нет, а информационное окно отображает статистику, поэтому сразу перейдем к настройке модуля DMON (рис. 13.28).

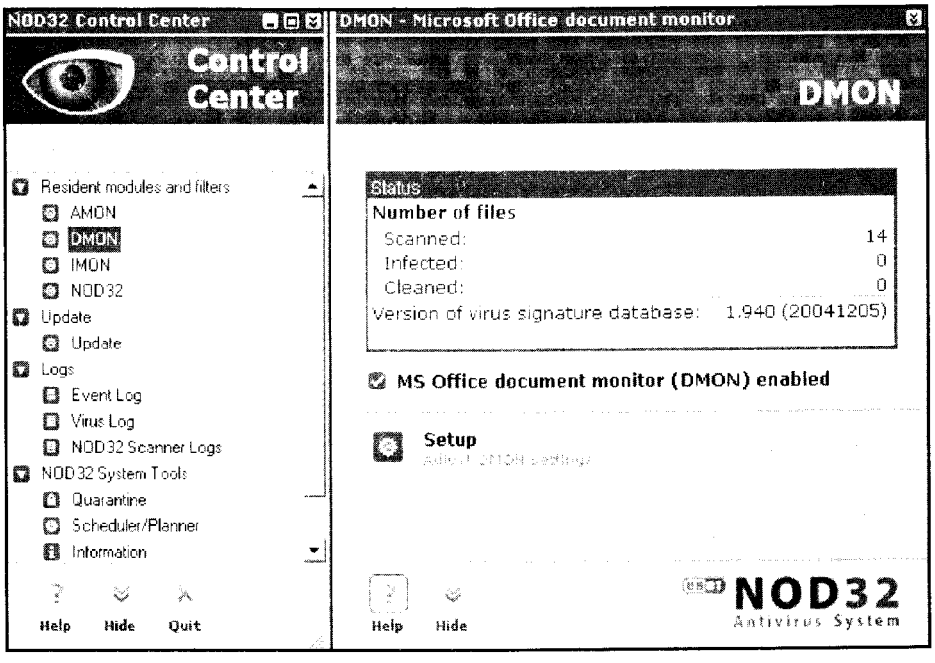


Рис. 13.27. Модуль настройки и управления сканером DMON

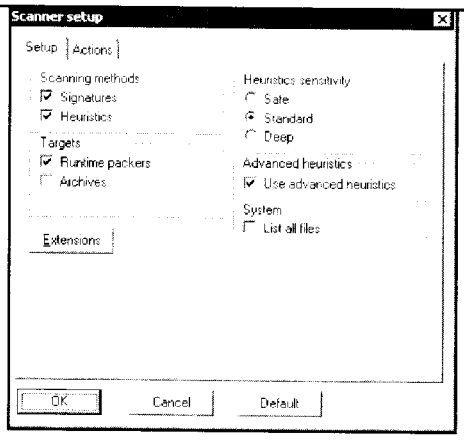


Рис. 13.28. Вкладка Setup окна настройки DMON Scanner setup

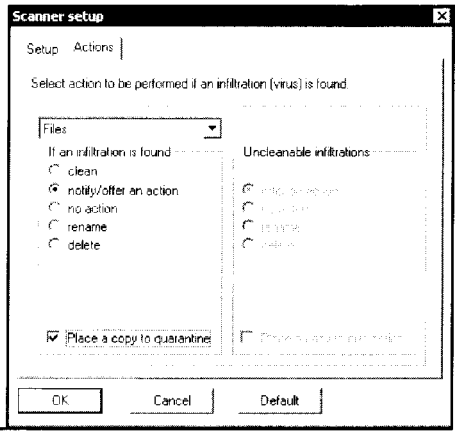


Рис. 13.29. Вкладка Action окна настройки DMON Scanner setup

Параметры этой вкладки отвечают за способы сканирования и сканируемые объекты.

- Группа параметров **Scanning methods** позволяет настраивать методы сканирования — сигнатурный (**Signature**) и эвристический (**Heuristic**).
- Группа параметров **Heuristic sensitivity** позволяет настраивать чувствительность эвристического анализатора (эти параметры описаны выше). Отмечу лишь, что, установив чувствительность на **Deep**, вы повысите уровень защиты, но при этом возрастает вероятность ложных срабатываний и повышается нагрузка на систему.
- Защищенность системы повышается и при установке параметра **Use advanced heuristics**. Группа параметров **Targets** определяет дополнительные цели для сканирования — архивы (**Archives**) и упаковщики времени выполнения (**Runtime packers**).

Вкладка **Action** отвечает за действия антивируса при обнаружении зараженного объекта (рис. 13.29).

- Группа параметров **If an infiltration is found** определяет действия антивируса при обнаружении зараженного файла: параметр **Clean** заставит антивирус вылечить файл, **Notify/offer an action** — оповестить пользователя и предложить выбрать действие самостоятельно, а опцию **No actions** выбирать не рекомендуется: антивирус ничего не будет делать при обнаружении инфицированного объекта. Параметр **Rename** позволит антивирусу переименовать файл с вирусом, сделав его безопасным, а **Delete** — удалить опасный файл. Здесь же желательно поставить галочку в поле **Place a copy to quarantine**: зараженные файлы будут помещены в специальную карантинную директорию.

- Немного выше группы параметров **If an infiltration is found** находится список выбора объектов, для которых настраиваются параметры. Это могут быть файлы (**Files**), самораспаковывающиеся архивы (**Self-extracting archives**) и упаковщики исполняемых файлов (**Run-time packers**).

Займемся теперь изучением параметров настройки модуля IMON, который отвечает за сканирование электронных писем и информации из Интернета (рис. 13.30).

Помимо обычных для NOD32 элементов управления, модуль настройки IMON содержит кнопку для остановки работы сервиса — **Quit**. В остальном все аналогично вышеописанным модулям. Остановимся подробнее на настройках IMON (рис. 13.31).

Вкладка POP3 (рис. 13.31) служит для настройки параметров проверки электронной почты.

- ❑ Группа параметров **Setup** содержит параметр **Enable E-mail checking**, который включает проверку почты, а в поле **Ports used by the POP3 protocol** можно вписать порты, которые использует ваш POP3-почтовый клиент. По умолчанию это порт 110.
- ❑ Группа параметров **Checked email adjustment** служит для настройки маркирования проверенных писем. При этом подгруппа **Append tag messages to email** определяет порядок добавления к письму сообщения о том, что это письмо просканировано антивирусом.

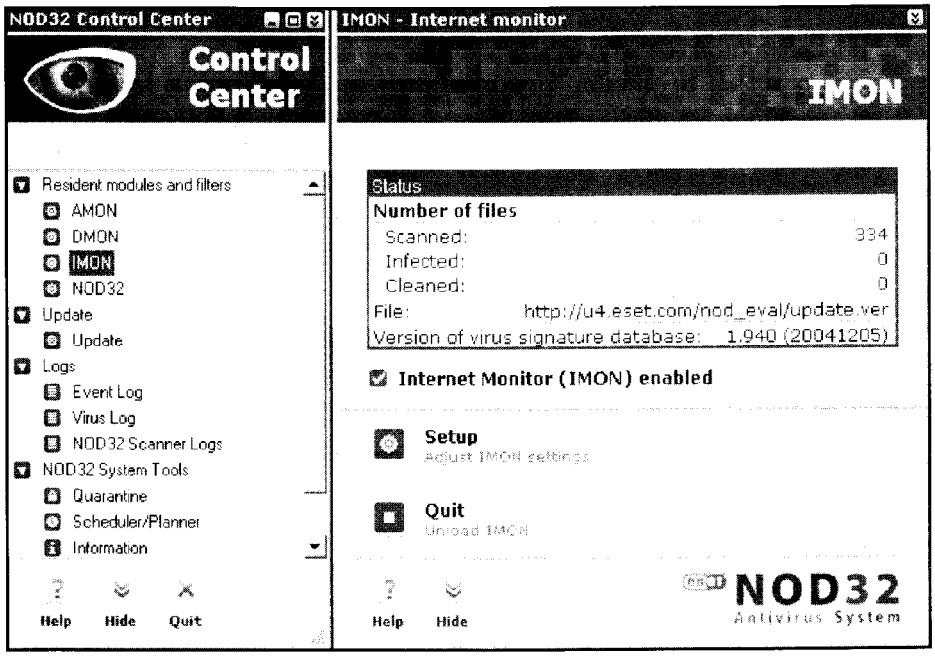


Рис. 13.30. Модуль настройки и управления сканера IMON

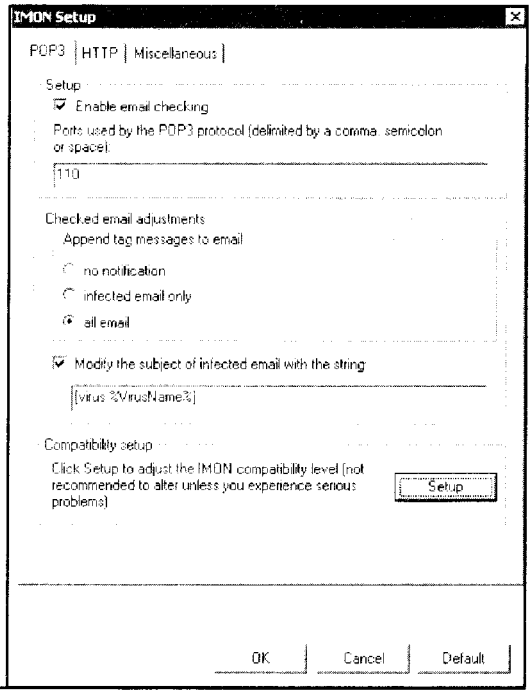


Рис. 13.31. Вкладка POP3 окна настройки IMON Setup

- Параметр **All email** заставляет антивирус добавлять это сообщение к каждому письму. Это быстро надоедает, и тогда можно переключиться на параметр **Infected email only** — тогда сообщение о том, что письмо просканировано, будет добавляться лишь к инфицированным письмам. Параметр **No notification** отключает уведомления, и его лучше не использовать.
- Параметр **Modify the subject of infected email with the string** позволяет антивирусу изменять тему письма на строку, содержащую слово «virus» и имя вируса, который был определен по базе программы.

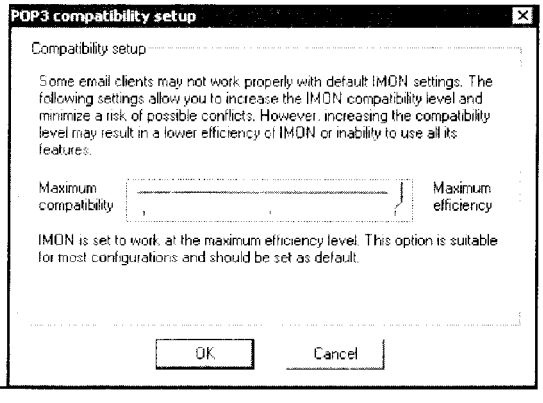


Рис. 13.32. Настройка параметров совместимости POP3 compatibility setup

Группа параметров **Compatibility setup** служит для настройки совместимости с почтовым клиентом (рис. 13.32).

Некоторые почтовые клиенты в случае, если антивирус занимается проверкой POP3-трафика в режиме **Maximum efficiency (Максимальная эффективность)**, работают некорректно. Если возникли проблемы с почтой, попробуйте увеличить уровень совместимости антивируса с почтовыми клиентами, переместив бегунок влево. При этом учтите: с повышением уровня совместимости снижается уровень защиты.

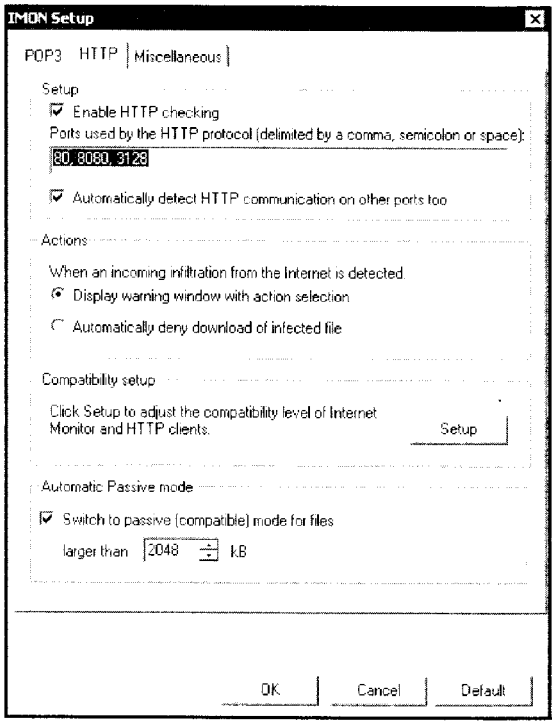


Рис. 13.33. Вкладка HTTP окна настройки IMON Setup

Рассмотрим теперь вкладку **HTTP** окна настройки IMON (рис. 13.33).

Эта вкладка служит для настройки параметров защиты от вирусов, которые могут проникнуть в ваш компьютер, воспользовавшись протоколом HTTP, то есть от всего, что загружает ваш веб-браузер в виде вебстраничек и файлов, которые вы скачиваете из Интернета.

- Группа параметров **Setup** служит для настройки сканирования.
  - Параметр **Enable HTTP checking** включает HTTP-сканер, параметр **Ports used by the HTTP protocol** позволяет задавать список портов, используемых протоколом HTTP.
  - Установка параметра **Automatically detect HTTP communication on other ports too** позволяет антивирусу самостоятельно определять другие порты, по которым осуществляется работа HTTP.

- Группа параметров **Actions** служит для определения действий антивируса в момент обнаружения зараженного файла.
  - Параметр **Display warning window with action selection** позволяет программе вывести сообщение об опасности и предоставить вам право самостоятельно решить, что делать дальше.
  - Параметр **Automatically deny download of infected file** запрещает загрузку зараженного файла.

Эта пара установок наглядно иллюстрирует возможность настройки разного уровня доверия пользователя к программе. Порой можно слышать что-то вроде «программа все делает сама, не спрашивая меня, иногда это не дает мне нормально работать». Понятно, что если эвристический анализатор вдруг принял полезную программу за зловредный код, при установленном параметре **Automatically deny download of infected file** вы тоже скажете именно так. Но, позволю себе заметить, что жалуются на своеволие программ в основном те, кто не умеет их настраивать. Ну а мы с вами к этой категории пользователей не относимся.

Переходим к следующей группе параметров — **Compatibility setup**. Она, подобно и аналогичной группе в настройке POP3, предназначена для определения уровня совместимости антивируса с веб-браузерами. Нажав кнопку **Setup**, попадаем в окно настройки совместимости (рис. 13.34).

В этом окне есть не только браузеры, но и другие программы, например менеджер закачек FlashGet. Для обеспечения максимального уровня защиты параметр напротив каждой из перечисленных в списке программ должен принимать значение **Higher efficiency**, а если вы хотите из-

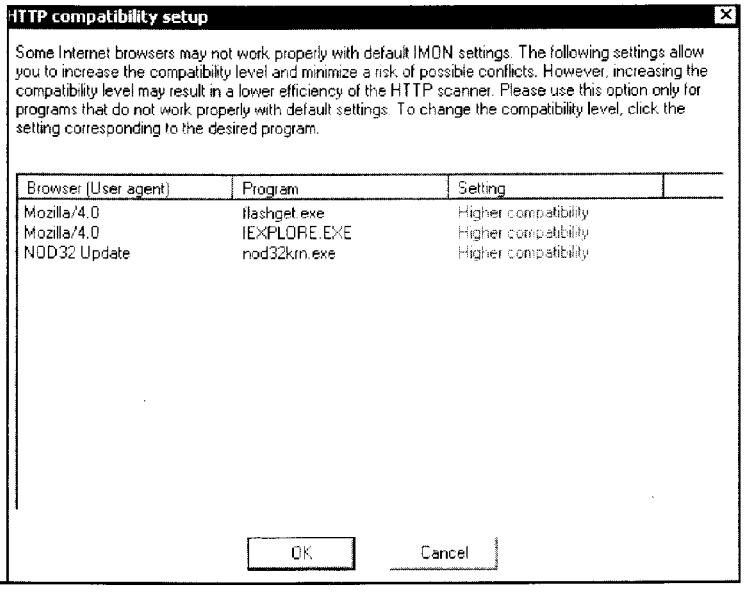


Рис. 13.34. Окно настройки совместимости с веб-браузерами

бежать проблем с совместимостью, несколько жертвуя эффективностью, достаточно параметра **Higher compatibility**. Режим совместимости можно включать автоматически при загрузке больших файлов, воспользовавшись установкой **Switch to passive (compatible) mode** группы параметров **Automatic Passive Mode**. Эта установка поможет избежать возможных проблем при загрузке больших файлов.

Перейдем к третьей вкладке окна настройки IMON, которая называется **Miscellaneous** (рис. 13.35).

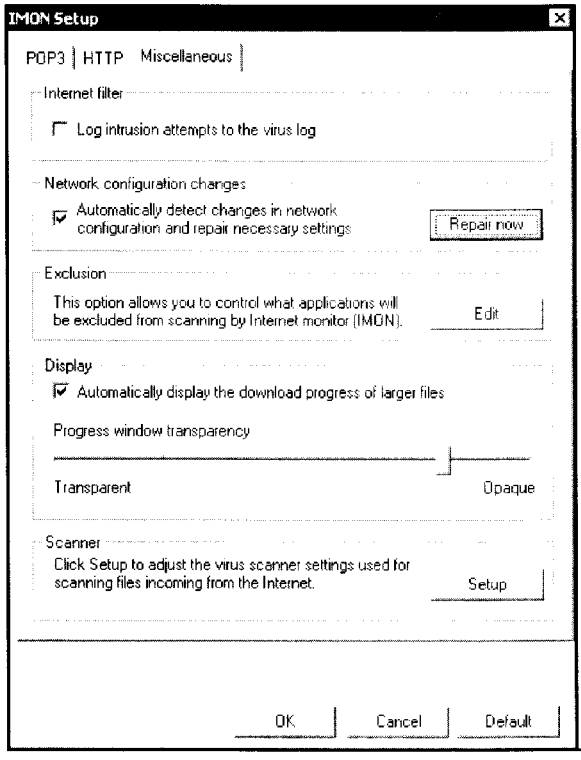


Рис. 13.35. Вкладка Miscellaneous окна настройки IMON Setup

- Параметр **Log intrusion attempts to the virus log** включает ведение протокола по зараженным объектам, перехваченным IMON.
- Параметр **Automatically detect changes in network configuration an repair necessary setting** позволяет антивирусу самостоятельно отслеживать вашу сетевую конфигурацию, внося при необходимости изменения в свои настройки.
- Параметр **Exclusion** позволяет задавать список объектов, исключаемых из проверки. Его лучше не трогать: исключения понижают уровень защищенности системы.

Группа параметров **Display** позволяет выводить окно, информирующее вас о процессе загрузки больших файлов (если включен параметр **Automatically display the download progress of larger files**). Бегунок

в этом окне настраивает его прозрачность: чем ближе он к **Transparent**, тем это окно прозрачнее.

Кнопка **Setup** в группе параметров **Scanner** открывает диалоговое окно настройки параметров сканера, которое практически полностью повторяет окна, детально описанные выше (см. комментарии к рис. 13.28 и 13.29).

Описав настройку IMON, переходим к управлению самим NOD32 (рис. 13.36).

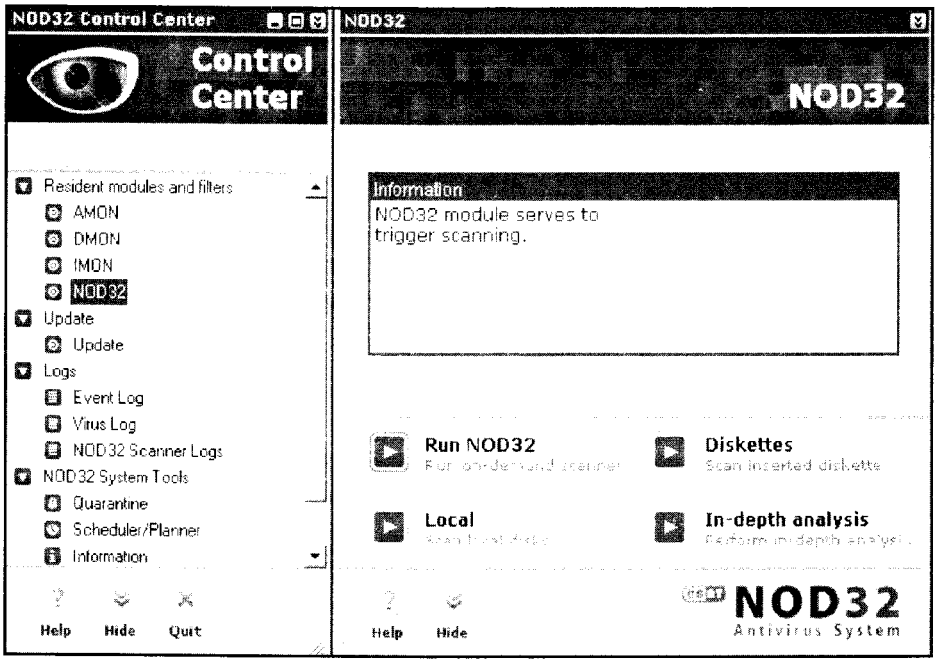


Рис. 13.36. Модуль настройки и управления NOD32

Этот модуль содержит четыре кнопки.

- Кнопка **Run NOD32** запускает окно настроек сканера NOD32, которое позволяет сканировать жесткие диски и папки компьютера, изменять параметры сканирования и так далее.
- Кнопка **Diskettes** включает сканирование дискет: фактически запускается то же окно NOD32 с предустановленным параметром сканирования диска A.
- Кнопка **Local** запускает сканирование локального жесткого диска.
- Кнопка **In-depth analysis** включает полное сканирование системы.

Остановимся подробнее на параметрах NOD32 (рис. 13.37).

При запуске окна NOD32 Antivirus program первым делом происходят сканирование системной памяти и проверка целостности NOD32.EXE — исполняемого файла антивируса. Здесь можно видеть результаты успешной проверки.

На вкладку **Scanning log** выводится информация о любых процессах сканирования системы. А вот запуск сканирования и определение списка сканируемых объектов осуществляются на вкладке **Scanning targets** (рис. 13.38).

На этой вкладке можно определить объекты, которые нужно просканировать. Здесь есть две группы параметров — Discs, позволяющая вы-

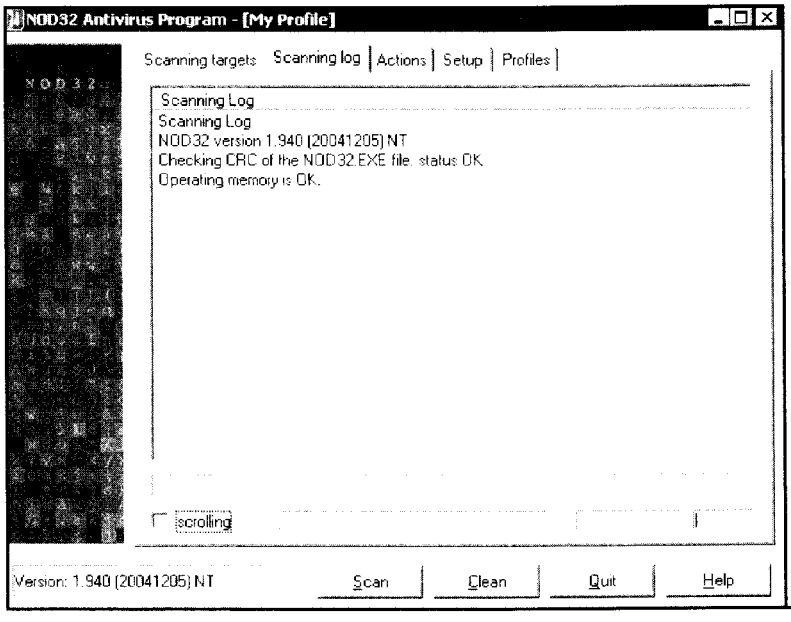


Рис. 13.37. Вкладка Scanning log окна NOD32 Antivirus Program

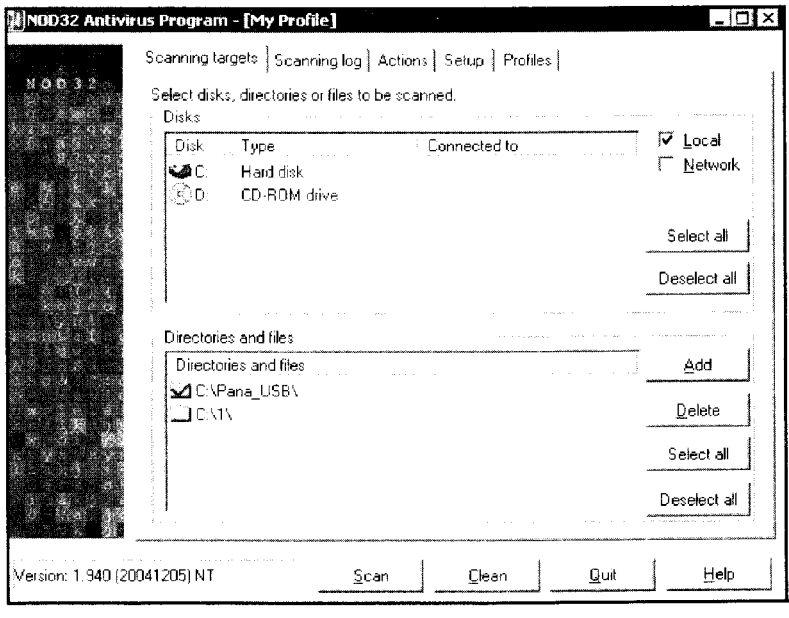


Рис. 13.38. Вкладка Scanning targets окна NOD32 Antivirus Program

бирать диски для сканирования, и **Directory and files**, которая позволяет выбирать отдельные файлы и папки.

- Кнопки **Select all** и **Deselect all** каждой группы позволяют отметить все объекты каждой группы как сканируемые (на них стоит галочка) или снять все галочки.
- Кнопка **Add** в группе **Directories and files** позволяет добавлять новые папки и файлы в список. Нажав ее, вы попадаете в диалоговое окно выбора файла или папки для сканирования. После добавления объект появляется в списке файлов.
- Кнопка **Delete**, в свою очередь, служит для удаления файлов или папок из списка. Чтобы выбрать отдельный объект в списках (или снять выбор), достаточно щелкнуть по нему дважды мышью.

После того как определены все нужные установки, можно кнопкой **Scan** в нижней части окна NOD32 Antivirus Program запустить процесс сканирования. Во время сканирования эта кнопка заменяется кнопкой **Stop**, нажав на которую, можно остановить сканирование. Кнопка **Clean** проводит сканирование с автоматическим лечением инфицированных объектов.

Рассмотрим теперь вкладку **Actions** (рис. 13.39).

Эта вкладка позволяет выбирать действия программы при обнаружении вируса в том или ином типе объекта. Мы обсуждали уже особенности действия подобных установок, поэтому здесь я ограничусь их краткой расшифровкой.

- Параметр **Clean** лечит файл.
- **Prompt for an action** задает пользователю вопрос о действии.
- **No action** — антивирус ничего не делает с найденным зараженным объектом.

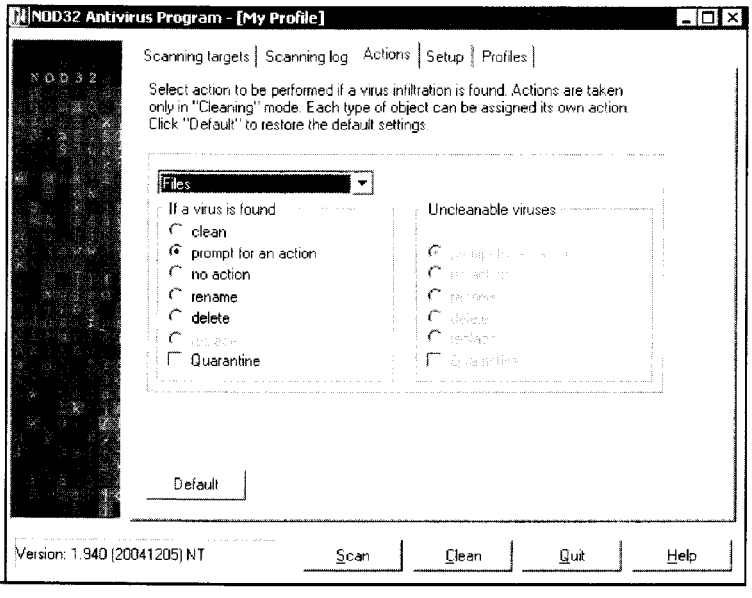


Рис. 13.39. Вкладка Actions окна NOD32 Antivirus Program

- **Rename** — переименовывает.
- **Delete** — удаляет.
- **Replace** — перемещает.

Галочка в поле **Quarantine** позволит антивирусу помещать все подозрительные объект в карантинную директорию.

Список объектов, которые следует сканировать антивирусу, задается при помощи одной из установок вкладки **Setup** (рис. 13.40).

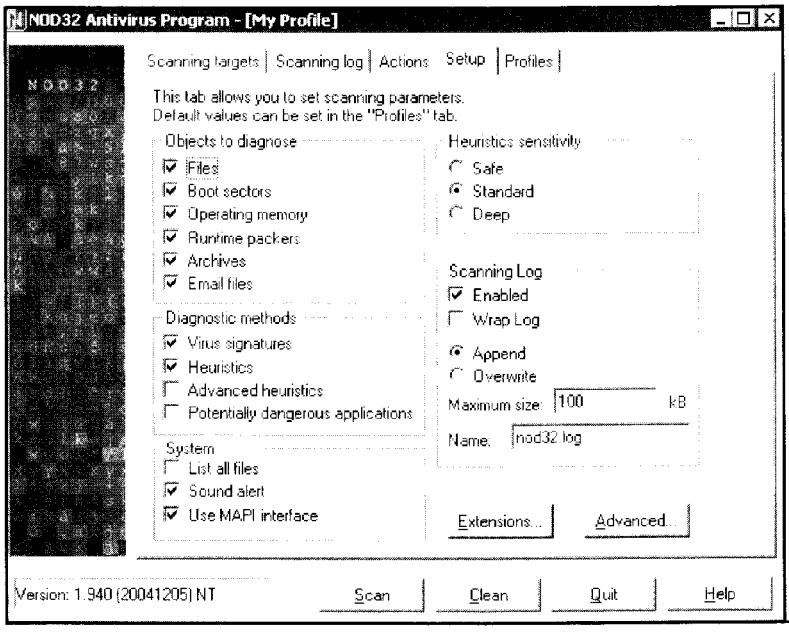


Рис. 13.40. Вкладка Setup окна NOD32 Antivirus Program

Эта вкладка содержит установки сканера, список объектов для сканирования (группа **Object to diagnose**), позволяет настраивать методы диагностики (**Diagnostic methods**, **Heuristic sensitivity**), настройки файла протокола (**Scanning log**) и опции группы **System**. Большинство аналогичных установок мы уже рассматривали выше, так что здесь остановимся лишь на тех, которым раньше не было уделено достаточно внимания.

- Среди параметров **System** есть **List all Files**, который позволяет включать в отчет о сканировании абсолютно все проверенные файлы. Эта опция сильно увеличивает размер лог-файла, но позволяет более детально провести анализ сканирования, в особенности если вы подозреваете какие-то файлы в том, что они заражены, а антивирус не подтверждает ваших подозрений.
- Среди параметров группы **Diagnostic methods** есть установка **Potentially dangerous applications**: благодаря ей антивирус будет реагировать на так называемые потенциально опасные приложения, например на программы-шутки, которые часто бывают не слишком смешными.

Вкладка **Profiles** окна NOD32 Antivirus Program позволяет создавать отдельные профили, хранящие установки программы. Использование нескольких профилей сканирования в домашних условиях встречается редко, да оно и почти ненужно. Поэтому мы сразу перейдем к описанию нескольких информационных модулей NOD32 (рис. 13.41).

Программа имеет несколько информационных модулей.

- На рис. 13.41 изображен модуль **Virus log** с протоколом обнаруженных вирусов.
- Модуль **Event log** содержит список событий.
- Модуль **NOD32 Scanner Logs** позволяет просматривать протоколы сканирования NOD32.
- Практически такую же роль играют модули **Quarantine**, где содержится список файлов, помещенных в карантин, и **Information**, выводящий информацию об антивирусе и системе, в которой он установлен.
- Модуль **Sheduler/Planner** позволяет создавать расписание запуска отдельных задач. Управление им аналогично управлению другими модулями (при помощи кнопки **Add** осуществляется добавление нового задания, при помощи кнопки **Delete** — удаление существующего).

А вот на модуле **NOD32 System Setup** (рис. 13.42) мы остановимся подробнее, так как он позволяет настраивать множество параметров антивируса, жизненно важных для его функционирования.

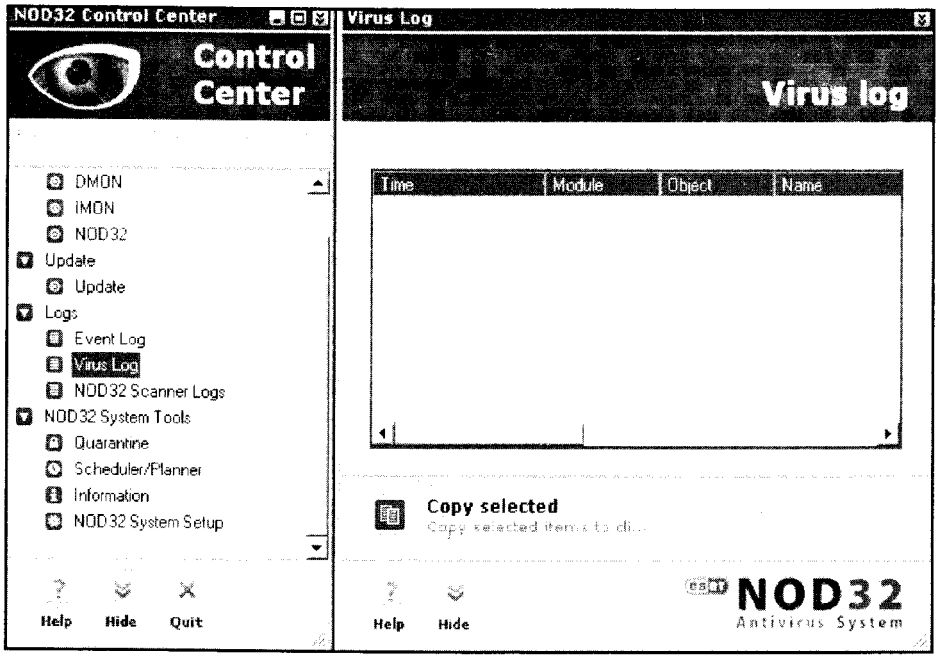


Рис. 13.41. Модуль Virus log NOD32

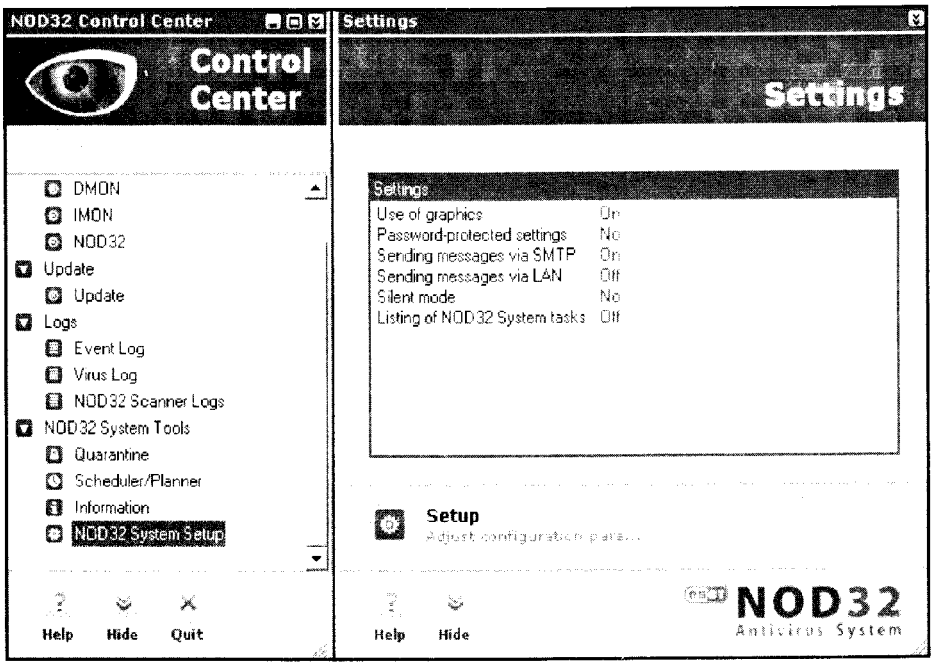


Рис. 13.42. Модуль Virus settings NOD32

Информационная панель этого модуля содержит данные о некоторых важных параметрах системы.

- Параметр **Use of graphics** сообщает о том, что включено использование графики в процессе работы антивируса. На медленных машинах этот параметр можно отключить, для того чтобы не создавать лишней нагрузки на систему.
- Параметр **Password protecting setting** сигнализирует о наличии или отсутствии пароля.
- **Sending messages via SMTP** и **Sending messages via LAN** сообщают о включении отправки уведомлений об обнаружении вирусов через локальную сеть или по e-mail.
- Параметр **Silent mode** говорит о том, что антивирус работает в автоматическом режиме, не тревожа пользователя лишними сообщениями.
- Параметр **Listing of NOD32 System tasks** говорит о том, что антивирус будет показывать сообщения о выполнении системных задач, которые проводятся модулями NOD32.

Кнопка **Setup** скрывает много интересных установок (рис. 13.43). Здесь мы рассмотрим лишь наиболее полезные из них.

Вкладка **General** окна настройки общесистемных параметров антивируса содержит следующие установки.

- ❑ Параметры группы **Graphics**, предназначенные для отключения излишнего графического оформления программы.

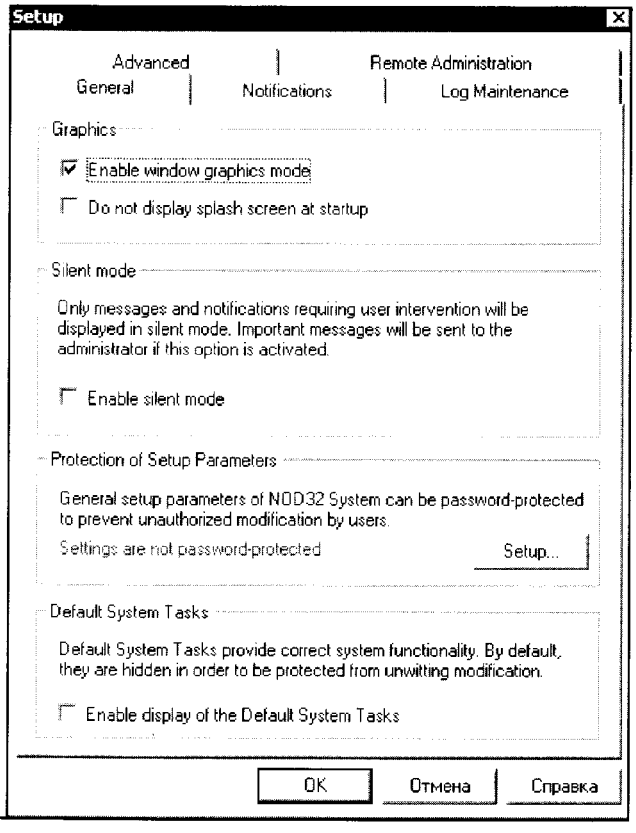


Рис. 13.43. Вкладка Generals окна настройки Setup

- Параметр **Enable window graphics mode** модифицирует окна NOD32, добавляя графическое оформление, характерное лишь для этой программы. Соответственно вырастает и нагрузка на систему. Если отключить этот параметр, то окна антивируса будут выглядеть как стандартные окна Windows-программ.
- Параметр **Do not display splash screen at startup** позволяет настраивать отображение заставки при запуске антивируса. Если параметр установлен, то заставка отображаться не будет.

❑ Группа параметров **Silent mode** интересна для системных администраторов: включение параметра **Enable silent mode** позволяет перенаправлять все сообщения, не требующие реакции пользователя, системному администратору.

❑ Параметр **Protection of Setup Parameters** и, в частности, кнопка **Setup** позволяют задавать пароль для защиты установок антивируса от неавторизованного вмешательства. Как и вышеописанный **Silent mode**, это актуально для системных администраторов.

❑ Параметр **Enable display of the default system task** нам с вами практически не нужен: он включает отображение системных задач, которые нужны для корректного функционирования антивируса.

Из других вкладок окна **Setup**, которые могут быть интересны нам с вами (остальное предназначено исключительно для системных администраторов, управляющих компьютерными сетями), отметим весьма условно полезную вкладку **Notifications** (рис. 13.44).

Она позволяет настраивать сообщения, генерируемые антивирусом и отправляемые по электронной почте или по локальной сети на компьютер администратора. Для настройки отправки сообщений по электронной почте необходимо заполнить поля группы параметров SMTP в соответствии с их обозначениями.

В поле **Server** надо внести адрес вашего SMTP-сервера, в поле **Sender address** нужно внести адрес отправителя, в поля **Send virus warnings to:** и **Send other warnings to:** — адреса, на которые вы хотите рассылать сообщения. В тех случаях, когда SMTP-сервер требует авторизации (это встречается все чаще — всему причиной спам), вам придется заполнить поля **User name** и **Password**.

Теперь вы сможете пользоваться возможностями антивируса NOD32. А ниже мы рассмотрим еще один антивирус, главным, но не единственным достоинством которого является его бесплатность.

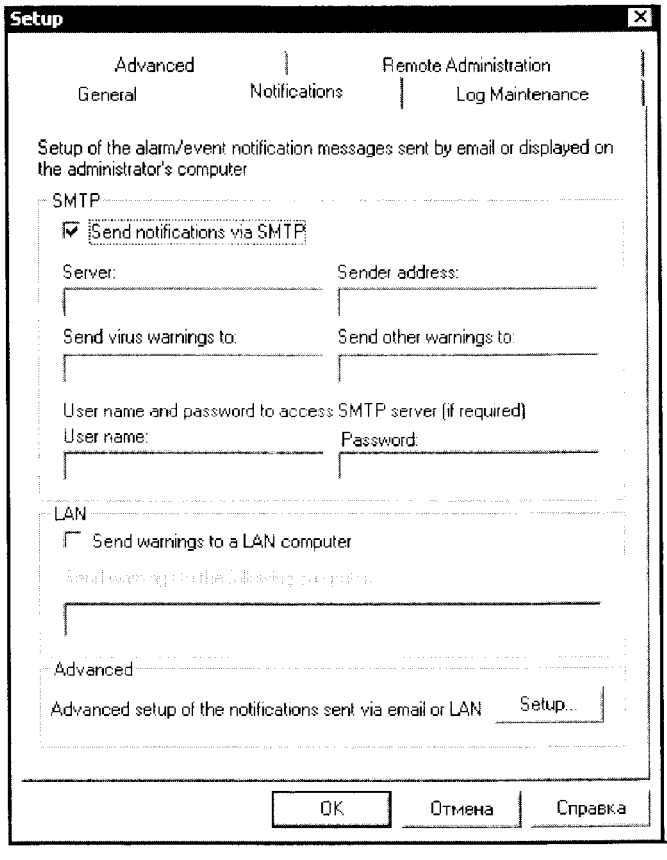


Рис. 13.44. Вкладка Notifications окна настройки Setup

13.3. ANTIVIR PERSONAL EDITION

Это бесплатный антивирус фирмы H+BEDV Datentechnik GmbH. Скачать его можно на сайте *http://www.free-av.com/*. Дистрибутив занимает около 6 Мб. Процесс установки стандартен и даже не требует перезагрузки после установки продукта.

Сразу после установки антивирус начинает сканирование системы и предлагает провести обновление антивирусных баз. После старта антивируса в системной панели Windows появляется иконка, похожая на раскрытый зонтик, который сигнализирует о том, что антивирус работает, защищая вашу систему. Если иконка выглядит как в закрытый зонтик, значит, антивирус неактивен.

Начнем с описания процесса обновления антивируса. Если антивирусные базы старше четырнадцати дней, программа предложит вам запустить процесс обновления (рис. 13.45).

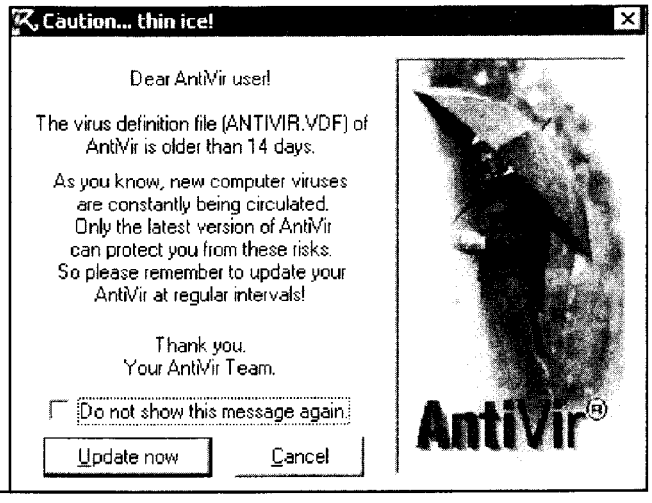


Рис. 13.45. Предупреждение о том, что антивирусные базы устарели

Самое правильное, что вы сможете сделать при появлении этого сообщения, — нажать кнопку **Update now**. Не устанавливайте галочку в поле **Do not show this message again:** этим вы отключите напоминания об устаревании вирусных баз и рискуете серьезно снизить защищенность вашего компьютера.

После нажатия на **Update now** вы увидите окно обновления антивируса (рис. 13.46).

Чтобы начать обновление, достаточно нажать кнопку **Start** в этом окне. Пакет обновлений состоит из четырех элементов — программного модуля (**Program**), сканера (**Scan engine**), собственно вирусной базы (**VDF file**) и динамически связываемой библиотеки (**AVRep.dll**).

Чаще всего обновляется вирусная база, и если вы обновляетесь регулярно, то загружать вам придется сравнительно небольшие объемы ин-

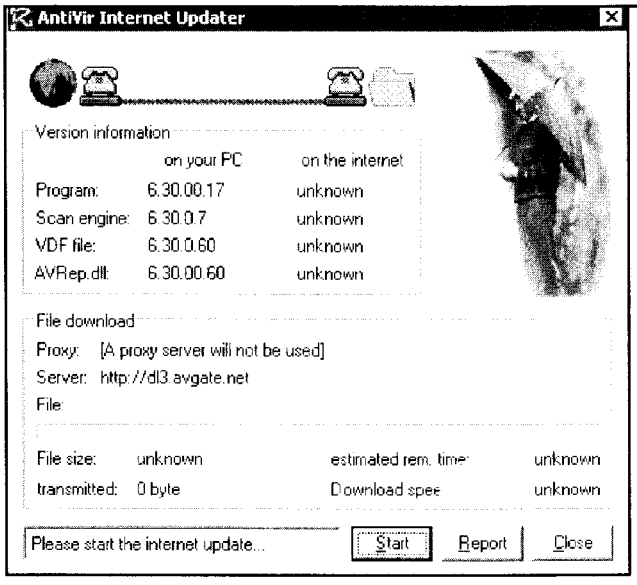


Рис. 13.46. Окно обновления антивируса

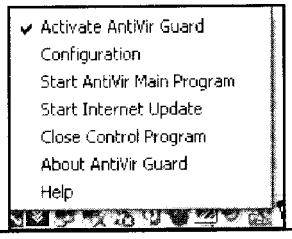


Рис. 13.47. Управление антивирусом при помощи меню

формации — от полутора до трех мегабайт. После проведения загрузки обновлений антивирус автоматически проведет обновление, задав вам еще несколько вопросов.

Обновить антивирус можно не только утвердительным ответом на предложение об обновлении. Запустить обновление можно, воспользовавшись меню, которое появляется после щелчка правой кнопкой мыши по значку антивируса в системной панели (рис. 13.47).

Галочка напротив параметра **Activate AntiVir Guard** означает, что резидентный сканер активен. Если ее снять, он перестанет защищать вашу систему.

Если щелкнуть мышкой по строчке **Configuration**, вы попадете в окно настройки параметров антивируса. Здесь строчка меню **Start AntiVir Main Program** запускает окно **AntiVir**, из которого можно провести некоторые действия с вашей системой, например просканировать жесткие диски на предмет наличия зараженных файлов.

По команде **Close Control Program** антивирус завершает свою работу, две нижние строчки меню предоставляют вам доступ к информации об антивирусе и его справочной системе.

Если сделать двойной щелчок мышью по значку антивируса, то появится окно **Control Program** (рис. 13.48), содержащее статистическую информацию о файлах, проверенных программой, и имеющее небольшую систему меню, которая дублирует меню, описанное выше.

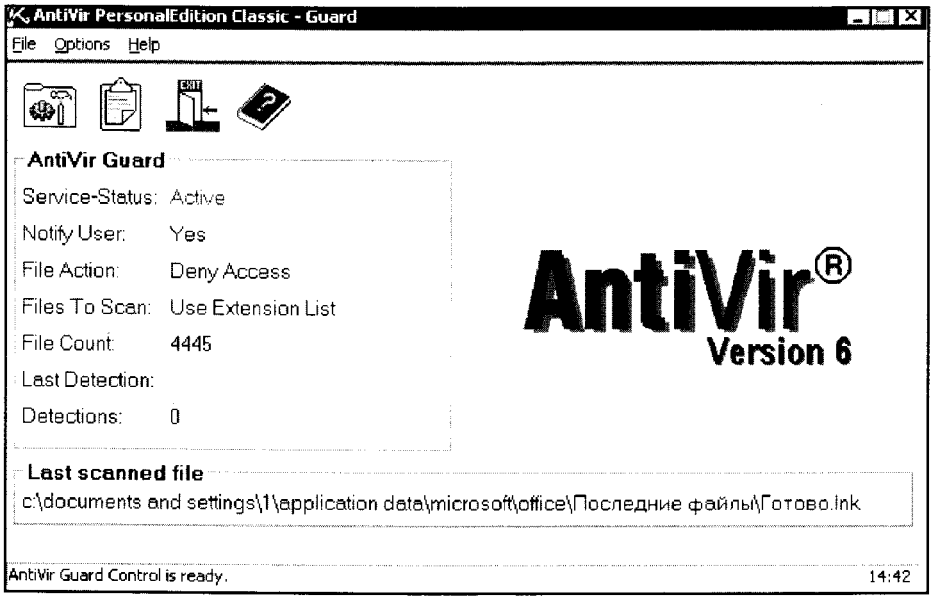


Рис. 13.48. Окно Control Program

Здесь можно посмотреть файл протокола, воспользовавшись соответствующей кнопкой панели инструментов этого окна или меню **Options ▸ Show logfile**. В самом окне **Control program** можно понаблюдать за процессом проверки файлов и посмотреть статистику проверки.

Теперь предлагаю вам подробнее ознакомиться с настройками резидентного монитора AntiVir Guard. Для начала рассмотрим настройки, собранные на вкладке **Scanner** (рис. 13.49).

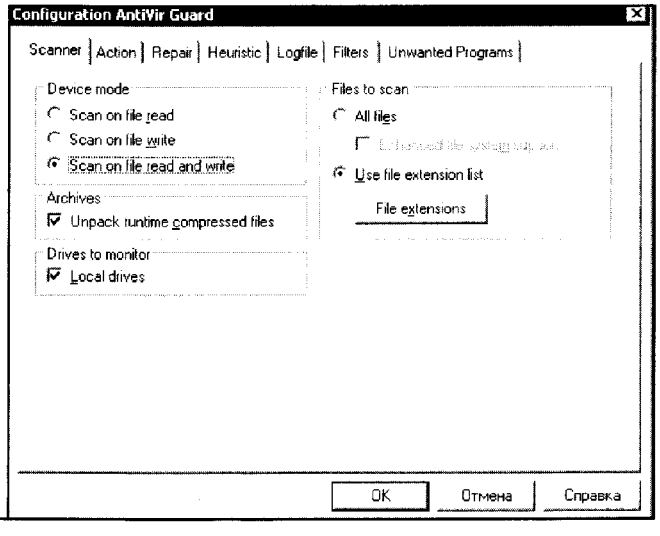


Рис. 13.49. Вкладка Scanner окна Configuration AntiVir Guard

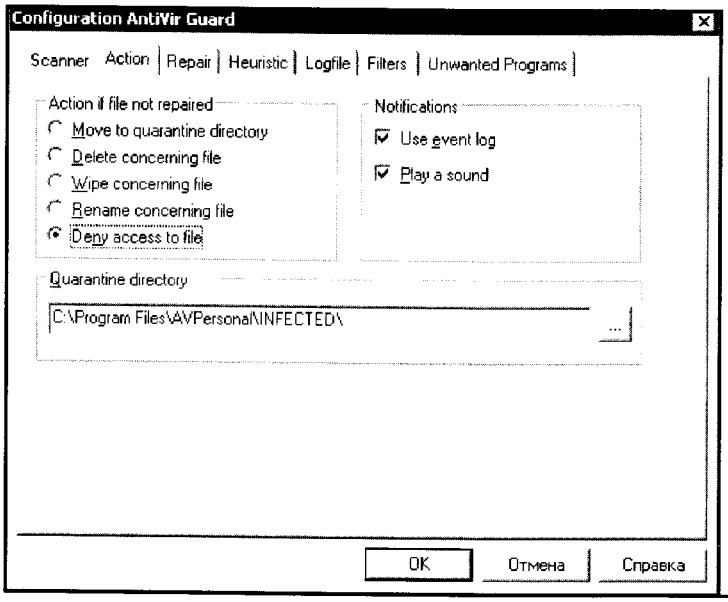


Рис. 13.50. Вкладка Action окна Configuration AntiVir Guard

Группа параметров **Device mode** определяет порядок сканирования файлов.

- Параметр **Scan on file read** включает сканирование файлов при чтении.
- Параметр **Scan on file write** включает сканирование файлов при записи.
- Параметр **Scan on file read and write** — сканирование файлов и при чтении и при записи.

Группа параметров **Files to scan** определяет, какие файлы будет сканировать антивирус. Если установлен параметр **All files**, он будет проверять все файлы, а если параметр **Use file extension list**, то проверку будут проходить только файлы, расширения которых совпадают с расширениями, заданными в списке расширений.

Просматривать и редактировать список расширений можно, нажав кнопку **File extensions**. Параметр **Unpack runtime compressed files** отвечает за сканирование файлов, сжатых при помощи упаковщиков времени выполнения, а группа параметров **Drives to monitor**, в которой доступен всего один параметр **Local drives**, отвечает за мониторинг событий, происходящих на локальных жестких дисках.

Перейдем к рассмотрению вкладки **Action** (рис. 13.50).

Эта вкладка определяет действия монитора при обнаружении вирусов.

- Группа параметров **Notifications** позволяет задавать тип оповещения при обнаружении вируса. Здесь параметр **Use event log** отвечает за занесение события в файл журнала, а параметр **Play a sound** — за проигрывание звукового оповещения.
- Группа параметров **Action if file not repaired** содержит установки, диктующие антивирусу действия с неизлечимо зараженным файлом.

- Параметр **Move to quarantine directory** позволяет антивирусу переместить неизлечимый файл в карантинную директорию (она задается параметром **Quarantine directory** на той же страничке).
- Параметр **Delete concerning file** удаляет файл. **Wipe concerning file** удаляет его содержимое; **Rename concerning file** переименовывает его, а **Deny access to file** запрещает доступ к нему.

Не рекомендуется устанавливать эти опции на значения Delete и Wipe — так вы рискуете потерять файл безвозвратно. Установка иного параметра сохраняет вероятность лечения неизлечимого файла с использованием другого антивируса.

Вкладка **Repair** отвечает за процесс лечения (рис. 13.51).

- Если вы не хотите, чтобы антивирус лечил зараженные файлы самостоятельно, активируйте параметр **Activate repair**.
- Чтобы программа делала резервные копии излечиваемых файлов, активируйте установку **Create backup before repair.** Эта установка особенно важна, так как не всегда лечение файла означает его последующую работоспособность.

Вкладка **Heuristics** отвечает за опции эвристического анализатора (рис. 13.52).

Об эвристических анализаторах мы говорили немало. Они способны выявлять новые, еще не известные антивирусу вредоносные программы. Если активирован параметр **Enable macro heuristic**, то антивирус будет исследовать файлы Microsoft Office на предмет наличия неизвестных ему макровирусов, а активация параметра **Win32 file heuristic** включает эвристический анализ обычных программ.

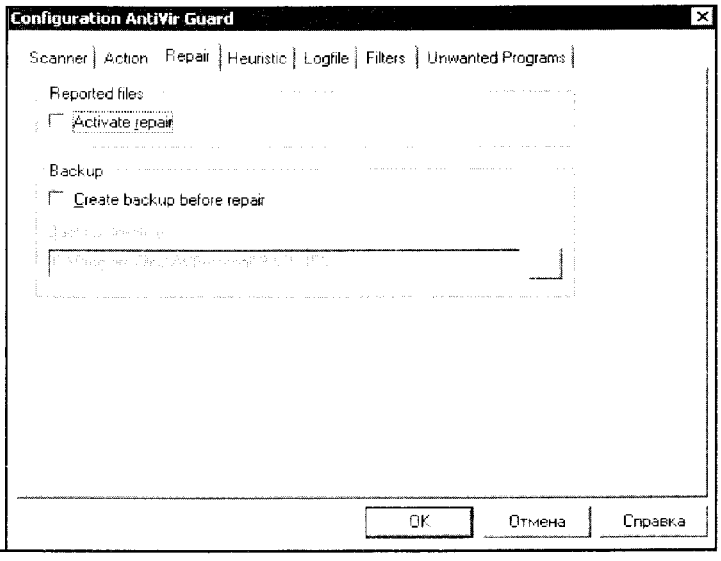


Рис. 13.51. Вкладка Repair окна Configuration AntiVir Guard

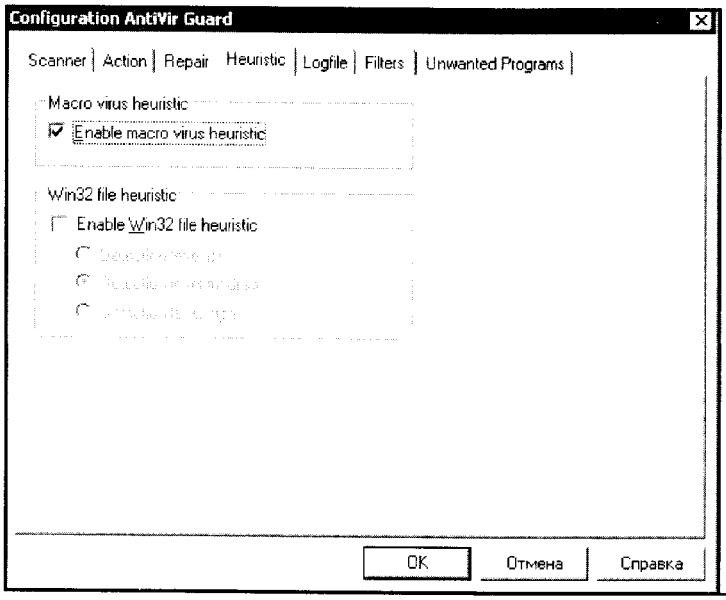


Рис. 13.52. Вкладка Heuristic окна Configuration AntiVir Guard

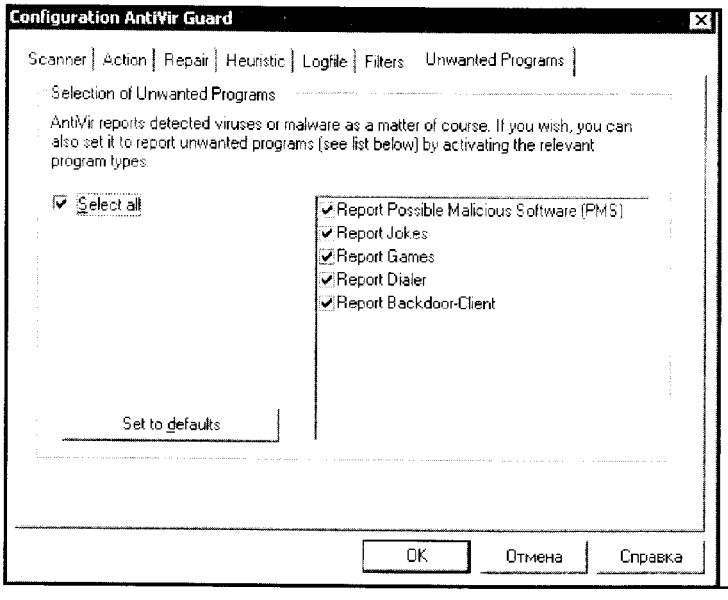


Рис. 13.53. Вкладка Unwanted Programs окна Configuration AntiVir Guard

Установив этот параметр, вы можете выбирать уровни чувствительности анализатора. Это может быть низкий, средний и высокий уровень, которым соответствуют параметры **Detection level low, Detection level medium** и **Detection level high**. Установив высокий уровень чувствительности анализатора, вы повысите защищенность системы, но и нагрузку на нее тоже.

Вкладки **Logfiles** и **Filters** не слишком интересны в повседневной деятельности. Первая позволяет задавать параметры лог-файла, которые

и так по умолчанию соответствуют запросам пользователей, а вкладка **Filters** позволяет задавать процессы, которые следует исключать из сканирования. Этой вкладкой лучше не пользоваться: ведь, как мы знаем, любые исключения снижают уровень защиты системы. А вот на вкладке нежелательных программ **Unwanted programs** (рис. 13.53), которая посвящена обнаружению различных шпионских и просто не вами установленных программок, остановимся подробнее.

Эти программы антивирус делит на несколько групп. Наиболее размытой категорией являются **PMS** или **Possible Malicious Software** — программы, которые могут оказаться опасными. Далее идут **Jokes**, то есть программы-шутки. Еще есть **Games** — игры, **Dialer** — программы, которые могут без вашего ведома набирать телефонные номера, и **Backdoor-Client** — бэкдор-клиенты, которые используются для удаленного управления компьютером.

Когда мы разобрались с резидентным модулем программы, посмотрим на ее главное окно (рис. 13.54). При его запуске антивирус проводит проверку оперативной памяти, загрузочных секторов жестких дисков, системных файлов и самопроверку.

Чтобы начать сканирование, достаточно выделить нужные объекты в окне **Folders** и нажать кнопку с изображением увеличительного стекла

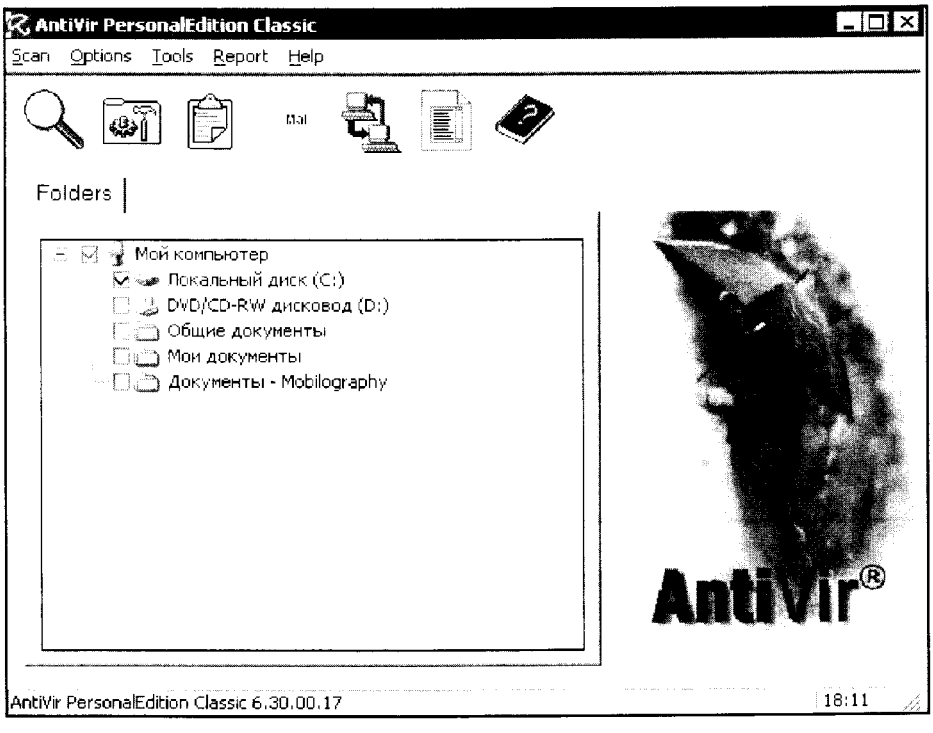


Рис. 13.54. Окно AntiVir PersonalEdition Classic

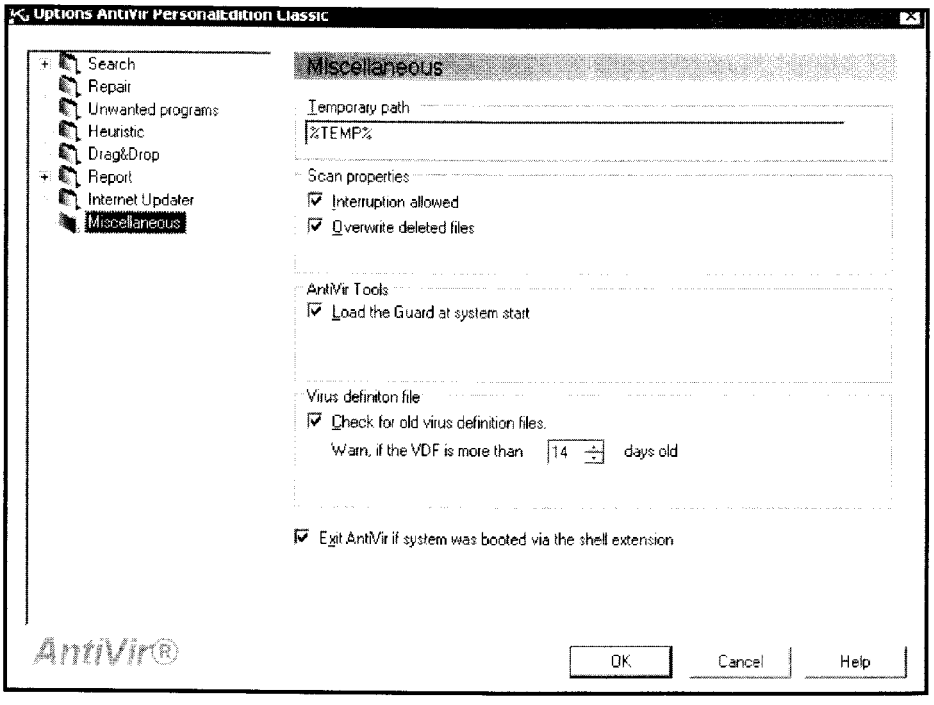


Рис. 13.55. Вкладка Miscellaneous окна Options модуля AntiVir PersonalEdition Classic

в левой части панели управления программы. В процессе сканирования будет отображаться окно, содержащее информацию о ходе проверки. Это окно содержит лишь одну кнопку **Stop**, которая предназначена для остановки процесса сканирования.

Воспользовавшись меню или панелью инструментов этого окна, можно провести обновление антивируса, посмотреть лог-файл, настроить его параметры. Настройки антивируса собраны в окне параметров, которое можно вызвать командой **Options ▸ Configuration**. Параметры настройки во многом совпадают с установками описанного выше резидентного сканера, и здесь мы остановимся лишь на существенных различиях.

Главные различия в настройке центральной программы и AntiVir Guard заключаются во вкладке **Miscellaneous** окна **Options** (рис. 13.55).

Среди параметров этой вкладки особенно интересны два. Во-первых, это параметр **Load the Guard at system start** — загружать резидентный монитор Guard при старте системы. Сняв галочку возле этого параметра, вы отключите загрузку резидентного модуля программы при старте Windows. Группа параметров **Virus definition file** позволяет задавать периодичность напоминания о необходимости обновить антивирус. По умолчанию это 14 дней, по желанию вы можете изменить этот параметр, лучше — в сторону уменьшения.

Поздравляю! Теперь вы умеете эффективно использовать этот бесплатный, но весьма полезный антивирус.

13.4. КОМПЛЕКСНАЯ ЗАЩИТА

Теперь, когда мы обсудили несколько антивирусов и файрволлов, попробуем подумать над комплексной системой защиты с их использованием.

Файрволл и антивирус — это программы, от которых зависит очень многое. Файрволл или антивирус должны быть удобны. Поэтому, чтобы остановиться на одной из этих программ, лучше перепробовать несколько. Иногда, правда, бывает так, что вы, увидев ту или иную программу и попользовавшись ею пару часов, понимаете, что это ваше.

Сам я прошел через несколько стадий приверженности к тем или иным программам. Несколько лет назад в моем личном рейтинге лидировали AntiVir в качестве антивируса и ZoneAlarm как файрволл. Немного позже пальму первенства среди антивирусов занял Norton Antivirus, а любимым файрволлом оставался ZoneAlarm. Но, когда я познакомился с NOD32 и Outpost Firewall Pro, я понял, что эти два продукта нравятся куда мне больше их предшественников, — тоже, впрочем, достойных уважения. Думаю, каждый из вас сможет составить для себя подобный «список предпочтений», после того как достаточно подробно ознакомится с различными антивирусами и файрволлами. Список программ для защиты далеко не ограничивается несколькими описанными выше, но если вы подробно познакомитесь хотя бы с несколькими продуктами, то оценить другие сможете самостоятельно.

Для полноценной защиты вам нужны как минимум антивирус и файрволл. Сегодня существуют удобные интегрированные решения, где файрволл объединен с антивирусом. Лично я полагаю, что предпочтительнее использование антивируса и файрволла в качестве отдельных продуктов. Скорее всего, в недалеком будущем, мы увидим отличные программы, совмещающие в себе все защитные функции. Мне, например, очень хотелось бы увидеть результат объединения антивируса NOD32 и файрволла Outpost Firewall Pro.

Не забывайте о регулярном обновлении ваших антивируса и файрволла: новые вредоносные программы рождаются каждый день, и антивирус двухнедельной давности может быть абсолютно бесполезным против «свеженьких» вирусов. Даже эвристический анализатор, несмотря на свои потенциально серьезные возможности, тут может и не помочь.

Но защита компьютера и вашей информации не ограничивается лишь антивирусом и файрволлом. Так, важное значение имеет обновление системы.

13.5. ОБНОВЛЕНИЕ СИСТЕМЫ

«Уж сколько раз твердили миру...», а мир все так же неохотно обновляет операционные системы и устанавливает патчи. По мысли некоторых пользователей, их операционная система и так достаточно хорошо защищена. Это не так. Довольно часто «исследователи» находят дыры в продуктах Microsoft, а Microsoft эти дыры оперативно (или не очень

оперативно) заделывает, выпуская обновления. Если вы не обновляете систему с достаточной регулярностью, вы ставите ее (и свои данные) под угрозу. Файрволлы и антивирусы — это очень важно, но зачем снижать уровень защиты вашей системы, лишая ей обновлений? Поэтому сейчас мы поговорим об обновлении Windows XP.

Windows XP имеет удобный механизм автоматического обновления. Но в любой автоматике есть положительные и отрицательные стороны. С одной стороны, включив автоматическое обновление, воспользовавшись вкладкой **Автоматическое обновление** окна свойств компьютера (рис. 13.56), вы можете работать спокойно, зная, что ваша система сама обновляется с заданной периодичностью.

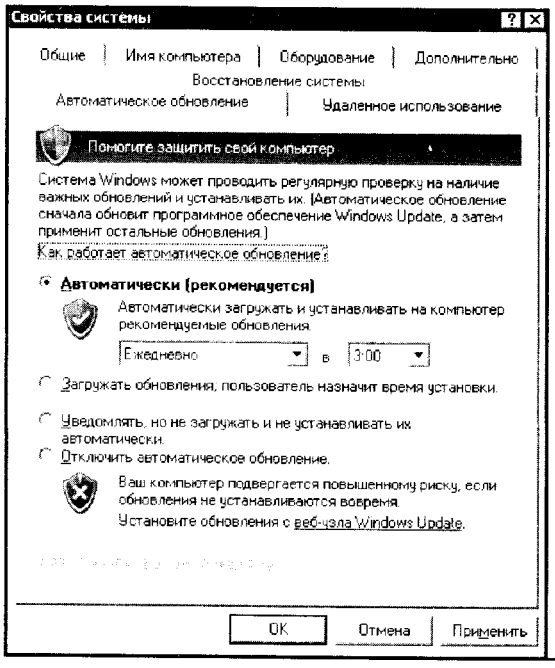


Рис. 13.56. Свойства обновления системы

С другой стороны, многие пользователи хотели бы контролировать процесс обновления вручную. Что, например, делать, если система «решила» обновляться в самый неподходящий для вас момент? Например, вы скачиваете из Интернета какой-нибудь важный файл и не хотите делить пропускную способность канала с нужным, но не настолько для вас срочным обновлением. Для таких случаев полезен пункт того же окна, изображенного на рис. 13.56, который называется **Уведомлять, но не загружать и не устанавливать их автоматически**. Вы будете получать уведомления о том, что появилась возможность загрузки нового обновления, и самостоятельно запускать эту загрузку.

Настоятельно не рекомендуется отключать возможности автоматического обновления. Вы можете просто забыть об обновлениях и снизите

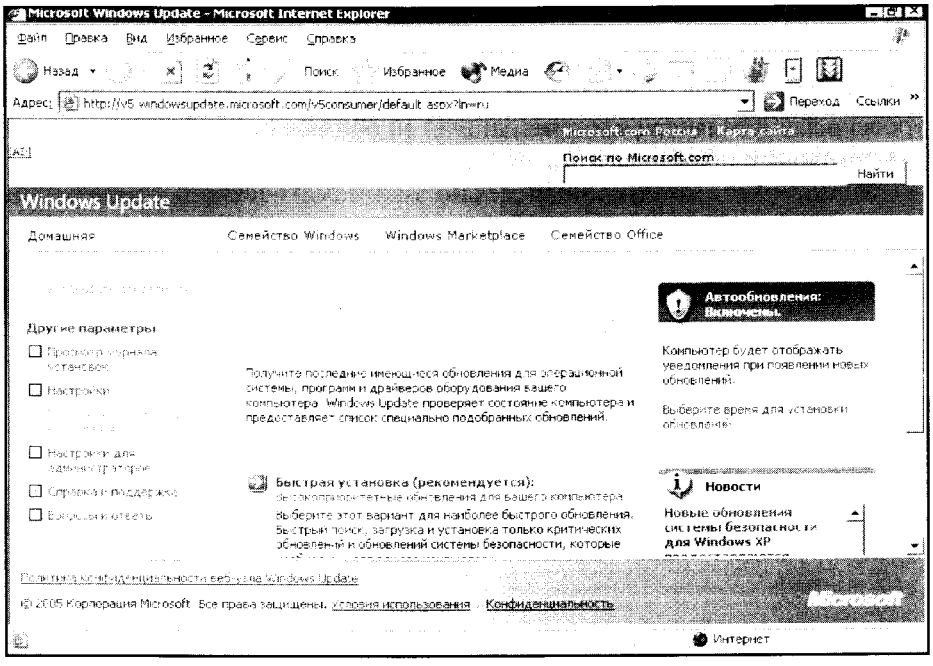


Рис. 13.57. Сайт windowsupdate.microsoft.com

этим защищенность вашей системы. Но, решившись проводить обновления вручную, можете воспользоваться веб-узлом Microsoft, перейти на который можно, щелкнув по ссылке **Установить обновления с веб-узла Windows Update**. Когда вы попадете на этот узел (рис. 13.57), ваша система будет автоматически проанализирована, а вы сможете выбирать варианты дальнейших действий самостоятельно.

Здесь же вы можете ознакомиться с журналом установок, провести быструю установку недостающих обновлений, выбрать компоненты установки вручную, почитать дополнительные материалы. На сайте Microsoft.com вы также сможете провести онлайновое тестирование вашего компьютера на наличие уязвимостей.

13.6. ВЫВОДЫ

Все, что вы прочитали в этой и других главах, поможет вам сделать систему достаточно защищенной. Но наш разговор о безопасности на этом не закончен. В одной из следующих глав, где будут рассмотрены установки реестра Windows XP, имеющие отношение к настройке сетевого обмена, мы так или иначе вернемся к вопросам безопасности. К тому же нам осталось рассмотреть еще кое-какие программы, способствующие повышению безопасности вашей системы и ваших данных.

ГЛАВА 14
СЕТИ В WINDOWS 98

Windows 98, вернее Windows 98 SE, сегодня потеряла актуальность: уже несколько лет Windows XP вытесняет 98-ю с домашних компьютеров. Но Windows 98 SE все еще работает на большом количестве достаточно слабых по современным меркам машин, да и драйверы для нее все еще выпускаются. Если у компьютера не слишком мощный процессор и меньше 256 Мб оперативной памяти, то стоит очень серьезно задуматься о целесообразности установки Windows XP. При прочих равных условиях Windows 98 на такой машине будет работать быстрее, чем Windows XP. К тому же Windows 98 можно установить и на какой-нибудь совсем уж древний, но способный работать в режиме печатной машинки Pentium 300 с 64 Мб RAM. Поэтому сети на основе этой операционной системы все еще встречаются.

Процесс настройки локальной сети в Windows 98 не слишком отличается от аналогичного процесса в Windows XP, но на случай, если вы не занимались этим прежде, рассмотрим его отдельно. Мы разберем установку сети на базе Ethernet, построим беспроводную сеть на базе Wi-Fi, свяжем проводной сетью компьютер на Windows XP и Windows 98 и настроим в сети Windows 98 общий доступ к интернет-подключению.

14.1. ПРОВОДА И ICS В WINDOWS 98 SE. СОЕДИНЕНИЕ С WINDOWS XP

Для начала установим в Windows 98 сетевую карту. Чтобы это сделать, нужно открыть окно свойств системы (**Мой компьютер** ▸ **Панель управления** ▸ **Система** либо вызвать контекстное меню щелчком правой кнопкой мышки по значку **Мой компьютер** на рабочем столе и выбрать в этом меню строку **Свойства**).

В окне **Свойства** выберите вкладку **Устройства** (рис. 14.1) и найдите в ней сообщение с вопросительным знаком, касающееся сетевой карты. Если сетевая карта уже установлена — возможно, это было сделано до вас в процессе установки системы, — тогда вопросительного знака на вкладке устройств вы не найдете.

Если же видно, что драйверы для сетевой карты не установлены (как на рис. 14.1), дважды щелкните по иконке сетевой карты и, открыв окно ее свойств, выберите вкладку **Драйвер**, на которой есть кнопка **Обновить драйвер**. С нажатия этой кнопки начинается установка драйверов для вашей сетевой карты. Процесс установки драйверов для сетевой карты в Windows 98 практически идентичен такому же процессу в Windows XP, поэтому он не стоит подробного рассказа. Если у вас появились проблемы с установкой драйверов сетевой карты для Windows 98, обратитесь к одной из предыдущих глав, все это описано в деталях.

После того как драйверы установлены, остается настроить некоторые сетевые параметры, а точнее, установить клиент для сетей Microsoft, а также установить и настроить протокол TCP/IP, дать имя компьютеру и рабочей группе, в которую он входит, и настроить установки общего доступа к ресурсам компьютера. Для начала откроем окно **Сеть**, воспользовавшись **Панелью управления** (рис. 14.2).

В нашем случае **Клиент для сетей Microsoft** был уже установлен, а если такового не оказалось, нажмите кнопку **Добавить** и установите этот клиент в систему. В процессе установки клиента вам может понадобиться компакт-диск, с которого осуществлялась установка вашей копии Windows 98.

Аналогично происходит инсталляция протокола. Возможно, вам понадобится еще какой-нибудь протокол (например, IPX/SPX, который используется в некоторых играх). Такой протокол устанавливается аналогично.

После установки компонентов их нужно правильно настроить. Настройка TCP/IP в Windows 98 подчиняется тем же правилам, которые были описаны применительно к настройке этого же протокола в Windows

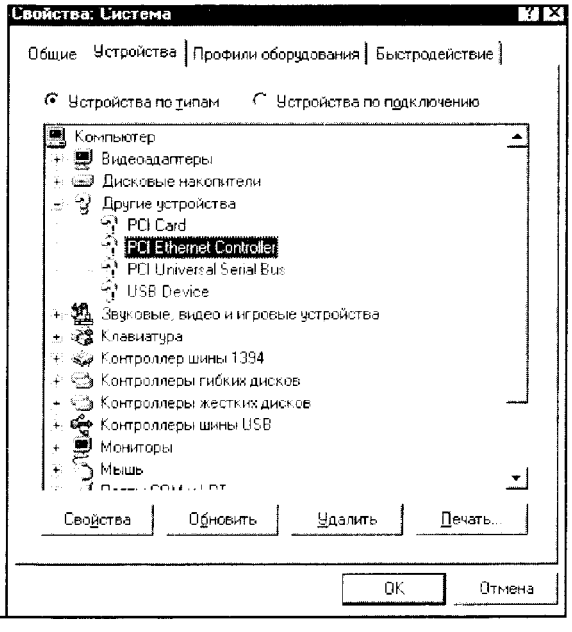


Рис. 14.1. Сетевая карта, для которой не установлены драйверы

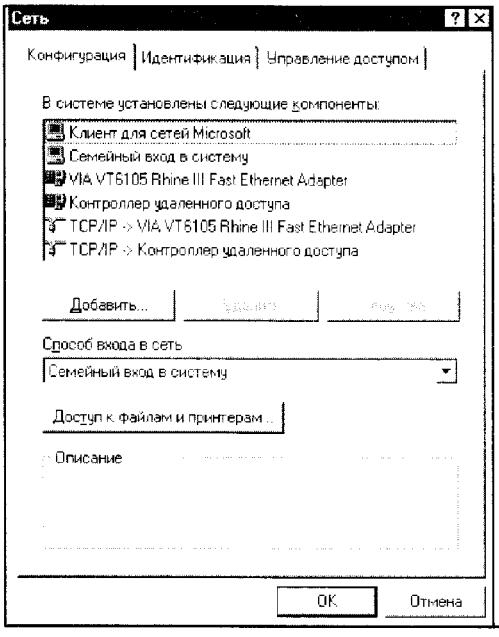


Рис. 14.2. Настройка свойств сетевых компонентов

XP. Кратко вспомним, чтобы читатели, которым нужно быстро настроить сеть в Windows 98, не тратили времени на поиски информации.

Чтобы компьютеры могли «видеть» друг друга в сети и обмениваться информацией, они должны иметь IP-адреса, принадлежащие к одной подсети, но имеющие различные номера узлов.

В нашем примере я использую IP-адрес 192.168.0.50 с маской подсети 255.255.255.0. Другие компьютеры сети должны иметь адреса, у которых три первых октета (октет — это восемь бит, или один байт) будут выглядеть как 192.168.0, а последний будет уникален для каждого компьютера. Получается, что компьютеры вашей сети могут иметь IP-адреса в диапазоне от 192.168.0.1 до 192.168.0.254. Подробный рассказ о структуре IP-адресов приводится в одной из предыдущих глав. Если допустить ошибку в настройке IP-адреса, проблемы с сетью начнутся буквально в ту же секунду.

Для настройки протокола TCP/IP нужно выделить его (в нашем случае это TCP/IP для VIA VT6105 Rhine III Fast Ethernet Adapter) и нажать кнопку **Свойства**. После этого вы увидите окно настройки протокола (рис. 14.3).

Настройка свойств TCP/IP уже обсуждалась, а здесь я лишь отмечу, что вам нужно включить параметр **Указать IP-адрес явным образом** и ввести в поля **IP-адрес** и **Маска подсети** соответствующие значения.

Продолжая настройку протокола, перейдем на вкладку **Шлюз** того же окна (рис. 14.4) и настроим там адрес шлюза по умолчанию. Эта установка пригодится нам чуть позже.

Точно так же нужно настроить TCP/IP на других компьютерах сети. Один из них будет шлюзом — он должен иметь IP-адрес 192.168.0.1. Это

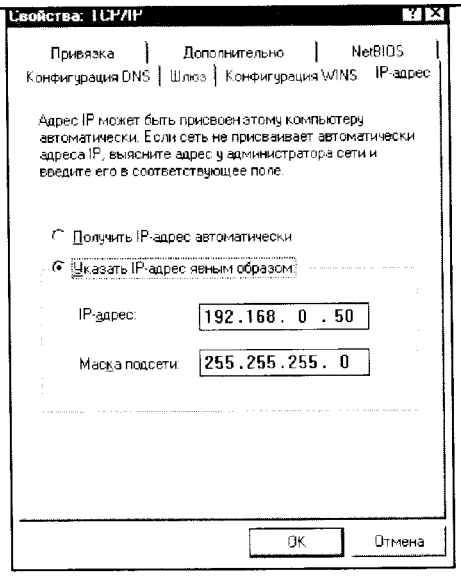


Рис. 14.3. Настройка TCP/IP

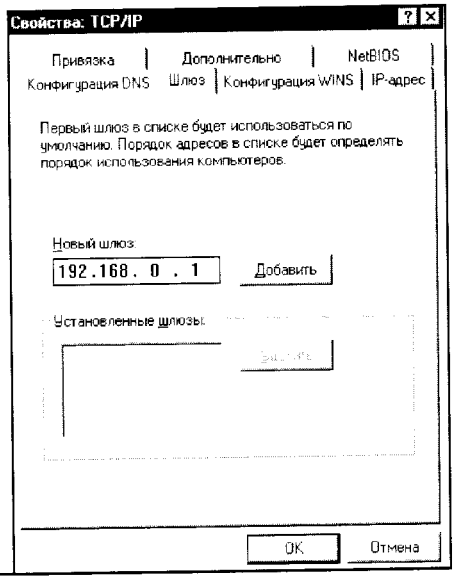


Рис. 14.4. Настройка шлюза, используемого по умолчанию

нужно, чтобы организовать в нашей сети общий доступ к интернет-соединению, ICS, но об этом чуть позже. Пока же продолжим настраивать сетевые параметры.

Следующий шаг настройки — вкладка **Идентификация** окна настройки сетевых параметров (рис. 14.5).

Напомню еще раз, что все компьютеры одной сети должны иметь одинаковое имя рабочей группы и разные имена компьютеров. Во избежание недоразумений, связанных с использованием кириллицы, в именах компьютеров и рабочих групп следует использовать латинские символы.

Теперь о соединении в сеть компьютеров с Windows 98 и с Windows XP Home Edition. Если компьютеры с этими разными операционными системами получат правильно настроенные IP-адреса, имена рабочей группы и компьютера и если на них будет разрешено использование общих ресурсов, то, чтобы заставить их работать вместе, никаких ухищрений не понадобится.

А вот что касается способов подключения компьютера с Windows 98 к системам на базе Windows XP Home и Windows XP Professional, то тут понадобится «лирическое отступление», полное практических замечаний.

Операционную систему Windows XP Home разработчики, исходя из предположения о том, что домашним пользователям не нужны дополнительные средства аутентификации в локальных сетях, лишили некото-

рых средств для обеспечения авторизованного доступа к системе. Это упростило порядок работы с системой, сделав, в частности, настройку сетей достаточно легким делом. Если вы работаете с Windows XP Home, то сможете пользоваться сетью, настроив описанные выше параметры.

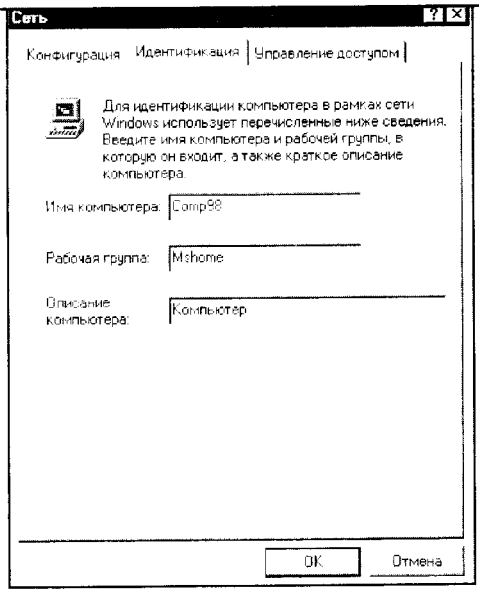
А вот Windows XP Professional просто не пустит ваш компьютер на Windows 98 к своим ресурсам без аутентификации. Для этого вам понадобится создать в Windows XP нового пользователя и использовать его имя и пароль в качестве параметров входа в систему для компьютера с Windows 98. Для управления учетными записями пользователей в Windows XP служит пиктограмма **Учетные записи пользователей** на **Панели управления**.

После того как заданы имя компьютера и рабочей группы, нужно перейти на вкладку **Конфигурация** и, нажав кнопку **Доступ к файлам и принтерам** (рис. 14.6), установить галочки против параметров, разрешающих общий доступ к этим ресурсам компьютера.

После того как проделаете все это, нажмите кнопку **OK** в окне настройки сетевых параметров. Система попросит вас перезагрузиться, и после перезагрузки компьютер будет готов к работе в сети. Настроив соответствующим образом другие компьютеры сети, вы легко и быстро создадите вашу локальную сеть.

Теперь рассмотрим процесс назначения общего доступа к папке в Windows 98. Щелкните правой кнопкой мыши по значку папки, доступ к которой хотите открыть пользователям всей сети, выберите строку контекстного меню **Свойства** и в меню **Свойств** перейдите во вкладку **Доступ** (рис. 14.7).

Рис. 14.5. Настройка параметров сетевой идентификации



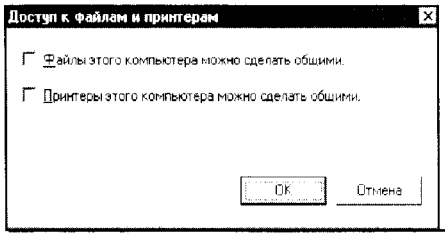


Рис. 14.6. Разрешение общего доступа к файлам и принтерам

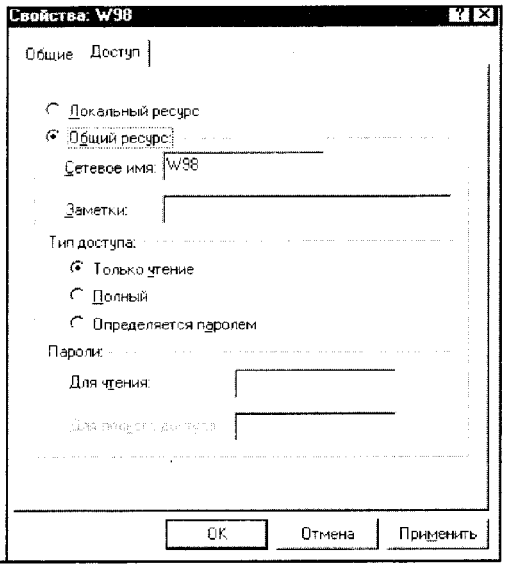


Рис. 14.7. Настройка общего доступа

На компьютерном жаргоне операцию назначения общего доступа к папке или к диску называют «расшаривание», от английского слова *share* («использовать совместно»).

Установив переключатель с параметра **Локальный ресурс** на **Общий ресурс**, вы включите общий доступ к папке. Здесь же можно настроить сетевое имя папки, тип доступа, а при желании ввести пароли для доступа к папке.

Как видите, настройка проводной сети в Windows 98 — занятие не слишком сложное.

Теперь рассмотрим настройку ICS в сети из компьютеров с Windows 98.

По умолчанию компонент **Общий доступ к Интернету** может быть не установлен. Поэтому первым делом надо установить его. Выполните последовательность действий **Панель управления ▶ Установка и удаление программ** и перейдите во вкладку **Установка Windows** (рис. 14.8).

В этом окне выберите группу параметров **Средства Интернета**, после чего в окне, детализирующем состав **Средств Интернета**, выберите компонент Общий доступ к подключению Интернета. После этого запустится **Мастер общего доступа к подключению Интернета** (рис. 14.9).

Этот Мастер попросит вас вставить в дисковод дискету, на котором он создаст файл Icsclset.exe. В процессе работы Мастер модифицирует некоторые параметры системы центрального ICS-компьютера. Так, этот компьютер будет выступать в качестве шлюза для других машин, его IP-адрес устанавливается в 192.168.0.1.

Запустив файл Icsclset.exe на других компьютерах сети, вы получите возможность настроить их для обеспечения общего доступ к интернет-подключению. Я не буду рассматривать здесь процесс настройки по-

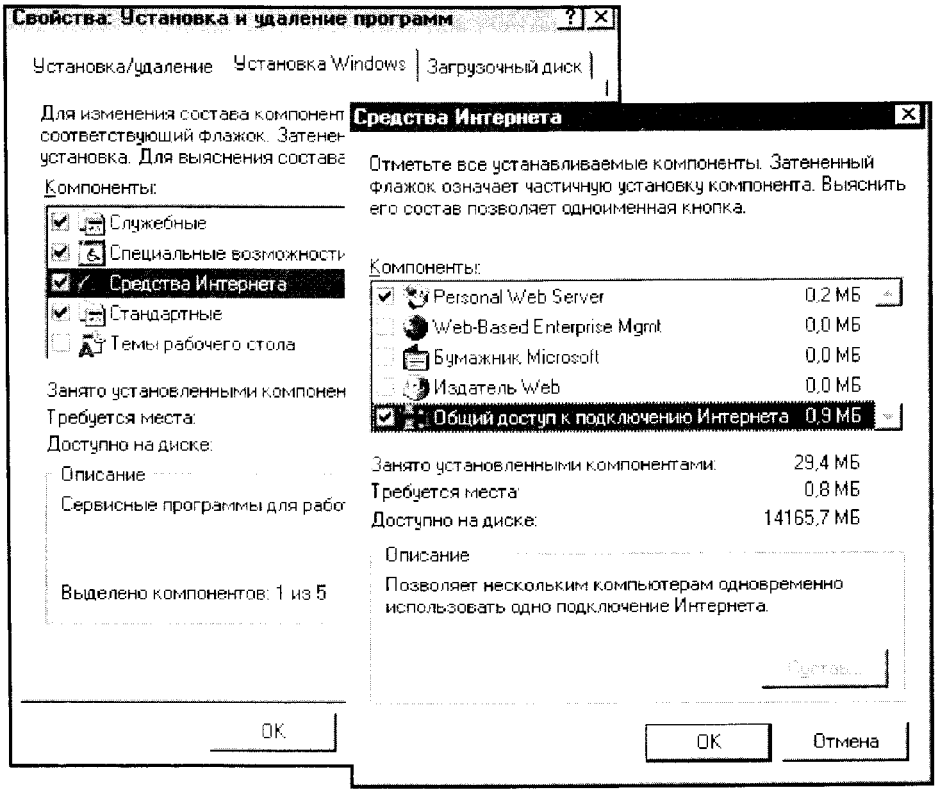


Рис. 14.8. Установка Общего доступа подключения к Интернету

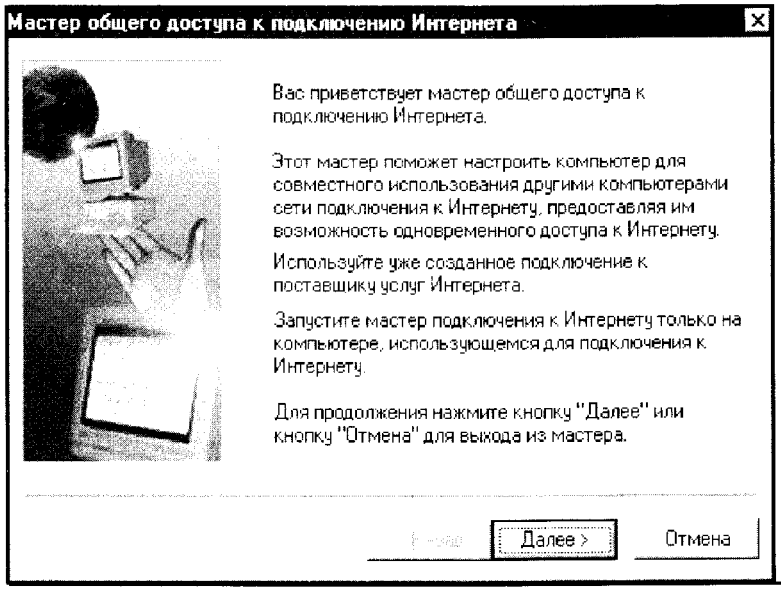


Рис. 14.9. Мастер общего доступа к подключению Интернета

дробно: по предыдущим главам вы знакомы с ICS, и настроить его для Windows 98, воспользовавшись приведенными там рекомендациями, не составит для вас труда.

Точно также нет надобности останавливаться здесь на настройке интернет-соединения и на установке модема в Windows 98: эти процедуры крайне незначительно отличаются от аналогичных, описанных для Windows XP. К тому же если вы, воспользовавшись вышеприведенными рекомендациями, настроили локальную сеть в Windows 98, то вы просто не могли не заметить пиктограммы **Панели управления**, ведущие к настройкам модема и удаленного доступа.

14.2. НАСТРАИВАЕМ БЕСПРОВОДНУЮ СЕТЬ В WINDOWS 98 И ДРУГИХ ВЕРСИЯХ WINDOWS

Windows 98 создавалась во времена, когда беспроводные сети не рассматривались в качестве альтернативы проводным сетям, и потому в этой операционной системе нет средств для управления беспроводными сетями. Но вы ошибаетесь, если считаете положение безвыходным: дело в том, что производители адаптеров беспроводных сетей обычно оснащают свои изделия соответствующим программным обеспечением, которое можно использовать для настройки беспроводной сети и в этой операционной системе.

В одной из предыдущих глав рассказывалось, как установить беспроводной адаптер ASUS WL-161 на компьютер с Windows XP. Здесь же мы установим его на компьютер с Windows 98. При этом главным вопросом будет обязательное включение установки фирменной утилиты для управления беспроводными сетями (рис. 14.10).

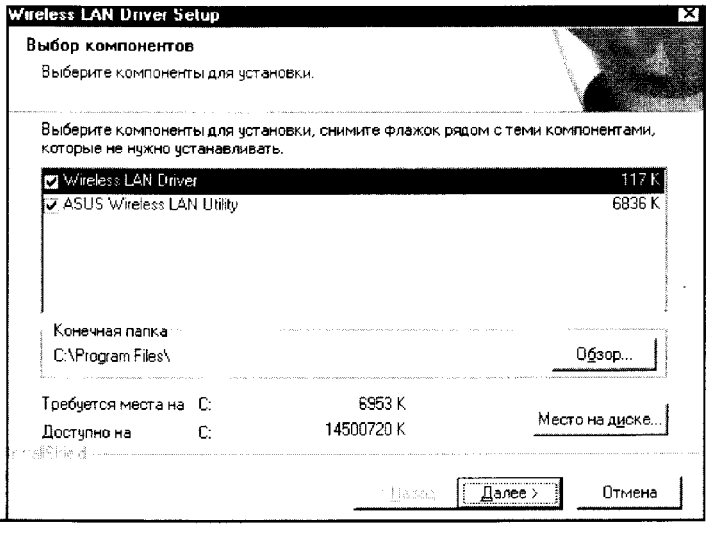


Рис. 14.10. Установка программного обеспечения для адаптера беспроводной сети

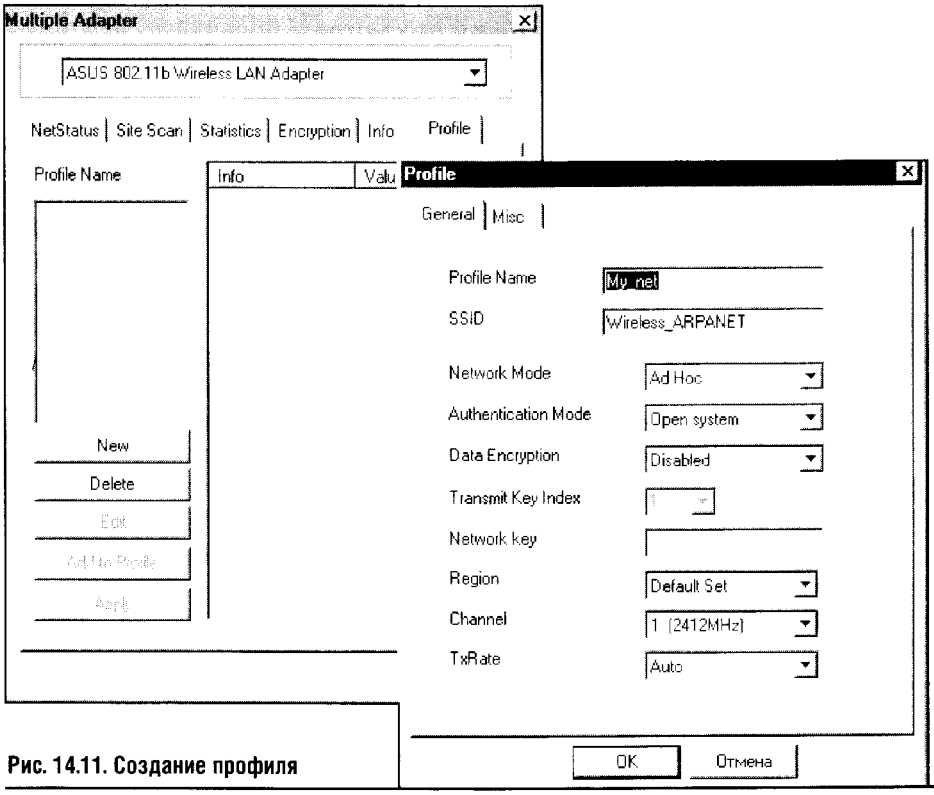


Рис. 14.11. Создание профиля

После установки драйверов и утилит и обязательной перезагрузки первым делом следует настроить IP-адрес новоустановленного сетевого адаптера. Я выбрал адрес, принадлежащий сети 192.168.0, чтобы быстро и эффективно соединить его с компьютерами, имеющими адреса из этой же подсети. В целом процесс настройки TCP/IP для беспроводного адаптера ничем не отличается от настройки этих же параметров для сети проводной. Самое интересное начинается при настройке беспроводного адаптера.

Когда Windows 98 перезагрузилась, запускаем фирменную утилиту ASUS для настройки беспроводных локальных сетей. (Для ASUS это выглядит как последовательность команд **Пуск ▸ Программы ▸ ASUS ▸ ASUScfg**, но в вашем случае последовательность может быть иной, в зависимости от того, как это задумал производитель вашего адаптера.)

После запуска утилиты в системной панели Windows появилась иконка этой утилиты, означающая, что она ищет доступную сеть. Изучим эту утилиту подробнее, особенно в части, касающейся создания новых беспроводных сетей и подключения к существующим.

На рис. 14.11 изображена вкладка **Profiles** окна настройки свойств утилиты для конфигурирования беспроводных сетей ASUS.

В этом окне можно добавлять новые профили. Смысл ваших дальнейших действий аналогичен добавлению новой беспроводной сети

в Windows XP: нажмите кнопку **New** и рассмотрите появившееся окошко с множеством установок. После чтения глав о беспроводных сетях эти установки не должны вызвать у вас ни малейших затруднений. На всякий случай снова расскажу об их значении.

- Поле **Profile Name** несет лишь информационную нагрузку: здесь можно написать все, что угодно. Это всего лишь имя, под которым данный профиль будет храниться в базе программы настройки беспроводных сетей.
- Поле **SSID** предназначено для ввода идентификатора сети.
- Параметр **Network Mode** может принимать значения **Ad Hoc** и **Infrastructure**. Как вы помните, сети Ad Hoc создаются между отдельными компьютерами без использования точек доступа, а сети Infrastructure создаются с использованием специальной точки доступа. В нашем случае строится сеть Ad Hoc, то есть обычная сеть между компьютерами без использования точки доступа.
- Свою сеть мы сделаем практически незащищенной — просто отключим шифрование данных (параметр **Authentication mode** установим в положение **Disabled**). Вообще-то делать этого не рекомендуется, поэтому, когда вы будете создавать локальную сеть, не деактивируйте этот параметр. Правда, тогда вам придется ввести **Network key**. Делать это вы уже умеете.
- Остальные параметры можно оставить без изменения, разве что в поле **Region** поставить **Default Set**.

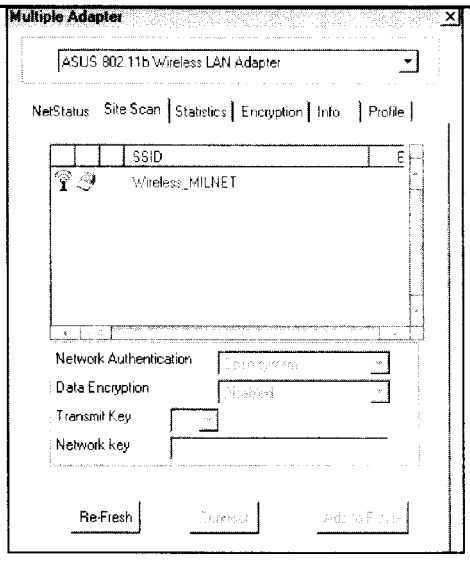


Рис. 14.13. Подключение к беспроводной сети компьютера с Windows 98

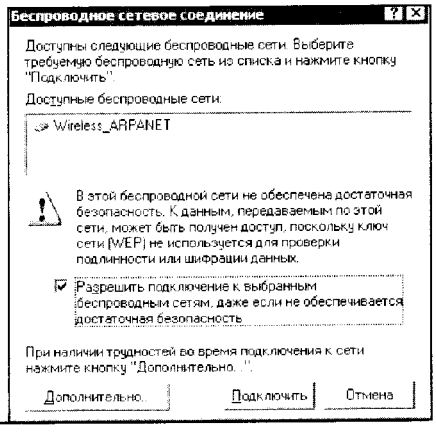


Рис. 14.12. Подключение к новой беспроводной сети

- После нажатия **OK** созданный профиль добавляется к уже существующим (в нашем случае это единственный профиль).

Теперь профиль можно активировать нажатием соответствующей кнопки.

Я попытался соединить мой компьютер с Windows 98 с компьютером на Windows XP. Как только был активирован профиль, XP-компьютер нашел новую беспроводную сеть. Так как мы создали ее, не используя средства программной защиты данных, система предупредила о низком уровне безопасности этого соединения (рис. 14.12).

После того как я ответил утвердительно на вопрос о подключении, сеть заработала. В остальном работа с беспроводной сетью аналогична работе с сетью на основе проводных коммуникаций.

Рассмотрим процесс подключения компьютера с Windows 98 к беспроводной сети, созданной на другом компьютере.

Менеджер беспроводных сетей от ASUS имеет вкладку, которая называется **Site Scan**. Перейдя на эту вкладку, можно видеть список доступных беспроводных сетей.

Для удобства я создал сеть Wireless_MILNET, которая, как и предыдущая, не использует шифрования и, значит, открыта для всех желающих. Эту сеть и нашла утилита поиска беспроводных сетей от ASUS (рис. 14.13). Теперь остается выделить мышкой найденную сеть и нажать кнопку **Connect**. Подключение произойдет через несколько секунд.

Зная приемы настройки беспроводных сетей в среде Windows 98, вы сможете настроить эти сети и в Windows 2000, и в Windows ME: процедура и в той и в другой системах очень похожа на описанные выше. Учтите, что для работы с ресурсами Windows XP Professional и других подобных операционных систем может понадобиться аутентификация.

14.3. ВЫВОДЫ

В этой главе мы ознакомились с созданием локальных сетей в Windows 98. Мы почти не касались здесь вопросов безопасности системы: для того чтобы защитить вашу Windows 98, следует обратиться к предыдущим главам, повествующим об антивирусах, файрволлах и сетевых угрозах.

Следующая наша глава посвящается использованию карманных компьютеров в локальной сети. Эти интересные устройства заслуживают отдельного рассмотрения.

ГЛАВА 15
СЕТЬ, КПК И МОБИЛЬНЫЕ ТЕЛЕФОНЫ

Карманные компьютеры появились сравнительно давно, но с падением цен эти устройства в последние годы они привлекли массовый интерес. Замечательный Windows Mobile-КПК, оснащенный практически всем, чем только пожелает душа, стоит сегодня около $ 350–400, а модель начального уровня можно найти еще дешевле.

Кроме того, карманные компьютеры, а особенно те из них, что оснащены средствами беспроводной связи, способны в некотором смысле заменить настольный ПК или ноутбук.

Популярность КПК растет, но они все еще остаются устройствами, о которых пользователям обычных ПК мало что известно. Поэтому первая часть этой главы посвящена общим вопросам использования КПК, а ее продолжение повествует о сетевом использовании этих и других устройств.

15.1. КПК: ОСНОВНЫЕ ПОНЯТИЯ

Для начала определимся с терминологией. Полное название карманных компьютеров звучит как «карманный персональный компьютер», или КПК. В английском варианте существует понятие *Personal Digital Assistant*, или PDA, что переводится как «персональный цифровой помощник» и имеет тот же смысл, который мы вкладываем в понятие КПК. Далее мы будем пользоваться всеми перечисленными выше понятиями как синонимами.

Несмотря на свои размеры, карманные компьютеры — достаточно мощные и серьезные устройства. По сути, если компьютер на базе Windows Mobile оснастить немного большим по размеру монитором, клавиатурой и мышью, получится весьма функциональный и недорогой ноутбук.

О ФУНКЦИОНАЛЬНОСТИ

Если сравнить КПК с типичным ноутбуком (или с обычным компьютером), то по функциональности, конечно же, он проиграет: карманные версии приложений обычно имеют некоторые ограничения по сравнению

с настольными. Порой эти ограничения кажутся надуманными, что не мешает «карманникам» эффективно выполнять возлагаемые на них функции.

Перечислим основные функциональные части КПК. Если у вас еще нет карманного компьютера, этот рассказ поможет решить, нужен ли он вам. Еще полезнее этот раздел будет для тех, кто уже обзавелся карманным помощником, но еще не изучил его достаточно глубоко.

Эта глава посвящена преимущественно КПК на Windows Mobile 2003. Многие ее положения справедливы и для карманных компьютеров, работающих под управлением других версий мобильных операционных систем от Microsoft. Учтите: здесь мы совершенно не затрагиваем PDA на ОС от Palm One.

Дисплей

Современные КПК Windows Mobile комплектуются цветными сенсорными TFT-дисплеями (рис. 15.1), достаточно яркими, контрастными и удобными.

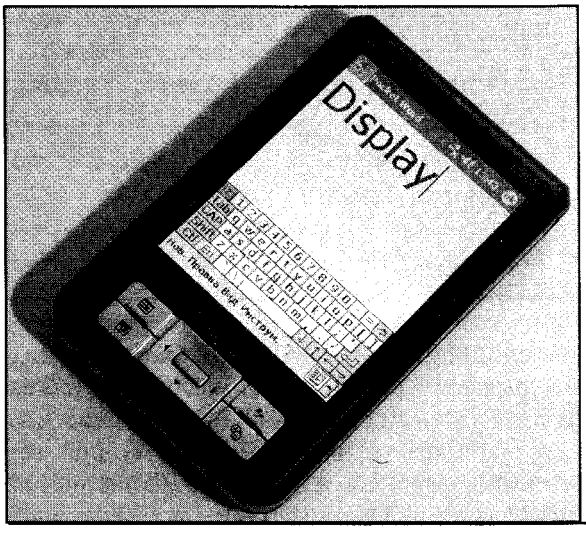


Рис. 15.1. Дисплей КПК

Дисплей типичного КПК имеет разрешение 240 × 320, но сегодня очень активно продаются компьютеры с дисплеем 480 × 640. Такого разрешения в большинстве случаев оказываются вполне достаточно для комфортного применения карманного компьютера. Не стоит забывать, что физические размеры дисплея карманного компьютера даже с ростом разрешения остаются практически неизменными — обычно их диагональ равна 3,5–3,7 дюйма. Конструктивные особенности накладывают на размер дисплея существенные ограничения, и вовсе не факт, что работать с экраном КПК 480 × 640 будет удобнее, чем с устройством, обладающим меньшим разрешением экрана.

Карманный компьютер с экраном любого разрешения можно использовать в качестве удобной «читалки» электронных книг. Большое разрешение экранов позволяет с комфортом играть в компьютерные игры и рассматривать изображения.

Ввод информации

У карманных компьютеров нет клавиатур. Их устройства ввода — различные кнопки на корпусе и сенсорный экран, реагирующий на прикосновения. Для работы с экраном служит специальное устройство, называемое стилусом или пером, похожее на тонкую пластмассовую палочку. Такой «палочкой» можно писать, касаясь кнопок на экране КПК (рис. 15.2).

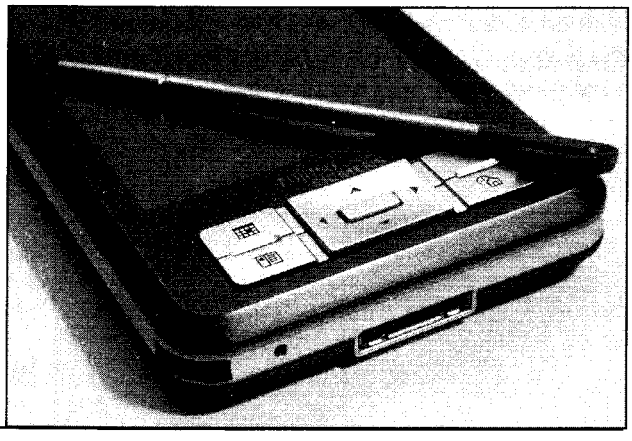


Рис. 15.2. Кнопки и стилус

Карманный компьютер не слишком пригоден для набора больших текстов: их все же удобней вводить с клавиатуры «нормального» размера, чем исхитряться в виртуозном владении стилусом. Но если оснастить КПК внешней клавиатурой, то набирать на нем тексты так же просто, как на обычном настольном компьютере. Но и без такого дополнения в КПК можно вводить короткие заметки, адресные книги и тому подобное. А если потренироваться «писать» на КПК, то можно научиться вводить информацию достаточно быстро. Тут все дело в привычке.

Но рукописному вводу и внешней клавиатуре есть альтернатива. Это виртуальная клавиатура — изображение клавиатуры (рис. 15.2), которое можно вызвать на экран КПК, и, касаясь стилусом ее букв, писать тексты. Так поступают очень многие владельцы КПК. Кроме того, в устройстве есть система подсказки слов, которая ускоряет ввод текста.

Но даже рукописный ввод позволяет достичь большей скорости набора. Другое дело, что такой способ не позволяет набирать тексты без ошибок: небольшое отклонение в написании буквы — и целое слово приходится набирать заново.

Накопители

В качестве накопителя PDA используют встроенную память. Она делится на RAM (оперативное запоминающее устройство), то есть некий аналог оперативной памяти настольного компьютера, и ROM (постоянное запоминающее устройство) — эта память по логике работы напоминает жесткий диск компьютера. На самом деле хранить данные можно и в RAM карманного компьютера, но такое сравнение более адекватно передает сущность ROM-памяти в КПК.

Различаются эти два вида памяти тем, что RAM-память быстрее ROM, а ROM-память является энергонезависимой. Если отключить питание или вынуть батарейки, то из ROM-памяти ничего не пропадет. Объем этих видов памяти в современных КПК может быть разным, от 64 до 256 Мб. На самом деле пользователю, как правило, доступен меньший объем памяти, чем номинальный: ведь некоторую часть встроенной памяти используют системные программы.

На первый взгляд, 64 мегабайта — это очень мало. На самом деле этого объема хватает для комфортной работы с компьютером. Дистрибутивы программ невелики и редко приближаются к 10 Мб, а электронных книжек в такой объем можно записать столько, что их вряд ли удастся прочесть за год. Но современные КПК умеют не только работать с текстами. В большинстве случаев их можно использовать как многофункциональные мультимедийные устройства.

На случай, если встроенной памяти не хватит, все КПК, за исключением самых дешевых, имеют слоты для карт памяти. Это обычные Flash-карты разных форматов (рис. 15.3).

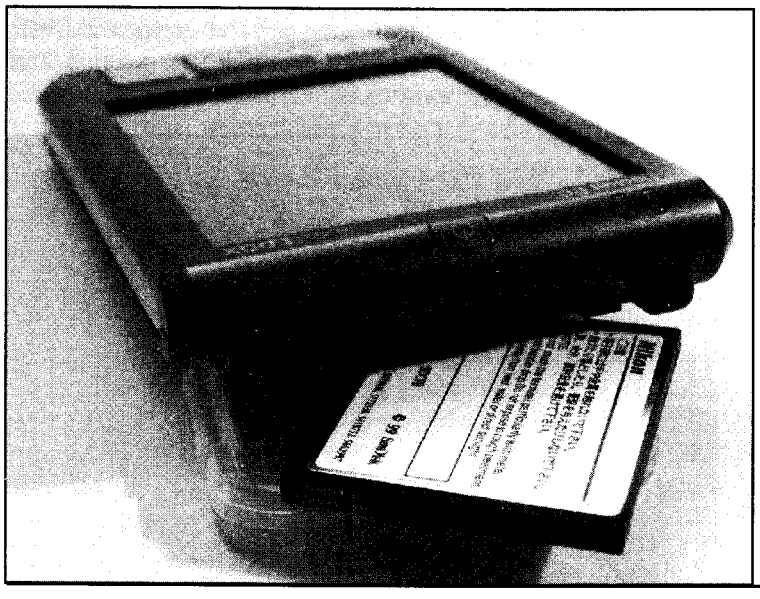


Рис. 15.3. Слот для Flash-карты в верхней части устройства

Функции

Некоторые «карманники» позволяют работать с CompactFlash-картами, некоторые — с SecureDigital, MMC, MS-картами, некоторые поддерживают несколько видов карт. Поэтому объем памяти карманного компьютера можно расширять практически неограниченно, а это важно для его мультимедийных возможностей. Ведь на КПК можно просматривать видеозаписи (хотя удобнее делать это на обычном телеэкране), можно использовать его как проигрыватель файлов MP3, цифровой фотоальбом или диктофон.

У большинства КПК есть встроенный микрофон, что позволяет использовать его как диктофон, а некоторые модели имеют гнездо для подключения внешнего микрофона. Практически все без исключения «карманники» имеют выход на наушники и встроенный динамик. Как и все динамики портативных устройств, его, как правило, нельзя назвать достаточно качественным, но со своими функциями звукового оповещения о системных событиях, встречах и срабатываниях будильника такие динамики справляются. А для всего остального существуют наушники.

Но главная аппаратная составляющая КПК, главная «вкусность», которой они прямо-таки набиты под завязку, — средства связи.

ВЫЧИСЛЕНИЯ И ВРЕМЯ АВТОНОМНОЙ РАБОТЫ

Функциональность КПК такова, что ставит их в один ряд с современными настольными компьютерами и ноутбуками. К тому же у карманных компьютеров есть мощные процессоры, частоты которых зашкаливают за 600 Мгц. Ведь КПК — это, помимо прочего, мультимедийные устройства, а максимальные частоты процессоров нужны там, где нужна максимальная производительность. Например, в играх,

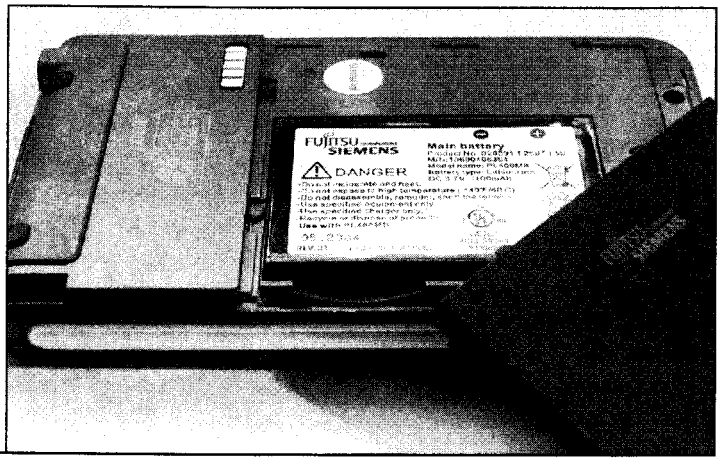


Рис. 15.4. Батарея КПК

при просмотре видео. А вот чтение электронных книг, работа с офисными программами, прослушивание MP3-аудио особо высокой производительности вовсе не требуют.

Мобильные процессоры, несмотря на высокую мощность, весьма скромно потребляют энергию (равно как и другие компоненты КПК), и потому «карманники» отличаются большим временем автономной работы: до 8–10 часов со стандартной батареей. Но обычно это время колеблется между 2–3 и 10–12 часами, в зависимости от батареи, от аппаратной конфигурации и от решаемых задач. Понятно, что на чтение электронной книги на минимальной подсветке энергии требуется куда меньше, чем на мощную, динамичную игрушку или просмотр видео.

Что до источников питания (рис. 15.4), то распространены аккумуляторные батареи для КПК емкостью от примерно 900 до 3000 и более мАч (микроампер в час). Чем больше емкость аккумулятора, тем дольше КПК будет от него работать. Дополнительную батарею можно приобрести отдельно, но некоторые «карманники» не поддерживают сменных батарей и работают только со встроенными.

СРЕДСТВА СВЯЗИ

У КПК есть средства связи с настольными компьютерами. Это док-станции, интерфейсы IrDa (инфракрасный), Wi-Fi (беспроводной) и Bluetooth.

Традиционный инфракрасный порт тоже может использоваться для связи КПК с некоторыми моделями сотовых телефонов, с ПК и, при установке определенного софта, также как пульт дистанционного управления для домашней техники. Правда, превратить в хороший пульт управления можно далеко не каждый КПК: зачастую производители сознательно уменьшают мощность встраиваемых в КПК инфракрасных портов, чтобы не создавать дополнительную угрозу безопасности передаваемых по ним данных.

Традиционный кабель для связи с настольным компьютером имеется у всех карманных компьютеров и используется для синхронизации данных, переноса файлов, установки программ. Многое, однако, можно сделать и без этого кабеля.

Обычно КПК комплектуются кредлом, или док-станцией (рис. 15.5). Кредл (от английского *cradle* — колыбель, люлька), или, как его еще называют, док-станция, напоминает подставку под КПК, которая служит для соединения карманного компьютера с настольным ПК и для подзарядки карманника. Дешевые КПК обычно не оснащают кредлом, а вот в комплектации дорогих «карманников» кредл обычно есть. Док-станцию подключают к настольному компьютеру, в нее устанавливается «карманник», после чего, как правило, начинается зарядка его батареи и появляется возможность работы с ним средствами ПК.

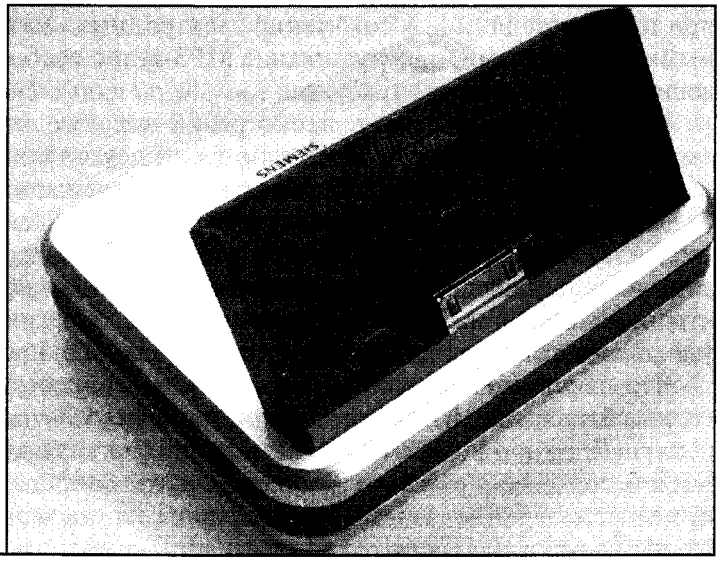


Рис. 15.5. Кредл

Одним из вариантов кредла является обычный USB-кабель. Им комплектуются самые дешевые модели. Правда, такой кабель можно встретить и в более дорогих моделях как «походный вариант».

Помимо проводного, а также теряющего популярность инфракрасного интерфейса, у КПК есть и беспроводные интерфейсы связи. Популярность беспроводных интерфейсов растет прямо-таки лавиной!

Bluetooth хорош для связи КПК с сотовыми телефонами и другой Bluetooth-периферией и подходит для сопряжения с настольным ПК.

Еще больше интереса у пользователей вызывает интерфейс Wi-Fi. Беспроводные сети Wi-Fi хорошо известны и популярны. К примеру, если у вас есть беспроводная локальная сеть, то КПК сумеет, естественно, в нее интегрироваться.

Bluetooth и Wi-Fi различаются по дальности работы (дальность Wi-Fi значительно больше), скорости передачи данных (у Wi-Fi она тоже больше), да и ориентированы эти интерфейсы на решение разных задач.

Дома можно реализовать такую схему: настольный компьютер или ноутбук подключены к Интернету, а карманный компьютер, связанный с ними по Wi-Fi, тоже получает доступ в Сеть. Браузеры КПК позволяют владельцу карманного компьютера с удобством пользоваться интернет-сервисами. Такой доступ позволяет работать с электронной почтой и при помощи веб-интерфейса почтовых служб, и через почтовый клиент.

А еще карманные компьютеры поддерживают расширение собственных возможностей при помощи специальных карт расширения. Такие карты устанавливаются в слот для карт памяти. При этом такой слот должен поддерживать режим работы с внешними устройствами. В формате

карты расширения может быть реализован Bluetooth или Wi-Fi адаптер, GPS-приемник, GSM-модуль и так далее. К примеру, вы сможете превратить свой КПК в мощную систему для ориентирования на местности, оснастив его GPS-приемником.

15.2. НАСТРОЙКА ДОСТУПА В ИНТЕРНЕТ ЧЕРЕЗ GPRS

Нашими «подопытными» будут КПК Fujitsu-Siemens Pocket LOOX 420 и мобильный телефон Alcatel 535, оснащенный инфракрасным портом и имеющий GPRS Class 10. Затем мы рассмотрим особенности подключения к GPRS-интернету по Bluetooth.

Когда я подключался к «МТС на Кубани», то при подключении активировал GPRS. Прежде чем начинать подключение КПК к Интернету через мобильный телефон, зайдите на сайт своего оператора и найдите страничку, посвященную подключению карманных компьютеров к Интернету с использованием сотовых телефонов. Это очень важно, так как у разных операторов могут различаться параметры настройки КПК для работы с телефоном. Чтобы сделать изложение максимально понятным, я приведу рекомендации, которые мне удалось найти на сайте *http://www.kuban.mts.ru*.

Для начала компания рекомендует подключить телефон к КПК. В нашем случае это будет инфракрасное (IrDa) соединение, но можно использовать и кабель, и Bluetooth, о котором мы поговорим позже. Чтобы установить соединение, активируйте инфракрасный порт трубки, а затем следует заняться настройкой параметров КПК, необходимых для подключения к Интернету. Когда наступит время, «карманник» сам попытается соединиться с телефоном, а ваша задача состоит в том, чтобы в этот момент был активирован инфракрасный порт мобильника.

На сайте компании рекомендуют установить драйверы модема. В моем случае драйверов не было, поэтому я решил пока обойтись без них. Далее следовало очень важное, как оказалось впоследствии, замечание, касающееся особых параметров настройки КПК для некоторых моделей телефонов. К примеру, для аппаратов от Siemens, Panasonic, Alcatel и Motorola в строке инициализации модема нужно было указать следующее:

```
AT+CGDCONT=1,"IP","internet.kuban".
```

На сайте оператора особо отмечалось, что для КПК HP iPAQ строка инициализации модема должна выглядеть вот таким вот образом:

```
+CGDCONT=1,"IP","internet.kuban".
```

После установки и настройки модема следует настроить параметры удаленного соединения, и самый первый из них — это номер телефона.

Для всех аппаратов кроме изделий Siemens этот номер выглядит как `*99***#`, а для Siemens — `*99***1#`. В качестве имени и пароля пользователя используется слово `mts` строчными буквами. На операторском сайте было особо подчеркнуто, что в правилах набора номера должен быть выбран тональный способ набора.

Вооружившись этой информацией, можно брать КПК и начинать его настраивать. Напомню, что установку модема трубки я не делал: у меня не было соответствующих драйверов, и к тому же я понадеялся на то, что инфракрасное соединение — вещь стандартная и позволит мне работать с модемом мобильного телефона без дополнительных драйверов. Словом, я сразу принялся за настройку соединения КПК. Как оказалось, некоторые установки потребовали, я бы сказал, интеллектуального подбора, но расскажу обо всем по порядку.

Для начала я прошел в меню **Старт ▸ Настройки ▸ Соединения ▸ Соединения** (рис. 15.6).

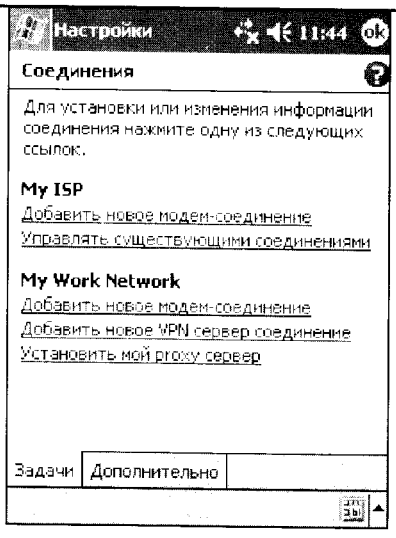


Рис. 15.6. Окно настройки соединений

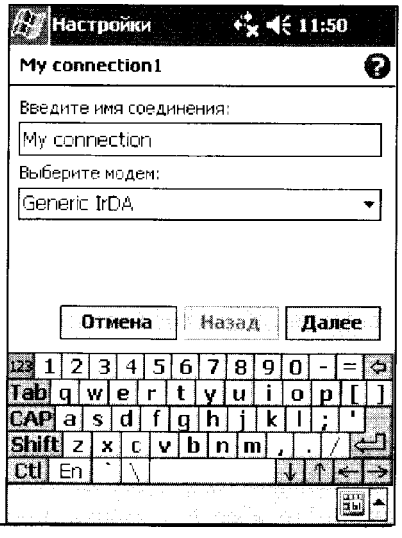


Рис. 15.7. Настройка имени и типа соединения

Появилось окно, которое позволяет управлять свойствами соединений. Меня интересовали свойства, касающиеся выхода в Интернет, поэтому я воспользовался группой ссылкой **Добавить новое модем-соединение**. После этого следовало ввести некоторые параметры, на которых мы остановимся подробнее.

Первым окном системы стало окно ввода названия соединения и типа подключения к модему. В качестве названия я выбрал **My Connection**, а тип подключения выбрал как **Generic IrDa** (рис. 15.7).

Нажав кнопку **Далее**, я попал в следующее окно для ввода номера (рис. 15.8). Здесь в соответствии с указаниями сайта сотового оператора я ввел `*99***#`.

Нажав еще раз **Далее**, я оказался в последнем окошке настройки соединения, где нужно было ввести имя пользователя и пароль (рис. 15.9). Здесь я снова ввел то, что было указано на сайте, то есть `mts` в качестве

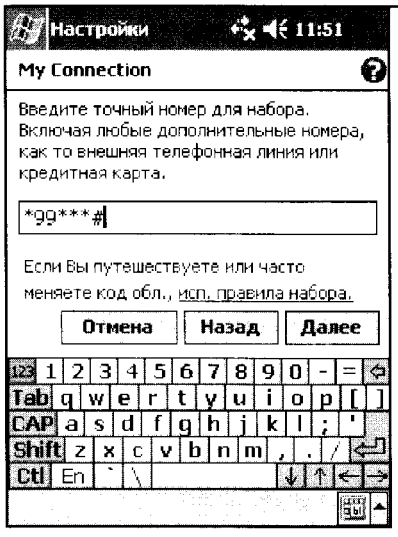


Рис. 15.8. Настройка номера

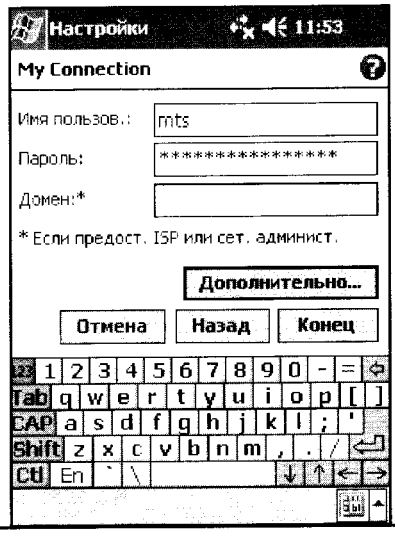


Рис. 15.9. Ввод имени пользователя и пароля

имени и пароля. Но, хотя на этом окне уже появилась кнопка **Конец**, нажимать я ее не стал. Ведь еще оставалась строка инициализации модема, с которой нужно было что-то делать.

Для доступа к этим параметрам я использовал кнопку **Дополнительно** в окне для ввода имени и пароля.

И тут-то меня ждал сюрприз. В инструкции на сайте было сказано, что все КПК кроме HP iPAQ нуждаются в строке инициализации такого вот вида: `AT+CGDCONT=1,"IP","internet.kuban"`. Добросовестно написав это в строке инициализации, я начал подключение и... ничего не добился.

То отключался инфракрасный порт мобильника, то оказывалось, что и мобильника-то поблизости нет. Я начал искать неточность в своих настройках, перебрал многое, а потом решил получше разобраться со строкой инициализации. Здесь я вспомнил, что где-то читал о КПК Fujtsu-Siemens Pocket LOOX 420, что он аппаратно похож на один из iPAQ. Не надеясь на удачу, я написал в строке инициализации вот такой вот текст: `+CGDCONT=1,"IP","internet.kuban"`, не трогая остальные параметры (рис. 15.10).

После этого все заработало и работает по сей день. Как видите, лишь случай помог справиться со вполне стандартной операцией настройки КПК для работы с GPRS.

Только что вы стали невольным свидетелем одного из методов работы, к которому часто приходится прибегать компьютерщикам, — метода подбора параметров настройки. Ситуации, похожие на описанную выше, складываются довольно часто. У них есть общий признак: есть про-

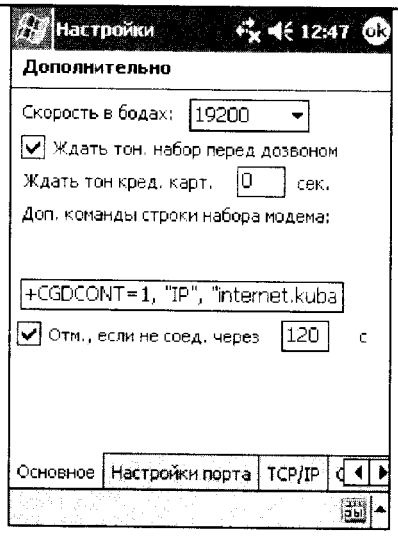


Рис. 15.10. Настройка соединения

Рис. 15.11. Ввод адреса

блема, но нет нужной документации для ее решения. Тут все зависит от интуиции пользователя или от его упорства — если вариантов подбора параметров достаточно много. Здесь, как видите, могут пригодиться практически любые ваши знания. Определенное значение имеет и ваше

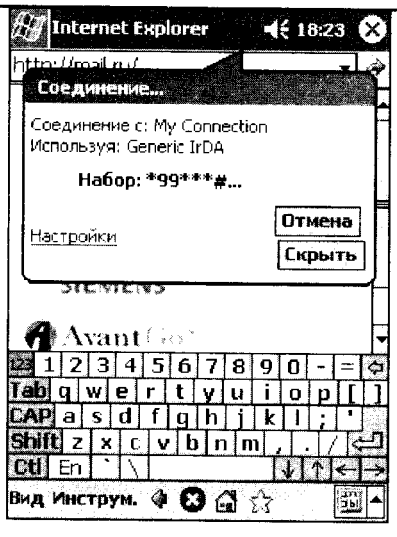


Рис. 15.12. Соединение

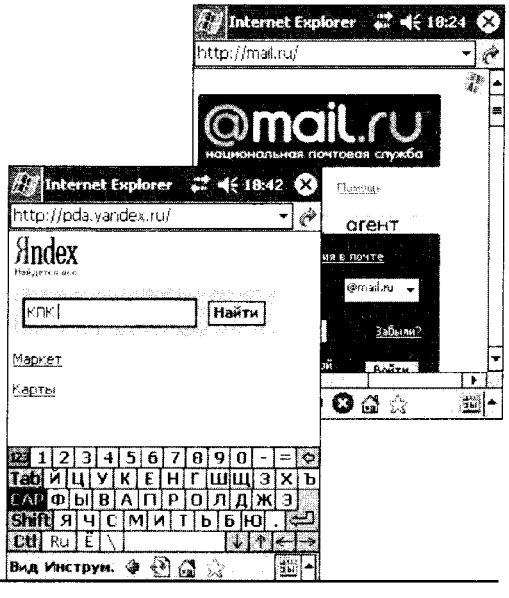


Рис. 15.13. Работа в Сети

желание справиться с проблемой. Главное — действовать уверенно, но при этом важно не переходить границу, за которой портится оборудование или безвозвратно теряются данные.

А теперь попробуем подключиться к Интернету при помощи только что созданного соединения.

Для начала я активировал инфракрасный порт сотового и разложил устройства таким образом, чтобы их инфракрасные порты располагались на расстоянии нескольких сантиметров. Запустив Internet Explorer на КПК, я ввел в строку **Адрес** адрес странички, на которую мне хотелось попасть. Это был сайт mail.ru (рис. 15.11).

После этого должно начаться соединение с указанными при настройке параметрами. КПК подключится к мобильному телефону и начнет набирать номер (рис. 15.12). Если все пройдет гладко, то вы окажетесь в Сети.

Дальнейшая работа с веб-сайтами ничем не отличается от обычной работы в Интернете (рис. 15.13).

Лучшим лекарством от проблем, связанным с беспроводным выходом в Интернет через сотовый телефон, служит перезагрузка и КПК, и телефона. У меня были случаи, когда правильно настроенное соединение, через которое я не раз выходил в Сеть, вдруг отказывалось работать. Выключив и включив мобильник, я эффективно боролся с такими «фокусами» соединения. А однажды для того, чтобы все заработало, пришлось перезагрузить КПК.

15.3. КПК В ЛОКАЛЬНОЙ WI-FI СЕТИ

КПК в домашней беспроводной сети позволяет вам пользоваться ресурсами стационарного компьютера в любой точке дома. К тому же если ваш настольный компьютер имеет выход в Интернет, вы сможете выйти в Сеть и с КПК.

Рассмотрим настройку нового КПК, впервые подключаемого к домашней беспроводной сети. Чтобы начать работу в беспроводной сети, включите ваш Wi-Fi адаптер. В моем случае это можно сделать нажатием стилуса на иконку беспроводного адаптера в нижней части окна **Сегодня** (рис. 15.14).

После щелчка по этому значку появляется меню, в котором есть пункт **Вкл. Wireless**. Выбором этого пункта мы включаем беспроводной адаптер. После этого на экране появится запрос о том, к какой из найденных беспроводных сетей нужно подключиться и какой метод подключения к сети при этом использовать (рис. 15.15).

В данном случае мы выбираем **Work**, так как это обычная домашняя сеть. После нажатия кнопки **Соединить** появляется второй запрос системы, в ответ на который надо ввести ключ сети. В моем случае в качестве

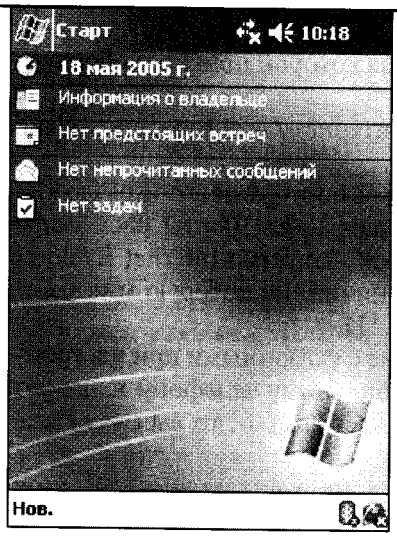


Рис. 15.14. Значок беспроводного адаптера в правом нижнем углу

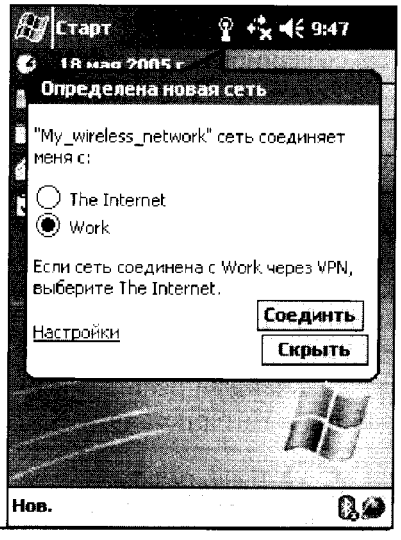


Рис. 15.15. Выбор сети и метода подключения

ключа использовалась простая последовательность символов 12345, которую я ввел в окно запроса (рис. 15.16).

После того как ключ введен, сеть должна заработать. Подключившись к беспроводной сети, вы получаете доступ к общим папкам компьютеров, входящих в нее.

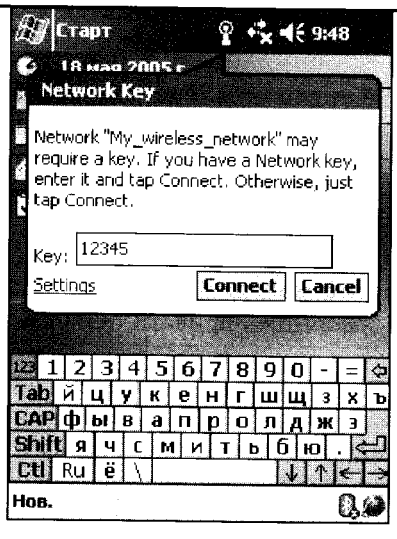


Рис. 15.16. Ввод ключа беспроводной сети

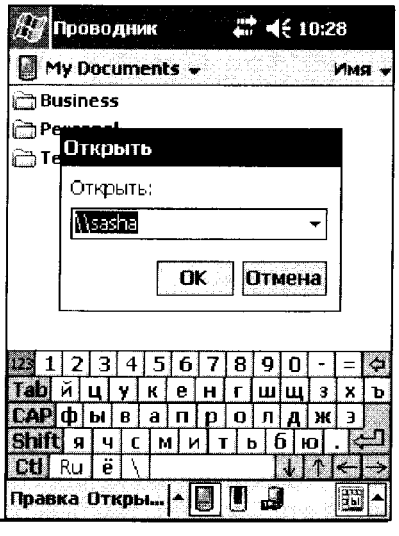


Рис. 15.17. Подключение к сетевому ресурсу

Чтобы подключиться к какому-нибудь компьютеру вашей сети с использованием стандартных средств Windows Mobile 2003, выполните команду **Старт ▸ Программы ▸ Проводник**, после чего нажмите в нижней части **Проводника** кнопку с изображением руки, держащей устройство хранения данных. Затем в ответ на вопрос об имени сетевого ресурса введите это имя в поле ввода (рис. 15.17).

После того как вы введете имя сетевого ресурса — в данном случае это компьютер, — может последовать вопрос, касающийся сетевой идентификации: вам предложат ввести имя и пароль. Если вы пользуетесь Windows XP Home, то ничего вводить не понадобится — просто ответьте на вопрос утвердительно. Ну а если же это Windows XP Professional, то вам могут понадобиться параметры одной из учетных записей.

После аутентификации вы сможете работать с общими ресурсами компьютеров вашей сети (рис. 15.18).

Порядок работы с общими ресурсами ничем не отличается от работы с ними с настольного ПК. Если разрешен полный доступ к общей папке, вы сможете копировать в нее файлы, удалять их, изменять и так далее. При этом вы сможете копировать файлы с КПК на настольный компьютер и наоборот.

Теперь пора заняться ручной настройкой параметров сети. Ручная настройка этих параметров может понадобиться, если что-то работает неправильно.

Чтобы получить доступ к настройкам параметров беспроводной сети на КПК, нужно открыть окно для настройки сетевых соединений: **Старт ▸ Настройки ▸ Соединения ▸ Соединения ▸ Дополнительно ▸ Сетевая карта**. Вы увидите окно настройки сетевой карты (рис. 15.19).

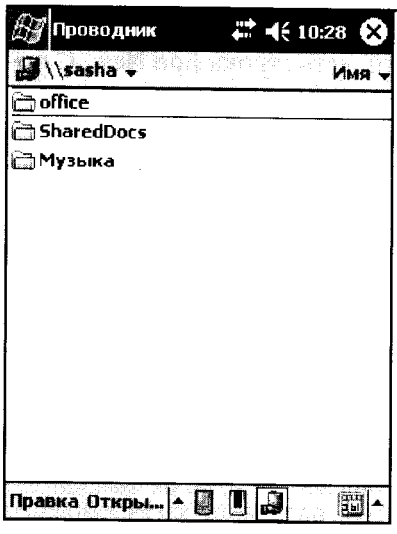


Рис. 15.18. Доступ к общим ресурсам компьютера

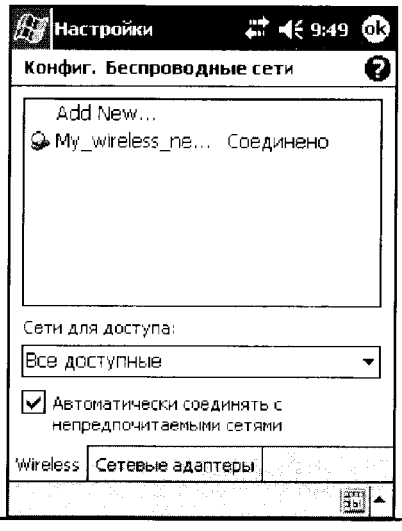


Рис. 15.19. Окно настройки сетевого адаптера

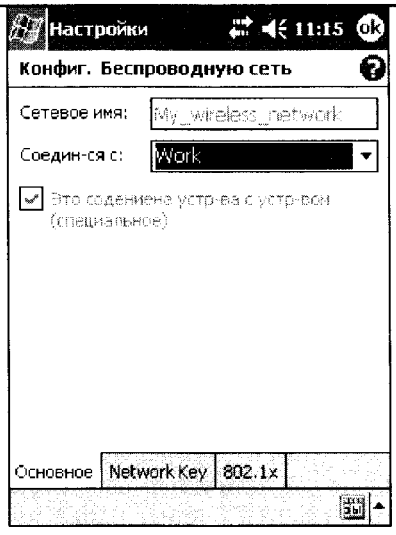


Рис. 15.20. Вкладка Основное окна настройки беспроводного соединения

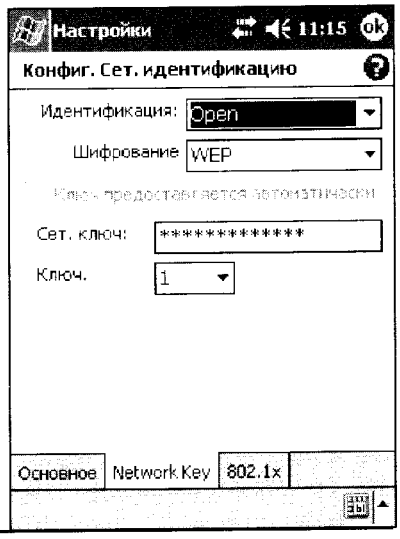


Рис. 15.21. Настройка сетевой идентификации

Когда адаптер беспроводной сети включен, в этом окне появляется вкладка Wireless, с помощью которой можно управлять беспроводными сетями. Здесь рекомендуется включить параметр **Автоматически соединять с непредпочитаемыми сетями**. Таким образом система будет выводить информацию обо всех доступных на данный момент сетях.

Теперь в этом окне можно видеть список доступных беспроводных сетей. В нашем случае это одна сеть **My_wireless_network**. Там же, немного выше строчки с описанием этой сети, есть строка **Add New**. С помощью **Add New** можно создавать новые беспроводные сети, но этим мы займемся чуть позже.

Чтобы получить доступ к настройкам нужной беспроводной сети, щелкните по ней стилусом. Появится окно настройки (рис. 15.20), состоящее из нескольких вкладок.

Первая вкладка называется **Основное**. Здесь можно увидеть полное имя сетевого соединения (это его SSID) и тип соединения (поле **Соединся с**). В этом поле выбран пункт **Work**. Если вы хотите соединиться с Интернетом через свою локальную сеть, нужно выбрать пункт **The Internet**.

Проблемы с настройкой Wi-Fi чаще всего вызваны неправильной настройкой подключения. К примеру, когда в качестве типа соединения выбрано поле **Work**, компьютер (у меня по крайней мере) хорошо работает с ресурсами локальной сети, но не выходит в Интернет. При выборе пункта **The Internet** все повторяется с точностью до наоборот. Если с этой проблемой столкнется неподготовленный человек, он будет долго искать ее источник. Источником проблем могут быть, помимо этой установки, и другие параметры.

Переходим на вторую вкладку. Она называется **Network Key** (рис. 15.21).

Здесь устанавливаются тип идентификации (в моем случае **Open**), тип шифрования и вводится сетевой ключ. Сетевой ключ был задан на одном из предыдущих этапах настройки беспроводной сети. Остальные параметры система устанавливает автоматически, но в случае возникновения проблем проверьте эту вкладку и проследите, чтобы установки беспроводной сети на стационарном компьютере и на КПК совпадали.

Вкладка 802.1x нужна для сетей с точками доступа. Я же работал с обычной сетью Ad Hoc, поэтому параметры этой странички были заблокированы. Параметров там не так уж и много: по правде говоря, всего одна галочка, включающая использование IEEE 802.1x для доступа к сети.

После того как все установки проверены, можно нажать OK и вернуться к окну управления беспроводными сетями. Здесь переходим во вкладку **Сетевые адаптеры** (рис. 15.22).

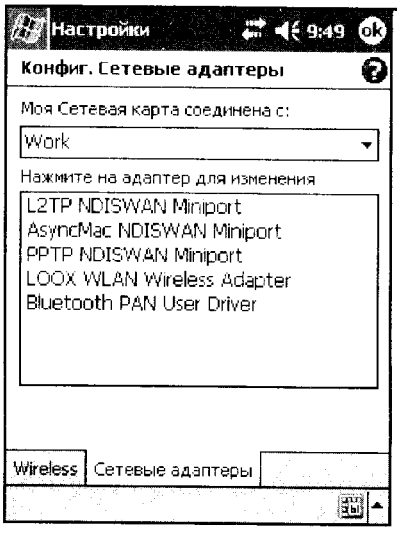


Рис. 15.22. Настройка сетевого адаптера

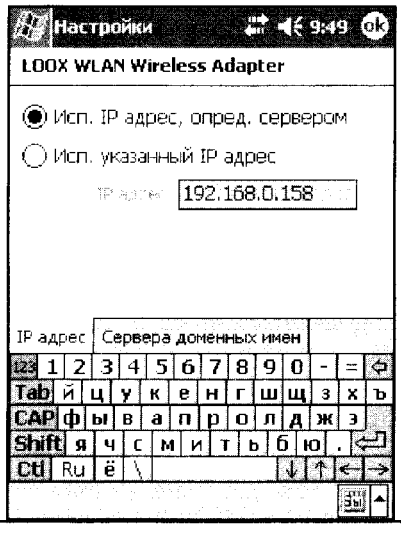


Рис. 15.23. Настройка IP-адреса адаптера

В поле **Моя Сетевая карта соединена с:** выбрано **Work**. Эта установка аналогична вышеописанному параметру беспроводного соединения. Щелкнув по названию интересующего нас адаптера (в моем случае это LOOX WLAN Wireless Adapter), можно заняться его настройкой, а в нашем случае — скорее даже проверкой правильности его настройки.

Первая вкладка окна настройки сетевого адаптера касается настройки его IP-адреса, маски подсети и шлюза по умолчанию (рис. 15.23).

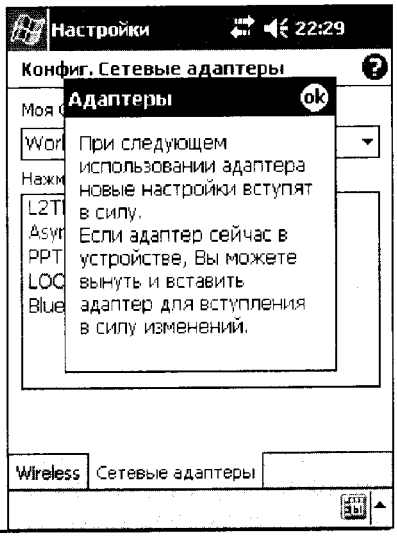


Рис. 15.24. Сообщение об изменении настроек сетевого адаптера

Если в вашей сети работает DHCP-сервер или если вы настраиваете сеть, использующую точку доступа, то здесь можно оставить параметр **Исп. IP адрес, опред. сервером**. Так сделано и в этот раз: на одном из компьютеров сети работает ICS. Как видите, адрес, присвоенный сетевому адаптеру автоматически, точно указывает на систему, которая это сделала.

Можно настроить адрес и вручную. Сеть, к которой мы подключили КПК, ориентирована на ICS, и в качестве IP-адресов компьютеров используются адреса из известной нам подсети 192.168.0. Если бы мы настраивали эти параметры вручную, адресом мог бы стать 192.168.0.200 при маске подсети 255.255.255.0, а в качестве шлюза по умолчанию использовался бы 192.168.0.1.

Вкладка **Сервера доменных имен** бесполезна в нашем случае и в обычной Ad Hoc-сети — обычно система обходится без ручных настроек этих параметров.

После нажатия кнопки **OK**, даже если мы не меняли никаких параметров, система выводит предупреждение (рис. 15.24).

Обычно для того, чтобы новые настройки заработали, достаточно выключить и включить беспроводной адаптер.

Теперь, когда мы разобрались с доступом к ресурсам локальной сети, самое время «выпустить» КПК в Сеть.

15.4. В ИНТЕРНЕТ ПО WI-FI

Чтобы ваш КПК успешно вышел в Интернет по соединению Wi-Fi, нужно правильно настроить настольный компьютер. Настройка эта ничем не отличается от настройки компьютера в качестве машины, предоставляющей доступ к общему подключению Интернета, описанной в одной

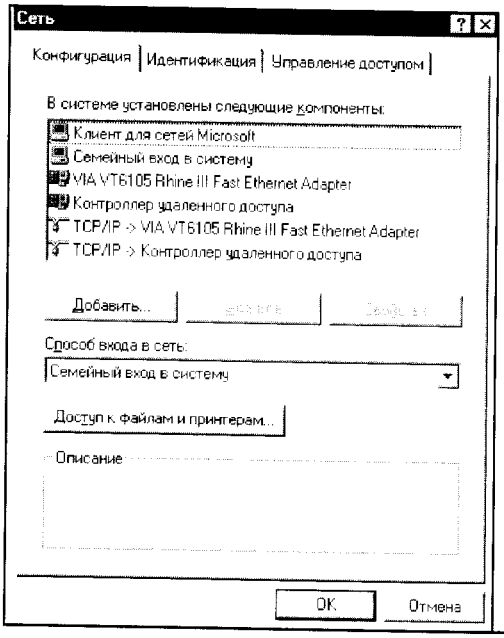


Рис. 15.25. Настройки общего подключения к Интернету

из предыдущих глав. Настройке ICS мы уделили немало внимания, здесь лишь повторим некоторые ключевые моменты этой настройки.

Наш ICS-сервер должен иметь IP-адрес 192.168.0.1, маску подсети 255.255.255.0, и подключение к Интернету должно разрешать доступ к нему других пользователей (рис. 15.25).

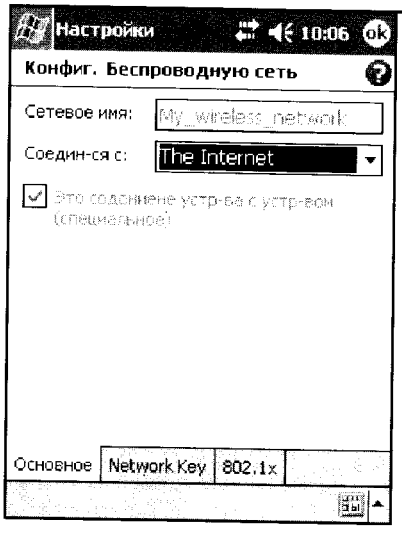


Рис. 15.26. Выбор типа соединения

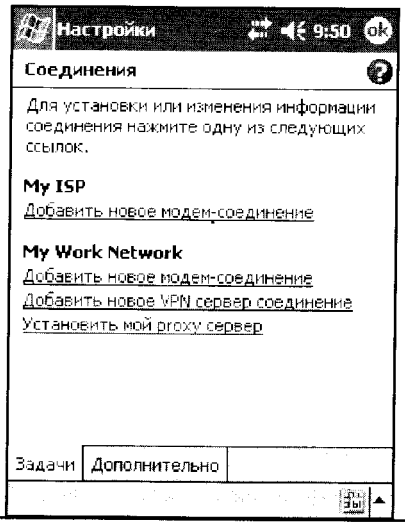


Рис. 15.27. Начало установки прокси-сервера

Обычно с этими делами хорошо справляется Мастер домашней сети, но если вдруг что-то пойдет не так, нужно будет проверить все это вручную.

Когда ICS настроен, следует заняться настройкой КПК для доступа в Интернет. Для начала нужно иметь рабочее соединение по Wi-Fi сети. Далее в настройках адаптера (или в окне конфигурации беспроводной сети, как на рис. 15.26) надо установить параметр **Соедин-ся с** в значение **The Internet**.

Как уже говорилось, чтобы работать с ресурсами локальной сети, этот параметр надо переключить в положение **Work**, а для пользования Интернетом — в **The Internet**.

Если вы пользуетесь прокси-сервером, следующим этапом настройки будет установка его параметров (рис. 15.27).

Его настройка начинается со ссылки **Установить мой proxy сервер** на вкладке **Задачи** настройки сетевых соединений. После щелчка по этой вкладке появляется окно, где нужно установить некоторые галочки и написать IP-адрес сервера (рис. 15.28).

Если вы сами не устанавливали прокси-сервер, значит, у вас его скорее всего нет, а следовательно, и настраивать ничего не нужно.

Вот и вся настройка КПК для доступа в Сеть. Зайдя в Internet Explorer и набрав в адресной строке нужную вам ссылку, вы, после того как центральный компьютер подключится к Интернету, оказываетесь на выбранном сайте (рис. 15.29).

Обычные сайты адекватно отображаются на экране КПК, даже Flash-анимацию можно увидеть, равно как и все остальное. Правда, полосы прокрутки приходится использовать в обоих направлениях.

Рис. 15.28. Настройка прокси-сервера

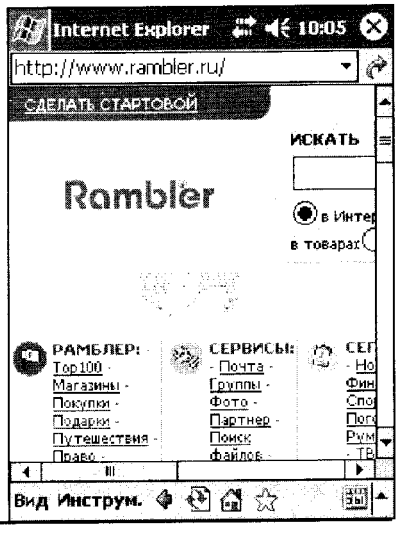


Рис. 15.29. Беспроводной веб-серфинг: обычный сайт

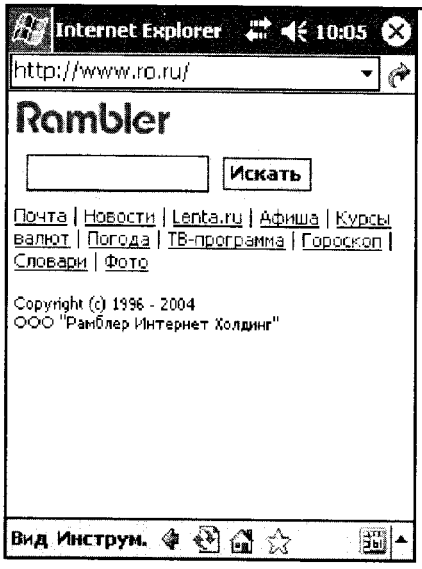


Рис. 15.30. Беспроводной серфинг: мобильная версия сайта

Рис. 15.31. Мобильный сайт The New York Times

Мобильное направление обычного Интернета постоянно развивается, именно поэтому многие сайты имеют мобильные разделы (рис. 15.30).

Как правило, мобильная версия в расчете на мобильные же каналы связи практически не использует графику, а странички ограничиваются лишь одной полосой прокрутки. При использовании КПК в качестве Wi-Fi-терминала для выхода в Интернет через сравнительно недорогое домашнее соединение это не слишком критично, а вот при использовании GPRS-модема — очень важно. К тому же при просмотре страничек, оптимизированных под экраны КПК (рис. 15.31), совершенно не чувствуешь себя обделенным. Ну а вертикальная полоса прокрутки — не слишком высокая цена за полноценный доступ к Сети в любое время и в любом месте.

Ценность мобильного Интернета можно почувствовать как минимум в двух случаях. Первый — это использование Wi-Fi Интернета дома, когда кто-нибудь из ваших домашних «отобрал» у вас компьютер, а вам в это время что-нибудь нужно в Интернете. А второй — когда вы ведете срочную переписку, находясь далеко от дома и используя лишь ваш КПК и сотовый. Повторюсь, что в качестве соединения с сотовым сейчас удобнее всего использовать Bluetooth, хотя и инфракрасный порт еще имеет право на жизнь.

А сейчас, раз уж речь зашла о мобильном доступе в Интернет, мы рассмотрим процесс вывода в сеть настольного компьютера или ноутбука с использованием сотового телефона.

15.5. МОБИЛЬНЫЙ ИНТЕРНЕТ

Для выхода в мобильный Интернет мы будем пользоваться сотовым телефоном Motorola C650, который подключен к ноутбуку Samsung P28 с помощью USB-дата-кабеля.

Перед началом использования телефона в качестве модема нужно установить драйверы для него. Лучше всего использовать фирменное программное обеспечение от Motorola, которое поставляется с дата-кабелями. Это программное обеспечение называется Mobile Phone Tools. Помимо драйверов модема оно включает в себя некоторые утилиты для работы с телефоном. Установка программ стандартна — вас проведет через все ее этапы Мастер установки, а вот остальные этапы работы требуют некоторых дополнительных знаний.

После подключения телефона к компьютеру открываем окно **Телефон и модем** на **Панели управления**, а в этом окне — вкладку **Модемы** (рис. 15.32).

На этой вкладке выбираем пункт, соответствующий нашему беспроводному модему (Motorola modem #2), и открываем его **Свойства**. В окне свойств модема, дабы убедиться в том, что он подключен и способен нормально работать, проходим на вкладку **Диагностика** и проводим диагностику модема (рис. 15.33).

Убедившись, что с модемом все в порядке, приступим к его настройке. Выше мы подробно разбирали настройку КПК для доступа к Интернету через GPRS. Рекомендации, которые обычно берутся с сайта сотового оператора или в его сервисном центре, остались точно такими же. Кратко повторю их в этом разделе.

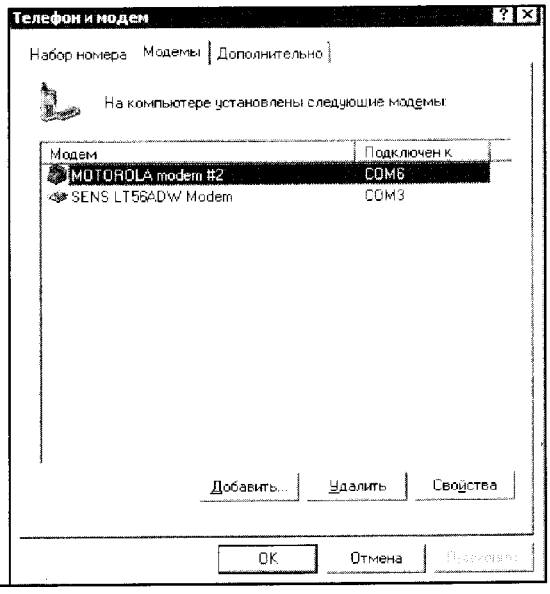


Рис. 15.32. Вкладка Модемы окна Телефон и модем

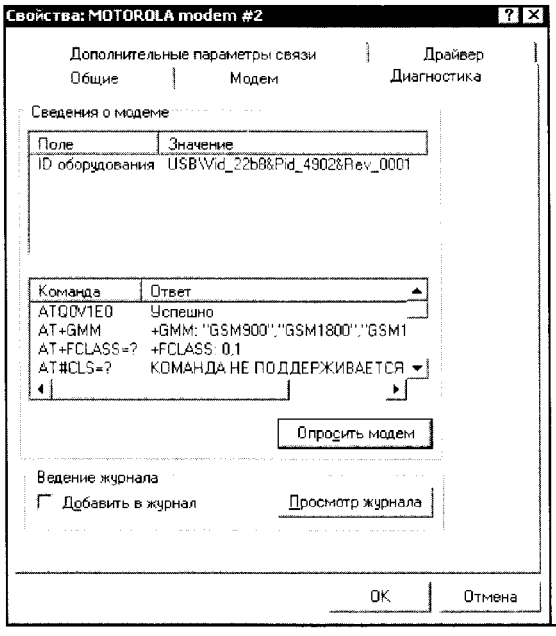


Рис. 15.33.
Успешный опрос модема

Для сотовых телефонов от Siemens, Panasonic, Alcatel и Motorola в строке инициализации модема нужно указать следующее: `AT+CGDCONT=1,"IP","internet.kuban"`. Для подключения используется номер `*99***#`, а если соединение осуществляется через аппарат Siemens — `*99***1#`, набор должен осуществляться тоновым методом. В качестве имени и пароля применяется слово `mts`, написанное строчными буквами. Напомню, что у вас будут другие параметры — все зависит от вашего оператора.

Ввод строки инициализации модема и других параметров обычно вызывает затруднения у начинающих пользователей, поэтому мы рассмотрим их здесь подробно. Собственно говоря, номер и строка инициализации — это то главное, что нужно настроить для того, чтобы получить выход в GPRS-интернет.

Для ввода строки инициализации модема используется вкладка **Дополнительные параметры связи** окна свойств модема (рис. 15.34).

После того как строка инициализации введена, нажимаем **OK** и, пройдя в папку **Сетевые подключения**, которая также доступна из **Панели управления**, запускаем мастер сетевых подключений. То же самое можно сделать, если запустить Internet Explorer, выбрать меню **Сервис ▸ Свойства обозревателя ▸ Подключения** и нажать там кнопку **Добавить**, которая находится в группе параметров **Настройка удаленного доступа и виртуальных частных сетей**.

В обоих случаях нам нужно установить подключение к Интернету (подробности смотрите в одной из предыдущих глав), здесь я рассмотрю лишь ключевые моменты этого процесса.

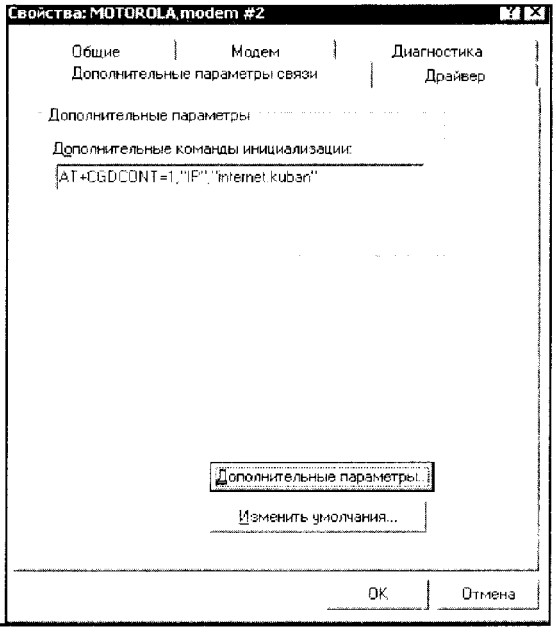


Рис. 15.34. Ввод дополнительных команд инициализации

Так, в качестве номера телефона вводим `*99***#` (рис. 15.35).

Затем, когда появится окно для ввода имени и пароля, вводим и туда, и туда `mts` (рис. 15.36).

В этом же окне снимаем галочку против пункта **Сделать это подключение подключением к Интернету по умолчанию**. Дело в том, что, привыкнув пользоваться обычным модемным соединением и случайно установив умолчание на GPRS-соединение, вы можете незаметно для себя выйти в сравнительно дорогой GPRS-интернет и потратить кучу денег. Но если вы собираетесь пользоваться этим соединением постоянно, галочку можно оставить.

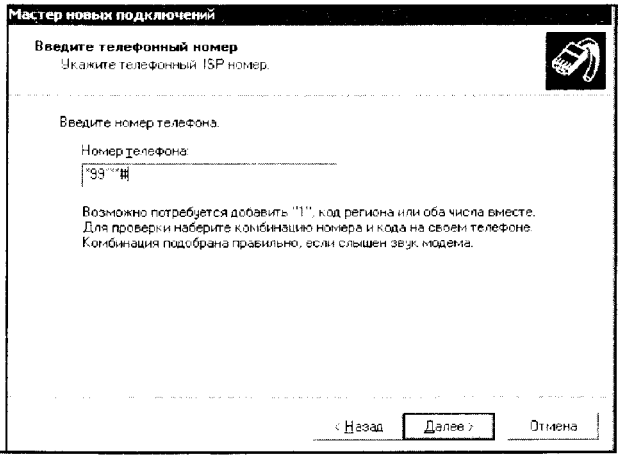


Рис. 15.35. Ввод номера телефона

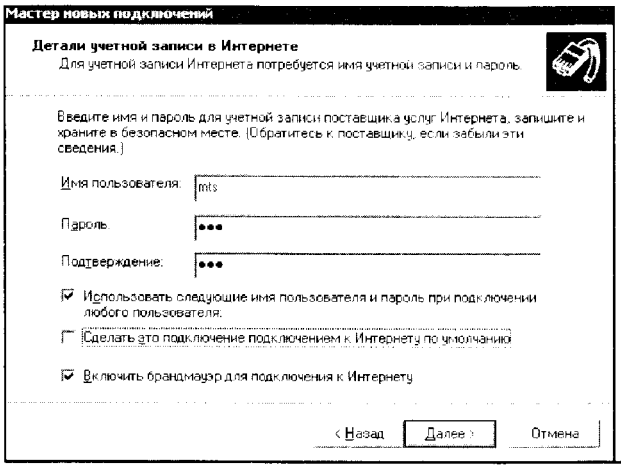


Рис. 15.36. Ввод имени и пароля

Теперь пора протестировать наше соединение. Запускаем Internet Explorer, набираем адрес любимого сайта, выбираем из списка подключений наше новое подключение и начинаем подключаться. За что я люблю GPRS, так это за высокую скорость подключения: многообещающая надпись появляется уже секунды через три (рис. 15.37).

К сожалению, реальная скорость передачи данных в несколько раз ниже, хоть и нельзя назвать ее слишком медленной: при закачке файла с использованием менеджера закачек Flash Get скорость прыгала от 0 до 4,4 Кбит/с, в основном находясь около 2,7 Кбит/с. Обычное *dial-up*-соединение в тех же условиях редко поднимается до 4 Кбит/с. В идеале GPRS-соединение должно достигать скорости 10 Кбит/с, но, видимо, не в наших перегруженных сотовых сетях.

Если в вашем регионе GPRS не слишком дорог, он может стать приемлемой альтернативой другим методам подключения к Сети. К примеру, если вы в течение дня не заняты в Интернете ничем особенным, а лишь периодически проверяете почту (или ваша почтовая программа занимается этим самостоятельно), почему бы не делать это через GPRS? Ведь в GPRS реализована очень полезная схема тарификации за трафик: если вы, подключившись к GPRS-интернету, в течение нескольких часов передадите пару сотен килобайт данных, то платить придется только за эти данные, а не за время вашего пребывания в Сети.

GPRS-соединение с программной точки зрения ничем не отличается от обычного модемного соединения, поэтому к нашему арсеналу мобильных средств полноценного доступа к Интернету добавляется ноут-

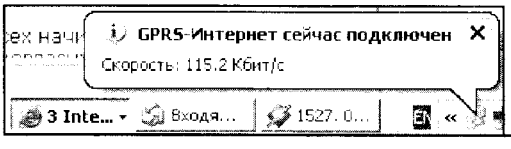


Рис. 15.37. Подключение GPRS-соединения

бук, соединенный с сотовым телефоном. Это уже полноценный доступ к Сети, в отличие от доступа через КПК.

Правда, у карманного компьютера есть бесспорное преимущество: высокая мобильность. Если вы собираетесь в дорогу и не знаете точно, понадобится ли в отъезде ноутбук, вряд ли вы возьмете с собой это дорогое и громоздкое, по сравнению с «карманником», устройство. Ноутбук кажется верхом мобильности, только пока человек не знаком с КПК достаточно хорошо. А карманный компьютер тем и хорош, что он карманный: его можно носить с собой всегда и везде. И если вдруг срочно понадобится доступ к электронной почте, вам поможет КПК. Кроме того, никакому ноутбуку не по силам 5–8 часов автономной работы, которые являются стандартом для большинства КПК.

Кстати, о путешествиях с КПК: для «мобильных путешественников» есть интересная программа, которая может принести пользу при поиске Wi-Fi сетей, а также для проверки доступности вашей Wi-Fi сети в различных частях здания или за его пределами.

Помните, что мы говорили о безопасности беспроводных сетей? Эта программа, которая называется WiFiFoFum, позволяет визуально наблюдать за беспроводными Wi-Fi сетями и делать из наблюдений соответствующие выводы.

15.6. WIFIFOFUM

WiFiFoFum — это сканер беспроводных сетей. Он работает на Windows Mobile 2003. Программа бесплатна, ее можно скачать вот здесь: *http://www.aspecto-software.com/WiFiFoFum/Download.htm*. Дистрибутив занимает около 300 Кбайт.

Программа не требует установки: достаточно просто скопировать ее на КПК. Вместе со всеми программными модулями она занимает около 600 Кбайт памяти «карманника».

Перед запуском программы нужно активировать беспроводной адаптер КПК, а затем щелкнуть по пиктограмме WiFiFoFum. Сразу после запуска WiFiFoFum начинает искать беспроводные сети (рис. 15.38).

Здесь, в табличке, отображаются сведения о найденных сканером беспроводных сетях. Информация о сети содержит много интересного: SSID, тип сети, уровень сигнала, шифрование и некоторые другие параметры. Но табличное отображение информации о сетях — не единственная возможность WiFiFoFum.

В нижней части окна программы есть несколько кнопок. При нажатии кнопки, на которой изображен лист бумаги, на экране появляется таблица найденных беспроводных сетей. Вторая кнопка, на которой изображено нечто вроде экрана радара, открывает окно с этим самым радаром (рис. 15.39).

Такой радар оказывает помощь в поиске «источника» беспроводной сети. Чем ближе значок сети к центру, тем ближе вы к точке доступа или

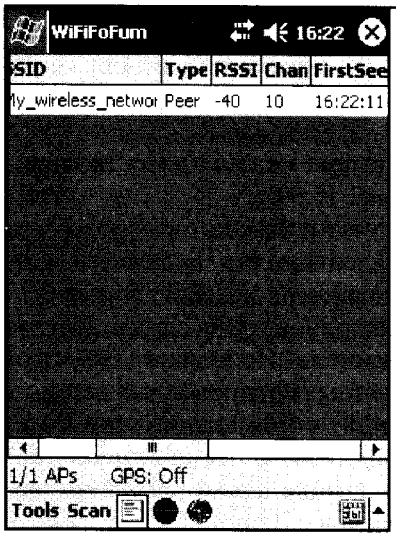


Рис. 15.38. Главное окно WiFiFoFum

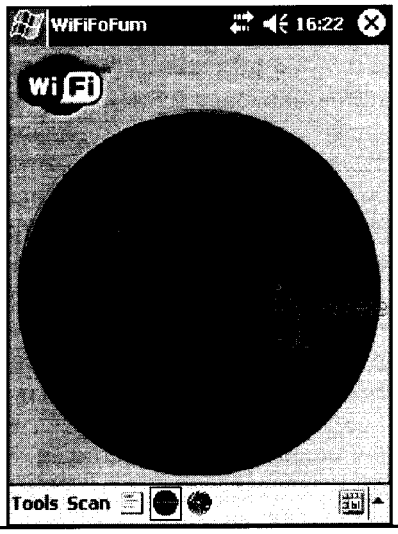


Рис. 15.39. Окно радара

к компьютеру, входящему в беспроводную Ad Hoc-сеть. А число рядом с наименованием сети — это то же самое, что в таблице называется RSSI.

По умолчанию, однако, радар настроен немного «криво». Чтобы это исправить, воспользуемся блоком настроек, который запускается нажатием на третью кнопку в нижней части окна программы (рис. 15.40).

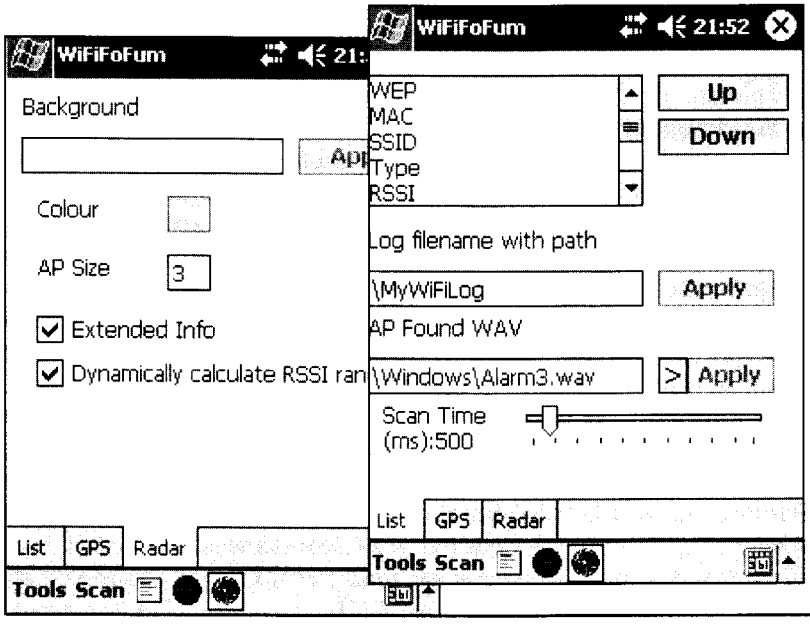


Рис. 15.40. Окна настройки WiFiFoFum

Вкладка **List** окна настройки служит для настройки параметров сканирования (**Scan Time** — периодичность сканирования), отображения и сохранения информации, а вкладка **Radar** (правое окно на рис. 15.40) отвечает за настройки параметров радара. Установив галочки в полях **Extended Info** и **Dynamically calculate RSSI range**, можно привести внешний вид радара к тому, что изображен на рис. 15.39.

Из других установок вкладки **Radar** полезна **Ap Size**, которая позволяет задавать размеры маркера, отмечающего найденные сети. Если сетей много, это значение можно уменьшить, чтобы марки «не мешали» друг другу.

Третью вкладку окна настроек я здесь не привожу. Она служит для настройки подключенного к КПК GPS-приемника. Используя GPS, программа может сохранять координаты найденных беспроводных сетей.

Полагаю, вы самостоятельно сможете найти применение этой интересной программе, а мы рассмотрим еще одну не менее полезную программу, которая делает связь настольного компьютера с КПК еще теснее. Я просто не могу не сказать здесь пару слов о Remote Display Control for Windows CE от Microsoft.

15.7. REMOTE DISPLAY CONTROL FOR WINDOWS CE

Эта программа стирает грани между настольным компьютером и КПК. Представите себе КПК, стоящий в кредле радом с компьютером. Внезапно он понадобился вам на «пару кликов стилусом», — вы берете стилус и начинаете работу. После работы на КПК при помощи стилуса так и хочется ткнуть им в дисплей монитора! Такая же ситуация возникает после перехода от мыши настольного компьютера к «перу» КПК: вот бы «перегнать» мышиный курсор на карманник! Эту мечту поможет осуществить программа от Microsoft, которая называется Remote Display Control for Windows CE.

Поищите эту программу в онлайновых архивах или на *http://www.microsoft.com/downloads*. После установки программы на настольный ПК и на КПК нужно запустить ее на том и на другом. При запуске на настольном компьютере появляется окно, в котором позднее будет виден рабочий стол КПК, а при запуске ее на КПК в на экране настольного компьютера появляется экран карманного, с которым можно работать при помощи мыши. Посмотрите на рис. 15.41. Здесь вы можете видеть диалог, который появляется при запуске программы на КПК.

Нажав на кнопку **Connect**, вы инициируете процесс подключения программы к серверной части, которая в это время должна быть запущена на настольном компьютере (**Пуск ▸ Все программы ▸ Remote display control ▸ Remote display control host**). На рис. 15.42 изображено окно серверной части приложения на настольном компьютере.

Теперь, пользуясь мышью и клавиатурой настольного компьютера, вы можете полноценно управлять вашим КПК.

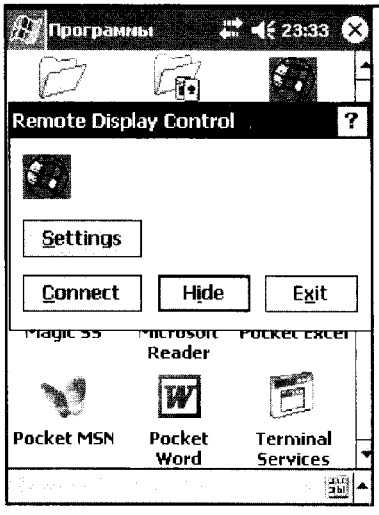


Рис. 15.41. Запуск программы

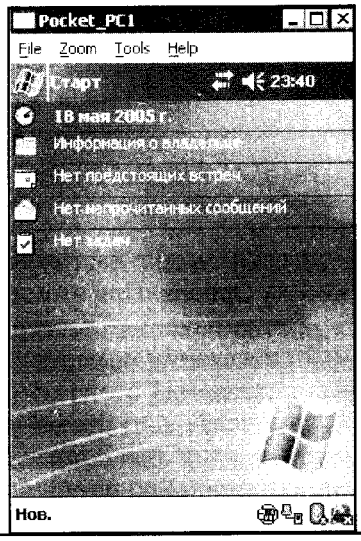


Рис. 15.42. Управление КПК с ПК

Remote Display Control for Windows CE совместима с Windows Mobile 2003, но найти эту программу в архивах удается не без труда. Тем не менее смело рекомендую ее поклонникам карманных компьютеров.

В следующем разделе мы займемся прямо противоположной задачей: приложение, которое мы рассмотрим, позволяет управлять настольным компьютером с помощью карманного.

15.8. PPC TABLET REMOTE CONTROL SUITE

Программа PPC Tablet Remote Control Suite, дистрибутив которой занимает около 1 Мб (*http://amorphous-media.com*), предназначена для превращения КПК в универсальный пульт управления настольным компьютером при условии, что компьютеры связаны Wi-Fiсетью. Таким образом, можно на расстоянии управлять некоторыми функциями настольного компьютера. В сущности, эта программа может выступать в качестве беспроводного Touch-pad'a: она позволяет полноценно управлять передвижениями курсора мыши по экрану настольного компьютера и нажимать на виртуальные кнопки мыши.

PPC Tablet Remote Control Suite поддерживает больше десятка так называемых профилей, оптимизированных под определенные задачи.

Установка вполне стандартна. Серверный модуль устанавливается на настольный ПК, а клиент — на карманный компьютер.

Чтобы воспользоваться программой, достаточно запустить серверный модуль (**Пуск ▸ Все программы ▸ PPC Tablet 2.0 ▸ Run PPC Tablet Server**) (рис. 15.43).

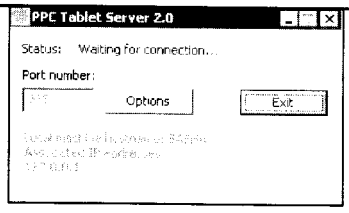


Рис. 15.44. Настройка сервера

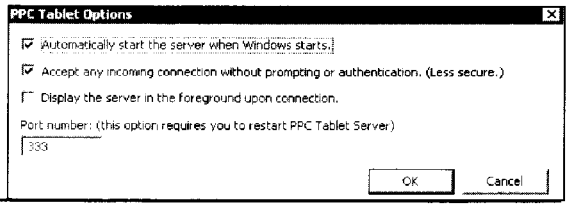


Рис. 15.43. Окно PPC Tablet Server 2.0

Сервер можно настраивать. Для открытия окна настроек нужно нажать кнопку **Options**. При этом появляется окно свойств сервера (рис. 15.44).

По умолчанию сервер ждет входящие соединения на порту 333, но при желании номер порта можно изменить. Если вы хотите постоянно пользоваться этой программой, поставьте галочки против параметров **Automatically start the server when Windows starts (Автоматически запускать сервер при старте Windows)** и **Accept any incoming connection without prompting or authentications (Принимать все входящие соединения без подтверждения или аутентификации)**. Последний параметр нужно устанавливать только в том случае, если в радиусе нескольких сотен метров не наблюдается других КПК с установленной на борту PPC Tablet. Подключение без подтверждения делает работу с программой очень удобной, но при этом снижается защищенность вашей системы от импровизированного «вторжения» со стороны другого владельца КПК.

После того как параметры сервера настроены, переходим на КПК. Здесь нужно запустить программу PPC Tablet Client (**Старт ▸ Програм-**

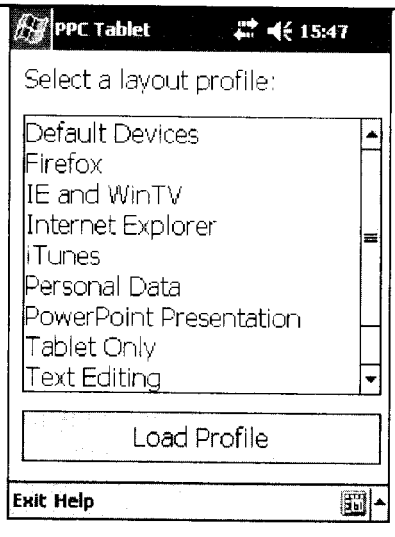


Рис. 15.45. Выбор профиля

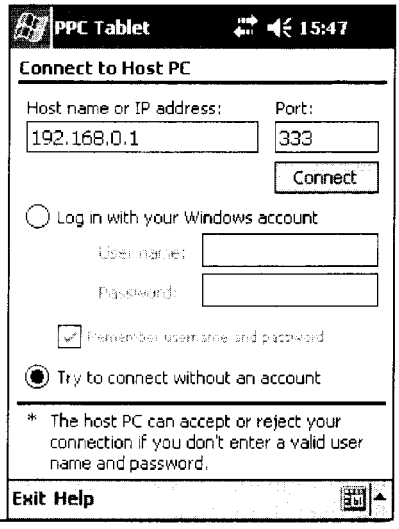


Рис. 15.46. Настройка параметров соединения

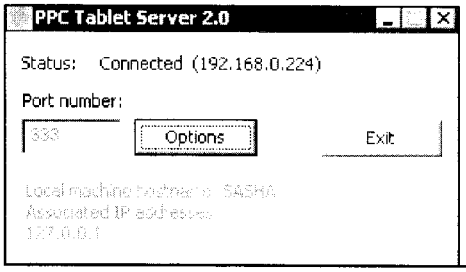


Рис. 15.47. Окно сервера после подключения

мы ▸ **PPC Tablet Client**). Первым делом она спросит о том, какой выбрать профиль (рис. 15.45).

Профили оптимизируют управление определенными программами, и чуть поздней мы посмотрим на внешний вид экранов некоторых из них.

После выбора профиля (пусть, например, это будет **Default Devices**) и нажатия на кнопку **Load Profile** мы попадаем в следующее окно программы, где нужно ввести данные, используемые при подключении к настольному компьютеру (рис. 15.46).

В поле **Host name or IP address** следует ввести IP-адрес или сетевое имя компьютера, на котором мы только что запустили серверную часть программы. В поле **Port** — порт, на котором сервер ждет соединение.

Параметры, которые находятся ниже, понадобятся в случае, если для подключения к компьютеру нужна аутентификация. Если ваша учетная запись защищена паролем, то в поля **User Name** и **Password** нужно ввести соответствующие данные, предварительно установив переключатель из позиции **Try to connect without an account** в позицию **Log in with your windows account**.

После заполнения всех необходимых полей нажмите кнопку **Connect**. Сервер примет соединение, а его окно будет выглядеть примерно так (рис. 15.47).

Вот и все. Теперь, пользуясь средствами загруженного профиля, вы можете управлять вашим компьютером. Например, тот профиль, который мы загрузили немного выше, позволяет управлять курсором мыши (рис. 15.48).

Думаю, здесь все ясно без пояснений. Водя стилусом по Touchpad'у, вы управляете курсором. Нажимая на кнопки **Left** или **Right**, вы словно нажимаете правую и левую клавиши мыши. Нажатия левой кнопки можно сделать и на самом планшете. Нажав кнопку с изображением карандаша, можно переключить программу в режим графического планшета и рисовать в какой-нибудь графической программе. Кнопка с двумя рядами клавиш включает режим ввода цифр.

Меню **Tools** в нижней части окна программы позволяет переключаться на другие профили (**Switch to another profile**), отключаться от хоста (**Disconnect from host**) и настраивать текущий профиль.

Вы сможете найти в этой программе профиль, который покажется вам самым интересным. Самому мне, кроме прочего, очень нравится профиль для управления проигрывателем WinAmp (рис. 15.49).

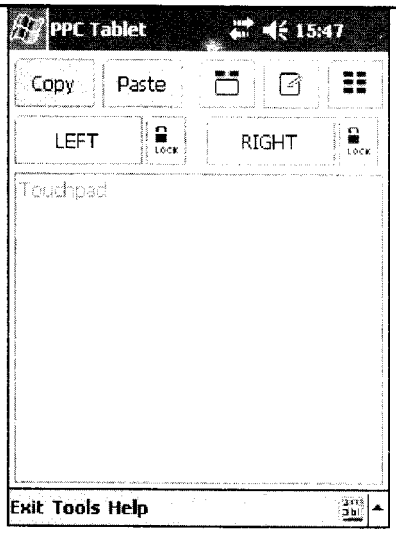


Рис. 15.48. Окно профиля Default Device

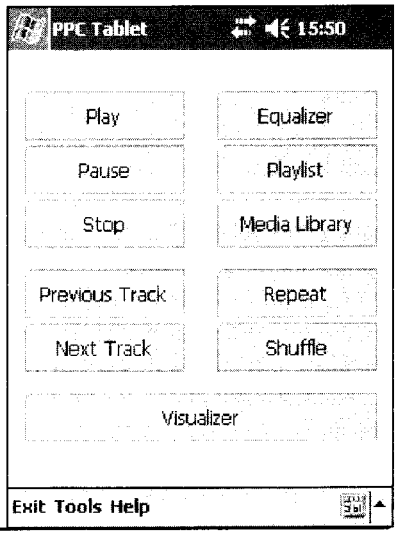


Рис. 15.49. Профиль для управления WinAmp'ом

Здесь не хватает только кнопок для управления громкостью, иначе это был бы полноценный пульт дистанционного управления программой WinAmp.

Программа PPC Tablet Remote Control Suite задумывалась как альтернатива беспроводной мыши и клавиатуре. И свои функции она выполняет весьма достойно, работая стабильно и быстро.

Самая интересная область применения этой программы — презентации, лекции и тому подобные мероприятия, где лектор или рассказчик по ходу действия должен выполнять определенные операции на компьютере. Применение PPC Tablet Remote Control Suite позволит ему свободно перемещаться по аудитории, управляя в то же время ходом презентации.

Обсудив программное обеспечение для КПК, вернемся к вопросам взаимодействия мобильных устройств и обсудим особенности подключения КПК к мобильному телефону по Bluetooth.

15.9. BLUETOOTH-СОЕДИНЕНИЯ

Мы уже немало говорили о Bluetooth, а здесь опишем процесс работы сотового телефона Motorola V535 с КПК Fujitsu-Siemens Pocket LOOX 420 (рис. 15.50).

Общение Bluetooth-устройств начинается с их взаимного обнаружения и последующей аутентификации. После первой аутентификации процедуру для данных устройств повторять не нужно.

В процессе обнаружения сотового телефона карманным компьютером осуществляется извлечение сервисов, а после того как вы захотите воспользоваться каким-нибудь сервисом телефона, будет инициирована процедура аутентификации. При этом происходит следующее. Когда карманный компьютер «видит» сотовый телефон, он «спрашивает», что телефон умеет. Телефон, например, может «ответить» компьютеру, что он умеет передавать файлы и имеет встроенный модем, воспользовавшись которым, КПК может выйти в Интернет. Карманный компьютер запоминает список возможностей мобильника, и на этом все заканчивается — до тех пор, пока «карманнику» не понадобятся сервисы сотового.

К примеру, вы впервые захотели скачать фотографии, отснятые камерафоном, на КПК. Прежде чем сотовый телефон позволит вам управлять файлами, хранящимися в нем, он проведет «проверку личности» (аутентификацию), чтобы убедиться в том, что КПК, который хочет с ним соединиться, это ваш КПК. Если аутентификация прошла успешно, вы получаете доступ к ресурсам сотового телефона с использованием КПК.

Итак, обсудив теорию, приступаем к практике.

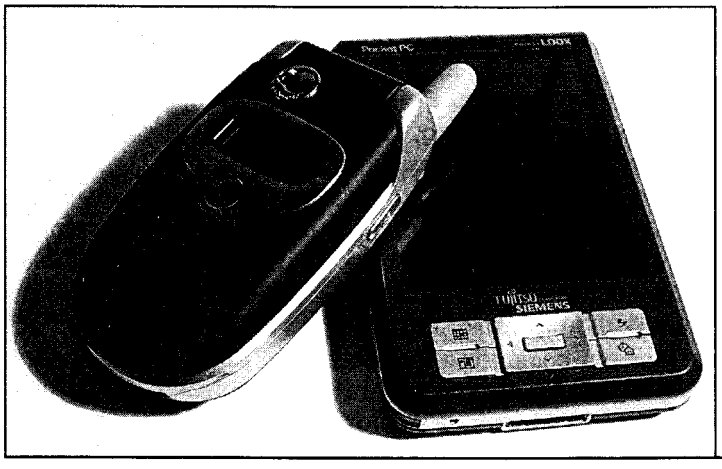


Рис. 15.50. Сотовый телефон и КПК

Для начала активируем Bluetooth на КПК. В нашем случае для этого достаточно щелкнуть по значку **Bluetooth** в нижней части домашнего окна карманного компьютера и выбрать в появившемся меню пункт **Вкл. Bluetooth**. После этого включите BT на мобильнике. Теперь из того же меню на КПК выберите пункт **Диспетчер Bluetooth** (здесь можно было выбрать **Диспетчер Bluetooth** напрямую, и BT-адаптер был бы включен автоматически) и в появившемся окне диспетчера щелкните по пункту меню **Нов**. Появится окно Мастера Bluetooth-соединений (рис. 15.51).

В нашем случае устройства «знакомятся» впервые, поэтому выберите пункт **Установить Bluetooth устр-во**. Так вы сможете обнаружить сервисы, предоставляемые устройством, и создать ярлыки соединений, то есть осуществить первичную настройку нашей системы.

Рис. 15.51. Окно мастера Bluetooth-соединений

Рис. 15.52. Выбор сервиса для создания ярлыка

После выбора пункта **Установить Bluetooth устр-во** начинается поиск устройств. Компьютер находит мобильный телефон и отображает сервисы, которые может предоставить ему аппарат (рис. 15.52).

В нашем случае это **Dial-up networking Gateway** и **OBEX file Transfer**. Первый сервис предоставляет возможность выхода в GPRS-интернет с помощью встроенного модема трубки, а второй позволяет обмен файлами между устройствами. Создаем ярлыки этих соединений, и в результате окно **Менеджера Bluetooth** принимает вид, изображенный на рис. 15.53.

После того как ярлыки соединений добавлены, можно попытаться установить соединение с телефоном, активировав, например, службу передачи файлов. Длинным нажатием на значок **Motorola Phone: OBEX file transfer** вызовите меню, из которого можно запустить эту службу.

Когда КПК в первый раз запросит подключение к мобильнику, телефон оповестит вас об этом, задав вопрос о разрешении или запрещении такого подключения. Ответьте на вопрос о подключении положительно. После начала процедуры первого подключения телефон и КПК нужно будет «познакомить», введя так называемые Bluetooth-ключи. Такой ключ обычно состоит из нескольких цифр, в нашем случае из четырех (рис. 15.54).

Вы должны ввести одинаковые ключи на телефоне и КПК (телефон тоже запросит ввод ключа). Если все прошло хорошо, вы сможете взаимодействовать с телефоном.

Эта процедура проводится однократно. Как вы помните, мы инициировали процедуру аутентификации телефона и КПК путем запуска сервиса для обмена файлами. Теперь на карманном компьютере можно про-

сматривать файловую систему телефона, копировать файлы между телефоном и компьютером, удалять их из телефона и так далее.

Вы заметили, во что превратились современные сотовые телефоны? Даже не смартфоны, которым сам бог велел быть похожими на компьютеры, а самые обычные мобильники. Та же Motorola V535, да и любой аппарат этого класса похож на устройство, применяемое героем какого-нибудь фантастического рассказа, написанного в недалеком прошлом. А мы ведь ко всему этому привыкли и отучились удивляться возможностям современных умных устройств.

На рис. 15.55 изображено окно, обеспечивающее доступ к файлам и папкам сотового.

Если вы добрались до этого места моего рассказа, то сможете разобраться с файлами самостоятельно. К примеру, можно копировать файлы с телефона в локальную папку на КПК (название этой папки видно в нижней части рис. 15.55).

Точно так же, скопировав файл с КПК, вы можете вставить его в одну из папок аппарата. Это неплохой способ закачки в аппарат мелодий и картинок, а также выгрузки из телефона фотографий и видеоклипов. По крайней мере, если вы оказались вдалеке от стационарного компьютера, а под рукой есть только КПК и мобильник, то память телефона можно освободить от переполнения интересными кадрами.

Передача файлов — интересное занятие, но есть дела поважнее: к примеру, настройка доступа в Интернет через Bluetooth. Она ничем не отличается от настройки доступа в Интернет с использованием инфра-

Рис. 15.53. Диспетчер Bluetooth после настройки

Рис. 15.54. Ввод Bluetooth-ключа

красного порта. Здесь я лишь расскажу о практических преимуществах такого подхода к мобильному Интернету и напомню основные направления такой настройки.

Инфракрасный порт хорош как интерфейс для связи мобильника и КПК до тех пор, пока вы не попытаетесь использовать эту связку, скажем, в транспорте. Одно неосторожное движение — и коннект потерян. Можно изловчиться, устойчиво расположить «карманник» и сотовый и попытаться попутешествовать в таком состоянии по Интернету, но это не слишком удобно. Другое дело — Bluetooth. Телефон может лежать где-нибудь в сумке или в вашем кармане, а Интернет все равно будет работать. Более того, будет он работать и метров за десять от вашего сотового. Это очень удобно, поэтому, повторюсь, попробовав Bluetooth, вы вряд ли захотите вернуться к инфракрасному порту.

Для настройки Bluetooth-подключения к Интернету следует выбрать соответствующее устройство в списке устройств, предназначенных для подключения КПК к Интернету (рис. 15.56), а все остальное вы уже читали немного выше — там, где мы подключались к Сети через инфракрасный порт.

С настройкой интернет-соединения проблем у вас быть не должно. Оно аналогично вышеописанному подключению с использованием инфракрасного порта.

Перед окончанием «мобильной» главы хочу рассказать вам, как показать человеку, имеющему смутное представление о беспроводных технологиях связи, их возможности. Такая демонстрация обычно оставляет неизгладимое впечатление.

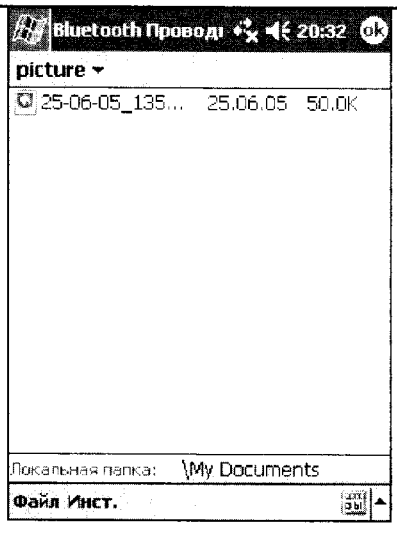


Рис. 15.55. Работа с файлами и папками сотового телефона

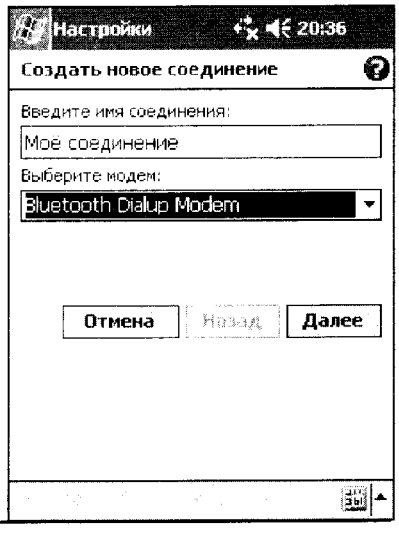


Рис. 15.56. Выбор Bluetooth-модема для подключения к Интернету

Возьмите мобильный телефон с камерой и Bluetooth-адаптером, «карманник», оснащенный Bluetooth и Wi-Fi, и обычный компьютер или ноутбук с Wi-Fi адаптером. Посадите перед компьютером своего знакомого и предложите ему по вашему сигналу открыть какую-нибудь папку, которая до этого была абсолютно пуста. Только не забудьте открыть общий доступ к этой папке и разрешить изменение файлов по сети.

Теперь возьмите телефон и сфотографируйте сидящего за компьютером человека. Активируйте в телефоне Bluetooth и положите аппарат куда-нибудь подальше. Затем, взяв в руки КПК, сядьте поудобнее в мягкое кресло и начните комментировать то, что вы делаете. «Подключаюсь к сотовому по Bluetooth». — «Скачиваю на «карманник» твою фотографию». — «Скачал». — «Подключаюсь к компьютеру по WiFi». — «Захожу в папку, о которой я тебе говорил». — «Копирую в нее твою фотографию». — «А теперь можешь попробовать ее открыть». — «Узнаешь?».

Я уверен: тот, кто слушал ваши речи и смотрел на демонстрацию возможностей беспроводной связи, уже никогда не забудет того, что ему довелось увидеть. Но, прежде чем проводить такую демонстрацию, настройте все беспроводные коммуникации и проверьте их работу, иначе вместо красивой сцены на тему wireless-технологий вы рискуете показать неискушенному в беспроводных вопросах зрителю спектакль с названием: «Подожди минутку, сейчас заработает».

15.10 ВЫВОДЫ

Теперь вы сможете полноценно использовать ваш КПК в локальной беспроводной сети. Мы рассмотрели здесь лишь малую часть доступных программ для карманных компьютеров. При желании вы сможете сделать из своего «карманника» практически все что угодно: IP-телефон, ICQ-терминал и так далее. Главное — владеть информацией о первоначальной настройке сетевых подключений.

А теперь мы возвращаемся в Windows XP: следующая глава посвящена тонкостям ее настройки.

ГЛАВА 16
WINDOWS XP: ТОНКОСТИ СЕТЕВОЙ НАСТРОЙКИ

Пришел черед одной из самых интересных глав во всей книге, посвященной тонкостям сетевой настройки Windows XP. Здесь мы коснемся некоторых продвинутых методик управления сетями в Windows XP: займемся реестром ключей, оптимизируем интернет-соединение путем тонкой настройки TCP/IP и превратим компьютер в маршрутизатор. При этом мы воспользуемся средствами, которые разработчики Windows спрятали довольно глубоко: их нередко приходится запускать при помощи командной строки.

Разные средства управления компьютером, и особенно те, что запускаются при помощи команд **Пуск ▸ Выполнить**, всегда таят опасность и могут довести вашу систему до краха. И если кто-нибудь из читателей станет излишне вольно или просто неаккуратно обращаться с реестром Windows, он столкнется с самыми серьезными проблемами. Не сочтите мои слова за запугивание, но, занявшись редактированием реестра, всегда будьте готовы к тому, что систему придется восстанавливать. Это означает, что перед тем, как приступить к работе, следует сделать копию реестра и надежно сохранить важные для вас данные. Полагаю, что, если вы будете точно следовать инструкциям, никаких случайностей не произойдет, но встречать возможные неприятности лучше во всеоружии.

16.1. РЕЕСТР

Если обойтись без преувеличений и громких слов, то реестр можно определить как фундамент, на котором стоит Windows. Это огромная база данных, хранящая различные конфигурационные настройки. Если с реестром что-нибудь случится, система работать не сможет. Что бы пользователь ни делал в Windows, в этих действиях всегда принимает участие реестр. Вы сделали двойной щелчок по значку файла — и Windows спрашивает у реестра, с помощью какой программы открывать этот файл. При установке любой программы она делает запись в реестр. В реестре также хранятся профили пользователей, сведения об установленном оборудовании и так далее.

Иногда создается впечатление, что Microsoft пытается защитить реестр от неопытных пользователей. В справочной системе Windows можно найти лишь самые общие сведения о реестре, то есть данные о его структуре и о редакторе реестра, но описаний конкретных параметров реестра там нет. К тому же, чтобы запустить редактор реестра, надо воспользоваться командой **Пуск ▸ Выполнить**, а в окне **Выполнить** написать имя файла редактора реестра `Regedit` — а это, согласитесь, означает, что пользователь, запускающий редактор реестра, должен обладать определенными знаниями.

Разработчики Windows правы: если каждый будет исследовать реестр своего компьютера, то компьютерные сервисные центры просто утонут в трудах по восстановлению системы. Реестр — один из самых незащищенных объектов Windows, и его очень легко повредить.

Чтобы своими глазами посмотреть на различные части реестра, рассмотрим его редактор.

ЗАПУСК РЕДАКТОРА РЕЕСТРА

Чтобы запустить редактор реестра, выполните последовательность команд **Пуск ▸ Выполнить** и в поле окна **Выполнить** введите **regedit**. На экране появится окно редактора реестра (рис. 16.1).

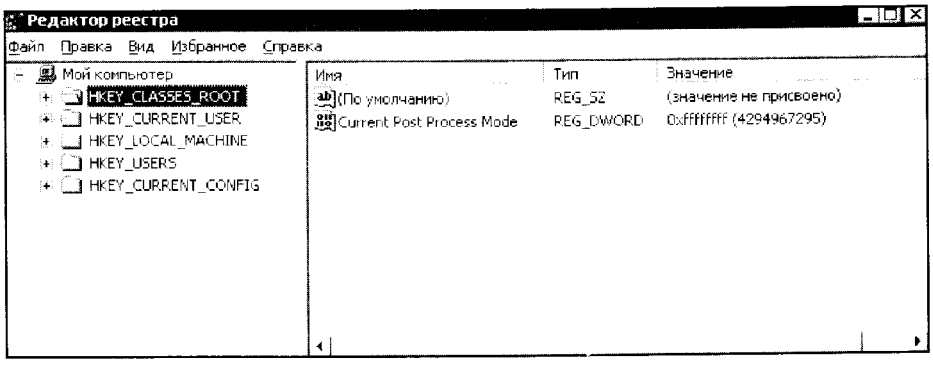


Рис. 16.1. Окно редактора реестра

СТРУКТУРА РЕЕСТРА

Внешне реестр напоминает **Проводник Windows**: слева — иерархическая структура папок, справа — содержимое этих папок.

Левая панель редактора называется **панелью разделов** (или **ключей**), правая — **панелью параметров** (или **значений**).

Работа с панелью разделов аналогична работа с файловой системой в **Проводнике**. Ключи реестра видны в панели разделов, похожи на пап-

ки Windows. Они, точно так же как папки, могут быть вложенными, а имена ключей реестра подчиняются тем же правилам, что и имена папок Windows.

В реестре, как и в файловой системе, существует понятие пути. Но в файловой системе путь всегда ведет к файлу, а в реестре путь может вести к параметру или к другому разделу реестра.

В правой части окна реестра отображаются параметры, хранящиеся в ключах реестра. Эти параметры очень похожи на файлы, хранящиеся в папках Windows. Параметры имеют определенную структуру: у параметра реестра есть имя, тип и значение.

Именование параметров реестра аналогично именованию ключей: в одном ключе не может быть двух параметров с одинаковым именем.

Тип параметра определяет тип данных, хранящихся в параметре. Реестр может хранить данные различных типов, но здесь мы рассмотрим наиболее распространенные. К примеру, тип **REG_BINARY** означает двоичное значение (рис. 16.2). Но, каким странным это вам ни покажется, параметр реестра **REG_BINARY** редактируется в шестнадцатеричной системе счисления.

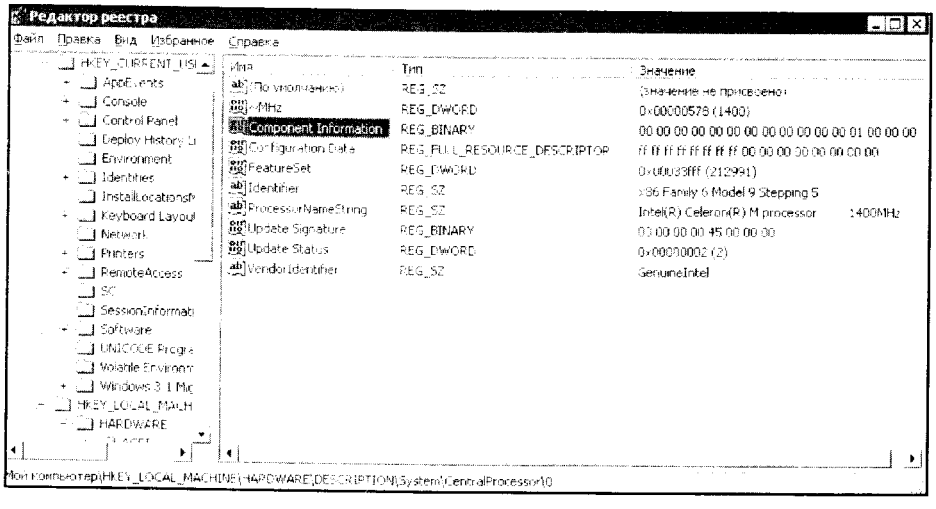


Рис. 16.2. Параметры реестра различных типов

Для быстрого перевода двоичных чисел в шестнадцатеричные и наоборот можно воспользоваться стандартным калькулятором Windows. Введя число, к примеру, в шестнадцатеричном виде и переключив систему счисления на двоичную, вы тем самым переведете число из шестнадцатеричной системы счисления в двоичную.

Следующий популярный в реестре тип параметра — **REG_SZ**, то есть текстовая переменная постоянной длины. В таких переменных

хранятся различные наименования (например, параметр **Vendor Identifier** на рис. 16.2 содержит значение **Genuineintel**). Есть еще тип **REG_MULTI_SZ** — параметр этого типа содержит список строк.

Еще один тип параметра называется **REG_DWORD** и хранит значение длиной в 32 бита, то есть двойное слово. В таких переменных можно встретить, например, численные выражения каких-нибудь параметров (например, параметр ~MHz с рис. 16.2 содержит значение 0 × 00000578 в шестнадцатеричной записи, или 1400 в десятичной). Параметры типа **REG_DWORD** часто содержат числа, характеризующие время выполнения какого-либо процесса (например, частоту мигания курсора или что-то подобное). Время измеряется в миллисекундах (1000 миллисекунд равны 1 секунде). Вводить данные **REG_DWORD** можно как в шестнадцатеричном, так и в десятичном виде.

Параметр типа **REG_FULL_RESOURCE_DESCRIPTOR** содержит список драйверов или ресурсов устройства. **Редактировать параметры этого типа НЕЛЬЗЯ.**

Мы не будем рассматривать остальные типы параметров реестра, так как они встречаются довольно редко, а для наших задач и вовсе не понадобятся. Ну а вывод вы можете сделать самостоятельно: значение параметра реестра — это хранящиеся в нем данные определенного типа.

Физически реестр хранится в нескольких файлах на жестком диске компьютера. Логически реестр состоит из разделов, подразделов, кустов и записей реестра.

Куст — это файл на жестком диске, содержащий часть реестра.

КОРНЕВЫЕ КЛЮЧИ РЕЕСТРА

Теперь поговорим о корневых ключах реестра, которые отображаются на экране сразу после запуска редактора реестра (рис. 16.3). Все пять корневых ключей мы рассматривать не будем и остановимся на тех, что для нас наиболее интересны. Это ключи **HKEY_USERS**, **HKEY_CURRENT_USER** и **HKEY_LOCAL_MACHINE**.

Ключ **HKEY_USERS** содержит информацию о пользовательских настройках.

Ключ **HKEY_CURRENT_USER** содержит настройки так называемого консольного пользователя, то есть пользователя, который в данный момент работает с системой. Если вы вошли в систему под своей учетной записью, это значит, что ключ **HKEY_CURRENT_USER** будет содержать ваши настройки. Это важный ключ реестра, и на его подразделах мы остановимся подробнее (рис. 16.4).

- Подраздел **AppEvents** содержит информацию о том, какие звуки должны сопровождать те или иные системные события.

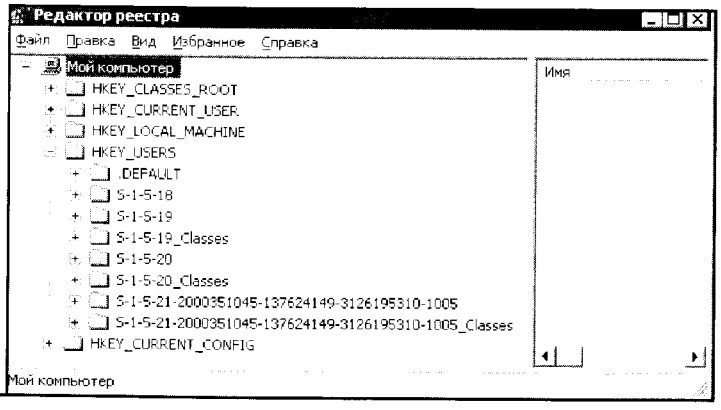


Рис. 16.3. Корневые ключи реестра

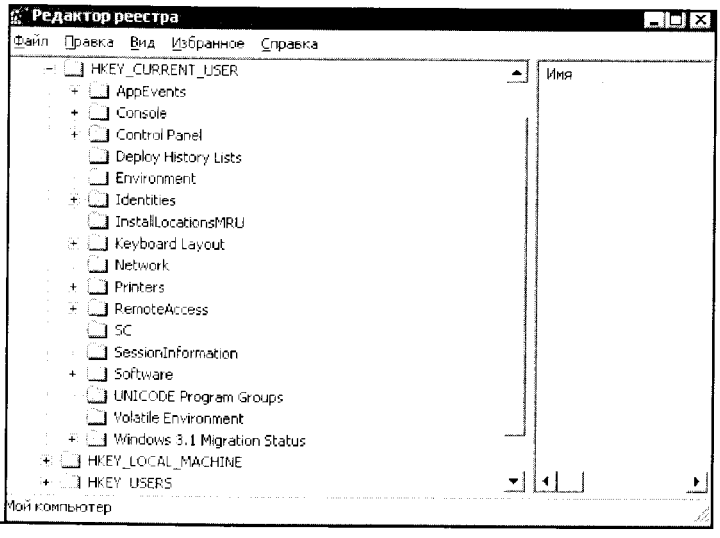


Рис. 16.4. Подразделы ключа HKEY_CURRENT_USER

- Подраздел **Console** содержит настройки подсистемы консольных приложений. Например, в соответствии с установками этого раздела работает командная строка MS DOS.
- В подразделе **Control Panel** хранятся настройки рабочего стола и некоторые другие настройки. Интересно, что одни из настроек этого подраздела можно настраивать только при помощи редактора реестра, а другие — при помощи средств **Панели управления** Windows.

Как видите, средства для настройки параметров Windows — это лишь «надстройки» над реестром, которые умеют работать с определенными ключами и параметрами реестра.

- Подраздел **Environment** содержит так называемые переменные окружения. Обычно это пути к определенным папкам, хранящим какие-то данные. Каждый такой путь имеет имя (фактически — имя параметра). Это имя используется системой в различных командах, а вместо имени подставляется путь, заданный значением параметра.

- Подраздел **Identities** содержит подключи учетных записей Outlook Express и хранит настройки каждого пользователя. Дело в том, что Outlook Express позволяет создавать несколько профилей пользователя, чтобы этим почтовым клиентом могли пользоваться несколько человек под одной учетной записью. На практике эта возможность Outlook Express применяется крайне редко: гораздо логичнее создать каждому пользователю компьютера отдельную учетную запись для входа в Windows.
- В подразделе **Keyboard Layout** содержатся данные о раскладках клавиатуры.
- Подраздел **Network** включает в себя данные о подключенных к системе сетевых дисках.
- Подраздел **Printers** содержит информацию о пользовательских настройках принтеров.
- Подраздел **Software** хранит сведения о настройках приложений, а подраздел **System** — наборы настроек Windows XP.

Теперь рассмотрим ключ **HKEY_LOCAL_MACHINE** (рис. 16.5). Этот ключ содержит настройки компьютера, общие для всех пользователей.

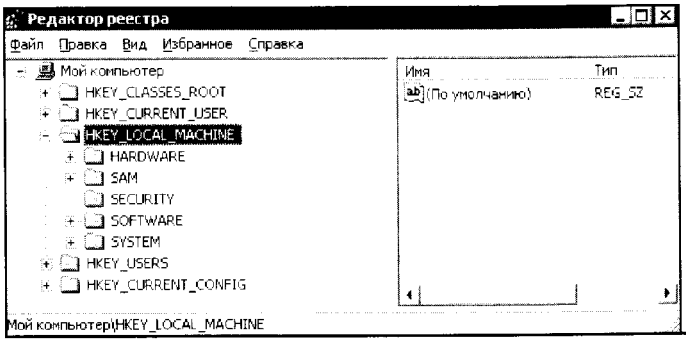


Рис. 16.5. Подразделы ключа HKEY_LOCAL_MACHINE

- Подраздел **Hardware** содержит данные о настройках устройств, об их драйверах и об используемых ресурсах.
- Подраздел **Sam** хранит базу данных локальных пользователей и групп.
- Подраздел **Software** хранит общие настройки программного обеспечения, а подраздел **Software** — наборы настроек Windows XP.

Разобравшись со структурой реестра, переходим к редактору реестра.

РАБОТА В РЕДАКТОРЕ РЕЕСТРА

Работа в редакторе реестра напоминает работу в **Проводнике Windows**, а перемещение по разделам и подразделам похоже на перемещение по папкам.

Для редактирования параметров реестра дважды щелкните по наименованию параметра. Появится окно для редактирования (рис. 16.6).

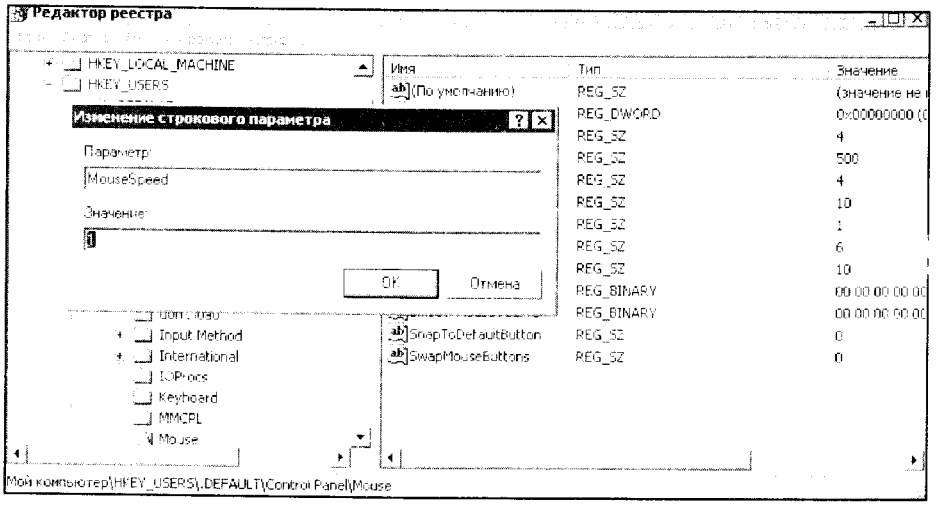


Рис. 16.6. Редактирование параметра реестра

Прежде чем редактировать параметры реестра, сделайте его резервную копию. Для этого выберите меню **Файл ▶ Экспорт**. В появившемся окне (рис. 16.7) выберите параметр **Весь реестр** и, задав имя файлу реестра, сохраните его. Так вы обезопасите себя от неприятностей, связанных с редактированием параметров реестра. Если, исправив или удалив какой-нибудь параметр, вы поймете, что система стала работать хуже, можно вернуться к исходному состоянию реестра, импортировав его из заранее сделанной копии (**Файл ▶ Импорт**).

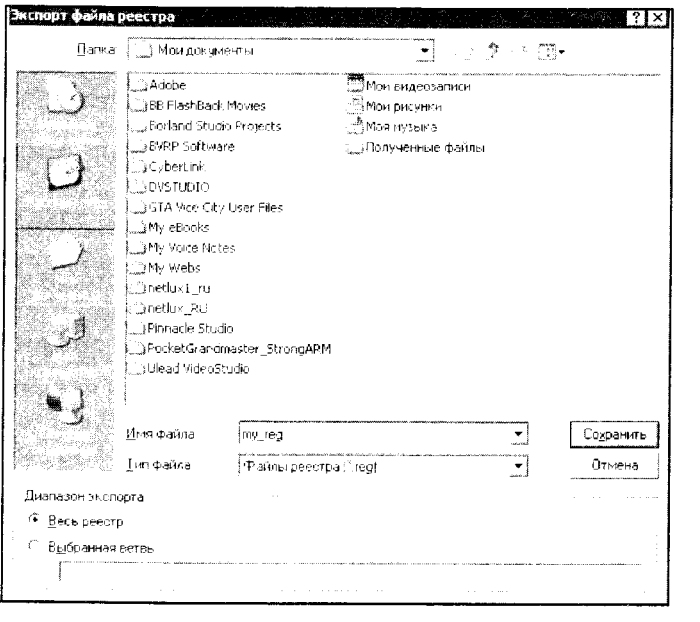


Рис. 16.7. Сохранение реестра

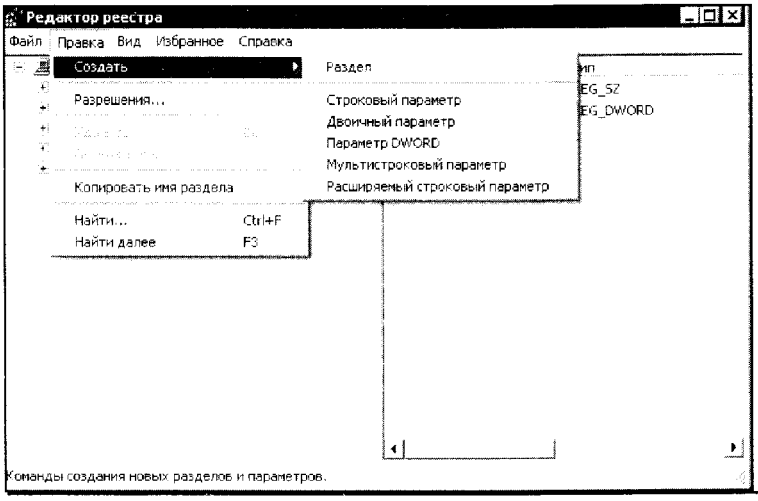


Рис. 16.8. Создание нового параметра

При редактировании реестра может понадобиться создать новые параметры. Для этого существует меню **Правка ▸ Создать** (рис. 16.8).

В меню **Правка** существует полезная команда **Найти**. С ее помощью легко искать конкретные значения параметров, сами параметры или разделы реестра.

НАСТРОЙКА TCP/IP

Настройка TCP/IP средствами реестра (начало)

Изучив сведения, изложенные в этом разделе, вы сможете самостоятельно оценивать информацию, связанную с редактированием реестра, и успешно применять его на практике.

Рассмотрим параметры реестра, отвечающие за настройку TCP/IP.

При написании этого материала были использованы некоторые данные с *http://www.speedguide.net*.

Стандартными средствами Windows тонкую настройку TCP/IP осуществлять нельзя, а средствами реестра — можно.

Настройки TCP/IP собраны в подразделе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip**. Кстати сказать, программы для оптимизации интернет-соединений оптимизируют параметры, которые расположены в этом разделе реестра.

Для начала рассмотрим подраздел **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** (рис. 16.9). Здесь собраны параметры TCP/IP.

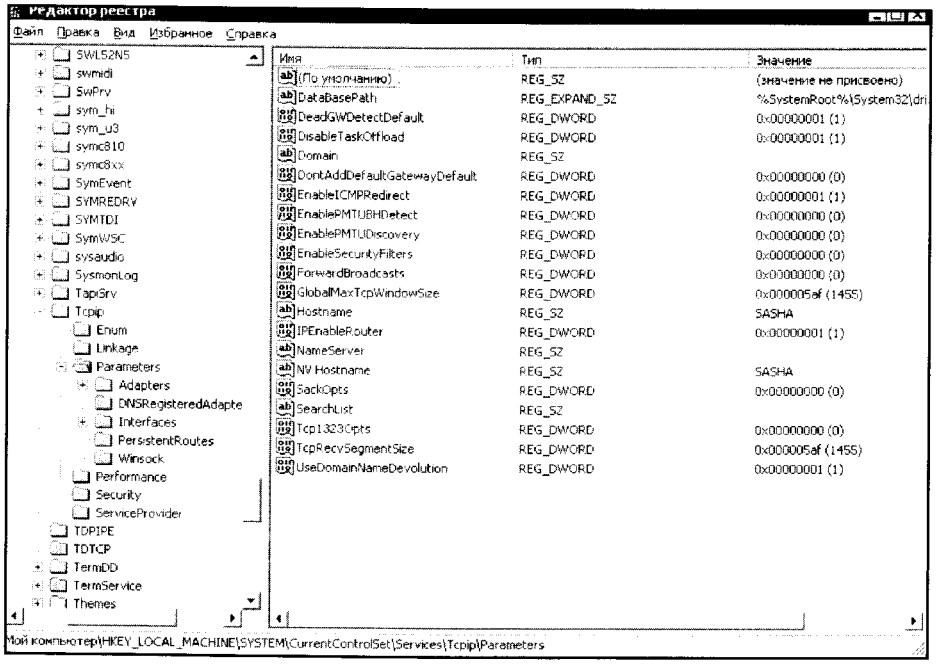


Рис. 16.9. Настройка параметров TCP/IP

Нам с вами особенно интересны параметры, отвечающие за размер скользящего окна TCP, а также TTL, MTU и некоторые другие. Мы не рассматривали эти параметры при обсуждении TCP/IP, поэтому остановимся на них подробнее.

Размер скользящего окна — это количество кадров или байтов, которое может быть передано без получения подтверждения. Когда размер окна равен одному кадру, система вынуждена ждать подтверждение приема этого кадра, чтобы отправить получателю следующий кадр данных. Механизм скользящего окна позволяет, передав один пакет, передавать остальные, входящие в состав последовательности кадров, называемой окном. Принимающая система может отправлять подтверждения не на каждый принятый кадр, а только на последний из них, если предыдущие кадры приняты.

Рассмотрим пример работы скользящего окна с размером, скажем, 10 пакетов и — для примера — не встречающуюся на практике ситуацию, когда данные передаются по одному пакету и система ждет подтверждения приема каждого кадра, приостановив на время ожидания передачу данных.

Пусть имеется некоторая последовательность пакетов, состоящая, скажем, из 100 пакетов. Размер скользящего TCP-окна пусть будет равен 1 пакету. Система начинает передавать пакеты, и передача останавливается после каждого переданного пакета — до получения подтверждения его приема принимающей стороной. Когда подтверждение получено

(или истек тайм-аут ожидания подтверждения — в таком случае пакет передается заново), передается следующий пакет. Линия связи при этом используется нерационально: между отправкой пакета и приемом подтверждения проходит некоторое время, в течение которого линия передачи данных простаивает.

Теперь увеличим размер скользящего окна до 10 пакетов. Система передает первый пакет и, не дожидаясь прихода подтверждения, начинает передавать остальные пакеты, находящиеся в пределах 10-пакетного окна. Пусть, например, когда передается 5-й пакет, система получает подтверждение на 1-й и так далее. Когда система получает подтверждение на 1-й пакет, она «сдвигает» окно на 1 пакет и теперь может передавать пакеты с номерами от 2 до 11 без ожидания подтверждения. В результате линию передачи данных удается нагрузить по полной программе, и она при этом не простаивает, ожидая подтверждения приема каждого пакета перед передачей следующего. В реальных сетях размеры окон немного другие, но принципы действия этого механизма сохраняются.

Традиционно считается, что использовать большие окна можно на надежных линиях связи: ошибки происходят редко, повторные передачи тоже случаются нечасто, и большой размер окна позволяет достичь максимальной эффективности передачи данных. А на ненадежных сетях размер окна нужно уменьшать, так как частые повторные передачи сведут на нет выгоды большого TCP-окна.

Теперь рассмотрим установки параметров реестра, отвечающие за размер TCP-окна.

В разделе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** есть параметр **TCPWindowSize**. Если на вашем компьютере его нет, этот параметр вы должны создать самостоятельно. Параметр имеет тип **REG_DWORD**.

Этот параметр содержит размер скользящего окна TCP. На сайте *http://www.speedguide.net* отмечено, что параметр **TCPWindowSize** для достижения максимальной эффективности должен в несколько раз превышать размер максимального сегмента (MSS — *Maximum Segment Size*).

MSS обычно вычисляется как (MTU — 40), где MTU (*Maximal Transfer Unit*) — максимальный размер пакета, который может быть передан по сети. MTU обычно не превышает 1500 байт.

Установка размера окна выглядит так: следует создать параметр **TCPWindowSize** и установить в желаемый размер окна, который назначают в интервале от MSS до 2^{30} байт.

Точно так же можно отредактировать параметр **GlobalMaxTcpWindowSize**. Этот параметр принадлежит к типу **REG_DWORD** и содержит размер окна в байтах.

Обратите внимание на параметр **TCP1323Opts**. Он нужен для того, чтобы разрешить использование TCP-окон размером больше 64 Кбайт. Чтобы активировать поддержку больших окон, установите этот параметр равным единице.

Узнать размер вашего MTU можно, воспользовавшись командой Ping. Например, вот что выдала эта команда на моей системе (листинг 16.1).

```
C:\Documents and Settings\1>ping -f -l 1500 www.yandex.ru

Обмен пакетами с www.yandex.ru [213.180.204.11] по 1500 байт:

Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.

Статистика Ping для 213.180.204.11:
Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),

C:\Documents and Settings\1>ping -f -l 1472 www.yandex.ru

Обмен пакетами с www.yandex.ru [213.180.204.11] по 1472 байт:

Ответ от 213.180.204.11: число байт=1472 время=715мс TTL=112
Ответ от 213 180.204.11: число байт=1472 время=203мс TTL=112
Ответ от 213.180.204.11: число байт=1472 время=191мс TTL=112
Ответ от 213.180.204.11: число байт=1472 время=180мс TTL=112

Статистика Ping для 213.180.204.11:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 180мсек, Максимальное = 715 мсек, Среднее = 322 мсек

C:\Documents and Settings\1>ping -f -l 1473 www.yandex.ru

Обмен пакетами с www.yandex.ru [213.180.204.11] по 1473 байт:

Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.

Статистика Ping для 213.180.204.11:
Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),
```

Листинг 16.1. Использование команды Ping для выяснения размера MTU

Сначала я запустил Ping с указанием использовать размер пакета в 1500 байт (это явно много) и обмениваться пакетами с сервером www.yandex.ru. Появилось сообщение об ошибке. Затем я запустил тот же Ping, но с размером пакета 1472 байта — команда прошла успешно. А при 1473 байтах снова было выдано сообщение об ошибке. Получилось, что 1472 байта — это реальный размер максимального нефрагментируемого пакета в моей системе.

К размеру пакета надо прибавить 28, тогда мы получим размер MTU. В моем случае это 1500. Если вы не знаете вашего MTU, попробуйте исследовать диапазон размеров пакетов, каждый раз деля его на два. Например, пусть сначала это будет 1472, если вы получили сообщение об ошибке — попробуйте взять 736, ну а если `Ping` с этим параметром выдаст ошибку, дальше можете не искать: даже 736 байт — это слишком мало, и такой (736+28) MTU может стать причиной замедления работы вашего интернет-соединения.

При этом нельзя забывать о том, что многое зависит от качества вашего интернет-соединения. Встречается мнение, что оптимальным для *dial-up*-соединения является MTU в 576 байт.

Изменения, которые вы вносите в конфигурацию TCP/IP, нужно проверять, к примеру, путем скачивания какого-нибудь небольшого файла (килобайт 200) с одного и того же сервера.

Чтобы установить MTU вручную, можно отредактировать параметр MTU (тип **REG_DWORD**, может принимать значения от 68 до максимального MTU, принятого в сети) в подразделе, посвященном конкретному адаптеру **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**. Однако ручную установку MTU лучше не использовать. Вместо этого корректней включить параметр **EnablePMTUDiscovery** (тип **REG_DWORD**, может принимать значения 1 — включено или 0 — выключено, находится в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ Parameters**). Этот параметр разрешает TCP автоматически определять размер MTU.

Параметр **EnablePMTUBHDetect**, который тоже относится к типу **REG_DWORD** и находится в том же разделе, что и описанный выше, лучше всего отключить, установив в 0.

Кроме того, желательно активировать параметр **SackOpts** из того же раздела, установив его в 1. Параметр **SackOpts** имеет тот же тип **REG_DWORD** и важен при работе с большими TCP-окнами.

Параметр **TcpMaxDupAcks** из этого же раздела желательно установить в значение 2 (он имеет тип **REG_DWORD** и может принимать значения от 1 до 3).

Оптимизация TCP/IP с помощью программы iSpeed for Windows

Для оптимизации TCP/IP можно воспользоваться специальными программами, например iSpeed for Windows (рис. 16.10).

Программу можно скачать с сайта *http://www.hms.com/ispeed.asp*. Кстати, у меня для вас хорошая новость: все, что мы делали выше (и даже больше), она прекрасно сделает и без нашей помощи. Зато, согласитесь, приятно понимать, чем именно будет заниматься эта программа на вашем компьютере.

iSpeed for Windows позволяет настраивать параметры TCP/IP, ведет журнал изменений, позволяет тестировать сетевую подсистему (скачи-

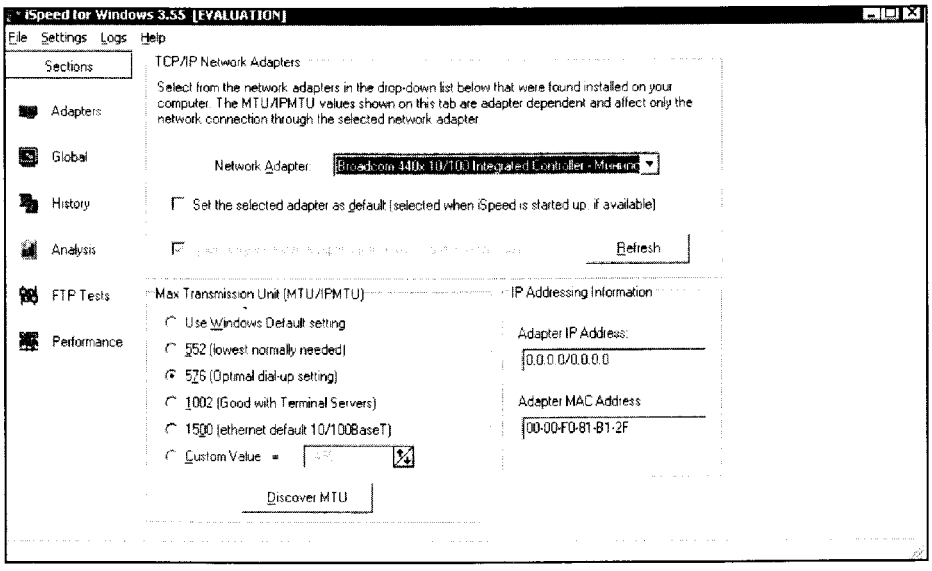


Рис. 16.10. Главное окно iSpeed

вая файл с сервера в Интернете). После каждого изменения вы можете протестировать свою интернет-подсистему: при этом вы увидите сами, как те или иные параметры влияют на скорость соединения. Ну а если вы изменяете реестр вручную, эту программу можно использовать для мониторинга изменения производительности.

Настройка TCP/IP средствами реестра (продолжение)

Чтобы ускорить загрузку веб-страниц, рекомендуется добавить в раздел реестра **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings** следующие параметры:

MaxConnectionsPer1_0Server, тип **REG_DWORD**, значение 00000020

MaxConnectionsPerServer типа **REG_DWORD** со значением 00000020.

Надо сказать, что эти установки могут стать причиной проблем с загрузкой некоторых веб-сайтов. Если после добавления этих параметров работа системы станет нестабильной, просто удалите их.

В локальной сети удаление ключа **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}** позволяет ускорить работу с сетевыми папками.

Теперь о реестре сказано достаточно для того, чтобы вы могли творчески относиться к этому бесценному инструменту оптимизации Windows и использовать его для тонкой настройки вашей системы.

А сейчас самое время поговорить о маршрутизации в Windows.

16.2. МАРШРУТИЗАЦИЯ

В этом разделе мы попытаемся сделать из компьютера с Windows XP программный маршрутизатор.

Вы уже знаете, что задача маршрутизатора — связь нескольких локальных сетей, или передача пакетов от компьютеров одной сети компьютерам другой. Чтобы компьютер мог работать в качестве маршрутизатора, он должен иметь как минимум два сетевых интерфейса: к примеру, интерфейс для подключения проводной сети и второй, для подключения к беспроводной сети. Также бывают случаи, когда нужно соединить два сегмента сети, один из которых построен на коаксиальном кабеле, а второй — на витой паре.

Программный маршрутизатор — решение вовсе не оптимальное, и, если есть возможность, следует ориентироваться на использование аппаратного маршрутизатора. Но если вы серьезно ограничены в средствах, программный маршрутизатор — единственно возможное решение. К тому же такой маршрутизатор может использоваться как временное решение до покупки аппаратного.

Для связи беспроводной Wi-Fi сети и Ethernet-сети лучшим решением будет точка доступа с поддержкой подключения по локальной сети. Эта точка доступа и будет выступать в качестве маршрутизатора.

Если говорить о программной реализации маршрутизатора, то самый простой способ настроить маршрутизацию в Windows XP — объединение сетевых подключений в сетевой мост. Если вы используете Мастер локальных сетей для установки локальной сети на компьютере, где активны несколько сетевых подключений, программа — Мастер установки се-

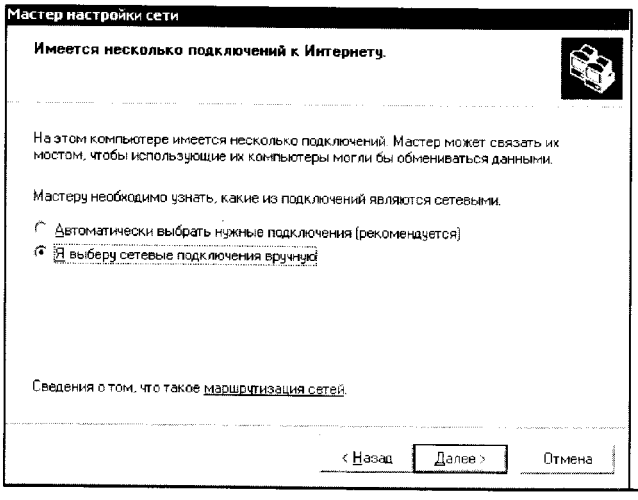


Рис. 16.11. Установка для ручного выбора подключений

ти — попытается создать мост по умолчанию. Но если такой мост вам не нужен, выберите опцию ручного указания интерфейсов (рис. 16.11), входящих в мост, и снимите галочки против всех интерфейсов

Возможна и обратная ситуация. Когда вы устанавливали сеть при помощи Мастера установки сети, некоторые сетевые интерфейсы были неактивны. В этом случае программа не станет предлагать вам создавать сетевой мост. Но затем настало время, когда выяснилось, что мост все-таки нужен. Чтобы создать его, пройдите в окно управления соединениями (**Пуск ▸ Панель управления ▸ Сетевые подключения**), выделите мышью нужные соединения и, открыв контекстное меню правой кнопкой мыши, выберите пункт **Подключение типа мост** (рис. 16.12).

Рис. 16.12. Объединение подключений в мост

После создания моста сегменты сети окажутся связанными между собой, а мост будет транслировать пакеты из сегмента в сегмент, обеспечивая таким образом их связь.

Для превращения компьютера с Windows XP в маршрутизатор можно использовать специальные программы. К примеру, с этой задачей может справиться программа WinGate (ее можно скачать на *http://www.wingate.com*). Практически то же самое может быть реализовано и стандартными средствами ОС, но если ваша сеть увеличилась до нескольких десятков машин, присмотритесь к WinGate.

Использование прокси-сервера с большим кэшем для организации доступа в Интернет с нескольких машин позволит увеличить скорость доступа к веб-контенту за счет того, что часть запрашиваемых пользователями страничек запрашивается повторно. Прокси-сервер делает запрос на обновление веб-серверу, и, если оказывается, что запрошенные данные не изменялись со времени последнего запроса, они выдаются клиенту из кэша прокси. В результате компьютеры быстрее получают данные, а нагрузка на интернет-канал снижается. Примерно так же работает обычный IE, который сохраняет на жестком диске загруженные веб-страницы. Улучшение ситуации от использования прокси возможно для достаточно большой сети, а небольшая может обойтись обычным ICS и локальными кэшами копий IE на клиентских машинах.

WinGate — интересное решение для крупной сети — позволяет, например, настроить DHCP-сервер, организовать массовый выход в Интернет с компьютеров сети, настроить HTTP-прокси и так далее.

Помните: если ваша сеть выросла, WinGate поможет вам управлять ею.

У Windows XP есть встроенное средство для обеспечения маршрутизации TCP/IP. Чтобы включить маршрутизацию пакетов TCP/IP в Windows XP, нужно войти в реестр (то есть запустить `regedit`) и в раздел **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** добавить новый параметр с именем **IPEnableRouter**, типом **REG_DWORD** и значением 1. Затем нужно закрыть редактор реестра и перезагрузиться.

После выполнения этих действий включится маршрутизация TCP/IP. Для управления маршрутизацией служит команда `Route`, которая выполняется из командной строки Windows.

Команда `Route` имеет следующий формат:

```
ROUTE [-f] [-p] [команда [узел] [MASK маска]
[шлюз] [METRIC метрика] [IF-интерфейс].
```

Чтобы просмотреть текущую таблицу маршрутизации, нужно выполнить команду `Route` с параметром `Print`. На рис. 16.13 вы можете видеть результаты выполнения этой команды.

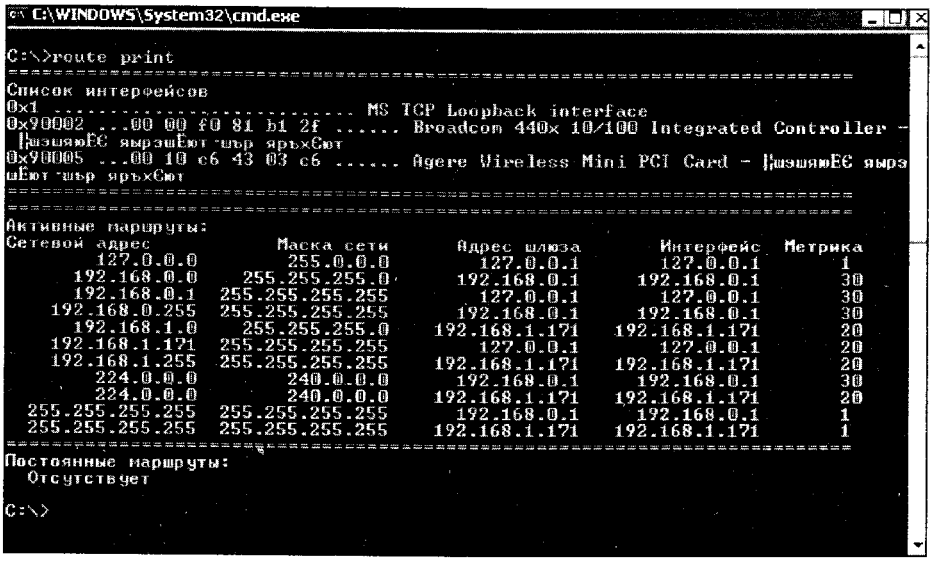


Рис. 16.13. Результаты выполнения команды Route Print на маршрутизаторе

Система автоматически добавляет в таблицу маршрутизации сведения о найденных коммуникационных портах. Так, интерфейс 192.168.0.1 закреплен за беспроводным сетевым адаптером, 192.168.1.171 — за Ethernet-картой, 127.0.0.1 — это стандартная системная «заглушка».

Теперь нужно сделать так, чтобы компьютеры из подсети 192.168.1.0 видели бы компьютеры из подсети 192.168.0.0.

Напомню, что подсеть 192.168.1.0 в нашем примере — это проводная подсеть. На компьютерах этой подсети я ввожу команду cmd и пишу такой текст: `Route add 192.168.0.0 mask 255.255.255.0 192.168.0.171.`

Теперь IP-пакеты, предназначенные для узлов подсети 192.168.0.0 из компьютера, находящегося в подсети 192.168.1.0, перенаправляются на IP-адрес 192.168.1.171, а на компьютере-маршрутизаторе они направляются на интерфейс 192.168.0.1, который отсылает их в подсеть 192.168.0.0. (рис. 16.14).

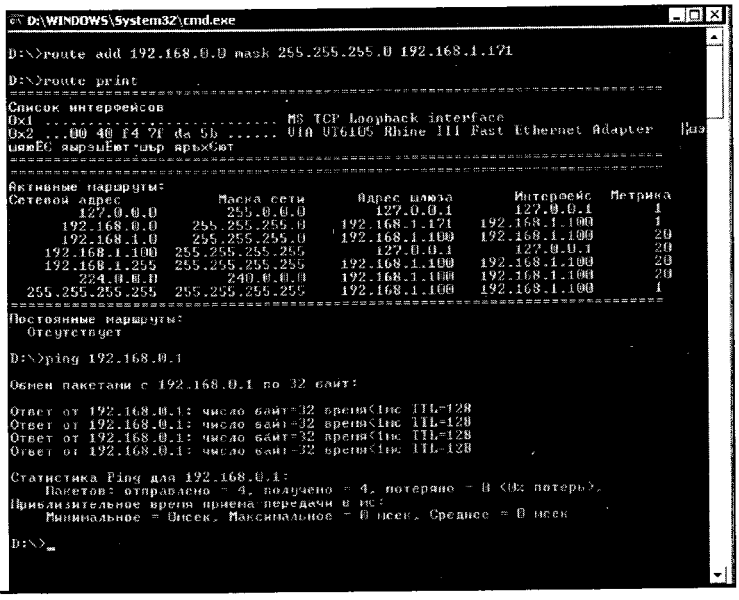


Рис. 16.14. Настройка таблицы маршрутизации на 192.168.1.100

Точно так же настраиваются компьютеры из подсети 192.168.0.0, только там нужно написать следующее: `Route add 192.168.1.0 mask 255.255.255.0 192.168.0.1.`

Надо сказать, что это простое и изящное средство маршрутизации Windows XP очень слабо документировано. Мне не удалось найти среди официальных документов Microsoft объяснения процесса настройки маршрутизации в подобной сети.

Теперь разберем некоторые моменты настройки маршрутизации: поговорим о параметрах запуска `Route` и рассмотрим несколько практических примеров настройки маршрутизации TCP/IP. В стандартной справке, которая прилагается к команде `Route`, немало информации, но ее недостаточно для того, чтобы позволить всем желающим эффективно пользоваться этим средством.

Ключ -p при использовании его с командой `add` позволяет сохранить введенный маршнут в реестре по адресу **HKEY_LOCAL_MACHINE\SYTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes**. Введенный с помощью ключа -p маршрут будет использоваться для инициализации таблицы IP-маршрутизации при каждом запуске TCP/IP. Перед тем как задавать постоянные маршруты, следует задать маршруты временные (без ключа -p), опробовать работу системы, а уже потом задавать постоянные маршруты.

Остальные сведения о настройке `Route` можно найти в его справочной системе. А здесь мы приведем несколько простых примеров настройки таблицы маршрутизации и работы с ней. Практика показывает, что подобные примеры — одна из самых ценных частей материала, которая позволяет применять информацию из книги в реальных сетях.

Для вывода на экран содержимого таблицы маршрутизации введите команду: `route print`.

Для удаления из таблицы маршрутизации всех маршрутов, которые начинаются на 123.162, введите команду: `route delete 123.162*`.

Для вывода на экран маршрутов, начинающихся со 123.162., введите команду: `route print 123.162*`.

Для удаления маршрута к конечной точке 123.162.0.0 с маской подсети 255.255.0.0 введите команду `route delete 123.162.0.0 mask 255.255.0.0`.

Чтобы добавить маршрут по умолчанию с адресом шлюза 192.168.0.2, введите команду `route add 0.0.0.0 mask 0.0.0.0 192.168.0.2`.

Чтобы добавить маршрут к точке 123.162.0.0 с маской подсети 255.255.0.0 и следующим адресом перехода 192.168.0.3, введите команду: `route add 123.162.0.0 mask 255.255.0.0 192.168.0.3`.

Для добавления постоянного маршрута с теми же параметрами команда будет выглядеть таким образом: `route -p add 123.162.0.0 mask 255.255.0.0 192.168.0.3`.

Если вам необходимо задать метрику пути, например, это будет метрика 8, то команда будет выглядеть так: `route add 123.162.0.0 mask 255.255.0.0 192.168.0.3 metric 8`.

Для изменения следующего адреса перехода вышеописанного маршрута с 192.168.0.2 на 192.168.0.6 введите команду `route change 123.162.0.0 mask 255.255.0.0 192.168.0.6`.

16.3. ВЫВОДЫ

Настройка реестра — сложная и противоречивая тема, но теперь вы понимаете, как работать с реестром. Мы разобрались и с вопросами маршрутизации. Внимательно изучив материалы этой главы, вы сможете сделать со своим TCP/IP все, что вам угодно.

ГЛАВА 17
КОММУНИКАЦИЯ В СЕТИ

Локальная сеть — не только среда для передачи файлов через общие папки, не только печать на общих принтерах и выход в Интернет через общие каналы связи. Локальная сеть — это еще и место для общения.

Высокая пропускная способность локальных линий связи и их бесплатность придают интереса общению в сети. Для общения пользователей существует немало программ. Здесь мы рассмотрим некоторые из них: несколько программ-чатов с различными возможностями, программу для голосового общения, а также известную и довольно удобную программу NetMeeting от Microsoft — она в Windows XP даже в меню Пуск не включена, хотя по-прежнему остается удобным инструментом для взаимодействия пользователей в пределах локальной сети. Еще мы разберем интересную программу для организации сетевой радиостанции.

Небольшая часть этой главы будет уделена популярнейшей ICQ. Если вы еще не в ICQ, срочно исправляйтесь! Здесь же мы рассмотрим работу с FTP-клиентами и, в частности, с CuteFTP и с менеджерами закачек, которые будут представлены программой Flash Get.

А начнем мы с простой программы для организации голосового общения.

17.1. ПРОСТОЙ ЧАТ И ГОЛОСОВОЕ ОБЩЕНИЕ

Начнем с предельно простой, но хорошо работающей программы для организации общения. Она называется Net Speakerphone. Дистрибутив программы можно загрузить на сайте http://clx-soft.narod.ru/, он занимает около 500 Кбайт. Установка программы стандартна, разве что она попросит вас перезагрузить компьютер после завершения инсталляции.

Запустить Net Speakerphone можно, воспользовавшись меню **Пуск ▸ Все программы ▸ Net Speakerphone ▸ Net Speakerphone**. После запуска в системной панели Windows поселяется иконка программы. После установки и запуска программы на всех компьютерах сети можно с ее помощью приступать к общению.

Основное окно программы открываем двойным щелчком по значку в системной панели. Отсюда можно управлять программой (рис. 17.1).

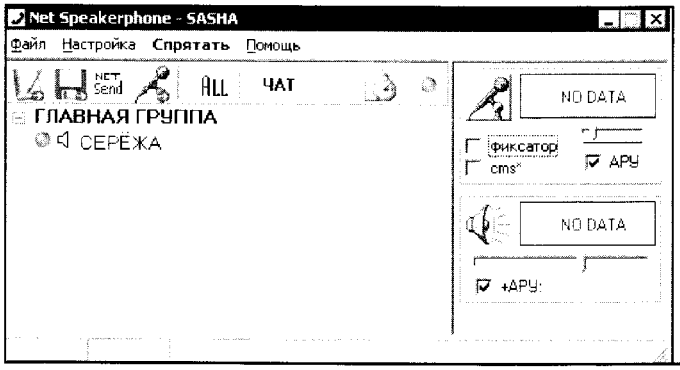


Рис. 17.1. Главное окно программы Net Speakerphone

Net Speakerphone автоматически определяет компьютеры локальной сети, на которых запущена ее копия. Компьютеры можно добавлять и вручную. Если рядом с именем компьютера отображается зеленая лампочка и значок динамика, это значит, что, во-первых, на компьютере запущена программа Net Speakerphone и, во-вторых, что он может воспроизводить звук. Компьютеры при этом можно разбивать на группы.

Основное предназначение программы — это обеспечение голосового общения между клиентскими компьютерами. Для ее работы сервер не требуется: передача голосового сообщения инициируется выбором клиентского компьютера из списка (можно выбрать несколько клиентов — для этого служит кнопка CTRL на клавиатуре) и нажатием кнопки с изображением микрофона. После этого можно говорить в микрофон, подключенный к звуковой карте вашего компьютера, а пользователи, которым вы передаете сообщение, услышат ваш голос из своих динамиков. Чтобы не держать кнопку с изображением микрофона нажатой вручную, в правой части окна программы, там, где изображен микрофон, есть поле **Фиксатор**. Если поставить в этом поле галочку, то звук будет передаваться непрерывно.

Во время передачи звука можно настраивать усиление сигнала, перемещая бегунок в этой же части окна. Советую также поставить галочку напротив параметра АРУ, то есть включить автоматическую регулировку усиления сигнала.

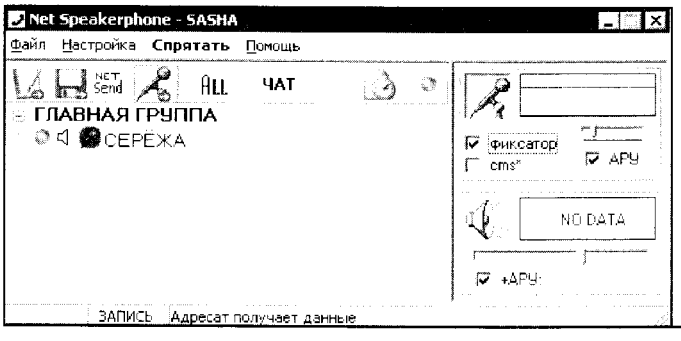


Рис. 17.2. Внешний вид программы при выключенном микрофоне

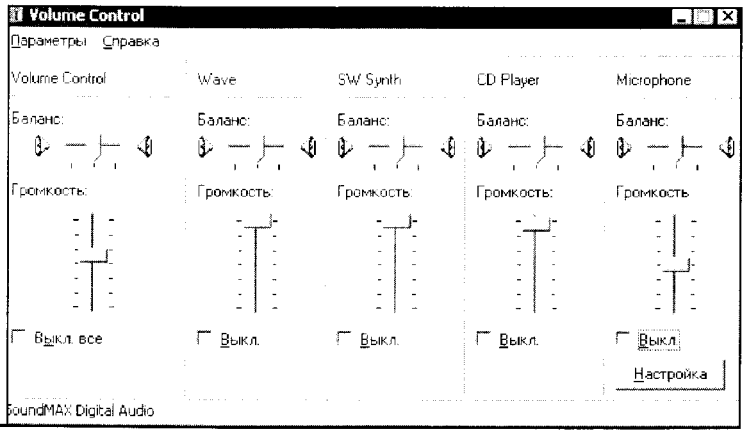


Рис. 17.3. Включение микрофона

Если после того, как вы нажали кнопку с микрофоном и включили фиксатор, звук «не пошел» (об этом вам подскажет прямая линия в окошке рядом с изображением микрофона, рис. 17.2), значит, вы забыли включить микрофон.

Для включения микрофона дважды щелкните по значку динамика в системной панели Windows и снимите галочку **Выкл**. в области регулировки микрофона (рис. 17.3).

После того как микрофон включен, тот, с кем вы пытаетесь поговорить, будет слышать ваш голос, а внешний вид окна программы изменится так, как показано на рис. 17.4.

Обратите внимание на то, что на рис. 17.4 волны, отображающие силу звукового сигнала, уходят далеко за пределы окошка. Это может вызвать ухудшение звука на принимающей стороне. Чтобы поправить дело, можно, отключив автоматическую регулировку усиления, настроить усиление вручную, а затем включить АРУ. Можно также просто говорить в микрофон с несколько большего расстояния.

Звук можно одновременно передавать на несколько компьютеров, но передача звуковых сообщений — далеко не единственная возможность Net Speakerphone. С пользователями, на компьютере которых запущена программа, можно общаться посредством коротких сообщений.

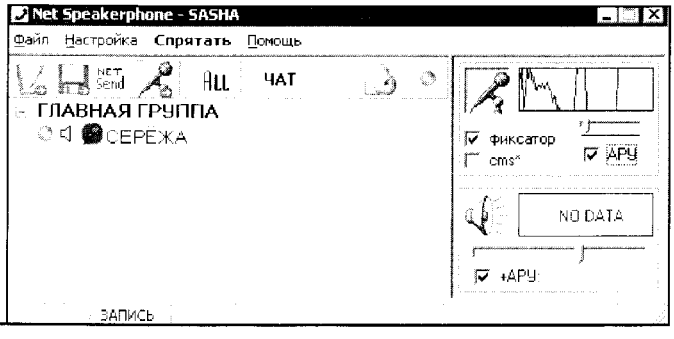


Рис. 17.4. Процесс передачи звука

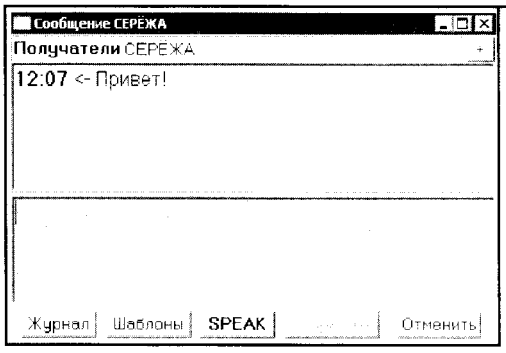


Рис. 17.5. Обмен сообщениями

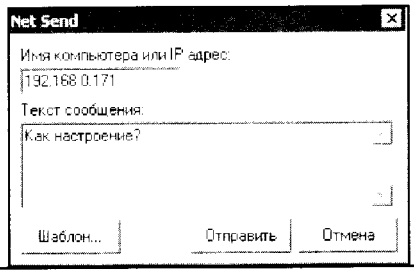


Рис. 17.6. Использование сервиса Net Send

Для этого существует кнопка **Послать текстовое сообщение**, крайняя слева на панели инструментов программы. Послать текстовое сообщение можно, воспользовавшись соответствующим пунктом меню. После того как вы выберете этот пункт, появится окошко для работы с короткими сообщениями (рис. 17.5).

Из этого же окна можно запускать сеансы голосовой связи, пользоваться немногочисленными шаблонами сообщений и просматривать журнал.

Для пользователей, на компьютерах которых программа не запущена, можно отправить сообщение, воспользовавшись стандартным сервисом Net Send. Для этого надо выбрать соответствующего клиента в списке и, нажав кнопку **Net Send**, заполнить поля появившейся формы, введя IP-адрес компьютера (или его имя) и текст сообщения (рис. 17.6).

После того как сообщение будет отправлено, на компьютере-получателе оно будет выглядеть следующим образом (рис. 17.7).

Пользователи этой программы также могут пообщаться в локальном чате. Для этого достаточно нажать кнопку **Чат**. В чат попадут все клиенты сети, которые нажали на эту кнопку (рис. 17.8).

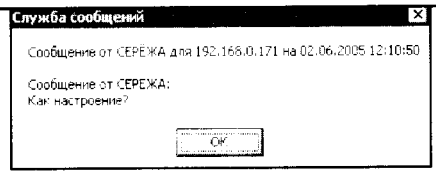


Рис. 17.7. Сообщение, полученное через сервис Net Send

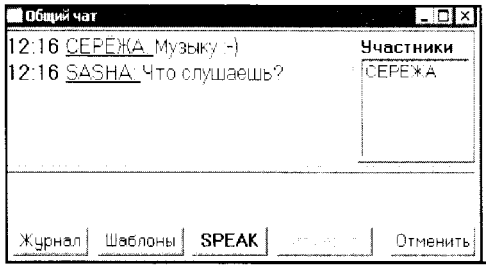


Рис. 17.8. Чат

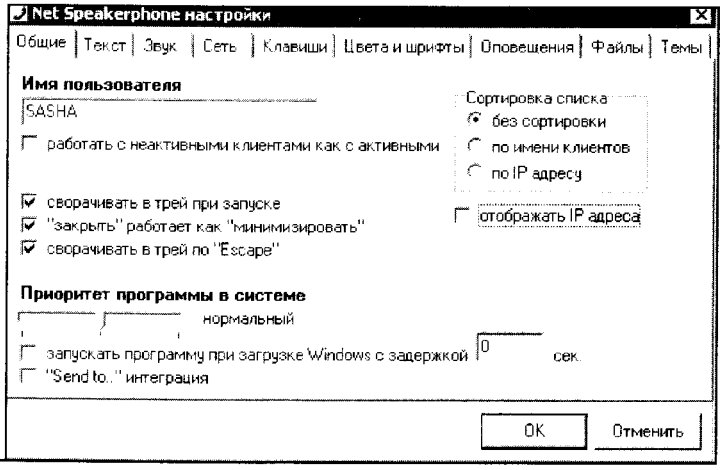


Рис. 17.9. Окно настройки программы

И, наконец, программа поддерживает передачу файлов между пользователями. Для инициализации передачи воспользуйтесь кнопкой **Послать файл** с изображением дискеты.

Net Speakerfone имеет довольно развитую систему настроек, которая может быть вызвана командой **Настройка ▶ Общие** (рис. 17.9).

Все настройки даны на русском языке, они довольно стандартны, поэтому ни для кого не составит труда разобраться с ними самостоятельно.

Мы разобрали маленькую, удобную и стабильно работающую программу. Ее интерфейс не отличается дизайнерскими изысками, но свою работу она выполняет неплохо.

Единственный случай, когда мне удалось «подвесить» Net Speakerfone, связан с настройкой звука. Чтобы добиться звука покачественней, я начал настраивать параметры, относящиеся к звуку. В результате программа отказалась работать с передачей звука, сославшись на внутреннюю ошибку.

Если вам нужно простое средство для организации общения в сети, тогда Net Speakerphone достойна вашего внимания.

17.2. VYPRESS CHAT

Vypress Chat — это программа, название которой говорит само за себя. Чат — это центр ее функциональности. Дистрибутив программы занимает около 2-х мегабайт, скачать ее можно с сайта *http://vypress.com/rus/*. Пользователю предоставляется время для оценки возможностей программы, после чего ее придется либо купить, либо прекратить использовать.

Интерфейс Vypress Chat (рис. 17.10) сразу выдает в ней профессионально написанную программу. Если первая описанная в этой главе про-

грамма подходит больше для небольшой домашней или офисной сети, пользователи которой видят интерес в голосовом общении, то вторая — серьезный продукт, который будет хорош в сети любого уровня.

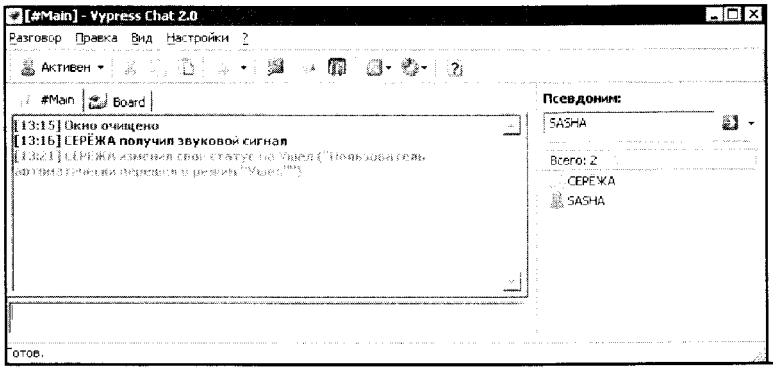


Рис. 17.10. Главное окно Vypress Chat

После установки и запуска на всех компьютерах, пользователи которых хотят участвовать в общении с использованием Vypress Chat, программы автоматически найдут компьютеры с установленными копиями и добавят пользователей в список, который находится в правой части программы. После этого можно будет пользоваться функциональностью чата.

В основном окне программы есть две вкладки, **#Main** и **Board**. Первая — окно канала чата по умолчанию, а вторая представляет собой доску объявлений. Эта доска объявлений доступна всем пользователям чата и выступает в качестве «официальной стенгазеты сети». На доску объявлений можно выкладывать объявления, которые содержат форматированный текст, графику, гиперссылки (рис. 17.11).

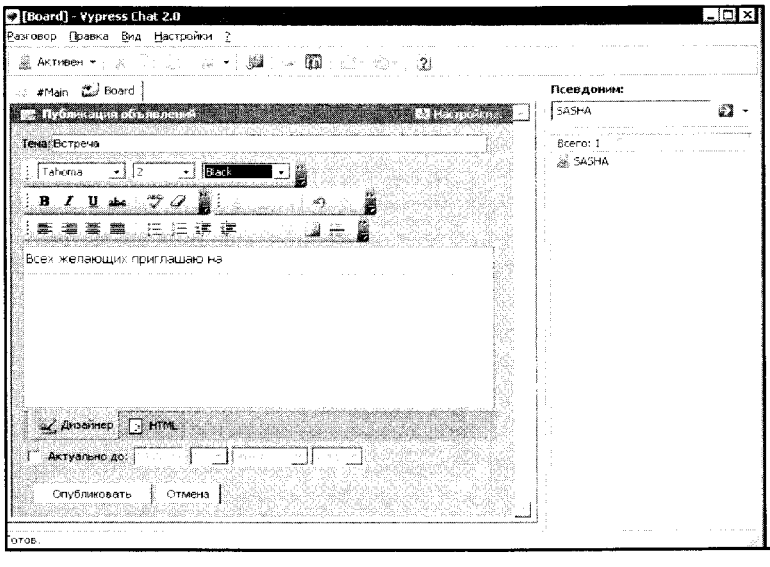


Рис. 17.11. Создание нового объявления

Объявлениям, помещенным на доску, можно присваивать срок актуальности, установив соответствующую галочку около параметра **Актуально до** и настроив дату и время, после которых объявление теряет свою значимость.

Чат — это основа программы, поэтому к отработке его деталей разработчики подошли ответственно. Во время беседы можно пользоваться смайликами, вводя их с помощью соответствующей панели инструментов или при помощи принятых для таких целей сочетаний клавиш.

В чате есть система команд, которые выглядят как косая черта и слово-команда. Например, команда **/name Новое_имя** вызовет смену имени общающегося в чате на **Новое_имя**. В чате предусмотрена система макросов, то есть комбинаций клавиш **<Shift>, <Ctrl>** и **F1–F12**.

Если следовать документации к программе, то сочетание <Shift+Ctrl+F1–F12> должно записывать выделенный участок текста в макрос, а сочетание <Shift+F1–F12> проводит обратную операцию — вставляет строку из макроса. Однако мне не удалось воспользоваться этой функцией программы по неустановленным причинам.

Помимо чата и доски объявлений, Vypress Chat содержит все остальные коммуникационные возможности, присущие подобным программам: пользователи могут обмениваться личными сообщениями, файлами, можно проводить широковещательные рассылки сообщений, использовать звуковые оповещения пользователей и так далее.

На рис. 17.12 изображено меню, которое иллюстрирует эти возможности программы. Думаю, дополнительных пояснений здесь не требуется, а те, кому они нужны, могут обратиться к описанию сходных возможностей программы Net Speakerphone.

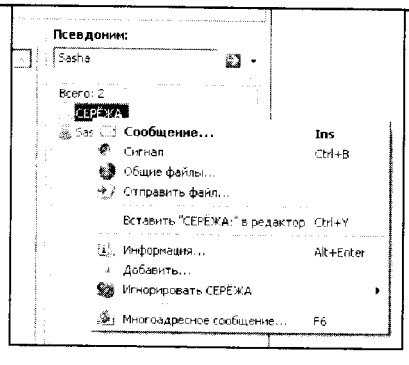
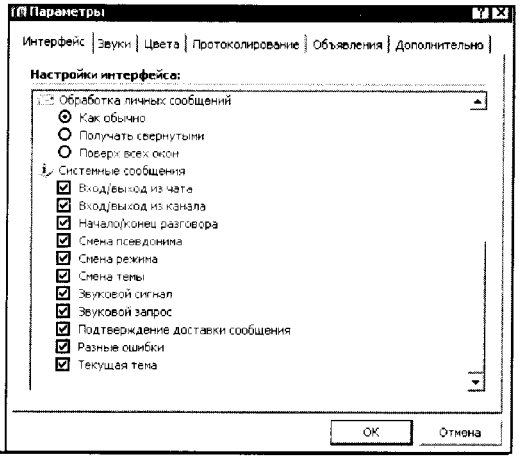


Рис. 17.13. Окно свойств программы

Рис. 17.12. Возможности программы по дополнительному общению



Система настроек программы достаточно логична (рис 17.13), выполнена на русском языке, поэтому здесь тоже проблем возникнуть не должно.

Одним из замечательных свойств подобных программ можно назвать то, что их не нужно настраивать. А раз так — переходим к описанию следующей программы. Ее можно найти на практически любом компьютере, по крайней мере на том, что работает под Windows XP.

17.3. WINDOWS NETMEETING

NetMeeting имеется в стандартной Windows XP, но найти ее непросто. По неизвестным причинам разработчики из Microsoft не сделали ссылку на нее в одном основных программ Windows и не вынесли ее ярлык на рабочий стол, — в общем, сделали ее случайный запуск практически невозможным.

И неудивительно. По мысли Microsoft, в операционной системе очень важное место отводится программе Windows Messenger. Возникает ощущение, что этот самый Messenger являет собой полную противоположность программе Net Meeting. Тем не менее разработчики из Microsoft не удалили Net Meeting из дистрибутива операционной системы, а это что-нибудь да значит. К тому же Net Meeting по-прежнему остается очень удобной программой для организации общения в локальной сети.

Сегодня NetMeeting — это единственная программа этого раздела, которая поддерживает организацию видеоконференций. Из других подобных программ можно отметить iVisit (*http://www.ivisit.com*), ICUII — I See You Too! (*http://www.icuii.com*) и другие. iVisit ориентирована на общение в Интернете, ICUII может применяться и в локальной сети, но их возможности сводятся к обычному видеочату, а NetMeeting — это все же гораздо больше, чем чат.

Для запуска NetMeeting в Windows XP нужно в окно **Выполнить** (**Пуск ▶ Выполнить**) ввести команду `Conf`. На рис. 17.14 изображено окно Мастера первоначальной настройки NetMeeting, которое появляется после ввода команды `Conf`.

Дальше следует череда диалоговых окон. Мы не будем рассматривать их все и остановимся лишь на ключевых и неочевидных моментах настройки.

Диалоговое окно на рис. 17.15 предназначено, чтобы включить автоматическое подключение к серверу каталогов, чтобы вы могли связаться с другими пользователями, подключенными к тому же серверу. Но подключение к серверу каталогов сегодня никого не интересует, так как есть множество куда более популярных программ для общения в Интернете — та же ICQ, например. Чтобы не подключаться к серверу каталогов при запуске программы и не регистрироваться на нем, нужно сбросить галочку в поле **Подключаться к серверу каталогов при запуске** и поставить отметку в поле **Не**

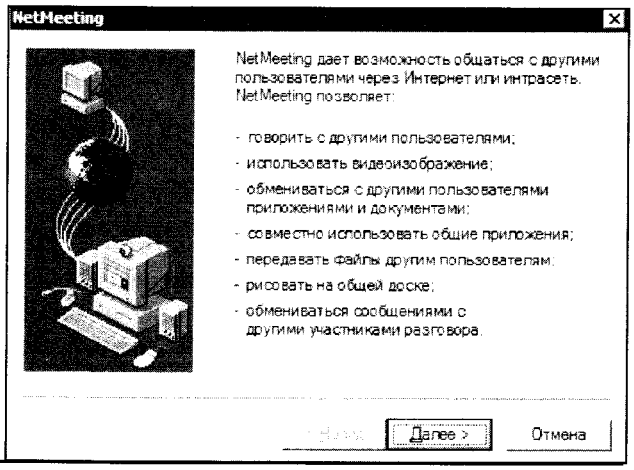


Рис. 17.14. Начало настройки NetMeeting

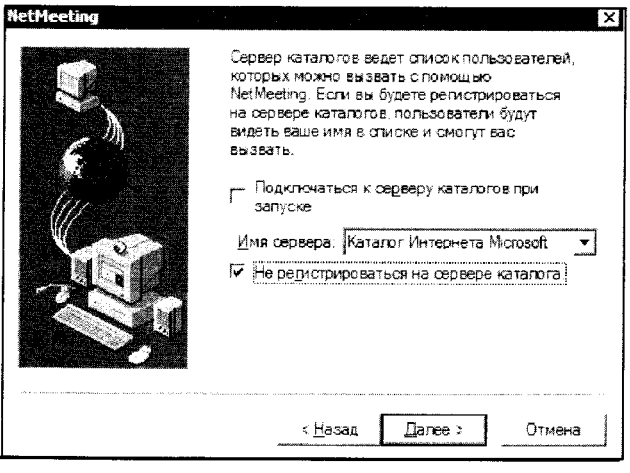


Рис. 17.15. Окно настройки подключения к серверу каталогов

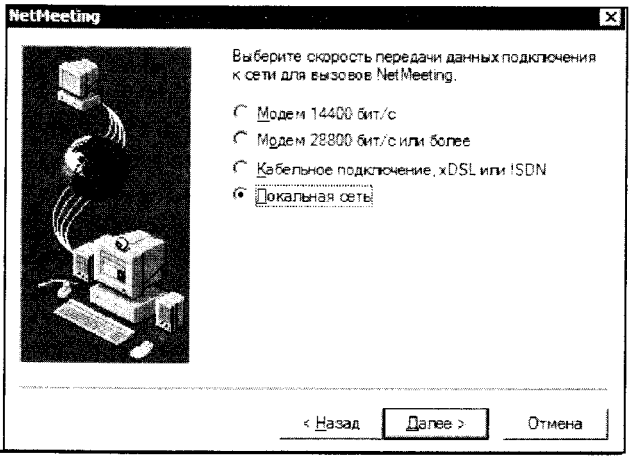


Рис. 17.16. Выбор скорости передачи данных подключения к сети

регистрироваться на сервере каталога. Так вы обеспечите себе удобную работу в локальной сети, NetMeeting не станет пытаться выйти в Интернет.

Следующий пункт настройки NetMeeting — окно, с помощью которого можно установить скорость подключения, которым вы будете пользоваться при работе с программой. В этом окошке нужно выбрать **Локальная сеть** (рис. 17.16).

Остальные окна можно обрабатывать одним нажатием кнопки **Далее**, так как они, как правило, особой роли в работе программы не играют. Но есть исключение: окно, предназначенное для настройки подсистемы передачи звука (рис. 17.17).

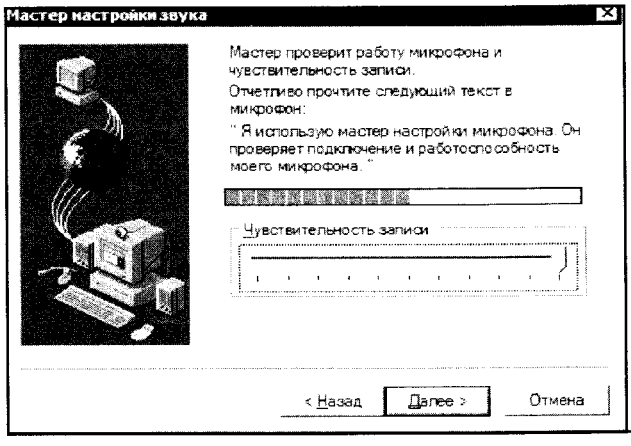


Рис. 17.17. Настройка микрофона

Допустим, вы собираетесь при работе с NetMeeting пользоваться микрофоном. При этом микрофон правильно подключен к звуковой карте и активирован в панели настройки звуковых устройств Windows. Тогда, если произнести в микрофон несколько слов, в окне появится полоса, отображающая уровень сигнала, поступившего с микрофона. Практика показывает, что ползунок чувствительности записи нет смысла перемещать влево и что обычно все нормально работает и без вмешательства в его настройку. Если микрофон не подключен к системе, система не станет показывать его в процессе настройки.

После окончания первоначальной настройки NetMeeting на **Рабочем столе** появится ярлык для ее запуска. Понятно, что для общения с использованием NetMeeting вам придется запустить ее на нескольких компьютерах сети.

При запуске программы на экране появляется ее главное окно (рис. 17.18).

Разумеется, пользователь этой программы желает подключиться к компьютерам других пользователей и начать общение. При этом в случае с NetMeeting общение выходит за рамки текстового чата, видеочата или обмена звуковыми сообщениями.

Чтобы вызвать пользователя на беседу, нужно нажать кнопку с изображением телефона и в появившемся окне (рис. 17.19) ввести имя или

Рис. 17.18. Главное окно NetMeeting

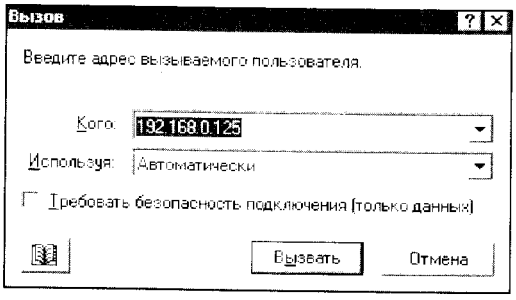


Рис. 17.19. Вызов пользователя с использованием IP-адреса

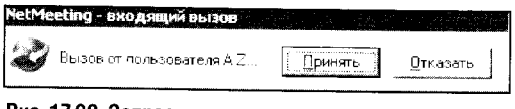
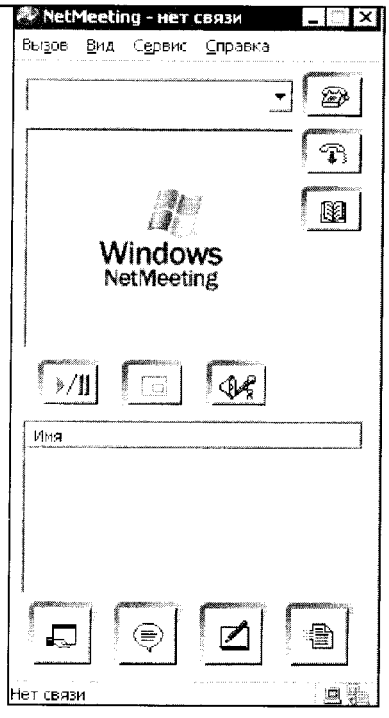
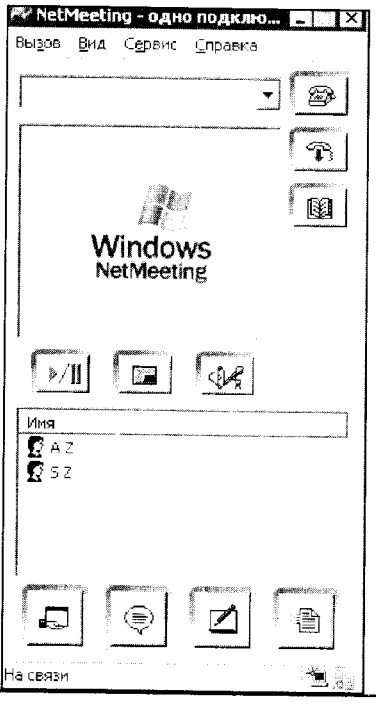


Рис. 17.20. Запрос на прием или отклонение входящего вызова





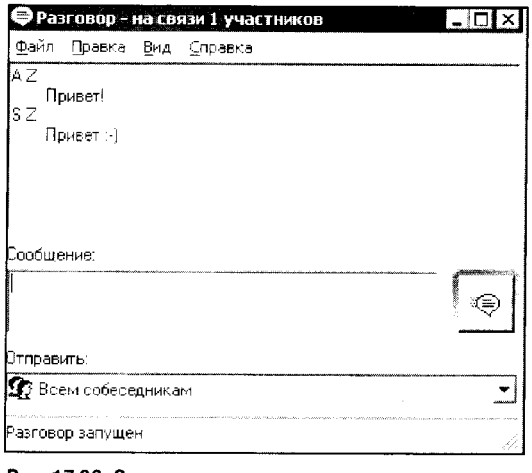


Рис. 17.22. Окно чата

Рис. 17.21. Окно NetMeeting после подключения пользователя к беседе

IP-адрес его компьютера. Как узнать имя и IP-адрес компьютера, вы уже знаете. Ну а если забыли, то я напомню.

Если вы подключены к локальной сети, почти наверняка вы видите в системной панели Windows пару зеленых экранчиков, сигнализирующих о сетевой активности. Чтобы узнать IP-адрес вашего компьютера, достаточно щелкнуть по этим экранчикам правой кнопкой мыши, выбрать **Состояние** и перейти в появившемся окне на вкладку **Поддержка**. Еще можно запустить сеанс командной строки: в окне **Выполнить** наберите `cmd` и выполните команду `ipconfig`. А имя вашего компьютера можете узнать, побродив вокруг папки **Сетевое окружение** или посмотрев вкладку **Имя компьютера** в меню **Мой компьютер ▸ Свойства**.

В случае с NetMeeting есть одна тонкость: вызвать пользователя, компьютер которого имеет имя, написанное кириллицей, у вас не получится. В этом случае можно использовать универсальный адрес для вызова пользователя, то есть IP-адрес.

Итак, один компьютер вызывает другой. На том компьютере, IP-адрес которого введен в поле **Кого**, отображается запрос на подключение (рис. 17.20).

Ответив на этот запрос нажатием кнопки **Принять**, вы подключаетесь к беседе с вызывающим вас пользователем. При этом внешний вид окна NetMeeting меняется: в его нижней части виден список пользователей, которые в данный момент подключены к системе (рис. 17.21).

Настройка и подключение пользователя к NetMeeting — самая сложная часть нашей работы. А дальше все пойдет очень просто. Выделив нужного пользователя мышью и нажав кнопку **Разговор** в нижней части окна программы (вторая слева), запускаем окно чата (рис. 17.22). Это самый обычный чат, где сообщения можно отправлять и каждому пользователю в отдельности, и всем вместе.

Другое средство общения, которое имеет ограниченную сферу применения, запускается при помощи нажатия кнопки **Доска** (вторая справа на рис. 17.23).

Этот интересный способ общения, который, как мне кажется, больше подходит для обсуждения разных проблем, которые требуют графических изображений. Правда, чтобы эффективно пользоваться средством **Доска** в рабочих целях, мышь лучше заменить графическим планшетом: рисовать мышью схемы и чертежи «от руки» не слишком удобно. Правда, если пользоваться в основном автофигурами, то это неудобство во многом устраняется.

Такая доска — неплохая игрушка для детей разных возрастов. Когда студенты одного вуза в перерыве запустили NetMeeting на уроке информатики и добрались до Доски, началось нечто невообразимое. Одна группа рисовала карикатуры на другую, а другая стирала то, что рисовали первые, и рисовала свою версию.

Нажатием кнопки **Общие приложения** (левая кнопка в нижней части окна программы) можно выбрать приложение, которое станет общим

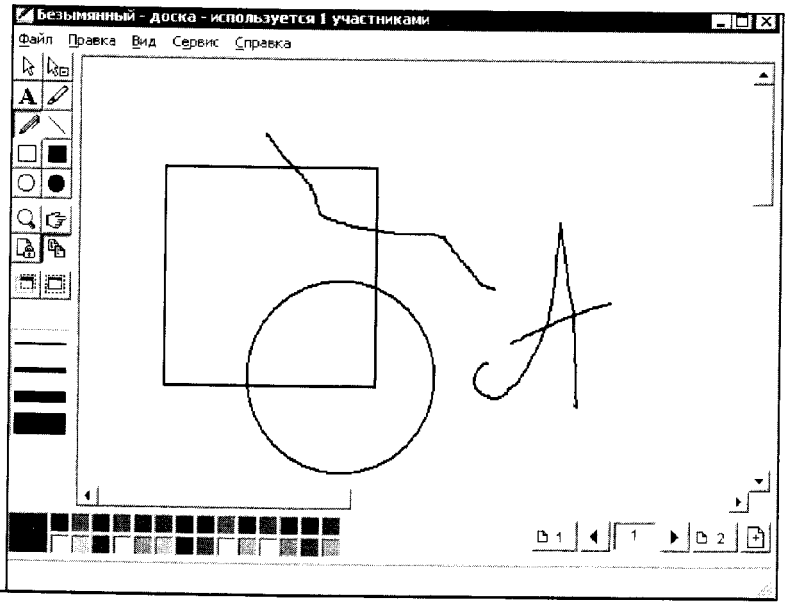


Рис. 17.23. Работа со средством Доска

для нескольких пользователей. Ну а чтобы дать полный доступ к рабочему столу и всем программам, достаточно нажать кнопку **Разрешить управление** (после этого она превратится в **Запретить управление**) и при желании установить галочку в поле **Автоматически принимать запросы на управление** (рис. 17.24).

Теперь доступ к вашему **Рабочему столу** можно получить с других компьютеров сети (рис. 17.25).

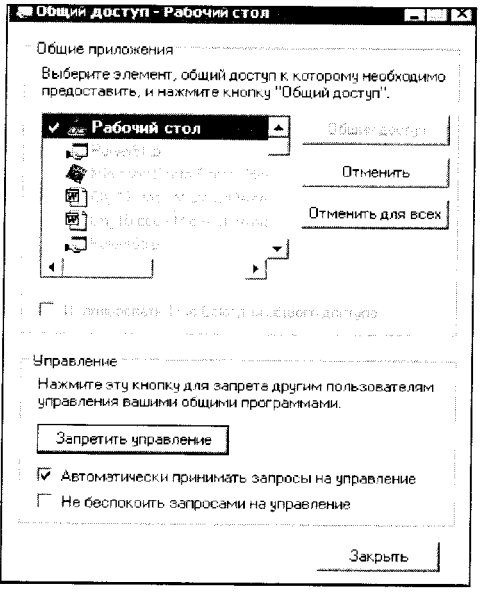


Рис. 17.24. Настройка удаленного управления

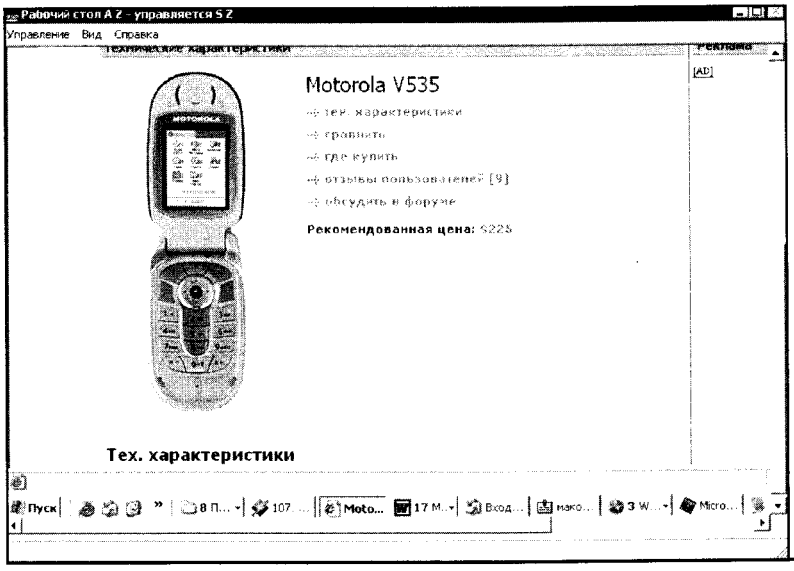


Рис. 17.25. Управление рабочим столом с другого компьютера

Чтобы управлять чужим рабочим столом, достаточно выбрать в окне управления меню **Управление ▸ Запросить управление**. При этом вы берете полную власть над чужим компьютером, а его собственные органы управления будут заблокированы. Чтобы завершить сеанс управления, на управляющем компьютере следует выбрать пункт меню **Управление ▸ Прекратить управление**.

В Windows XP появилось одно любопытное средство — **Подключение к удаленному рабочему столу**. Правда, для его использования нужен выход в Интернет, поэтому в локальной версии достойной альтернативы NetMeeting я пока не вижу. Учитывая широчайшее распространение Интернета, необходимость выхода в Сеть для управления другим компьютером не кажется неоправданной роскошью.

Кнопка **Передача файлов** (правая в нижнем ряду) служит, ясное дело, для передачи файлов. Средства передачи файлов в NetMeeting устроены вполне стандартно, поэтому подробно на них останавливаться незачем.

NetMeeting поддерживает и средства видеосвязи, но этот вид связи все еще не слишком популярен, ведь для беседы обычно хватает текстовых сообщений.

Если к компьютерам, участвующим в соединении, при запуске NetMeeting подключить веб-камеры, то программа станет автоматически поддерживать передачу и прием видеоизображения. Для настройки параметров видеосвязи служит вкладка **Видео** окна параметров программы, которое можно вызвать командой **Сервис ▸ Параметры** (рис. 17.26).

NetMeeting позволяет организовывать связь посредством обычного телефона, но возможности такой связи ограничены.

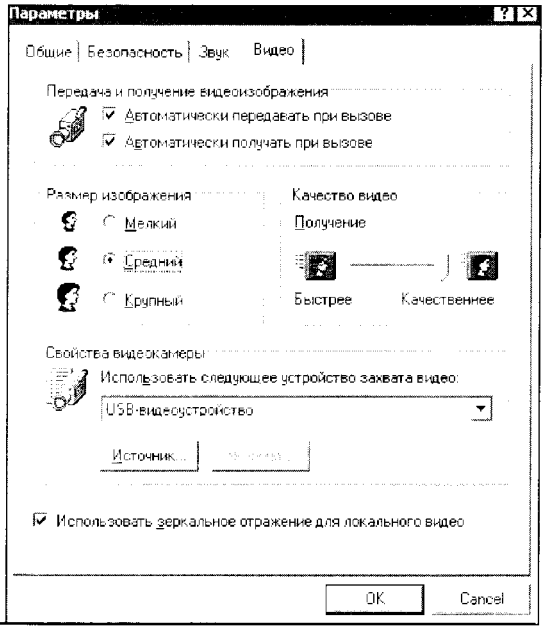


Рис. 17.26. Настройка видеопараметров NetMeeting

Словом, NetMeeting — хорошая программа, и к тому же она достаточно проста, чтобы вы в полной мере оценили ее удобства.

Следующей темой нашего рассказа станет полезная утилита Hyper Terminal, которая позволяет связываться с использованием обычных телефонов.

17.4. HYPER TERMINAL

Hyper Terminal — морально устаревшая утилита, и потому она в последнее время не пользуется должным вниманием. А между тем установка связи между парой компьютеров по обычной телефонной линии все еще бывает нужна и полезна. Hyper Terminal, помимо соединения пары компьютеров по телефонной линии, умеет многое, но это «многое» сегодня реализуется более современными средствами. Поэтому в рассказе о Hyper Terminal мы сосредоточимся на описании сеанса связи посредством обычного телефона.

Запустить Hyper Terminal можно, выполнив последовательность команд **Пуск ▸ Все программы ▸ Стандартные ▸ Связь ▸ Hyper Terminal**. Сразу после первого запуска программа спросит вас о том, желаете ли вы сделать Hyper Terminal Telnet-приложением, используемым по умолчанию. Вы можете ответить ей **Да** и продолжать работу. Ну а дальше вам останется лишь дать имя подключению (рис. 17.27).

Введя имя подключения и выбрав для него соответствующий значок, вы попадаете в следующее окно программы, где вам предложат выбрать

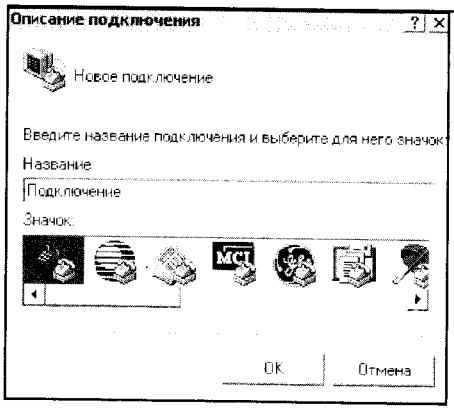


Рис. 17.27. Ввод имени подключения

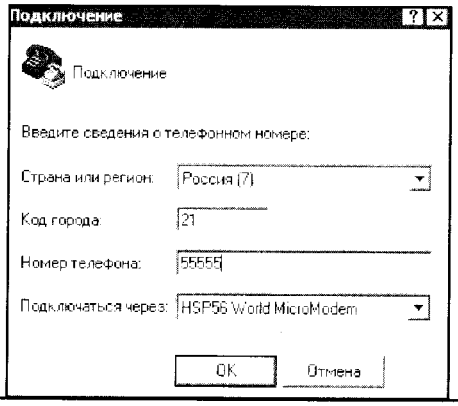


Рис. 17.28. Настройка параметров подключения

способ подключения и, в нашем случае, ввести номер телефона, к которому следует подключиться.

В окне выбора способа подключения есть, кроме названия вашего модема (рис. 17.28), другие параметры.

Например, выбрав параметр TCP/IP (Winsock) и соответствующим образом заполнив поле набора номера, можно подключиться к другому компьютеру по TCP/IP. Но эта возможность HyperTerminal сегодня неактуальна, поэтому переходим к следующему этапу настройки соединения.

Отметим, что в предыдущем окне (рис. 17.28) помимо номера телефона имеется еще и не всегда нужный код города. Здесь эти параметры можно и не трогать, а вот в следующем окне (рис. 17.29) их нужно отредактировать таким образом, чтобы номер телефона выглядел правильно.

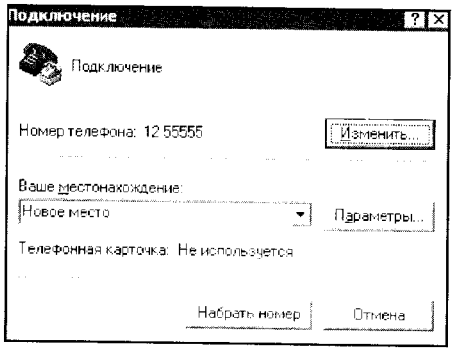


Рис. 17.29. Окно подключения

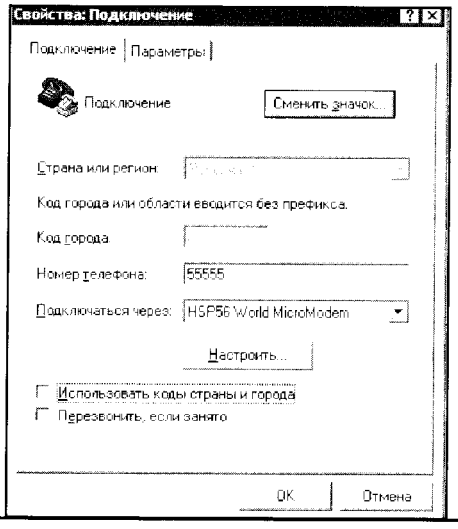


Рис. 17.30. Настройка свойств подключения

В этом окне напротив описания номера телефона, который в данном случае должен быть местным, нажмите кнопку **Изменить**. В появившемся после этого окне (рис. 17.30) снимите галочку, которая включает набор номера с кодом города.

Теперь один из компьютеров готов к сеансу связи. Очередь за вторым.

Логика работы с Hype Terminal в качестве коммуникационной программы состоит в том, что один из модемов настроен на прием вызова, а второй совершает этот вызов. Такая схема очень напоминает соединение с интернет-провайдером посредством обычного модема.

Второй компьютер настраивается точно так же, за исключением того что не нужно вводить номер телефона, а в окне **Подключение** (рис. 17.29) следует нажать кнопку **Отмена**. После этого в главном окне Hyper Terminal выбираем пункт меню **Вызов ▸ Ждать звонка** (рис. 17.31).

Вот и все. Теперь на первом компьютере вызовите окно **Соединение** (**Вызов ▸ Вызов**), ну а если это окно все еще на экране, нажмите кнопку **Набрать номер**. Компьютер наберет номер и, когда произойдет подключение к другому компьютеру, динамик модема начнет издавать характерные звуки, знакомые любому, кто хотя бы раз выходил в Интернет через *dial-up*.

Когда подключение состоится, вы и ваш партнер сможете обмениваться репликами и передавать файлы. Почему же я не называю это общение чатом?

Во-первых, мне не удалось наладить диалог с использованием кириллического алфавита: для сообщений приходится использовать латиницу. Во-вторых, Hype Terminal предназначен для общения с машинами — к примеру, с BBS, — поэтому в нем нет никаких способов организации текста. И, в-третьих, если вы и ваш партнер начнете писать одновременно, ваши слова могут перемешаться самым причудливым образом.

Вывод: Hyper Terminal позволяет быстро устанавливать соединение между двумя компьютерами по телефонной линии и совершенно бес-

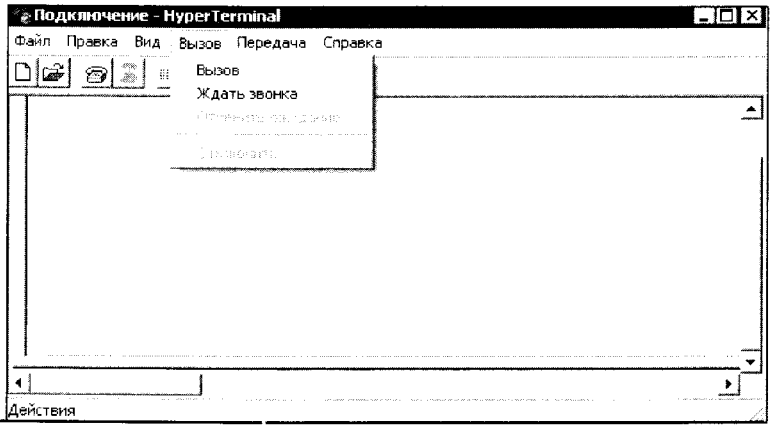


Рис. 17.31. Переключение второго компьютера в режим ожидания звонка

платно (если вы не платите за услуги телефонной связи повременно) передавать любые разумные объемы информации. В любом случае Hyper Terminal — интересное приложение, на которое стоит обратить внимание. Несмотря на явное несовершенство, эта программа неплохо подходит для быстрой организации связи.

17.5. FTP-КЛИЕНТ

FTP — *File Transfer Protocol*, то есть протокол передачи файлов, — один из старейших протоколов Интернета. С его помощью можно работать с файлами на удаленном компьютере. Причем действия с файлами, проводимые через FTP, практически ничем не отличаются от аналогичных операций на локальном компьютере.

Для работы по протоколу FTP могут использоваться различные программы, скрывающиеся под общим название FTP-клиентов. Простейший FTP-клиент, который есть на компьютерах всех читателей этой книги, — всем известный Internet Explorer. Но FTP-функциональность у IE — это скорее «бесплатное приложение» к его основному предназначению, и те, кому нужно работать с FTP, рано или поздно приходят к необходимости обзавестись специальной программой.

Таких программ довольно много, а мы здесь рассмотрим одну из них — довольно популярную и распространенную CuteFTP, точнее CuteFTP 7 Home. Скачать программу можно с сайта *http://cuteftp.com/cuteftp/*. Размер дистрибутива — около 5 мегабайт. С сайта скачивается пробная 30-дневная версия.

Для начала немного теории. В общем случае для подключения к FTP-серверу вам нужно иметь FTP-клиент, выход в Интернет и знать некоторые параметры подключения к серверу — обычно это адрес сервера (**Host Adress**), имя пользователя (**User Name**) и пароль (**Password**). Зная эти параметры, вы сможете подключиться к серверу через FTP-клиент. Имя пользователя, пароль и адрес сервера можно получить, например, при регистрации сайта на каком-нибудь хостинге.

Некоторые серверы общего анонимного доступа позволяют подключаться к ним без имени и пароля.

Установка CuteFTP совершенно стандартна, поэтому перейдем сразу к настройке этой программы. Я опишу здесь общий вариант настройки, обойдя вниманием некоторые автоматические функции программы. Зная этот способ, вы без труда сможете настроиться на нужный вам сервер, используя CuteFTP. Итак, посмотрите на рис. 17.32. Здесь изображено главное окно программы. Некоторые данные этого окна скрыты.

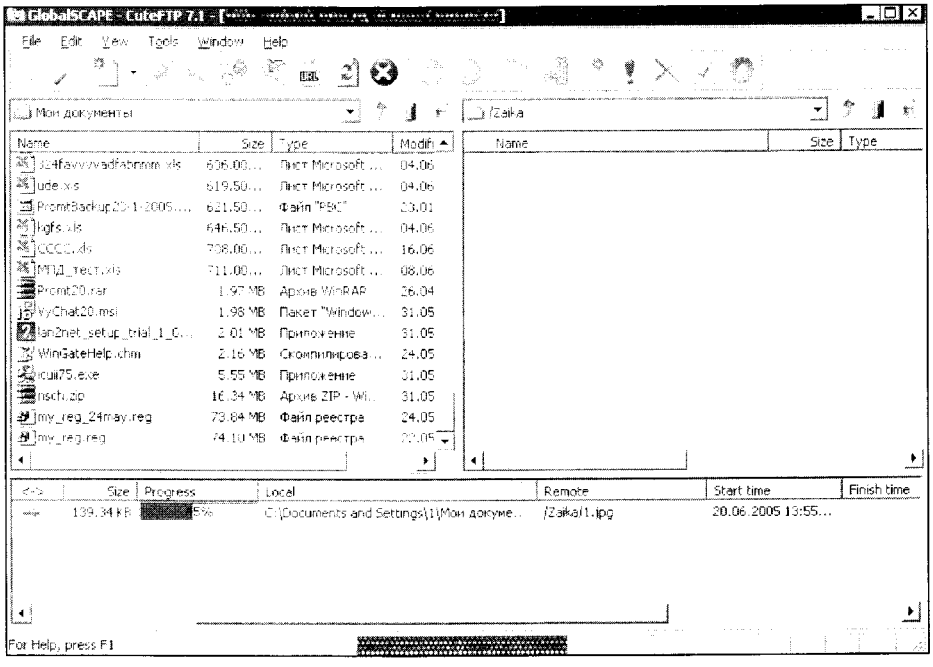


Рис. 17.32. Рабочее окно CuteFTP

Чтобы ввести идентификационную информацию, необходимую для подключения к FTP-серверу, можно воспользоваться так называемым **Site Manager** (программный модуль **Менеджер сайтов**). **Менеджер сайтов** позволяет создавать наборы учетных данных, объединенные под единым именем, и управлять ими. Для запуска модуля выберите меню **Tools ▸ Site Manager ▸ Display Site Manager** или нажмите на крайнюю левую кнопку панели инструментов с изображением раскрытой книги.

На рис. 17.33 изображено окно модуля **Site Manager**.

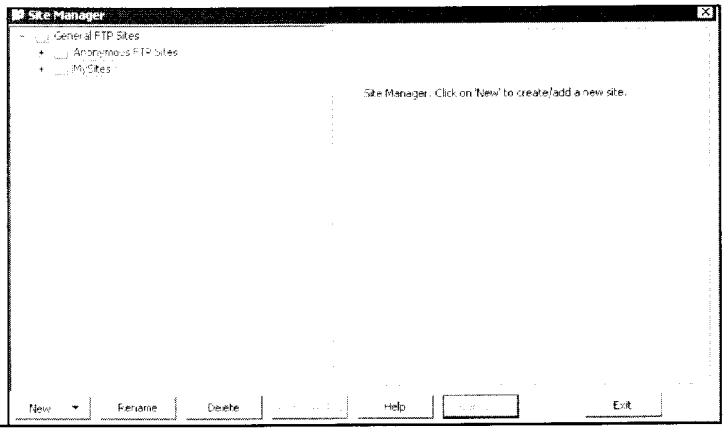


Рис. 17.33. Окно Site Manager

Это окно состоит из двух панелей. В левой панели показана структура хранящихся в **Site Manager** учетных записей, а в правой можно просматривать данные этих записей и редактировать их.

Учетные записи (или сайты) можно объединять в папки. По умолчанию **Site Manager** хранит множество предустановленных сайтов различных организаций и архивов. Как правило, это FTP-серверы, для входа на которые не требуется авторизации. Сайты можно «раскладывать» по папкам, которые объединяются в древовидную структуру. Работа с этими папками ничем не отличается от работы с обычными папками **Проводника Windows**.

Чтобы создать новую учетную запись FTP-сервера, достаточно нажать кнопку **New** и в выпавшем меню выбрать **FTP Site**. После этого новый сайт будет добавлен в активную папку и в правой части окна **Site Manager** вы увидите панель для правки его свойств (рис. 17.34).

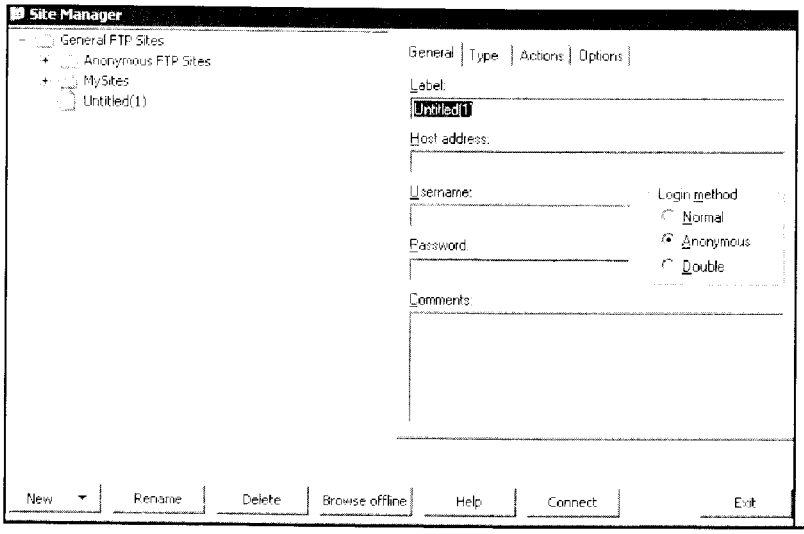


Рис. 17.34. Добавление учетной записи

- В поле **Label** нужно ввести метку, по которой вы сможете легко идентифицировать данную учетную запись. Это название FTP-сайта, которое дает ему сам пользователь (например, **Интересные мелодии**, **Программы для друзей** и так далее).
- Поле **Host Adress** предназначено для ввода адреса сервера. Например, это может быть что-то вроде *ftp.site.com* (это условный пример).
- В поле **Username** нужно ввести имя пользователя. Например, что-то вроде firstuser.
- Поле **Password** предназначено для ввода пароля.
- Обратите внимание на группу параметров **Login Method** (метод входа в систему). Если вы входите на сервер под определенным именем и используете пароль, следует переключить метод входа в систему на **Normal**. Иначе вы либо не войдете на сервер, либо войдете, но совсем не туда, куда планировали.

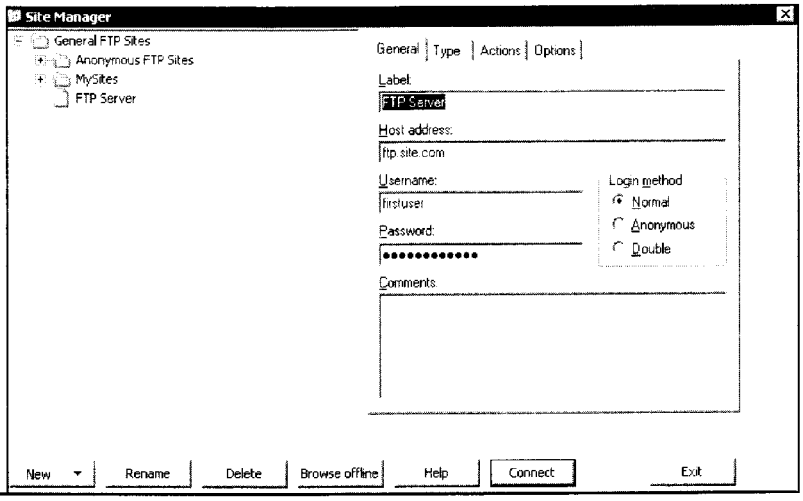


Рис. 17.35. Окно Site Manager после ввода данных

Вот и вся настройка FTP-клиента. Введенные вами параметры будут использованы для быстрого подключения к серверу.

После того как параметры введены, окно приобретает вид, показанный на рис. 17.35.

Теперь, чтобы подключиться к FTP-серверу, достаточно вызвать **Site Manager**, выбрать в его окне нужный вам сервер и нажать кнопку **Connect**. Если вы подключены к Интернету, то через некоторое время произойдет подключение к серверу.

Вернемся к основному окну программы. В процессе работы с сервером оно напоминает **Проводник Windows**. Разница состоит в том, что «проводник», отображающийся в левой части окна, служит для навигации по папкам локального (то есть вашего) компьютера, а тот, что находится справа, — для обзора папок FTP-сервера, к которому вы подключены. Копирование файлов с компьютера на сервер и наоборот осуще-

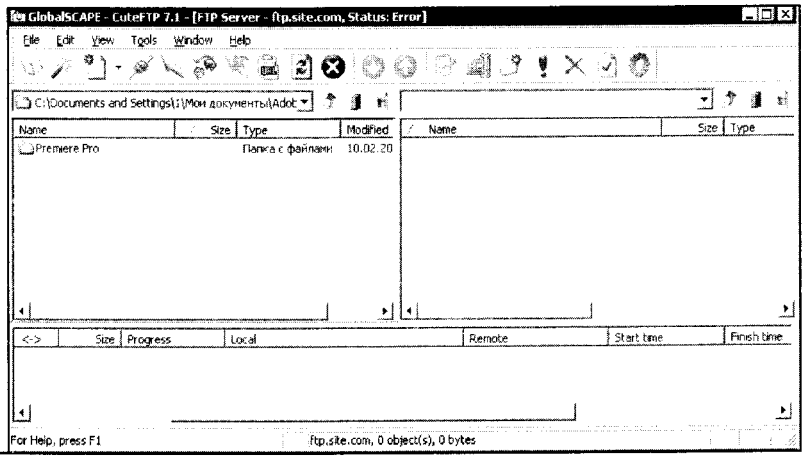


Рис. 17.36. Окно CuteFTP

ствляется простым перетаскиванием этих файлов: все делается в точности так же, как с локальными папками.

В процессе работы удобно пользоваться кнопками быстрого вызова функций программы (рис. 17.36).

- Как вы уже знаете, левая кнопка на панели инструментов в виде книжки служит для вызова менеджера файлов.
- Следующая кнопка с изображением волшебной палочки служит для вызова так называемого **Connection Wizard — Мастера соединений**. Этот Мастер позволяет создавать новые соединения.
- Кнопка с изображением документа позволяет вызвать диалог создания учетной записи. Этот диалог аналогичен тому, который возникает при нажатии кнопки **New** в **Site Manager**.
- Третья кнопка слева, изображающая соединенные провода, служит для установления соединения. К примеру, вы выбрали в **Site Manager** нужное соединение, попытались подключиться к серверу, но ничего не вышло. Для последующих попыток подключения к этому же серверу вам достаточно нажать на эту кнопку.
- Кнопка с изображением молнии служит для вызова панели быстрого подключения к серверу. На этой панели есть несколько полей, которые служат для ввода учетных данных, необходимых для входа на сервер.
- Кнопка с изображением разомкнутого кабеля служит для разрыва соединения.

Мы не будем рассматривать остальные кнопки панели инструментов, так как нужда в них возникает крайне редко.

Управлять файлами в программе CuteFTP можно из контекстных меню, которые вызываются щелчком правой кнопки мыши по соответствующему файлу.

Теперь посмотрите на рис. 17.37. Здесь изображен полный вид окна программы со всеми включенными панелями (для управления ими служит пункт меню **View ▸ Show panes**).

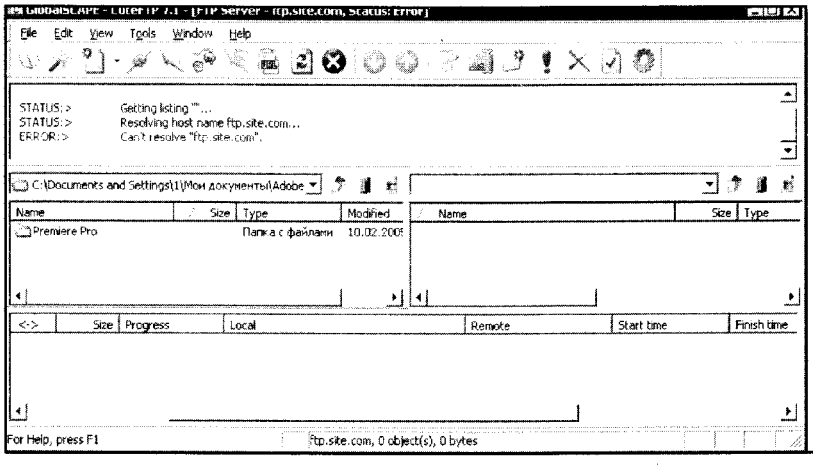


Рис. 17.37. Окно CuteFTP

- Самая верхняя — панель протокола (**Log Pane**). На ней отображается информация о командах, которые использует FTP-клиент.
- Назначение двух центральных панелей вы уже знаете. Правая — панель FTP-сервера, левая — панель локальной системы.
- Нижняя панель — панель очереди (**Queue pane**): когда вы выгружаете файлы на сервер или загружаете их с сервера, здесь появляется список загружаемых/выгружаемых файлов с информацией о ходе выполнения операции.

Кроме прочего, программа умеет «докачивать» файлы, передача которых по каким-то причинам была прервана.

В программе CuteFTP немало и других возможностей, но сейчас нам важно научиться работать с FTP-серверами. Если вы внимательно читали страницы, посвященные этой программе, вы сможете работать с любым FTP-клиентом и с любым FTP-сервером.

Порой начинающие пользователи спрашивают: «Зачем мне FTP-сервер, если есть, скажем e-mail?» Все очень просто. Решив создать свой сайт, вы не сможете обойтись без использования FTP-клиента. Ну а если у вам нужно регулярно передавать достаточно большие файлы, то скоро вы заметите: при передаче их по электронной почте примерно третья часть вашего трафика тратится впустую. К примеру, файл размером 1000 Кбайт при передаче по e-mail может превратиться в письмо объемом 1,3 Мб. В таких случаях личный FTP — это очень удобный выход.

Поговорив о FTP-клиенте, переходим к не менее полезной программе — менеджеру закачек.

17.6. МЕНЕДЖЕР ЗАКАЧЕК

Все интернет-пользователи скачивают из Сети нужные им файлы. Байты файлов тонкой струйкой текут по каналам связи и на локальных компьютерах собираются в программы, текстовые документы и картинки. Стандартные средства для загрузки файлов из хранилищ информации Интернета представлены довольно примитивной (хотя в то же время простой, удобной и стабильной) функцией браузера Internet Explorer. Другие браузеры тоже имеют средства для загрузки файлов, но в любом случае эти средства — лишь небольшая часть основной программы. А частям и частностям уделяют куда меньше внимания, чем основным функциям. Разработчики придают им лишь базовую функциональность, а пользователи, которым нужна удобная и стабильная программа, вынуждены использовать продукты сторонних разработчиков. В случае с программами для загрузки файлов все обстоит именно так. К примеру, стандартный загрузчик IE не умеет докачивать файлы и не имеет средств управления своей работой, оставляя на усмотрение пользователя лишь имя, которое получит загружаемый файл и место на жестком диске, куда он будет сохранен. К тому же закачиваемый файл загружается без разбиения его на части, а это не позволяет использовать для загрузки всю пропускную способность даже такого сравнительно «тонкого» канала, как *dial-up*.

Менеджеры закачек нужны, чтобы удобнее и быстрей скачивать файлы из Сети. Один из них называется FlashGet (в нашем случае это версия 1.65), его дистрибутив можно скачать на сайте *http://www.amazesoft.com/*. Ранее программа называлась JetCar, иногда можно встретить это название при ее упоминании.

FlashGet следит за ссылками в веб-браузере: если вы нажали на ссылку, ведущую к закачке файла, FlashGet предложит вам свои услуги. Перехватив закачиваемый файл у стандартного загрузчика, FlashGet поместит его в список загрузки и займется им вплотную. Программа разобьет файл на несколько частей и начнет их параллельную загрузку. Этот процесс наглядно отображается в ее рабочем окне (рис. 17.38).

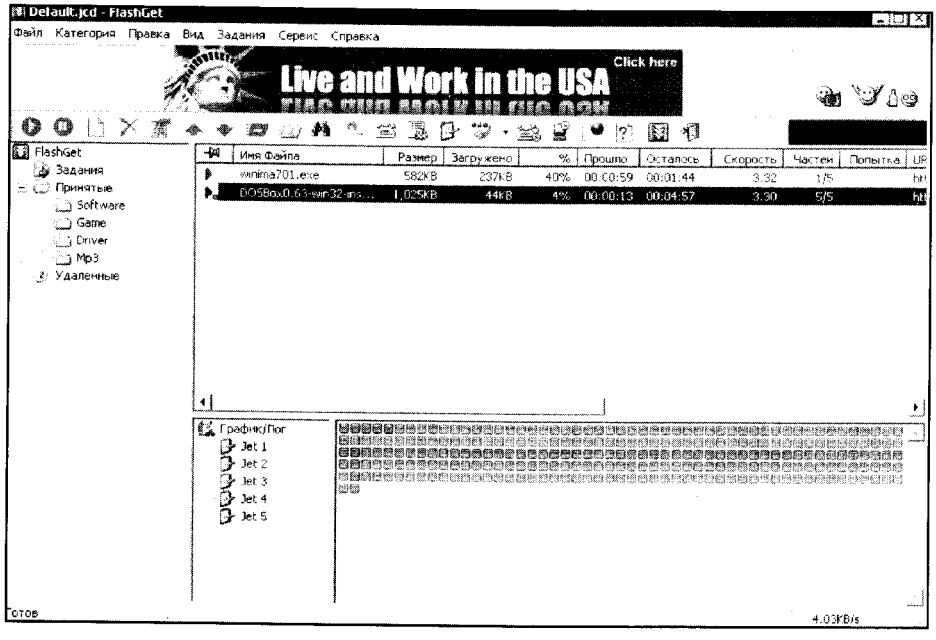


Рис. 17.38. Окно FlashGet во время загрузки файлов

Программа может одновременно закачивать несколько файлов. После выкачивания из Сети определенного фрагмента файла этот фрагмент сохраняется на диске. Программа сможет докачать файл с сохраненного места.

Докачивание обычно проходит без проблем. Если вы ранее не сталкивались с подобными программами, то вам наверняка знакомы проблемы, которые возникают при их неиспользовании для закачки файлов.

Случайное обесточивание вашего компьютера, неожиданный обрыв соединения с Интернетом, зависание компьютера — все это почти наверняка приведет к необходимости скачивать файл снова. Используя FlashGet, вы застрахованы от подобных неожиданностей. Это особенно

важно при загрузке больших файлов по медленным каналам связи: здесь без докачивания просто не обойтись.

Помимо удобной закачки файлов, программа FlashGet поддерживает различные сервисные операции. К примеру, можно указать программе, чтобы она разорвала соединение или выключила питание компьютера после окончания закачки последнего файла в очереди. Сейчас мы рассмотрим назначение некоторых наиболее полезных в практической работе пунктов меню программы, благодаря которым реализуется ее функциональность.

Самыми полезные и часто используемые функции программы скрываются в меню **Сервис**.

Пункт меню **Сервис ▸ Отключить питание по завершении заданий** позволяет выключать питание компьютера после завершения закачки.

Пункт **Сервис ▸ Разорвать соединение по завершении** разрывает соединение после завершения закачки.

Пункт меню **Сервис ▸ Режим использования трафика** позволяет настраивать отношение программы к трафику: если этот параметр установить в значение **Сервис ▸ Режим использования трафика ▸ Неограниченный**, программа заберет для своих целей максимум ресурсов соединения. На обычном модемном соединении это приводит к тому, что другие программы оказываются практически полностью отрезанными от Интернета, зато закачка файлов ведется на максимально возможной скорости.

Наиболее употребительные настройки программы вынесены в так называемую **Корзину FlashGet**. Ее полупрозрачная пиктограмма по умолчанию появляется в правом верхнем углу рабочего стола. На рис. 17.39 изображены **Корзина** и меню, которое появляется при щелчке по ней правой кнопкой мыши.

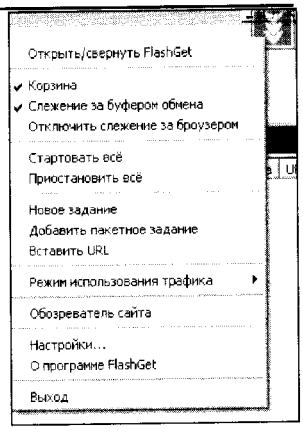


Рис. 17.39. Меню Корзины FlashGet

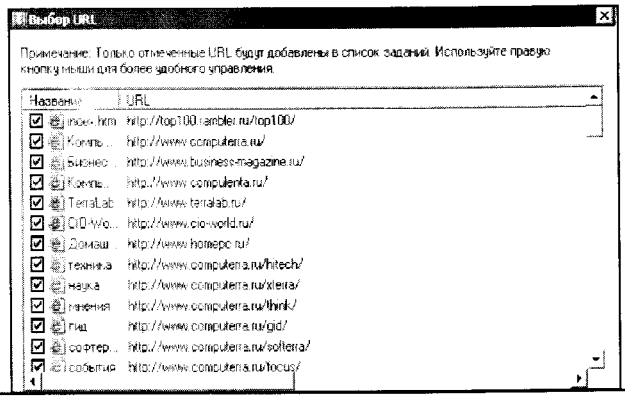


Рис. 17.40. Закачка нескольких файлов, выбор URL

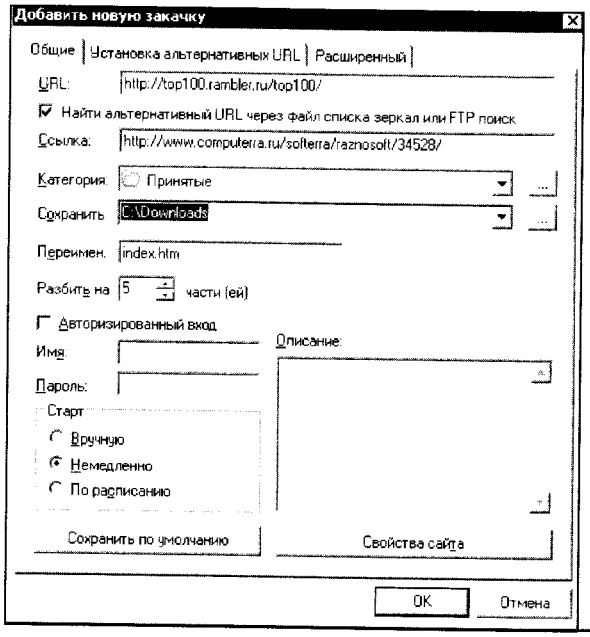


Рис. 17.41. Добавление новой закачки

Как мы уже говорили, чтобы добавить новое задание на закачку файла, можно просто щелкнуть по подходящей ссылке в браузере. Если на веб-страничке есть несколько файлов, которые нужно скачать, то можно выполнить операцию добавления нескольких файлов. Делается это так: сделайте щелчок правой кнопкой по нужной страничке и в появившемся меню выберите параметр **Закачать все при помощи FlashGet**. После этого появится диалог добавления нового задания (рис. 17.40).

Чтобы удалить из закачки ненужные файлы, достаточно снять стоящие против них галочки.

В программе есть еще одна очень полезная возможность: использование фильтра. Фильтр позволяет выбирать файлы определенных расширений с определенных серверов. Если нажать кнопку **Фильтр** в окне **Выбор URL**, появится небольшое окошко. В левой части этого окна отображается список адресов серверов, на которых находятся файлы, добавленные в задание автоматически, а в правой — список расширений файлов. Можно быстро отфильтровать ненужные вам файлы, снимая и устанавливая галочки напротив ненужных или нужных вам расширений и адресов. Скажем, если вам нужно скачать с некой странички все *.RAR и *.ZIP-файлы, можно выбрать в списке расширений эти два расширения, а остальное программа сделает автоматически.

После выбора файлов для загрузки и нажатия кнопки **OK** появится окно добавления нового задания (рис. 17.41).

В этом окне будет представлена одна из закачек группы. Настраиваемые для нее параметры будут автоматически применены для других файлов группы. Самая полезная настройка из имеющихся здесь — па-

раметр **Сохранить**. Он указывает папку, в которую следует сохранить загружаемые файлы. По умолчанию здесь указана папка, общая для всех загрузок, но пользователь может указать иную папку или просто написать новое имя папки. К примеру, если ввести в поле текст: **C:\Dodnloads\New_soft**, файлы будут загружены в папку New_soft.

Остальные установки не слишком важны. В большинстве случаев пользователю достаточно определить папку для загрузки выбранной группы файлов. После нажатия кнопки **OK** задания будут добавлены в очередь и начнется их загрузка.

В процессе загрузки можно удалять текущие задания, выделяя их и вызывая контекстное меню нажатием правой кнопки мыши. Если вы желаете начать закачку нескольких файлов после перерыва, для этого следует использовать пункт меню **Задания ▸ Стартовать все**. Для приостановки всех заданий можно использовать пункт меню **Задания ▸ Приостановить все**.

Теперь рассмотрим некоторые полезные настройки программы. Чтобы открыть окно свойств FlashGet, выберите пункт меню **Сервис ▸ Настройки**. Начнем с вкладки **Общие** окна настроек FlashGet (рис. 17.42).

Настройки вкладки **Общие** достаточно очевидны. Отметим, что в сложных условиях работы (например, при очень плохом модемном соединении, которое то и дело рвется) можно попытаться уменьшить параметр **Записывать на диск каждые x KB**. Это может сэкономить довольно много времени.

Параметр **Автосохранение списка каждые x мин**. позволяет настроить промежуток времени для автосохранения списка закачиваемых файлов. Если компьютер по неким причинам работает нестабильно, например случаются частые зависания, этот параметр следует уменьшить.

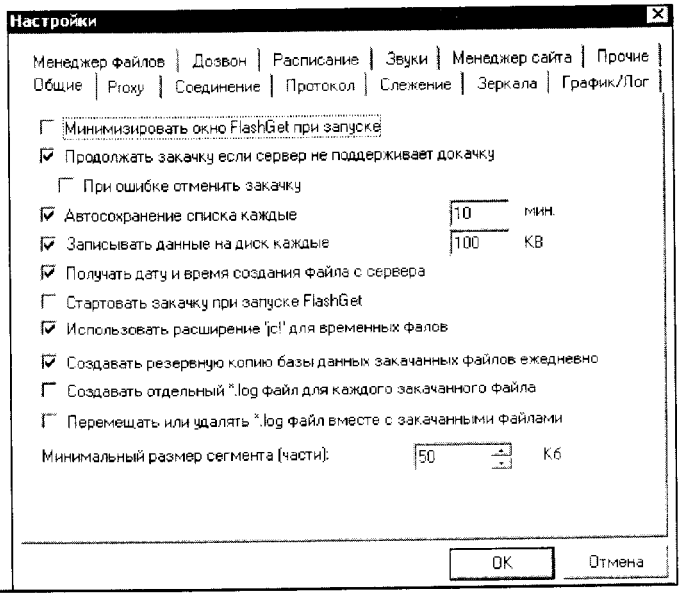


Рис. 17.42. Настройка общих параметров FlashGet

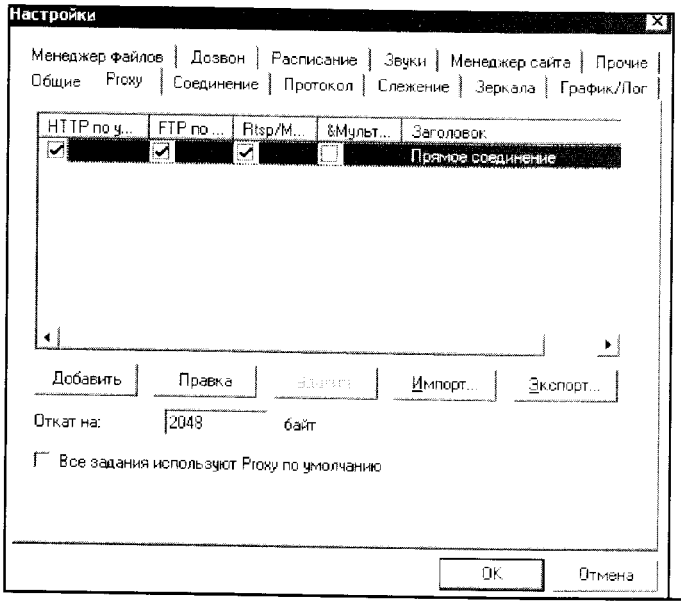


Рис. 17.43. Настройки Proxy-сервера

Вряд ли нужно объяснять, для чего нужен параметр **Создавать копию базы закачанных файлов ежедневно**. Эта база по умолчанию хранится в файле Default.jcd. Если информация о выполняемых заданиях будет утеряна, продолжить закачку недогруженных файлов будет невозможно. При включенном параметре **Создавать копию базы закачанных файлов ежедневно** FlashGet ежедневно создает копию этого файла. Копии имеют вид default.bk1, default.bk2, default.bk3. При потере или повреждении базы данных загрузки эти файлы можно использовать для замены поврежденного Default.jcd.

Следующая вкладка называется **Proxy**. Здесь вводятся настройки для использования программы совместно с прокси-сервером (рис. 17.43).

В список прокси-серверов можно добавлять новые серверы нажатием кнопки **Добавить**. После нажатия этой кнопки появится диалоговое окно, где нужно заполнить свойства сервера. Те, кто используют прокси, легко настроят эти параметры.

Обратите внимание на параметр **Откат на: х байт**, который по умолчанию установлен в 2048. Дело в том, что при использовании HTTP-прокси ошибки, которые возникают в процессе закачки файла, добавляются в файл. Единственное «лекарство» от подобных проблем — перекачивание файла заново. Опция **Откат на: х байт** используется, чтобы оперативно исправить ошибку.

Группа параметров **Соединение** позволяет настраивать параметры интернет-соединения (рис. 17.44).

Параметр **Макс. количество заданий** по умолчанию установлен на три задания. Это оправданно, если вы выкачиваете из Сети крупные архивы. Но при загрузке длинного списка небольших файлов ситуация резко

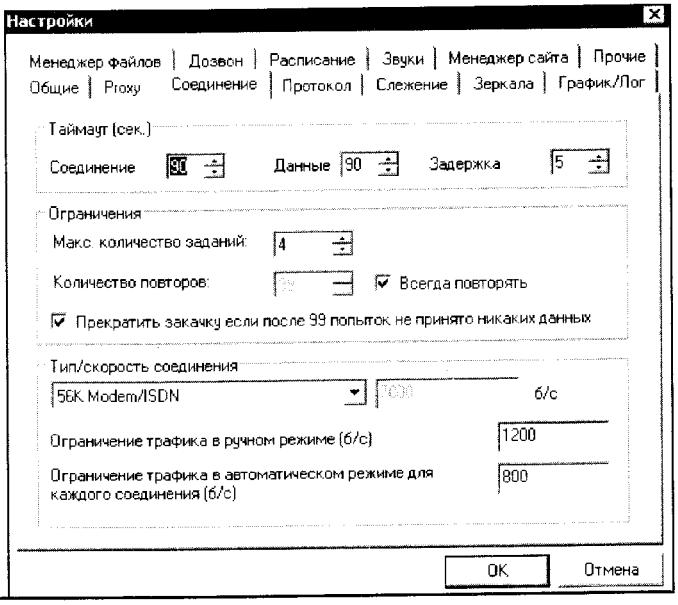


Рис. 17.44. Настройки параметров соединения

меняется. В этом случае лучше увеличить значение максимального количества заданий до пяти или семи. Запустив достаточно много параллельных закачек, вы более полно и рационально загрузите свой канал связи.

Скачивание небольших файлов, скажем, размеры которых находятся в пределах 150–200 Кбайт, не позволяет разбивать их на достаточное количество фрагментов. Если большой файл разбивается по умолчанию на пять параллельных потоков, то маленький, скажем, 200-килобайтный, — от силы на 3–4. В результате не все ресурсы соединения используются на полную мощность.

Следующая вкладка окна свойств называется **Протокол** и служит для настройки некоторых параметров, касающихся имитации FlashGet'ом браузеров и других подобных программ. В ручной настройке протокол нуждается редко, поэтому мы не будем останавливаться на этой вкладке, а также на остальных вкладках окна настройки, за исключением вкладки **Дозвон**.

Пропущенные нами вкладки любопытны, но их параметры редко нуждаются в ручной настройке и не настолько важны, чтобы их настройка могла привести к серьезным изменениям в работе программы. К тому же, как вы уже могли заметить выше, основная масса параметров программы довольно очевидна. По крайней мере, для достаточно продвинутых пользователей.

Мы продолжим разговор о настройках программы с вкладки **Дозвон** (рис. 17.45).

По умолчанию FlashGet не использует дозвон. Для удобства работы с программой эту функцию можно включить, выбрав в списке **Соединение** соответствующее интернет-соединение.

С помощью FlashGet вы сможете легко справиться с любой закачкой. Или почти с любой. Есть один довольно специфический вид закачек, который требует не менее специфических инструментов: речь идет о загрузке на локальный компьютер не отдельных файлов и даже не их списков, а целых сайтов или, по крайней мере, их разделов. О программе, предназначенной для выполнения этой операции, читайте дальше.

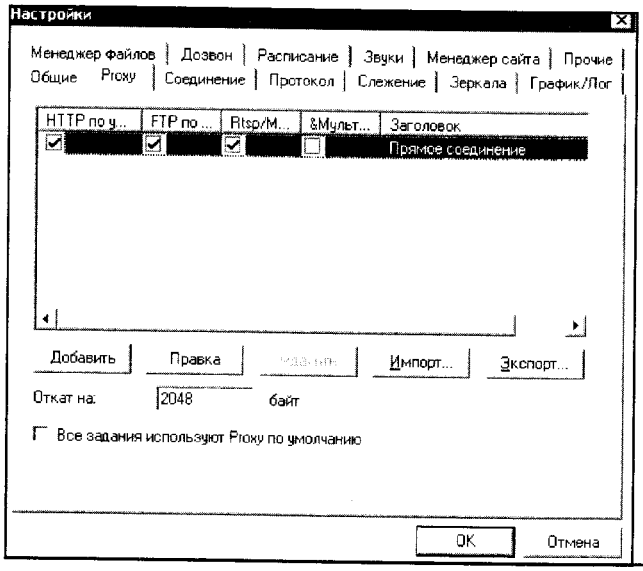


Рис. 17.45. Вкладка Дозвон

17.7. ЗАГРУЖАЕМ САЙТЫ

Порой на просторах Интернета встречаются такие сайты, что хочется скачать их на свой компьютер целиком или выкачать сотню-другую страничек этого сайта — да чтобы с картинками и чтобы работало это все на локальной машине «как родное». Как правило, это хорошие электронные учебники или книги, авторы которых желают, чтобы их читали только на их собственном сайте.

Если для копирования сайта использовать вышеописанный FlashGet или другой менеджер закачек, получится совсем не то, чего вы ожидали, да и вряд ли удастся получить достаточно удобную, с нормальной навигацией, локальную копию сайта. Для таких операций есть специальные программы, к примеру программа Teleport Pro. Ее дистрибутив, «весящий» порядка 700 Кбайт, можно скачать с сайта *http://www.tenmax.com/*.

Работать с такими программами просто. Вы указываете ей страничку, копию которой хотите получить (вместе со страницами, ссылки на кото-

рые есть на этой странице, а при необходимости и более «глубокие» документы), указываете глубину вложенности страниц и объекты, которые желательно загрузить. После этого программа стартует и начинает загружать материалы сайта или раздела сайта на ваш компьютер. Teleport Pro умеет разбивать закачиваемые в процессе выполнения задания файлы на параллельно загружаемые части, а это хорошо сказывается на полноте использования канала связи. Программа также умеет создавать зеркала сайтов, осуществляет фильтрацию закачки, выполняет поиск документов по ключевым словам и так далее.

Рассмотрим пример настройки закачки, после разбора которого вы сможете справиться с остальными функциями программы самостоятельно.

На рис. 17.46 изображено рабочее окно программы Teleport Pro.

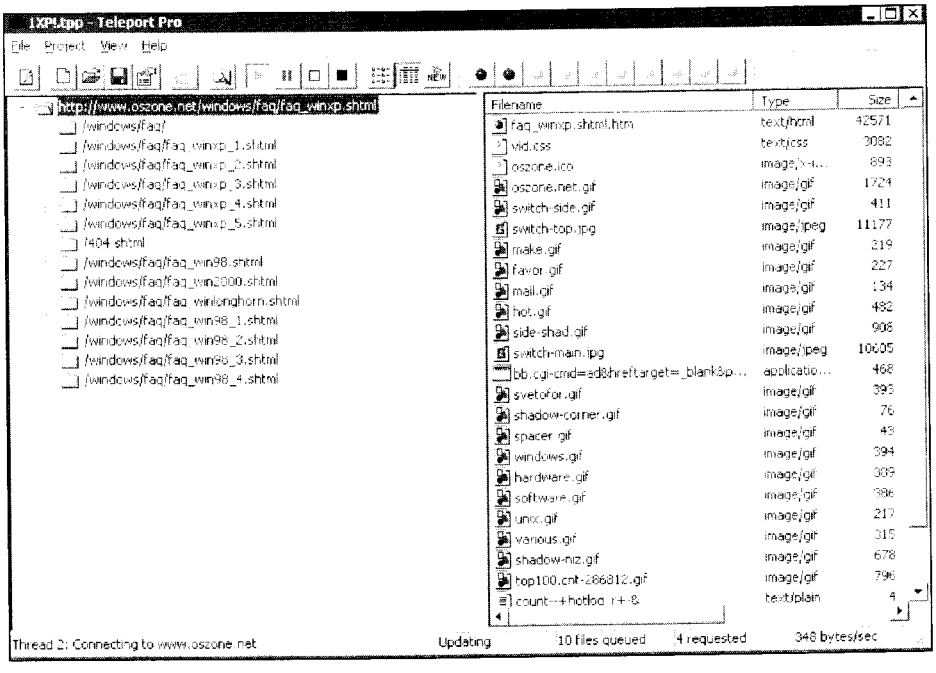


Рис. 17.46. Рабочее окно Teleport Pro

В левой панели видно древовидное изображение загруженных страничек, а в правой — относящиеся к выделенной страничке файлы.

Чтобы начать закачку, достаточно запустить программу и выполнить команду меню **File ▶ New Project Wizard**. Этой командой запускается Мастер настройки нового проекта и подготавливается все, что нужно для загрузки. На рис. 17.47 изображено первое окно Мастера.

В окне **New Project Wizard** виден длинный список опций. Здесь собраны все основные возможности программы, и дальнейшие ее дейст-

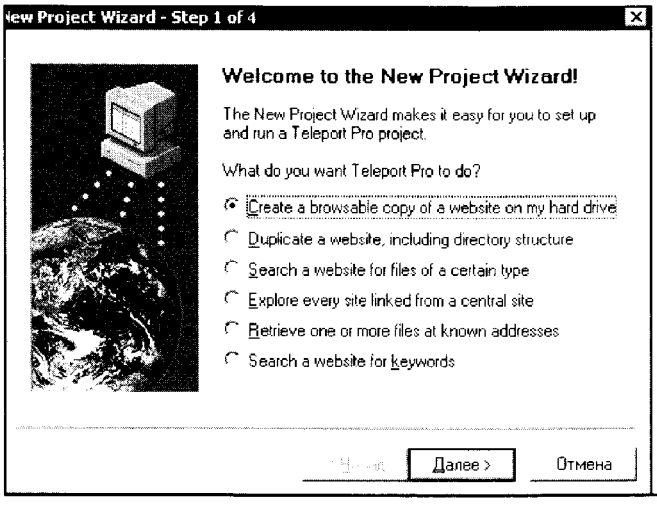


Рис. 17.47. Первое окно New Project Wizard

вия напрямую зависят от выбора типа проекта, сделанного вами в этом окне. Мы разберем назначение каждого из пунктов, а потом пройдемся по одному из них.

Проекты Teleport Pro оперируют понятием «стартовая точка» (или стартовый адрес — **Starting Address**). Стартовая точка — это страничка, с которой начинается загрузка. К примеру, вы нашли в Интернете электронный учебник. На сайте есть оглавление учебника, ссылки которого ведут на страницы с главами. В качестве стартовой точки следует указать страницу с оглавлением. Точно так же вам придется поступить и в других случаях определения стартового адреса.

- Опция **Create a browsable copy of a website on my hard drive** позволяет создать «плоскую» копию сайта на вашем жестком диске. Эта копия будет содержать все файлы, необходимые для работы сайта. При скачивании программа создает файл проекта и папку, хранящую загруженные файлы сайта. Этот тип проекта чаще всего применяется для создания копий сайтов. При этом все загружаемые файлы располагаются в одной папке, то есть программа не пытается восстановить структуру папок на сервере. Поэтому некоторые файлы в процессе закачки могут быть переименованы, чтобы избежать проблем с именами.
- Опция **Duplicate a website including directory structure** используется для создания зеркал сайта. Работая в этом режиме, программа сохраняет структуру папок и фактически копирует сайт на ваш компьютер точно в том же виде, в каком он находится на сервере. Если вы хотите уверенности в том, что все имена файлов скачанного вами сайта будут совпадать с оригиналом, выберите эту опцию.
- Опция **Search a website for files of a certain type** позволяет заниматься поиском определенных файлов на сайте и загружать на свой компьютер только их. Это могут быть, например, графические файлы, файлы архивов, исполняемые файлы и так далее. С помощью этой

- Меню **File ▸ Proxy Server** позволяет настроить свойства прокси-сервера.
- Меню **File ▸ Dial-Up Connection** настраивает свойства модемного соединения.
- Меню **File ▸ Free Space Limit** позволяет устанавливать минимальный объем свободного места на диске, после которого следует прекратить закачку. По умолчанию это 24 мегабайта. Этот параметр адресован обладателям небольших жестких дисков.
- Меню **File ▸ Minimize to System Tray** сворачивает программу в системную панель Windows, если она не используется.

Разобраться в настройках программы Teleport Pro стоит хотя бы для того, чтобы эффективно скачивать нужные сайты и наслаждаться их чтением и просмотром, не думая о деньгах, утекающих через дорогое *dial-up*-соединение.

Следующая программа, которую мы рассмотрим, называется ICQ и пользуется заслуженной любовью всех, кто с ней знаком.

17.8. ICQ

Придумано множество способов и программ для общения в Сети. Да и сама Всемирная Сеть создана, в сущности, ради того, чтобы один человек обменялся с другим парой фраз.

Программы для мгновенного обмена сообщениями (их также называют мессенджерами — от английского слова *messenger*) по своей сути ближе всего к реальному общению людей. Электронные письма путешествуют довольно быстро, но никто не требует от адресата мгновенного ответа. Это формирует особый стиль общения: письма пишутся долго и вдумчиво, их перечитывают и переписывают, чтобы лучше выразить свои мысли. И совсем другое дело — программы для мгновенного обмена сообщениями: здесь общаются коротким, отрывочными фразами, что формирует особый стиль письменной речи. Кроме слов, при общении по интернет-мессенджеру используют самые разные смайлики, или эмотиконы. Общение в ICQ часто отличается эмоциональностью.

Программа ICQ очень, очень популярна. В последнее время номер ICQ (он называется UIN, то есть уникальный идентификационный номер) превращается в нечто вроде телефонного номера: его указывают на визитках, на страничках служб технической поддержки и так далее.

Для установки ICQ потребуется скачать ее дистрибутив со страницы *http://www.icq.com/download*. Программа полностью русифицирована, поэтому можно скачать ее локализованную версию. Общаются в ICQ посредством ICQ-сервера, и в этом смысле работа с программой напоминает обычную электронную почту.

Установка программы стандартна, а регистрация ее на сервере ICQ довольно проста.

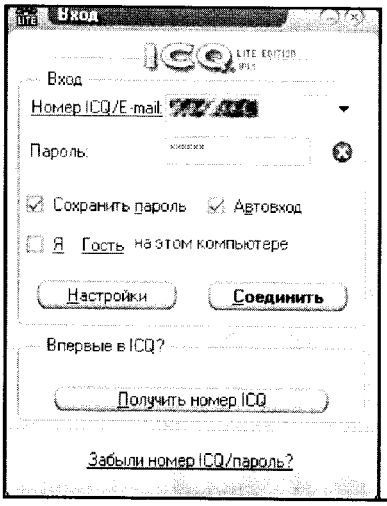


Рис. 17.50. Стартовое окно ICQ

Регистрация может запуститься автоматически. Ну а если автоматической регистрации не произошло, запустите ICQ, выбрав ее из списка **Все программы** или дважды щелкнув по иконке на системной панели Windows. Кстати сказать, этот значок сделан в виде цветка, который меняет цвет в зависимости от состояния программы.

На рис. 17.50 изображено стартовое окно программы, из которого можно запустить процесс регистрации или, введя свои учетные данные, войти в ICQ.

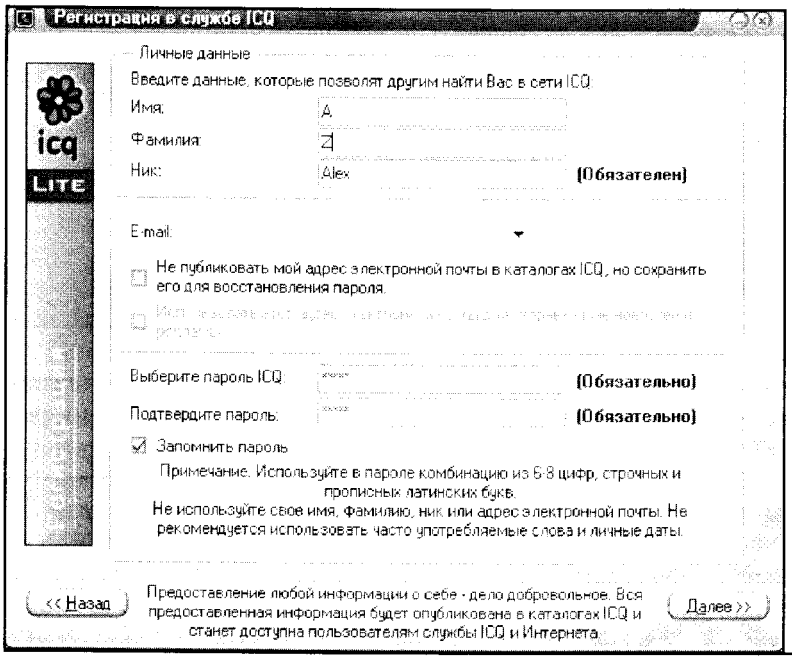


Рис. 17.51. Начало регистрации в ICQ

Процесс регистрации начинается с нажатия кнопки **Получить номер ICQ**. Вам зададут множество вопросов: спросят имя, фамилию, ник, e-mail и даже попросят назначить пароль к ICQ (рис. 17.51). Напротив полей, заполнить которые необходимо, есть надпись **Обязателен**, но таких полей крайне мало: свои данные можно ограничить ником да паролем к ICQ.

Программа предупреждает, что вся введенная информация будет опубликована в каталогах ICQ и будет доступна пользователям ICQ и Интернета. Если вы хотите оставаться инкогнито, не заполняйте необязательных полей.

В следующем окне регистрации множество полей для заполнения, но все они необязательны. После нажатия на очередную кнопку **Далее** программа попытается зайти на сервер ICQ, чтобы зарегистрировать вас. Для этого нужно подключение к Интернету. Если все прошло успешно — вы получите вот такое сообщение (рис. 17.52).

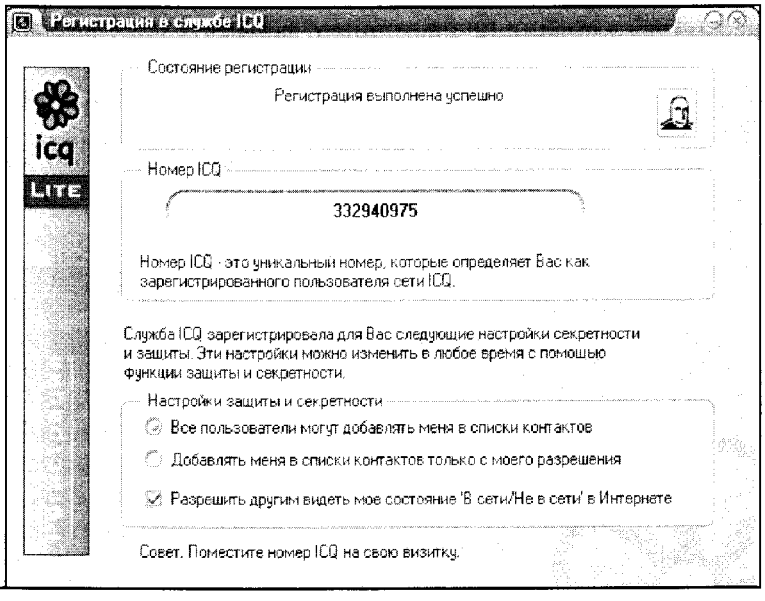


Рис. 17.52. Успешно завершенный процесс регистрации

При желании можно позднее войти в параметры программы и ввести дополнительную информацию о себе, то есть после завершения регистрации.

Система регистрации ICQ весьма «любопытна» и предлагает вам ввести о себе множество данных. Но это дело сугубо добровольное: можно ограничиться минимумом сведений, которые вы хотите сообщить о себе, ну а если вы желаете интенсивно общаться и находить новых друзей, тогда заполняйте подробную анкету.

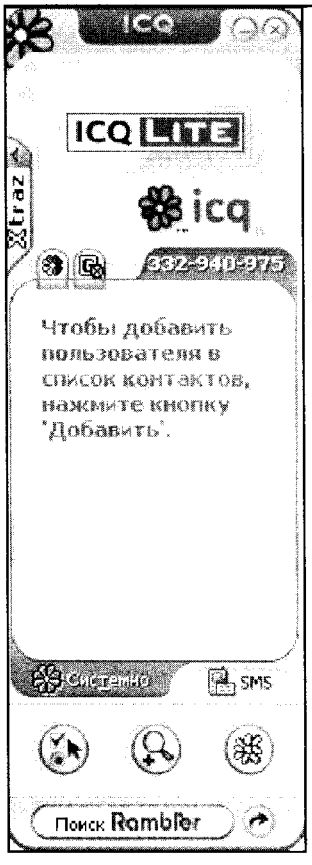


Рис. 17.53. Главное окно ICQ

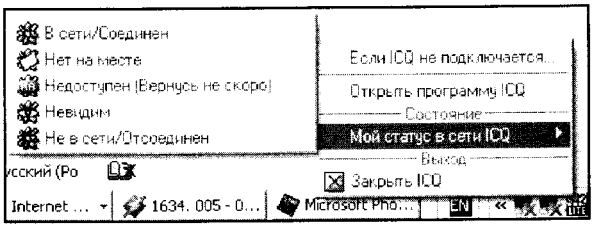


Рис. 17.54. Меню и значок ICQ в системной панели Windows

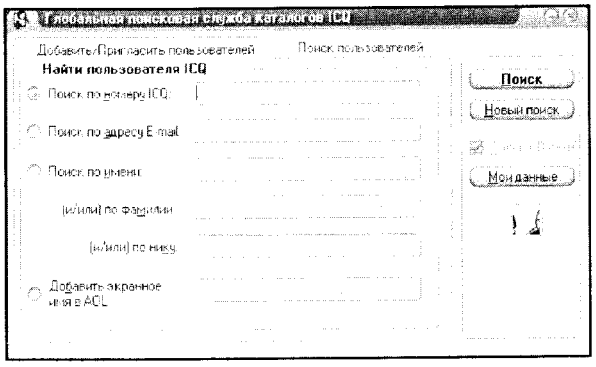


Рис. 17.55. Глобальная поисковая служба каталогов ICQ

В результате регистрации сервер присваивает вам ICQ UIN (*Universal Identification Number*). Этот номер сейчас представляет собой девятизначное число, например что-то вроде 000-000-000. UIN — это ваша основная «координата» в ICQ.

Далее описывается версия ICQ Lite Edition v. 4.1.

Установив ICQ на домашнем компьютере, вы можете включить опции сохранения пароля и автоматического входа, чтобы не вводить каждый раз UIN и пароль для входа в систему.

После нажатия кнопки **Запуск** (рис. 17.52) произойдет запуск программы с вашими учетными данными и ее окно примет вот вид, изображенный на рис. 17.53. Это основное окно ICQ, с которым вам придется работать. Большую его часть занимает список контактов. В нашем случае он пуст, так как программа только что установлена.

Взгляните на меню, которое вызывается двойным щелчком по значку программы в системной панели. Этот значок оповещает пользователя о состоянии программы. Красные лепестки логотипа ICQ означают, что она не соединена с сервером, а зеленые показывают, что программа подключилась к серверу и что по ней можно общаться.

Между этими крайними состояниями есть промежуточные. Посмотрите на рис. 17.54. Здесь изображено меню, появляющееся при щелчке на пиктограмме программы в системной панели правой кнопкой мыши.

Им удобно пользоваться для открытия программы (пункт **Открыть программу ICQ**) и для смены вашего статуса в сети ICQ (пункт **Мой статус в сети ICQ**).

Когда вы входите в Интернет, программа устанавливает соединение с сервером и вы готовы к общению. Если вам напишут сообщение в то время, когда вы не подключены к системе, это сообщение сохранится на сервере и придет во время следующего подключения. Если вы находитесь в Сети и кто-нибудь из вашего списка контактов войдет в Сеть, программа оповестит вас об этом весьма характерным звуком, напоминающим стук в дверь, — послушайте сами.

Для заполнения списка контактов нужно добавить в него пользователей, а для этого сначала найти их. Для запуска поиска нажмите кнопку **Добавить/пригласить пользователей** в нижней части окна программы (на ней изображено увеличительное стекло). При этом появится окно для поиска и добавления новых пользователей в ваш контакт-лист (рис. 17.55).

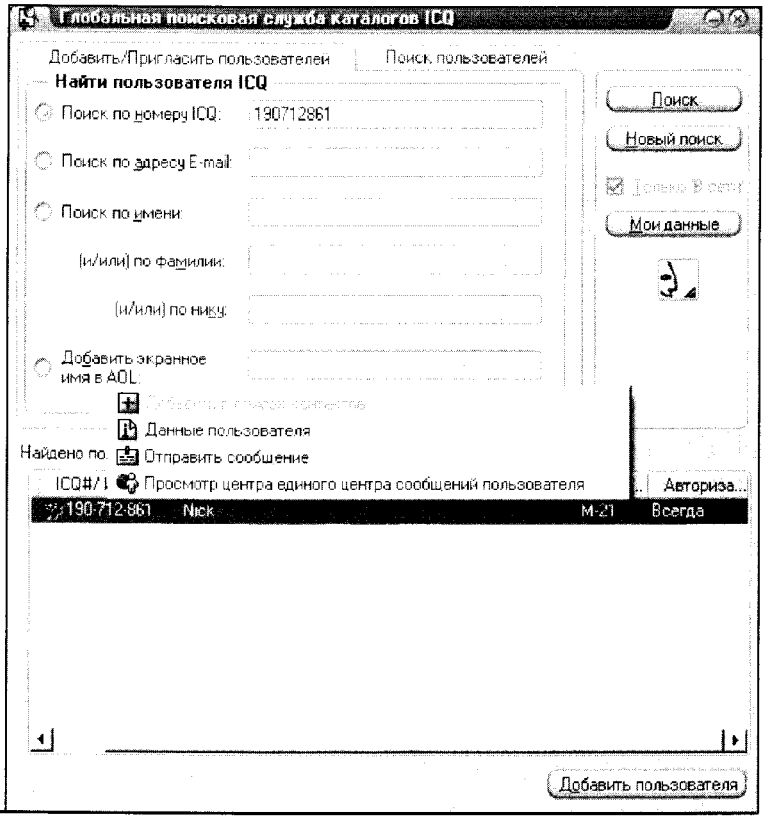


Рис. 17.56. Поиск и добавление пользователя

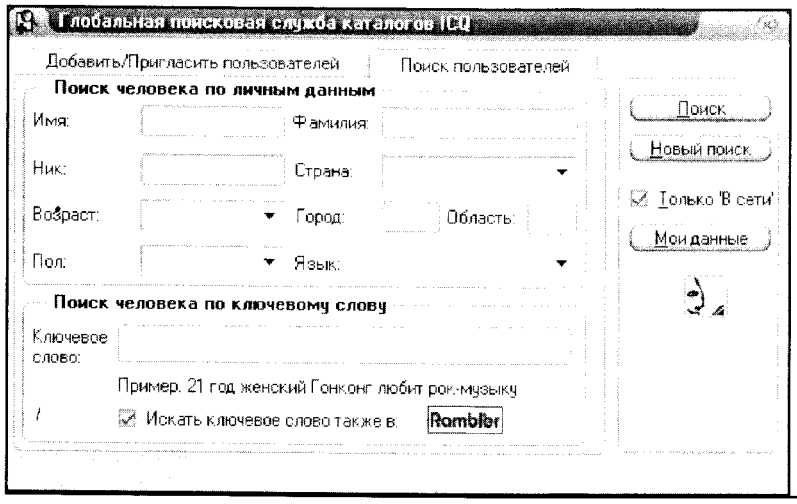


Рис. 17.57. Поиск человека по личным данным и по ключевому слову

По умолчанию в данном окне активирована вкладка **Добавить/пригласить пользователей.**

Введите известный вам ICQ UIN в окошко **Поиск по номеру ICQ**. Если вы ввели ICQ UIN правильно, вы увидите результаты поиска, то есть данные пользователя, которому принадлежит этот номер (рис. 17.56).

Щелкнув правой кнопкой мыши по строке с информацией о найденном пользователе, можно просмотреть его данные, добавить пользователя в список контактов или отправить ему сообщение.

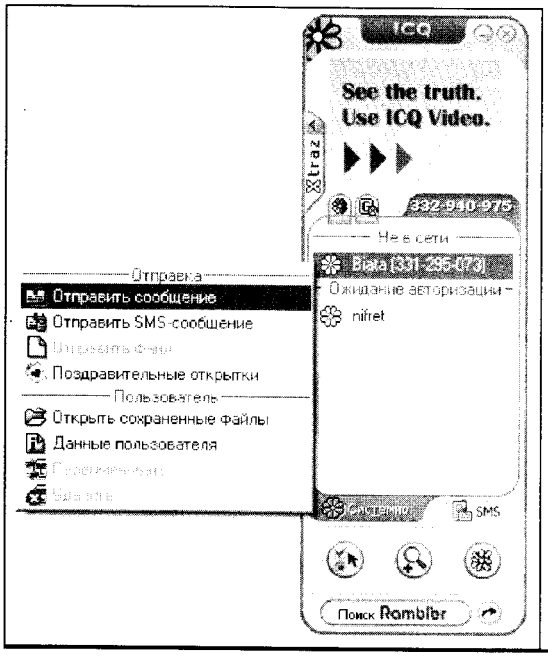


Рис. 17.58. Работа с контактами в списке контактов

Помимо номера ICQ можно использовать для поиска пользователя его e-mail, ник, имя фамилию. Для этого нужно активировать соответствующие переключатели в окне поиска и добавления пользователей.

В ICQ есть еще один вид поиска, где в качестве параметров можно задавать личные данные человека или ключевые слова (рис. 17.57). Такой поиск осуществляется на вкладке **Поиск пользователей** окна **Глобальная поисковая служба каталогов ICQ**. Если вы ищете пользователей на этой вкладке, подумайте над тем, чтобы снять галочку параметра **Только «В сети»**, который расположен в правой части окна. Если включить этот параметр, то служба поиска ICQ будет перебирать только тех пользователей, что в данный момент подключены к серверу, а нужный вам человек может находиться в оффлайне. К примеру, если вы живете в небольшом городе и хотите найти друзей, введя его название в поле **Город**, то при установленной галочке **Только в сети** вы рискуете не найти никого или найти одного-двух пользователей.

Когда ваш список контактов начнет заполняться, окно ICQ примет примерно такой вид (рис. 17.58).

Щелкнув правой кнопкой мыши по строке с ником пользователя, можно, воспользовавшись контекстным меню, отправить ему сообщение, SMS-сообщение, отправить файл, посмотреть данные пользователя. Самым распространенным способом общения в ICQ является от-

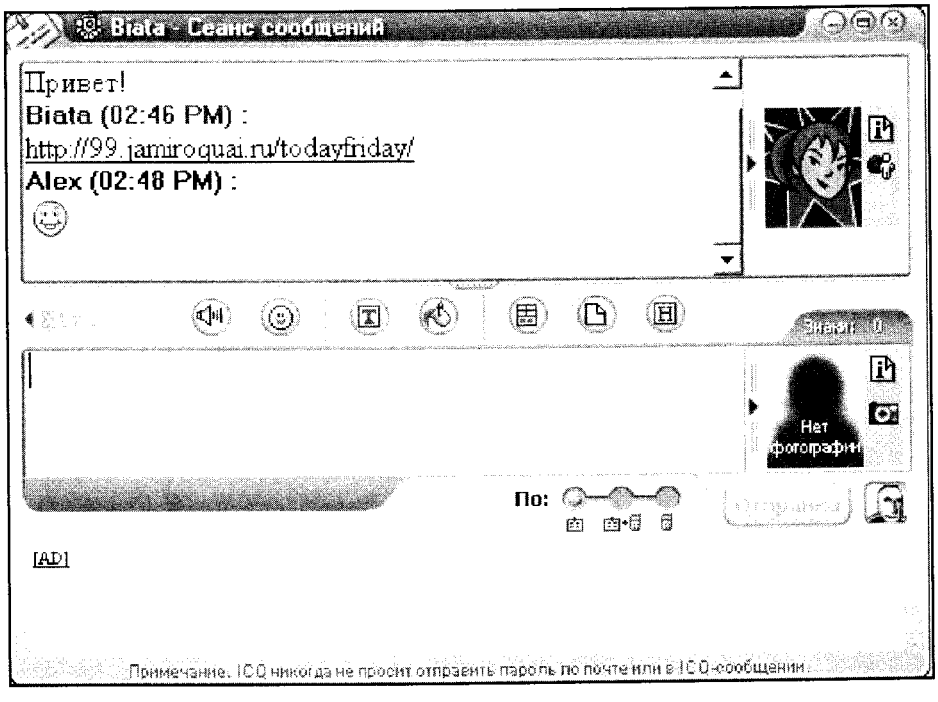


Рис. 17.59. Сеанс сообщений

правка текстовых сообщений, но это не единственный способ начать общение: тот же эффект достигается при помощи двойного щелчка по нику пользователя.

Общение происходит вот в таком окошке (рис. 17.59).

В нижнем окне вы пишете свои сообщения, в верхнем отображается ход вашей беседы. В процессе «разговора» можно использовать смайлики — их неплохой набор скрывается под кнопкой **Значки настроения**. Остальные пиктограммы, присутствующие в этом окне, вполне стандартны. Приход нового сообщения сопровождается характерным звуком.

Если пришло новое сообщение от пользователя из вашего контакт-листа, против имени этого пользователя замигает значок сообщения.

Обратите внимание на кнопку **Системное** в нижней части окна программы: она открывает доступ к некоторым сообщениям иного рода — к запросам на авторизацию или к сообщениям новых пользователей.

Теперь вы умеете использовать ICQ для общения.

Чтобы получить доступ к опциям программы, достаточно нажать кнопку **Главное меню** в окне программы (крайняя слева) и выбрать там пункт **Настройки и безопасность** (рис. 17.60).

Настройка параметров ICQ проста и очевидна для тех, кто работал с этой программой, и поэтому останавливаться на них не стоит. Как ис-

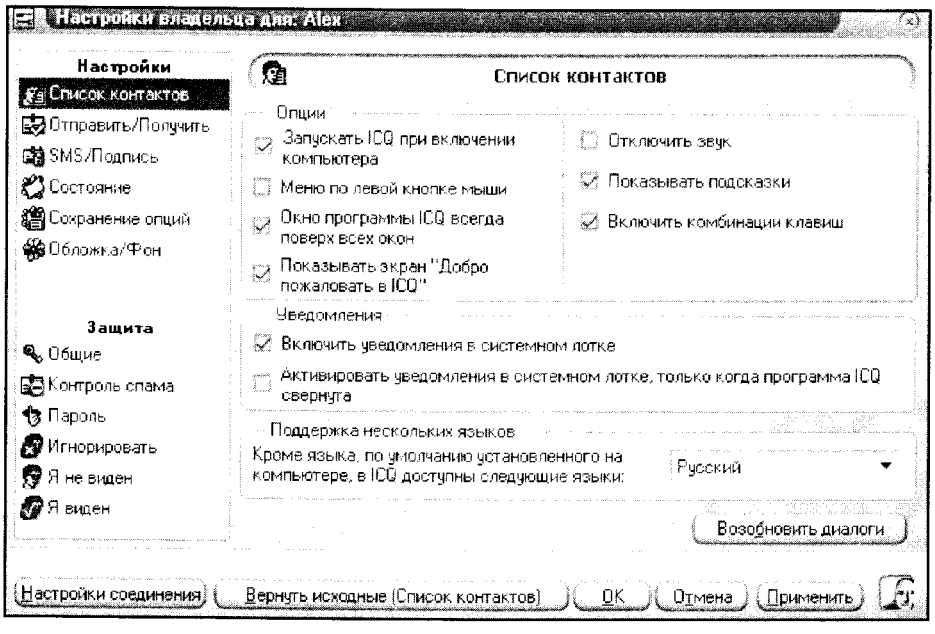


Рис. 17.60. Настройка параметров программы

пользовать множество важных «мелочей», вы без труда поймете, пообщавшись по ICQ недельку-другую. Остановимся лишь на том, как отредактировать введенные вами в процессе регистрации данные о пользователе. Для изменения собственных данных следует выбрать пункт **Просмотреть/изменить данные** в главном окне программы.

17.9. МУЗЫКА В СЕТИ

Сетевая радиостанция — это обычный компьютер, который передает в локальную сеть музыку. Прочитав этот раздел, вы тоже сможете развернуть подобный музыкальный сервис.

Принцип работы такой системы состоит в следующем. Один из компьютеров (как правило, это сервер) может передавать в сеть аудиоданные. Другие, на которых установлены специальные программы-клиенты, могут принимать эти данные и выводить их на собственные звуковые системы.

Для устройства сетевой радиостанции можно использовать простую программу под названием Vypress Tonecast. Скачать программу можно с http://www.vypress.com/. Ее дистрибутив занимает около 300 Кбайт.

Установка программы стандартна. В процессе инсталляции в системе оказываются клиентская и серверная части программы. Сервер, как вы помните, должен быть запущен на одном из компьютеров сети, клиент — на всех остальных.

Для запуска сервера следует выполнить команду **Пуск ▸ Все программы ▸ Vypress Tonecast ▸ Vypress Tonecast**. После запуска появится окно управления сервером (рис. 17.61).

Чтобы начать трансляцию, нужно настроить некоторые параметры сервера. Для этого нажмите кнопку **Settings** и в появившемся окне выберите вкладку **Network** (рис. 17.62). Здесь введите текущий IP-адрес сервера (**Current IP address**) и IP-адреса клиентских компьютеров, на которые будет транслироваться ваша радиопрограмма (параметр **Broadcast addresses**).

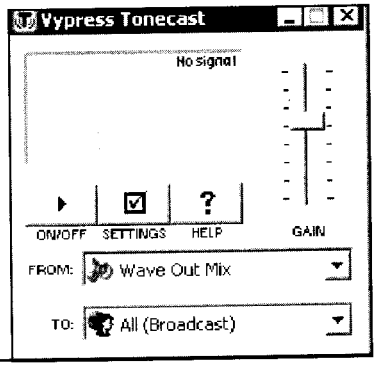


Рис. 17.61. Окно управления сервером Tonecast

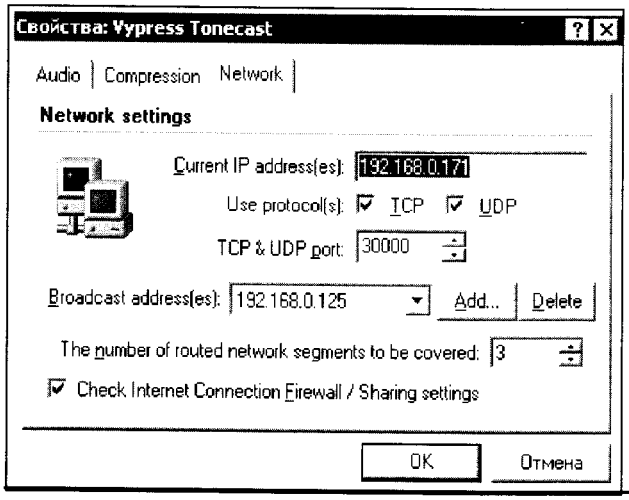


Рис. 17.62. Настройка параметров передачи

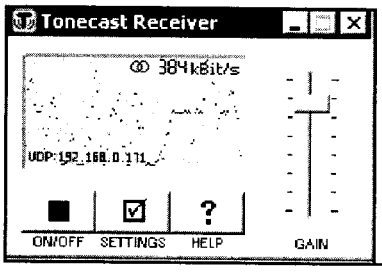
После настройки этих параметров можно выйти из окна свойств программы и попытаться активизировать трансляцию. Для этого запустите клиент на одном из сетевых компьютеров, а на сервере выберите источник сигнала (поле **From** в окне сервера) и включите трансляцию кнопкой **On/Off**. Если все сделано правильно, окно сервера примет вид, изображенный рис. 17.63.

При этом клиентская часть программы во время приема данных выглядит вот так (рис. 17.64).

Обратите внимание на индикацию битрейта в окнах сервера и клиента.

Битрейт (от английского **bit rate**) — скорость передачи данных в битах. Как правило, битрейт измеряется в битах в секунду, но есть и другие единицы измерения битрейта, например килобит в секунду.

Рис. 17.63. Сервер, транслирующий аудиоданные



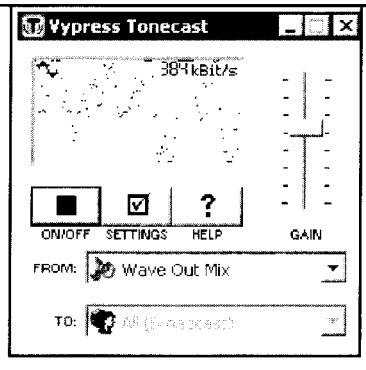


Рис. 17.64. Клиентская часть программы

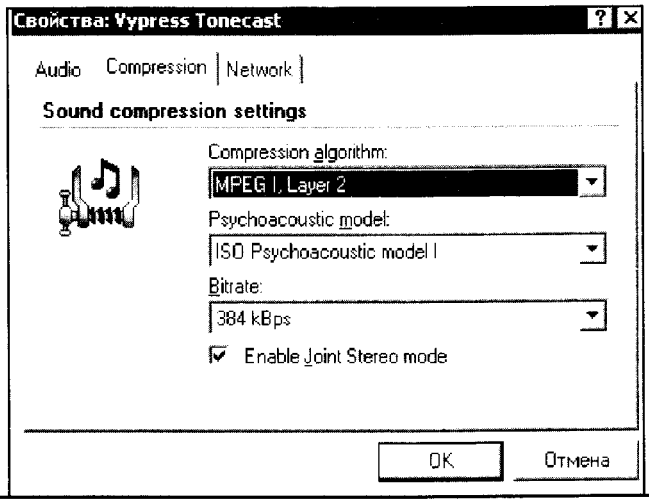


Рис. 17.65. Настройка параметров аудиосжатия

В нашем случае битрейт равен 384 Кбит/с. Это значение можно изменить: чем больше битрейт — тем выше качество звука, но и тем большая нагрузка ложится на вашу компьютерную сеть.

На рис. 17.65 изображена вкладка окна свойств программы, предназначенная для настройки опций аудиокомпрессии.

Для улучшения качества передаваемого аудиосигнала можно поэкспериментировать с этими настройками.

Главная опция вкладки **Audio** — параметры сэмплинга. Мне удалось обнаружить здесь всего пару настроек. Одна — 44 КГц 16-битный стереозвук, вторая — то же самое для монофонического звука.

По всей видимости, именно в ограниченном числе настроек скрыта причина не слишком высокого качества звука, которое удается получить с помощью этой программы. И все же Vypress Tonecast позволяет всем желающим организовывать простые сетевые радиостанции. Ну а если окажется, что для полного счастья вам не хватало лишь сетевой радиостанции, у вас будет случай, чтобы поискать более продвинутую программу.

17.10. СЕТЕВЫЕ ИГРЫ

Сетевые игры — увлекательное времяпрепровождение. Как правило, сетевые механизмы, заложенные в играх, достаточно просты и позволяют их настраивать. Чтобы сетевые игры могли работать в вашей сети, проследите, чтобы у вас были установлены все необходимые протоколы. Как правило, это наш старый знакомый TCP/IP, хотя встречаются игры, использующие IPX/SPX.

После проверки протоколов можно запускать игру и действовать по обстоятельствам. Некоторые игры сделают за вас все — они сами автома-

тически сконфигурируют сетевое взаимодействие, а вам останется лишь выбирать партнеров для игры. Такая схема реализована в старой, но не потерявшей привлекательности игре StarCraft.

Другая схема взаимодействия заключается в том, что один из компьютеров становится игровым сервером и к нему подключаются клиентские машины. Как правило, разработчики игр стараются сделать процесс их сетевой настройки как можно более простым. Однако каждая игра имеет свои особенности. Тем не менее, зная общие принципы их сетевой работы, вы сможете воспользоваться справочными материалами к ним и настроить любые игры для работы в вашей локальной сети.

Проследите, чтобы настройки вашего файрволла позволяли игре передавать данные в сеть и получать их оттуда, иначе поиграть не получится.

17.11. ВЫВОДЫ

В этой главе мы обсудили программные средства для различных видов коммуникации в сети. Мы общались, искали эффективные способы закачки файлов и сайтов, строили сетевую радиостанцию и обсуждали настройку сетевых игр. Казалось бы, семнадцатая глава этой книги прочитана, и нам с вами осталось лишь попрощаться. Но перед тем как проститься. я предлагаю вам почитать словарь сетевых технологий, который вы найдете в Приложении.

ЗАКЛЮЧЕНИЕ

Перевернута последняя страница этой книги. Надеюсь, она принесла вам пользу, расширила границы вашего сетевого и компьютерного кругозора. Компьютерное образование и самообразование — непрерывный процесс, и прочитанная вами книга — лишь ступенька на пути к вашему персональному компьютерному развитию.

Вы не могли не заметить: чем подробней знакомишься с какой-нибудь областью знаний, тем лучше понимаешь, как мало тебе известно. Это нормальное и закономерное ощущение: чем выше человек поднимается по лестнице знаний, тем шире неосвоенная территория, открывающаяся его взгляду. Чем дольше сохраните вы это чувство, тем больше будете знать и уметь.

Сетевые технологии постоянно совершенствуются и изменяются. Но то, что вы узнали, прочтя эту книгу, еще долго будет актуальным — возможно, три или пять лет. А некоторые технологии, скажем Wi-Fi или Bluetooth, еще лишь начинают массовое вхождение в жизнь. Ну а классика сетей вроде технологии Ethernet вряд ли претерпит серьезные изменения в ближайшее десятилетие.

Много времени мы посвятили изучению основ TCP/IP. Полагаю, вы почувствовали преимущества, получаемые от понимания работы этого стека протоколов. Модемные соединения, выход в Интернет через GPRS-модемы сотовых телефонов, работа с КПК в качестве сетевых устройств — все это для вас теперь не слишком сложная задача. Вы сумеете настроить домашние сети, используя для этого большинство из доступных сетевых технологий, подключить к ним все, что угодно и все, что уместно, и наслаждаться правильной работой вашей умной техники. Выход в Интернет и работа с сетевым программным обеспечением тоже не составят для вас проблем. Ну а если вы столкнетесь с проблемами или вам понадобится справка по домашним сетям, перелистайте еще раз страницы этой книги, и вы непременно найдете нужные и полезные сведения.

Главное, что я пытался сказать читателю на протяжении всей книги, состоит в том, что очень многие сетевые и компьютерные технологии и устройства работают по одним и тем же принципам. Умея работать с Outlook Express, вы сможете освоить любой почтовый клиент; сумев регистрировать почтовый аккаунт на mail.ru, вы без труда сделаете это на любом из бесчисленного количества почтовых серверов Сети, а разобравшись с настройкой некоторых сетевых параметров реестра, вы сможете эффективно использовать этот мощный инструмент в других целях.

Я выражаю благодарность всем тем, кто так или иначе причастен к написанию мною этой книги и тем, кто помог мне справиться с этим трудом.

До свидания, читатель. До новых встреч на страницах моих книг.

Ваш А.З.

ПРИЛОЖЕНИЕ

СЕТЕВОЙ СЛОВАРЬ

Словари понятий, имеющих отношение к сетевым технологиям, обычно помещают в приложения. И все же не следует относиться к словарям как к необязательному и неинтересному фрагменту книги: порой словарь может дать едва ли не столько же знаний, сколько книга в целом.

В этом словаре вы найдете некоторые наиболее распространенные термины сетевой лексики. Часть словаря посвящена техническим терминам, другая часть — некоторым общеупотребительным словам сетевого и технического жаргона. Обратите внимание: некоторые слова сетевого жаргона переходят в повседневную речь.

Особенности общения в сети познаются с опытом, но основы этого опыта поможет заложить представленный вашему вниманию словарь.

A

Access method — метод доступа. Набор правил, описывающих управление доступом к среде передачи данных. Например, в Ethernet-сетях используется метод доступа CSMA/CD.

Account (учетная запись, аккаунт) — учетная запись, которая создается при регистрации пользователя в какой-либо компьютерной системе. Аккаунт характеризуется именем пользователя (логином, от *log in* — войти в систему) и паролем (*password*).

Address — адрес, то есть неповторяющийся идентификатор, который присваивается сетевому устройству или сети, чтобы другие сетевые устройства или сети могли распознавать его при обмене данными.

Address mask — маска адреса. Двоичная маска, служащая для выделения части IP-адреса в целях определения адреса подсети и адреса узла подсети.

Amplitude — амплитуда сигнала. Расстояние между максимальным и минимальным уровнем сигнала, для обозначения амплитуды сигнала применяется также термин размах.

Analog signal — аналоговый сигнал. Сигнал, который представлен непрерывным изменением какой-либо физической величины. Аналоговый сигнал отличается от дискретного цифрового, который может принимать лишь ограниченное количество значений.

ANSI — American National Standards Institute (Американский национальный институт стандартов). Организация, представляющая США в Международном комитете по стандартизации (ISO). Занимается разработкой и стандартизацией различных сетевых и компьютерных технологий.

API — Application Program Interface (Интерфейс прикладных программ). Совокупность соглашений, которые определяют особенности вызова функций и передачи параметров прикладными программами.

Application Layer (Прикладной уровень). — Верхний уровень эталонной модели OSI, представляющий собой набор протоколов, предоставляющих пользователям сети доступ к различным ресурсам (к электронной почте, к передаче файлов).

ARP (Address Resolution Protocol) — протокол разрешения адресов, используемый для установления соответствия между сетевыми (IP) и локальными (физическими, аппаратными) адресами в компьютерных сетях.

ARPANET — компьютерная сеть, применявшая коммутацию пакетов и созданная в начале 70-х годов агентством ARPA. ARPANET стала прообразом современной сети Интернет. В июне 1990 ARPANET перестала существовать.

ASCII Character Set (набор символов **ASCI**) — американский стандартный код для обмена информацией (American Standard Code for Information Interchange). Стандартный набор символов ASCII представляет собой 128-символьную таблицу символов.

Attenuation (затухание сигнала) — уменьшение амплитуды или мощности сигнала при прохождении его по линиям связи. Измеряется в децибелах.

Authentication (аутентификация) — процедура проверки достаточности прав пользователя для принятия решения о предоставлении доступа к запрашиваемым им ресурсам. Термин аутентификация может применяться и в более широком смысле, охватывая не только пользователей, но и приложения.

AWG — American Wire Gauge System (американская система оценки проводов). Принятые в США (и применяемые во всем мире) стандарты на классификацию проводов по их диаметру.

B

Bandwidth (полоса пропускания) — непрерывный диапазон частот, при которых сигнал передается по линии связи (или через устройство) без значительных искажений. От широты полосы пропускания зависит максимальный объем информации, который линия может передать в единицу времени: чем шире полоса пропускания, тем больше данных по ней можно передать.

Baud (бод) — количество изменений сигнала в секунду, скорость передачи данных. Скорость передачи данных в бодах не совпадает со скоростью передачи в битах, так как одним изменением сигнала может быть закодировано несколько бит, то есть сигнал имеет несколько различимых состояний. В то же время скорость передачи в бодах при использовании сигнала с двумя различимыми состояниями может быть ниже битовой скорости передачи данных по линии связи.

Bit (бит) — наименьшая единица информации, с которой может работать компьютер. Бит может принимать два значения — 1 или 0.

BOOTP (Bootstrap Protocol) — протокол, который используется для загрузки удаленных бездисковых рабочих станций, «тонких клиентов» с помощью протокола TFTP. В результате рабочая станция получает IP-адрес.

BPS (Bits Per Second) — бит в секунду. Единица измерения скорости передачи информации, актуальна для последовательных каналов связи.

Bridge (сетевой мост) — сетевое устройство, разделяющее единую среду передачи данных на сегменты и передающее пакеты данных из одних сегментов в другие только тогда, когда в этом возникает необходимость. Мосты могут фильтровать пакеты и изолируют трафик сегментов так, чтобы повышалась общая производительность сетевой системы. Как правило, при передаче данных между сегментами мосты используют адреса канального уровня, то есть аппаратные или MAC-адреса. Применение моста накладывает определенные ограничения на структуру сети: в сети с мостом не должно быть замкнутых контуров.

Broadcasting (широковещательная передача) — при широковещательной передаче пакетов копия пакета передается всем компьютерам сети. В качестве примера широковещательной сети можно привести Ethernet.

Browser (браузер) — программа, позволяющая просматривать документы в Интернете. Среди наиболее распространенных браузеров можно отметить Microsoft Internet Explorer, Mozilla Firefox, Opera.

Bus (шина) — канал передачи данных. Шина реализуется как электрическое соединение, в котором используется один или несколько проводников. К шине подключаются устройства, которые получают проходящие через нее сигналы. Шины бывают параллельными — такие шины передают биты данных параллельно, и последовательными, передающими данные последовательно, бит за битом.

Bus topology (шинная топология сети) — в шинной топологии сети используется единая шина, обычно коаксиальный кабель, к которому подключаются сетевые устройства. Шинная топология в настоящее время практически не используется, так как она характерна для морально устаревших Ethernet-сетей на коаксиальных кабелях. Такая топология ставит под угрозу целостность всей сети при повреждении даже одного кабеля или соединения. Шинная топология сети ограничивает возможности расширения сети и смены места расположения компьютеров.

Byte (байт) — единица информации, равная 8 битам. Всего существует 256 восьмибитных последовательностей.

C

Channel (а также **circuit, facility, link, line**) — канал передачи электрических сигналов между устройствами. Например, кабельная система Ethernet-сети.

Clock (тактовый генератор) — устройство, которое генерирует тактовые сигналы, использующиеся в целях синхронизации различных устройств и для передачи данных.

Collision (конфликт, коллизия) — ситуация, возникающая в сети с методом доступа CSMA/CD, когда несколько (обычно две) рабочих станций одновременно начинают передавать пакет. Когда коллизия обнаружена, передающие пакеты станции прекращают передачу, после чего пытаются начать ее снова через случайный интервал времени.

Collision domain (домен коллизий) — сегмент сети, станции которого используют общую среду передачи данных.

Compression (сжатие, компрессия) — один из методов, позволяющих уменьшить число битов, представляющих информацию. В результате компрессии достигается экономия пространства для хранения информации и более рациональное использование полосы пропускания линий связи при передаче по ним сжатой информации.

Connectionless (без установления соединения) — обмен данными, при котором не требуется устанавливать соединение. По такому

принципу работают протоколы IP и UDP. В качестве некомпьютерного примера можно привести обмен обычной почтой.

Cookie (прямой перевод — печенье) — некоторое количество информации, посылаемое веб-сервером веб-браузеру. Браузер сохраняет эту информацию, которая предоставляется серверу при следующем подключении к нему этого браузера. С помощью *Cookies* осуществляется идентификация пользователей: сервер может «запоминать» их, сохранять их персональные настройки и так далее.

Connection-oriented (с установлением соединения) — обмен данными, при котором устанавливается соединение, а процесс обмена делится на три фазы: установление соединения, обмен данными, разрыв соединения. По такому принципу работает протокол TCP. Некомпьютерный пример связи с установлением соединения — обычный телефонный разговор.

CRC (Cyclic Redundancy Check) — циклическая проверка четности с избыточностью. Метод контроля целостности данных при передаче и хранении. Вычисленная особым образом контрольная сумма передаваемого блока данных передается вместе с ним. Устройство, получившее данные, заново вычисляет их контрольную сумму и сравнивает с принятым CRC. Если вычисленная контрольная сумма совпадает с принятой, это с высокой вероятностью означает целостность принятых данных.

CSMA/CD (Carrier sense multiple access/collision detection) — метод множественного доступа с опознанием несущей и обнаружением коллизий. CSMA/CD — это метод доступа к среде передачи данных, определенный для сетей Ethernet (IEEE 802.3). В соответствии с методом CSMA/CD каждый узел, передающий данные, должен «слушать» сеть, чтобы обнаружить коллизию — попытку одновременной передачи данных другим устройством. После возникновения коллизии устройства, вызвавшие ее, останавливают передачу данных, после чего передача возобновляется через случайный промежуток времени. Увеличение количества узлов в Ethernet-сети с разделяемой средой передачи данных снижает эффективность работы из-за увеличения числа коллизий.

D

Data Link Layer (канальный уровень модели **OSI**) — второй уровень модели OSI, который занимается передачей кадров (frames), отслеживает доступность среды передачи данных и обеспечивает корректность передачи данных, используя механизмы обнаружения и коррекции ошибок.

Data Rate (скорость передачи данных) — скорость передачи данных, измеряемая в бит/с (bps). Существуют и другие показатели скорости, например Кбит/с (kbps), Мбит/с (Mbps) и так далее.

DCE (Data Communications Equipment) — оборудование передачи данных, то есть оборудование, связывающее компьютеры или локальные сети с линиями передачи данных. Это пограничное оборудование, которое обеспечивает управление соединением. Типичным DCE является, например, модем.

DHCP (Dynamic Host Configuration Protocol) — протокол динамической настройки хостов. С его помощью TCP/IP-клиентам передаются конфигурационные параметры.

Digital (цифровой) — так обозначается двоичная, цифровая информация, используемая компьютером. Термин применяется для обозначения оцифрованных данных (цифровой звук и так далее). Этим же термином обозначают дискретную передачу данных.

Domain (домен) — множество доменных имен, у которых совпадают старшие части, часть иерархии имен в Интернете. Доменное имя состоит из последовательности имен, которые разделены точками. Например, это может быть mysite.narod.ru.

DNS (Domain Name System) — система доменных имен, то есть механизм, использующийся в Интернете для перевода доменных адресов в IP-адреса. Доменные имена имеют символьную форму. С ними удобно работать, так как они сравнительно легко запоминаются и выглядят гораздо привычнее, чем цифры IP-адресов.

E

EMI (Electromagnetic Interference) — электромагнитное излучение. Электромагнитное излучение, выходящее за пределы среды передачи данных. EMI можно снизить за счет экранирования. Электромагнитное излучение воздействует на электронные устройства и на человека, хотя вопрос о воздействии EMI на здоровье людей до сих пор остается открытым.

Encapsulation (инкапсуляция) — вложение структур данных протоколов. Протоколы разных уровней формируют собственные структуры данных (пакеты, кадры, сообщения), добавляя к структурам данных других протоколов собственные заголовки. Применительно к Интернету пакет — это заголовок физического уровня, за которым идет заголовок сетевого уровня (IP-заголовок), следом идет TCP-заголовок (транспортный заголовок), за которым идут данные протоколов уровня процессов и приложений.

Encryption (шифрование) — совокупность технологий обеспечения безопасности данных. С помощью шифрования передаваемые и хранимые данные кодируются так, чтобы доступ к ним могли получить только пользователи, имеющие право на работу с этими данными. Существует множество алгоритмов шифрования, а применение шифрования позволяет увеличить защищенность системы и данных, хранящихся и передаваемых в ней.

Ethernet — набор правил организации локальных сетей, описанный в стандартах IEEE и других организаций. Регулированию Ethernet посвящен постоянно развивающийся набор стандартов IEEE 802.3. На сегодняшний день Ethernet-сети являются одними из наиболее распространенных в мире, в качестве среды передачи данных они применяют преимущественно витую пару.

F

FAQ (Frequently Asked Questions) — часто задаваемые вопросы. Подобие справочника, созданное из наиболее типичных вопросов по конкретной теме. В FAQ часто можно найти интересные сведения, однако иногда это слово используется для того, чтобы подчеркнуть общеизвестность тех или иных фактов.

Fiber Optics (волоконная оптика) — оптическая среда передачи данных, состоящая из стеклянных или полимерных волокон, по которым проходит свет, генерируемый светодиодами или лазерами. Волоконно-оптические линии связи отличаются высокой пропускной способностью, невосприимчивостью к электромагнитным помехам и высокой дальностью связи. Современные высокоскоростные технологии связи (Gigabit Ethernet и так далее) во многом ориентированы на применение волоконно-оптических линий связи.

Firewall (файрволл, брандмауэр, межсетевой экран) — аппаратное и/или программное средство (чаще аппаратно-программное), используемое для защиты сетей. Файрволл делит сеть на части, занимается фильтрацией трафика, не пропуская в сеть (и не выпуская из нее) потенциально опасные данные и данные, заблокированные системным администратором к отправке или получению.

Fragmentation (фрагментация) — разбиение IP-пакета на части для передачи его по сети, параметры которой не позволяют передать по ней пакет существующего размера. Во многом благодаря возможности фрагментации TCP/IP стал таким распространенным в наши дни.

FTP — File Transfer Protocol (протокол передачи файлов) — один из протоколов стека TCP/IP для обмена файлами. Существуют специальные программы — FTP-клиенты, позволяющие использовать этот протокол для управления файлами на удаленных компьютерах и файлообмена.

G

Gateway (шлюз) — аппаратное или программное устройство, используемое для обеспечения доступа из одной системы (одной сети, например) в другую.

H

Hop (буквально: прыжок) — транзитная передача между сетями, представляющая собой путь между двумя сетевыми устройствами (как правило, между маршрутизаторами), проходимый пакетом данных до достижения адреса назначения.

I

IMHO (*In My Humble Opinion*, по моему скромному мнению) — сокращение, которое часто можно встретить в сетевом общении. Как правило, используется, если высказывающий мнение говорит от собственного имени. Ближайшие аналоги — «мне кажется» или «я думаю». Это сокращение применяется и в русском написании, то есть ИМХО.

Interface (интерфейс) — способ соединения устройств. Параметры интерфейсов определяются характеристиками разъемов и необходимыми параметрами передачи данных. Понятие *интерфейс* используется также в значении элементов оформления программ, позволяющих организовывать их взаимодействие с пользователем.

Internet address (интернет-адрес) — 32-битный адрес, присвоенный компьютеру или другому устройству, использующему TCP/IP. Иногда используется как синоним к понятию IP-адрес.

IP — Internet Protocol — Протокол сетевого уровня стека TCP/IP.

IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange) — стек протоколов, использующихся в сетях Novell NetWare для обмена информацией. В последнее время теряет актуальность, усту-

пая более популярному и распространенному TCP/IP. Тем не менее современные операционные системы поддерживают IPX/SPX в целях обеспечения совместимости с программами, которые использует для работы этот стек протоколов.

ISO (International Organization for Standardization) — международная организация по стандартизации. Занимается разработкой и поддержкой международных стандартов в сфере обмена информацией. Этой организацией была, к примеру, предложена семиуровневая модель ISO/OSI, разработанная на основе существующих на момент разработки сетевых технологий.

ISP (Internet Services Provider) — провайдер интернет-доступа, то есть компания, предоставляющая доступ в Интернет.

ITU (International Telecommunication Union) — Международный союз электросвязи. Международная организация, занимающаяся разработкой стандартов в области передачи информации.

L

LAN (Local Area Network) — локальная сеть, локальная вычислительная сеть, ЛВС. Совокупность компьютеров и других устройств, соединенных высокоскоростными линиями связи и расположенных на небольшом удалении друг от друга.

M

Modem (Modulator-Demodulator) — модем, модулятор-демодулятор. Устройство для преобразования цифровых данных, поступающих в него из компьютера или другого устройства, в аналоговый сигнал для передачи по телефонной линии. Аналогично модем осуществляет обратное преобразование, то есть полученный им по телефонной линии аналоговый сигнал преобразуется в цифровые данные. С помощью модема осуществляется так называемое *dial-up*-подключение к Интернету. Такое подключение отличается достаточно низкой скоростью передачи данных, но в силу дешевизны решения пользуется большой популярностью в России.

MTU (Maximum Transmission Unit) — максимальная единица передачи данных. Определяемое каким-либо протоколом максимальное значение, которое может иметь длина поля данных. Например, для Ethernet MTU равняется 1500 байтам. Настройка MTU для интернет-соединений имеет значение для их оптимизации.

N

NetBEUI (NetBIOS Extended User Interface) — сетевой протокол, содержащий функции сетевого, транспортного и сеансового уровней OSI. Используется в операционных системах корпорации Microsoft. Этот протокол стал результатом развития NetBIOS.

Network Layer (Сетевой уровень) — третий уровень эталонной модели OSI. Он отвечает за межсетевой обмен и за построение единой транспортной системы, которая объединяет несколько сетей.

P

Packet (пакет) — в терминах семиуровневой модели OSI пакетом называется сообщение сетевого уровня (например, IP-пакет). Пакет имеет заголовок, содержащий служебную информацию (адреса отправителя, получателя и так далее), и поле данных, содержащее переносимую пакетом полезную информацию. Понятие «пакет» иногда используют в общем виде, понимая под пакетом упорядоченную совокупность данных и управляющей информации, которая передается по сети как часть сообщения.

Packet Switching (коммутация пакетов) — при коммутации пакетов данные делятся на пакеты, передаваемые по сети, а линии связи могут гибко загружаться этими пакетами. Пакеты, входящие в состав одного сообщения, могут доставляться адресату разными путями.

Physical Layer (Физический уровень) — низший уровень модели OSI. Он обеспечивает физический перенос данных через линии связи. На физическом уровне определяются физические характеристики оборудования, параметры среды передачи данных, сигналов. Например, к физическому уровню модели OSI относятся кабельные системы, разъемы.

R

Repeater (повторитель) — сетевое устройство, передающее электрические сигналы с одного кабеля на другой, усиливая этот сигнал, но не производя ни фильтрации пакетов (в отличие от моста, который может это делать), ни их маршрутизации, ни иной обработки. Повторитель работает на физическом уровне OSI.

RFC (Request For Comments) — группа документов, содержащая спецификации протоколов Интернета и другую связанную с ними информацию. Первые RFC выпущены в конце 60-х годов, наряду со стандартами Internet документы RFC описывают некоторые другие стандарты.

RTFM (Read The Fucking Manual) — наряду с IMHO это одно из наиболее употребительных сокращенных выражений. По-английски звучит довольно грубо, а по-русски означает примерно следующее: «Прежде чем задавать вопросы, читай руководство пользователя».

Router (маршрутизатор) — устройство (или специально настроенный компьютер), отвечающее за передачу сетевого трафика по определенным маршрутам, то есть за маршрутизацию трафика. Маршрутизация основывается на информации о структуре сети, которая хранится в таблице маршрутизации. При выборе оптимального маршрута используются специальные алгоритмы, а маршрут выбирается на основании нескольких критериев, которые называются метрикой маршрутизации. Маршрутизаторы работают с так называемыми маршрутизируемыми протоколами (примером маршрутизируемого протокола может служить IP). Маршрутизаторы относятся к сетевому уровню эталонной модели OSI.

S

Session Layer (Сеансовый уровень) — пятый уровень эталонной модели OSI. Обеспечивает управление диалогом между системами.

SMTP (Simple Mail Transfer Protocol) — протокол, используемый в системах электронной почты.

Spam (спам) — незапрошенная и нежелательная почта, рассылаемая по электронным адресам. Как правило, содержит рекламные сообщения либо является попыткой мошенничества. Слово Spam применяется для обозначения любой нежелательной корреспонденции, причем приходящей не только по каналам электронной почты, но и, например, по ICQ.

STP (Shielded Twisted Pair) — экранированная витая пара, то есть кабельные системы на основе экранированных витых пар медных проводников. Обладают большей надежностью, нежели кабели на основе UTP.

T

TCP (Transmission Control Protocol) — транспортный протокол стека TCP/IP. Обеспечивает надежную доставку сообщений, ориентирован на связь с установлением соединения.

TCP/IP (Transmission Control Protocol/ Internet Protocol) — стек протоколов, основной для Интернета и многих современных локальных сетей.

Traffic — трафик, то есть объем данных, принимаемых или передаваемых сетевым устройством.

Transport Layer — транспортный уровень. Четвертый уровень эталонной модели OSI. Отвечает за надежность доставки сообщений между узлами сети. Предоставляет протоколам более высокого уровня нужную степень надежности доставки сообщений.

U

UDP (User Datagram Protocol) — протокол стека TCP/IP, обеспечивающий передачу данных дейтаграммным способом без подтверждения доставки. Используется как связующее звено между протоколом сетевого уровня (IP) и протоколами прикладного уровня. Приложение, использующее для работы UDP, должно самостоятельно заниматься контролем надежности доставки данных.

UTP (Unshielded Twisted Pair) — неэкранированная витая пара, то есть кабельная система, построенная на основе скрученных медных проводников без дополнительного экранирования. Находит широкое применение при создании локальных сетей.

W

WAN (Wide-Area Network) — глобальная сеть, а также сеть, передающая информацию на большие расстояния. Для построения WAN используются специальные каналы связи, например, это могут быть коммутируемые линии связи, выделенные линии. Традиционно глобальные компьютерные сети отличались более низкой скоростью передачи данных, чем локальные, но в последнее время наблюдается тенденция к сближению этих технологий.