серия "Учебный курс"

NEW!

С. В. Глушаков, А. М. Мирошник, Т. С. Хачиров

Сеть своими руками

Vista

Авторитетные специалисты поделятся с Вами профессиональными секретами организации компьютерных сетей дома и в офисе.

Многочисленные иллюстрации, пошаговые инструкции и советы опытных администраторов позволят сразу же применить полученные знания на практике. Вы научитесь соединять и настраивать сеть из двух и более компьютеров, подключать их к Интернету, обеспечивать бесперебойную совместную работу и безопасность, а также эффективно и с удовольствием использовать свое время в сети!

- Маршрутизация • Протоколы • Оборудование
- Dial-Up • ADSL • GPRS • Wi-Fi
- Общие папки • Сетевая печать
- UserGate • µTorrent • DC++ • Radmin
- Google • Skype • и многое другое...

www.iboox.ru

ISBN 978-5-17-053639-9

9 785170 536399

КОМПЬЮТЕР·HOUSE
iBOOX.RU

iBOOX.RU

Учебный курс

С. В. Глушаков
А. М. Мирошник
Т. С. Хачиров

Сеть своими руками

NEW!

NEW!

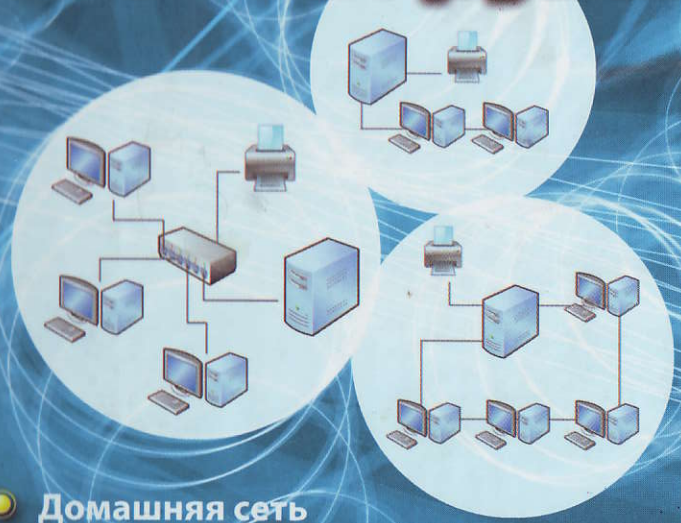
Учебный курс

САМОУЧИТЕЛЬ

С. В. Глушаков
А. М. Мирошник
Т. С. Хачиров

Сеть своими руками

Vista



- Домашняя сеть
- Беспроводные технологии
- Подключение к Интернету
- Защита информации
- Обмен файлами в сетях

КОМПЬЮТЕР·HOUSE
iBOOX.RU

Серия «Учебный курс»

С. В. Глушаков
А. М. Мирошник
Т. С. Хачиров

Сеть своими руками

Москва
АСТ
ВКТ
Владимир

КОМПЬЮТЕР·HOUSE
iBOOX.RU

УДК 004.382.7
ББК 32.973
Г55

Шеф-редактор С.В. Глушаков

Художник-оформитель В.В. Бабанин

www.iBoox.ru

Макет подготовлен
редакционным отделом «COMPUTER-HOUSE iBoox.Ru»
«Харьковский институт информационных технологий»

Глушаков, С.В.

Г55 Сеть своими руками/ С.В. Глушаков, А.М. Мирошник, Т.С. Хачиров. – М.: АСТ: АСТ МОСКВА; Владимир: ВКТ, 2008. – 286, [2] с.– (Учебный курс).

ISBN 978-5-17-053639-9 (ООО «Издательство АСТ»)
ISBN 978-5-9713-8348-2 (ООО Издательство «АСТ МОСКВА»)
ISBN 978-5-226-00869-6 (ВКТ)
(б/с)

ISBN 978-5-17-053638-2 (ООО «Издательство АСТ»)
ISBN 978-5-9713-8347-5 (ООО Издательство «АСТ МОСКВА»)
ISBN 978-5-226-00870-2 (ВКТ)
(Обложка)

В книге представлена исчерпывающая информация, необходимая для построения домашней локальной сети. Рассмотрены теоретические основы построения и взаимодействия локальных сетей, а также приведены практические примеры соединения в сеть двух и более компьютеров. Следуя пошаговым инструкциям, читатель сможет построить проводную или беспроводную сеть, подключить компьютер к Интернету, используя технологии ADSL, Dial-Up или GPRS, и предоставить доступ к Интернету другим компьютерам домашней сети.

Описано множество полезных программ для работы в Интернете и файлообменных сетях: браузеры, программы для обмена файлами и сообщениями, менеджеры закачки файлов и сайтов, брандмауэры, интернет-сервисы и т.д.

УДК 004.382.7
ББК 32.973

© С.В. Глушаков, А.М. Мирошник, Т.С. Хачиров, 2008
© В.В. Бабанин, художественное оформление, 2008

Оглавление

Предисловие 6

Часть I. Построение локальной сети

Глава 1. Знакомство с локальными сетями 9
Развитие локальных сетей 9
Основные термины и определения 10
Общие сведения о компьютерных сетях 11
Типы сетей 14
Примеры использования локальных сетей 16

Глава 2. Основы построения локальных сетей 17
Топологии построения локальных сетей 17
Технологии передачи данных в локальных сетях 21
Открытая модель межсетевого взаимодействия OSI/ISO 25
Порты 30
Адресация в IP-сетях 32
Классы IP-адресов 34
Маршрутизация пакетов 40
Имена компьютеров в сети 41
Прикладные протоколы в сетях TCP/IP 44
Оборудование для построения локальных сетей 46

Глава 3. Введение в беспроводные сети 55
Технологии и протоколы беспроводных сетей 55
Оборудование для построения беспроводных сетей 59
Вопросы безопасности в беспроводных сетях 63

Глава 4. Домашняя сеть: шаг за шагом 66
Общие рекомендации 66
Одноранговая сеть из двух компьютеров 67

Проверка работоспособности системы ... 78
Соединение трех и более компьютеров без выделенного сервера ... 83
Использование общих папок ... 84
Предоставление общего доступа к папкам ... 86
Сетевая печать ... 90

Глава 5. Создание беспроводной локальной сети ... 95

Выбор оборудования ... 96
Настройка DWL-G122 ... 97
Настройка DI-624+ ... 104
Публичные точки доступа Wi-Fi ... 112

Глава 6. Подключение к глобальной сети ... 114

Технологии подключения к сети Интернет ... 114
Dial-Up ... 115
Мобильные устройства и сети ... 116
G.SHDSL ... 121
ADSL ... 122
Домашние сети ... 123
Оборудование для подключения ... 124
Критерии выбора провайдера, предоставляющего услуги доступа к глобальной сети Интернет ... 126
Подключение по технологии ADSL ... 130
Подключение по технологии Dial-Up ... 135
Подключение по технологии GPRS ... 137

Глава 7. Мини-провайдер в домашних условиях ... 142

Варианты подключения сети к Интернету ... 143
Применяемые технологии ... 145
Программа UserGate ... 147

Часть II. Полезные программы

Глава 8. Обмен файлами в сетях ... 162

Принцип действия ... 162
µTorrent ... 163
DC++ ... 165

Глава 9. Удаленное администрирование ... 170

Удаленный рабочий стол ... 170
Remote Administrator (Radmin) ... 175

Глава 10. Брандмауэры ... 178

Брандмауэр Windows ... 179
ZoneAlarm Pro ... 185
Norton Internet Security 2008 ... 191
Agnitum Outpost Firewall Pro 2008 ... 196

Глава 11. Безопасный серфинг в Интернете ... 201

Internet Explorer ... 201
Opera ... 206
Mozilla Firefox ... 212

Глава 12. Закачка файлов из Интернета ... 216

Teleport Pro ... 216
ReGet ... 219
Download Master ... 225

Глава 13. Общение в Интернете ... 228

ICQ ... 228
QIP ... 239
Windows Live Messenger ... 244

Глава 14. Веб-камеры и Skype ... 249

Описание устройства ... 249
Интернет-телефония Skype ... 252
Веб-камеры в Интернете ... 261

Глава 15. Интернет-сервисы Google ... 266

Поисковый сервер Google ... 266
Почтовый сервис Gmail ... 269
Календарь Google ... 273
Карты Google ... 274
Google Планета Земля ... 278

Заключение ... 287

Предисловие

В настоящее время практически в каждом доме можно увидеть компьютер – он стал неотъемлемой частью нашей жизни. Чаще всего домашний компьютер является центром развлечений, поскольку может выступать в роли игровой приставки, музыкального центра или DVD-проигрывателя.

Компьютерная сеть, т.е. соединение нескольких компьютеров между собой при помощи сетевых кабелей, позволяет передавать информацию от одного компьютера к другому с очень большой скоростью и без необходимости использования каких-либо носителей информации.

В настоящее время часто встречается ситуация, когда жители одного дома объединяют свои компьютеры в локальную сеть, а затем подключают ее к Интернету. Это дает большие преимущества, так как пользователи могут обмениваться друг с другом различными файлами, общаться в реальном режиме времени, играть в сетевые игры и т.д.

Эта книга поможет вам объединить несколько компьютеров в локальную сеть и подключить их к Интернету. В первой части книги приведены общие сведения о компьютерных сетях, основные термины и определения. Рассмотрены технологии передачи данных в локальных сетях, типы межкомпьютерного обмена данными, понятие IP-адресации и классы IP-адресов, маршрутизация пакетов, понятие доменной системы имен и протоколы в TCP/IP сетях. Особое внимание уделено беспроводным сетям, которые в настоящее время получили широкое распространение. Приведены особенности беспроводных сетей, стандарты, технологии построения и защиты. Подробно рассмотрено оборудование для построения проводных и беспроводных сетей.

Отдельная глава посвящена построению домашней сети из двух и более компьютеров, в которой подробно описаны этапы

построения сети, начиная от разводки кабеля и заканчивая предоставлением общего доступа к папкам и принтерам.

Рассмотрены современные технологии подключения к Интернету, методика подключения ноутбуков к мобильным сетям GSM и CDMA, приведены советы по выбору интернет-провайдера. Вы узнаете, как подключить все компьютеры локальной сети к Интернету, используя технологии Dial-Up, ADSL и GPRS.

Во второй части книги приведено описание самых последних версий программ для загрузки файлов из файлообменных сетей (µTorrent и DC++), загрузки файлов и сайтов из Интернета (Teleport Pro, Dowload Master), удаленного администрирования (Radmin). Подробно описаны брандмауэры (ZoneAlarm Pro, Norton Internet Security, Agnitum Outpost Firewall Pro). Вы узнаете об особенностях безопасного веб-серфинга в популярных браузерах (Internet Explorer, Opera, Mozilla Firefox) и освоите программы для общения в режиме онлайн (ICQ, QIP, Windows Live Messenger, Skype). Также рассмотрены возможности популярных интернет-сервисов Google (электронная почта и поиск, Планета Земля, Карты, Фотографии).

КОМПЬЮТЕР·HOUSE iBOOX.RU

Книга подготовлена авторским коллективом редакции «Компьютер-House iBoox.Ru».
Мы будем рады вашим отзывам и приглашаем посетить наш интернет-портал
www.iboox.ru

Часть I
Построение локальной сети

Глава 1
Знакомство с локальными сетями

В этой главе рассматриваются краткая история создания и развития локальных вычислительных сетей, а также основные термины и определения, касающиеся непосредственно работы в локальных вычислительных сетях (ЛВС). Кроме того, дано немного теории, без понимания которой крайне сложно, практически невозможно постичь практикум проектирования и построения локальных сетей.

Развитие локальных сетей

Началом развития локальных вычислительных сетей считается 1969 год, когда в Калифорнийском университете был установлен первый узел локальной вычислительной сети, носившей в то время название ARPAnet – именно так называлась компания, которая финансировала развитие данной сети. В 70-е годы в Америке было принято решение создать некую надежную, децентрализованную, отказоустойчивую структуру – информационную сеть, которая бы могла обеспечить передачу информационных пакетов между участниками процесса информационного взаимодействия, даже если часть систем, обеспечивающих передачу данных, оказалась бы поврежденной, например в случае ядерной войны. Конечно же, изначально разработка данной сетевой структуры велась под покровительством военных и для военных.

К 1971 году сеть данного проекта уже насчитывала порядка 200 компьютеров и к ней имели доступ в рамках данного проекта около 30 университетов США.

Естественно, в то время не было четких стандартов, регламентирующих построение и передачу данных в сетях, не существовало четких договоренностей о форматах пакетов передачи данных, что было крайне необходимо для роста ЛВС. Поэтому в 80-х годах было принято использовать в качестве стандарта передачи данных в ЛВС стек протоколов TCP/IP (Transmission Control Protocol / Internet Protocol), в который входило ряд стандартов, регламентирующих передачу пакетов между всеми участниками межсетевого взаимодействия. Подробнее об этом будет рассказано ниже.

Основные термины и определения

Рассмотрим основные понятия, которые будут использоваться при изучении материала, изложенного в данной книге:

- *протокол* – набор правил, методов, свойств, регламентирующих взаимодействие всех объектов сетевой инфраструктуры;
- *топология сети* – это схема физического соединения компьютеров. Во второй главе нашей книги мы более детально поговорим о различных топологиях, используемых при построении локальных сетей;
- *сетевой объект* – объект, участвующий в процессе межсетевого взаимодействия. Примерами сетевых объектов могут выступать: компьютеры, коммутаторы, концентраторы, сетевые принтеры и т.д;
- *повторитель* – простейшее сетевое устройство, которое физически соединяет различные сегменты кабеля локальной сети, с целью увеличения общей длины сети. В настоящее время уже не используется;
- *концентратор (hub)* – сетевое устройство, используемое для объединения компьютеров в единый физический сегмент сети, работает по принципу «все – всем», т.е. все сетевые объекты, которые объединяет данный коммутатор, получают все пакеты, передаваемые в данном физическом сегменте, независимо от того, кому именно из них предназначались данные пакеты. Решение о том, кому именно предназначался данный пакет, принимается на уровне сетевого объекта;
- *коммутатор (switch)* – сетевое устройство, используемое для объединения компьютеров в единый физический сегмент сети. Он работает по принципу «один к одному», т.е. коммутатор, в отличие от того же концентратора, сам принимает решение, кому именно из сетевых устройств, расположенных в его физическом сегменте, передать информационный пакет основываясь на служебной информации, передаваемой в информационном пакете;
- *маршрутизатор (router)* – служит для соединения двух или более ЛВС в единую сеть;
- *физический порт* – разъем на сетевом устройстве, с помощью которого происходит подключение данного устройства к сегменту сети. Примером порта может выступать порт на коммутаторе или концентраторе, к которому с помощью кабеля происходит подключение сетевых устройств;
- *IP-адрес* – это 32-битное число, однозначно идентифицирующее сетевой объект. По сути своей IP-адрес — это уникальный номер сетевого объекта, он состоит из адреса сети, в которой находится сетевой объект, и адреса самого сетевого объекта;
- *маска сети* – это 32-битное число, которое задается одновременно с IP-адресом и определяет, какие биты IP-адреса относятся к идентификатору сети, а какие – к идентификатору сетевого объекта;
- *терминатор* – устройство, используемое в коаксиальных сетях для предотвращения явления отражения сигнала. Устанавливается на концах коаксиального кабеля.

Конечно же, это не полный список всех терминов и определений, необходимый для глубокого понимания материала, изложенного в данной книге. Это лишь необходимый фундамент, на котором будут строиться и систематизироваться ваши знания о сетях и сетевых технологиях, каждый из этих терминов мы будем более детально рассматривать в последующих главах.

Общие сведения о компьютерных сетях

Общее определение компьютерной сети – это система, которая позволяет производить обмен информацией между устройствами, которые подключены к системе. Минимальный набор компонентов, составляющих базовую коммуникационную модель, выглядит так:

- источник;
- приемник;

- среда передачи;
- сообщение.

В сети источником и приемником могут быть соответственно персональный компьютер и сервер; спутник и принимающая антенна.

Средой передачи, или каналом, может быть телефонная линия, кабель или радиоэфир, по которому распространяются радиоволны. Сообщение представляет собой информацию, передаваемую от источника к приемнику.

Также рассмотрим два важнейших компонента любой сети – сервер и клиент.

Сервер – в первую очередь программное обеспечение, запущенное на компьютере, которое предоставляет клиентам некоторые ресурсы компьютера, на котором оно работает. Например, сервер электронной почты – программа, обеспечивающая процесс обмена электронными сообщениями. Сервером также называют высокопроизводительный компьютер, на котором запущено ПО определенного типа.

Клиент – система, которая пользуется услугами, предоставляемыми сервером. В свою очередь, клиент не оказывает каких-либо услуг другим клиентам. В действительности же клиентом может выступать любое сетевое устройство, поскольку оно обязательно будет взаимодействовать с другими сетевыми устройствами и пользоваться их услугами. Например, любой сервер периодически выполняет обновление своих файлов, загружая новые из интернет-ресурсов компании-разработчика. В этом случае сервер также является клиентом. Чаще всего клиентом называют пользователя и его компьютер.

К преимуществам использования сетей относят:

- быстрый обмен информацией между пользователями;
- общий доступ к ресурсам;
- оптимальное распределение нагрузки между несколькими ЭВМ;
- возможность резервирования данных, сервисов сети, различных служб для повышения устойчивости всей системы к отказам;
- создание гибкой рабочей среды.

История совершенствования обмена данными отмечена улучшениями во всех компонентах коммуникационной модели. Эти

улучшения сделали сети более быстрыми, простыми в обращении и эффективными. Компьютерная сеть включает все аппаратное и программное обеспечение, необходимое для подключения компьютеров и другого электронного оборудования к каналу, по которому они могут общаться друг с другом. Устройства, которые взаимодействуют с другими устройствами в сети, называются *узлами*, *станциями* или *сетевыми устройствами*. Число узлов может составлять несколько тысяч.

ОДНОРАНГОВЫЕ СЕТИ (PEER-TO-PEER NETWORKS)

Когда узлы сети выполняют одинаковые коммуникационные функции, они называются равными (peer). Коммуникации между такими узлами обычно называются одноранговыми. В таких сетях нет каких-либо выделенных компьютеров, предоставляющих пользователям данной сети такие сетевые услуги, как:

- доступ к локальным ресурсам на основе аутентификации пользователей;
- доступ к онлайн-чатам и форумам;
- доступ к файловым архивам;
- доступ к глобальной сети Интернет.

Это далеко не полный список услуг, который могут предоставлять выделенные сервера. В одноранговых сетях все компьютеры равны и выполняют функции как клиентов, так и серверов. Примерами одноранговых сетей могут быть домашние сети или сети небольших офисов.

СЕТИ КЛИЕНТ – СЕРВЕР (CLIENT – SERVER NETWORKS)

В противоположность одноранговым сетям существуют сети, состоящие из множества компьютеров, называемых рабочими станциями или клиентами, которые обмениваются информацией практически исключительно с одним или с несколькими компьютерами, называемыми серверами.

Сети клиент – сервер предлагают централизованный доступ к сервису, приложениям и/или устройствам, упрощающим доступ к информации. Поскольку в таких сетях ресурсы сконцентрированы на сервере, они могут быть более эффективными, в отличие от распределенных по сети ресурсов в одноранговых сетях. Благодаря многочисленным преимуществам использования сервера сети клиент – сервер практически полностью вытеснили одноранговые локальные сети.

Типы сетей

Сети часто разделяют на три основных типа в зависимости от размера географической области, которую они охватывают. Небольшая область обычно связывается с термином «локальная вычислительная сеть» (Local Area Network – LAN), а большие области – с терминами «региональная вычислительная сеть» (Metropolitan Area Network – MAN) и «глобальная вычислительная сеть» (Wide Area Network – WAN).

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ

Если сеть привязана к одному месту (обычно одному зданию или комплексу различных зданий), то она называется локальной вычислительной сетью (ЛВС). ЛВС объединяет компьютерные системы и периферийные устройства (накопители на жестких дисках, стримеры, принтеры и т. п.) в группы, которые сообща используют данные и периферийные устройства (рис. 1.1).

Отличительными чертами ЛВС являются: большая скорость передачи данных, низкий уровень ошибок, использование дешевой среды передачи данных. Большинство ЛВС принадлежат какой-либо конкретной организации, которая их поддерживает.

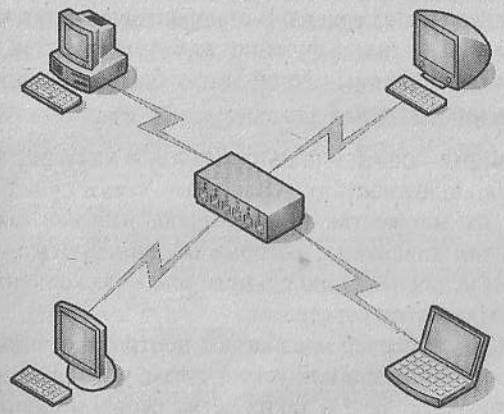


Рис. 1.1. Локальная вычислительная сеть

РЕГИОНАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ

Если сеть охватывает целый город, то она является региональной вычислительной сетью (РВС). РВС имеют много общего с ЛВС.

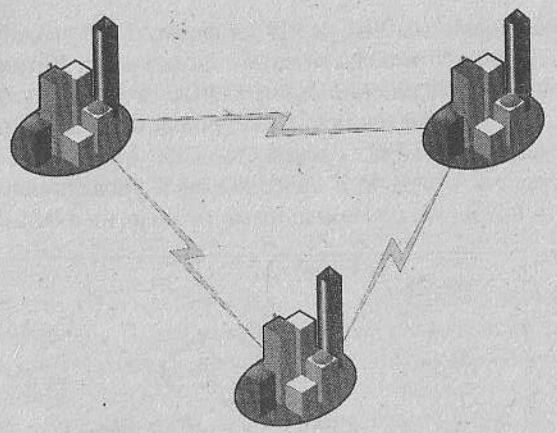


Рис. 1.2. Региональная вычислительная сеть

Однако по многим параметрам они сложнее последних, поскольку расстояния между компьютерами достаточно велики и для их соединения требуется использование выделенных линий связи, в том числе оптических. Таким образом, РВС разработаны для поддержки бóльших расстояний, чем ЛВС (рис. 1.2). Они могут использоваться для связывания нескольких ЛВС вместе в высокоскоростные интегрированные сетевые системы. РВС сочетают лучшие характеристики ЛВС (низкий уровень ошибок, высокая скорость передачи) с большей географической протяженностью. В настоящее время РВС завоевывают все большую популярность за счет предоставления пользователям такой сети гигантского количества ресурсов. Существуют региональные сети, насчитывающие более 70 000 пользователей и предоставляющие файловые архивы размерами в сотни терабайт.

ГЛОБАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ

Если сеть распространяется на большие площади, такие как страны, она называется глобальной вычислительной сетью (ГВС). Коммуникации по ГВС осуществляются посредством телефонных линий, спутниковой связи или наземных микроволновых систем. В последнее время все чаще и чаще применяются технологии передачи данных по оптоволоконным каналам. Такие каналы быстрее и стабильнее, чем радио или спутниковые каналы. Однако такие каналы и на порядок дороже. Такие сети зачастую создаются путем объединения ЛВС и РВС. Фактически объеди-

нение изолированных ЛВС и РВС в форму ГВС является современной тенденцией в области сетей. Поскольку ГВС, как правило, включают объединение многих ЛВС и РВС, то они часто представляют собой соединение различных технологий (рис. 1.3).

По сравнению с ЛВС большинство ГВС отличают более медленная скорость передачи и более высокий уровень ошибок. Разрешить эти проблемы призваны новые технологии в области ГВС.

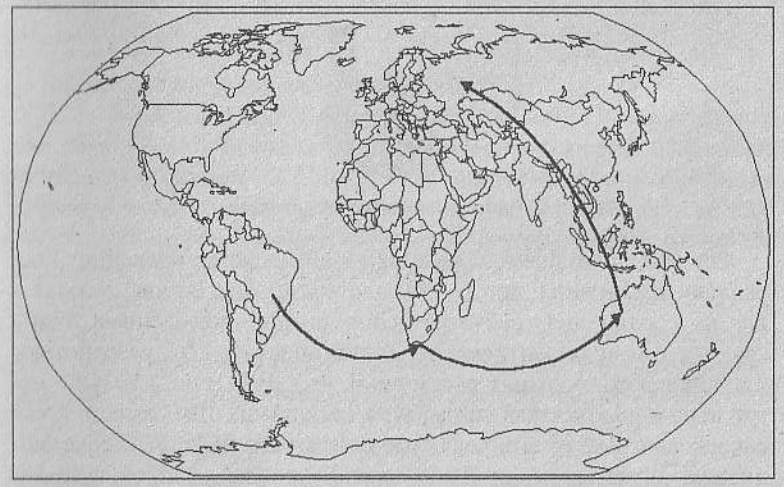


Рис. 1.3. Пример линий связи глобальной вычислительной сети

Примеры использования локальных сетей

Где же в настоящее время применяются локальные сети? Область их применения крайне широка: это и объединение вычислительных мощностей многих компьютеров на больших предприятиях для решения сложных вычислительных задач, так называемые «кластерные системы»; это и объединение удаленных филиалов фирм для обмена данными, например между офисом и складами; это и объединение компьютеров жильцов одного подъезда, дома или даже района, для совместного общения, игр, обмена новыми фильмами, музыкой или программами. В наше время каким бы мощным и современным не был компьютер, без подключения к локальной сети его возможности крайне ограничены.

Без ЛВС невозможно представить любое более или менее серьезное учебное заведение. В вузах локальные сети применяются для распространения электронной документации, организации дистанционного обучения, онлайн-конференций.

В настоящее время проще встретить компьютер без дисковода, чем компьютер, не подключенный к какой-нибудь локальной сети или Интернету. Интернет называют еще «мировой паутиной» или «всемирной сетью», и данное название как нельзя более точно характеризует эту сеть. Всемирная сеть охватывает миллиарды компьютеров по всему миру и насчитывает сотни миллионов пользователей. В ней сосредоточены сотни тысяч терабайт информации – от развлекательных порталов до хранилищ научной литературы. Однако для того, чтобы пользоваться этой информацией в полной мере, необходимо применение различных сетевых технологий и программного обеспечения, чему и будет посвящена данная книга.

Глава 2
Основы построения локальных сетей

В данной главе уделяется внимание теоретическим основам функционирования локальных сетей, физическим топологиям построения сетей, различным технологиям передачи данных в сетях. Рассматривается модель межсетевого взаимодействия OSI/ISO, а также протоколы и стандарты, которые используются для сетевого обмена данными. Дается понятие адресации и маршрутизации в IP-сетях.

Топологии построения локальных сетей

Прежде чем начать процесс построения локальной сети, необходимо определиться с некоторыми принципиальными вопросами, ответы на которые помогут вам более рационально и правильно спроектировать и построить локальную сеть. Итак, прежде всего, необходимо понять:

- сколько компьютеров будет в вашей сети;
- какую топологию при объединении компьютеров вы будете использовать;

- насколько удалены друг от друга все участники процесса межсетевого взаимодействия;
- какие сетевые устройства планируются в сети;
- будет ли сеть однородна по своей физической структуре, т.е. какой вид физического соединения будет между всеми сетевыми объектами, будет ли это только медный кабель или будет использоваться еще и радиоканал для подключения компьютеров;
- какие службы и сервисы будут предоставлены в сети;
- планируется ли в дальнейшем организовывать подключение к другим локальным сетям или к глобальной сети Интернет.

Ответы на эти несложные вопросы помогут сэкономить материальные средства и время, сведя к минимуму необходимость модернизации сети в дальнейшем.

На что же влияет количество компьютеров, которое будет подключено к локальной сети? Определившись с количеством компьютеров, сетевой топологией и территориальным распределением сетевых устройств, вы сможете определиться с количеством и стоимостью активного и пассивного сетевого оборудования, необходимого для построения сети. Иначе говоря, сразу станет понятно, сколько и какого типа кабеля, концентраторов, коммутаторов или маршрутизаторов необходимо будет приобрести, чтобы построить сеть.

Нельзя знать заранее, как будет развиваться сеть в будущем и сколько в ней будет компьютеров, поэтому при построении сети рекомендуется имеющееся количество компьютеров умножать в 2–3 раза и строить сеть, исходя из полученных параметров. Перейдем к вопросам выбора топологии локальной сети.

На этом этапе нужно понять разницу между физическими и логическими связями.

Конфигурация физических связей определяется физическими соединениями компьютеров между собой, т.е. как компьютеры соединены между собой с помощью линий связи, проводов, оптоволоконных каналов, радиоканалов. Физическая конфигурация вполне может отличаться от конфигурации логических связей.

Логические связи – это маршруты передачи данных между узлами сети. Они образуются при помощи настроек коммуникационного оборудования. Другими словами, компьютеры могут быть связаны между собой кабелем одним образом, а передавать друг

другу информацию по другому принципу. Например, имеются в одном задании три офиса, которые соединены в единую локальную сеть с помощью физической структуры, но у каждого имеется свой отдельный канал выхода в Интернет – почтовое сообщение из одного офиса в другой будет передаваться через внешние роутеры, а не по локальной сети.

При изучении существующих топологий сети речь будет идти о физических связях. При выборе топологии необходимо понимать преимущества и недостатки различных топологий.

ЗВЕЗДА

Наиболее функциональной и стабильной на сегодняшний день является локальная вычислительная сеть, имеющая топологию «звезда» (рис. 2.1), при использовании которой каждый компьютер сети подключается к особому устройству, называемому *концентратором* (*hub*) или *коммутатором* (*switch*).

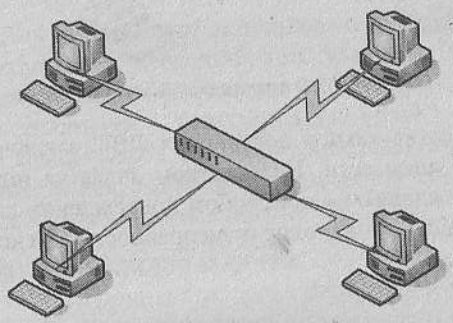


Рис. 2.1. ЛВС с топологией «звезда»

Преимуществом этой топологии является ее устойчивость к повреждениям кабеля – при обрыве одного соединяющего кабеля (сегмента сети) перестает работать только один из элементов сети и поиск повреждения значительно упрощается. Кроме этого, данная топология позволяет производить расширение сети, при котором не затрагивается текущая структура. Например, для добавления или соединения двух сетей достаточно соединить одним кабелем коммутаторы.

ОБЩАЯ ШИНА

В настоящее время данная технология практически не встречается. При использовании топологии с общей шиной (рис. 2.2)

компьютеры соединяются в одну линию, на концах которой устанавливаются *терминаторы* – специальные сопротивления для сброса приходящего сигнала. Без них сигнал, дойдя до конца кабеля, отражался бы и создавал помехи.

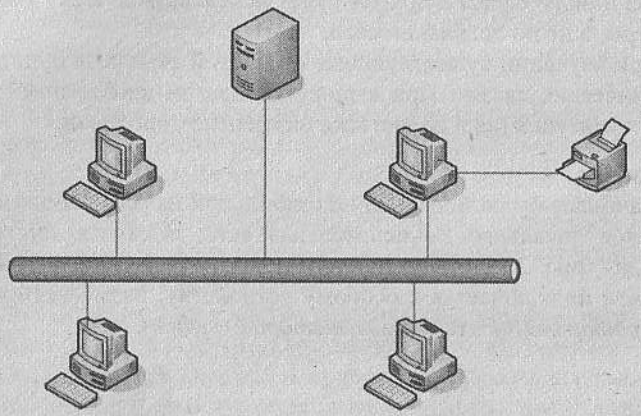


Рис. 2.2. ЛВС с топологией «общая шина»

Преимущества такого построения ЛВС заключаются в простоте организации сети. Недостатком является низкая устойчивость к повреждениям – при любом повреждении кабеля вся сеть перестает работать, а поиск неисправности представляется затруднительным.

КОЛЬЦО

При такой топологии узлы сети образуют кольцо, т.е. концы кабеля соединены друг с другом (рис. 2.3). Каждый узел сети соединен с двумя соседними. Преимуществом кольцевой топологии является ее достаточно высокая надежность, получаемая за счет избыточности сети. Однако стоимость такой ЛВС высока за счет расходов на адаптеры, кабели и дополнительные устройства, обеспечивающие работу сети.

В настоящее время для построения локальных сетей, в том числе и домашних, используется топология «звезда», поскольку она заложена в основу технологии *Fast Ethernet*, которая обеспечивает высокую надежность и быстрый обмен информацией. Две другие топологии используются или в очень старых сетях, или в каких-либо исключительных ситуациях.

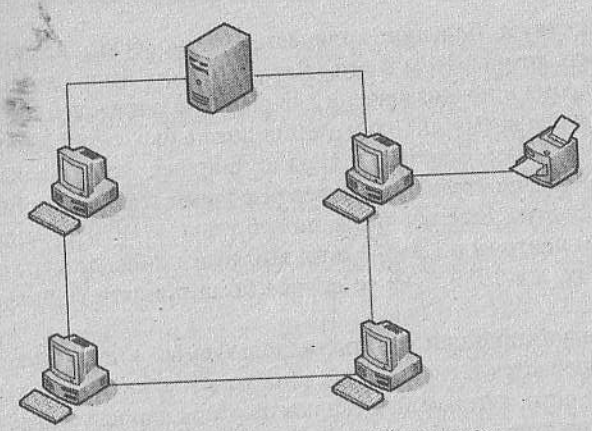


Рис. 2.3. ЛВС с топологией «кольцо»

Кроме того, существуют так называемые «гибридные» топологии соединения компьютеров, такие как:

- *иерархическая звезда* – при использовании данной топологии в сети присутствует несколько коммутаторов, иерархически соединенных между собой связями типа звезда.
- *смешанная топология* – характерна для сетей с большим количеством компьютеров. В таких сетях выделяют отдельные физические подсети, которые связаны между собой, и в то же время каждая из сетей имеет свою топологию.

ТОПОЛОГИИ БЕСПРОВОДНЫХ СЕТЕЙ

Существуют следующие топологии беспроводных сетей:

- *одноранговая* – два и более беспроводных адаптера соединены либо точка – точка, либо с помощью одной точки доступа.
- *инфраструктура* – несколько точек доступа, объединяющих беспроводные устройства, соединены между собой либо выделенной точкой доступа, либо с помощью выделенного радиодиапазона, если эти точки доступа двухдиапазонные.

Технологии передачи данных в локальных сетях

Рассмотрим технологии передачи данных, используемых в проводных локальных сетях.

Существует большое количество технологий, позволяющих соединить компьютеры в сеть. Каждая из них была разработана в разное время и предназначена для решения определенной задачи. В настоящее время для построения локальных сетей используют технологии Fast Ethernet и Gigabit Ethernet, которые являются наиболее распространенными реализациями технологии Ethernet.

Технология Ethernet была разработана в 1970 г. исследовательским центром в Пало-Альто, который принадлежит корпорации Xerox, а в 1980 г. на ее основе была принята спецификация IEEE 802.3.

Основной принцип работы, используемый в данной технологии, заключается в следующем. Для того чтобы начать передачу данных в сети, сетевой адаптер компьютера «прослушивает» сеть на наличие какого-либо сигнала. Если его нет, то адаптер начинает передачу данных, если же сигнал есть, то передача откладывается на определенный интервал времени. Время монопольного использования разделяемой среды одним узлом ограничивается временем передачи одного кадра.

Кадр – это единица данных, которыми обмениваются компьютеры в сети Ethernet. Кадр имеет фиксированный формат и наряду с полем данных содержит различную служебную информацию, например адрес получателя и адрес отправителя. После того как адаптер отправителя поместил кадр в сеть, его начинают принимать все сетевые адаптеры. Каждый адаптер проводит анализ кадра, и если адрес совпадает с их собственным адресом устройства (MAC-адрес), кадр помещается во внутренний буфер сетевого адаптера, если же не совпадает, то он игнорируется.

В том случае, если два или более адаптера, «прослушав» сеть, начинают передавать данные, возникает *коллизия* (*collision*). Адаптеры, обнаружив коллизию, прекращают передачу данных, а затем, повторно «прослушав» сеть, повторяют передачу данных через разные промежутки времени.

Такой метод доступа к среде передачи данных получил название *CSMA/CD* (*carrier-sense multiple access/collision detection*) – множественный доступ с контролем несущей и обнаружением коллизий (столкновений).

Как следует из вышесказанного, при большом числе компьютеров в сети и при интенсивном обмене информацией очень быстро растет число коллизий, и, как следствие, пропускная способность сети падает. Не исключен случай, когда пропускная способность может упасть до нуля. Но даже в сети, где средняя нагрузка не превышает рекомендованную (30–40% от общей полосы пропускания), скорость передачи составляет 70–80% от номинальной.

Однако в настоящее время данная проблема практически решена, поскольку разработаны устройства, способные разделять потоки данных между теми компьютерами, для которых эти данные предназначаются. Другими словами, трафик между портами, подключенными к передающему и принимающему сетевым адаптерам, изолируется от других портов и адаптеров. Такие устройства называются *коммутаторами* (*switch*).

Существуют различные реализации данной технологии – Ethernet, Fast Ethernet, Gigabit Ethernet, которые могут обеспечивать скорость передачи данных 10, 100 и 1000 Мбит/с соответственно.

Стандарт IEEE 802.3 содержит несколько спецификаций, отличающихся топологией и типом используемого кабеля. Например, 10 Base-5 использует толстый коаксиальный кабель, 10 Base-2 – тонкий, а 10 Base-F, 10 Base-FB, 10 Base-FL и FOIRL используют оптический кабель. Наиболее популярна спецификация IEEE 802.3 100 Base-TX, в которой для организации сети используется кабель на основе неэкранированных витых пар с разъемами RJ-45.

Таблица 2.1

Реализации сети Ethernet

Параметр	Ethernet	Fast Ethernet	Gigabit Ethernet
Номинальная скорость передачи информации, Мбит/с	10	100	1000
Среда передачи	Витая пара, коаксиальный кабель, оптоволокно	Витая пара, оптоволокно	Витая пара, оптоволокно
Варианты реализации	10 Base-2, 10 Base-T,	100 Base-TX, 100 Base-FX,	1000 Base-LX 1000 Base-SX

Параметр	Ethernet	Fast Ethernet	Gigabit Ethernet
	10 Base-5, 1 Base-5, 10 Broad-36	100 Base-T4	1000 Base-T
Топология	Общая шина, звезда	Звезда	Звезда

Перечисленные выше спецификации Ethernet можно описать следующим образом. Первое число в имени спецификации указывает максимальную скорость передачи данных, например «10» обозначает скорость передачи сигнала 10 Мбит/с. «Base» означает использование в стандарте Baseband-технологии (baseband – это узкополосная передача). При таком способе передачи данных по кабелю каждый бит данных кодируется отдельным электрическим или световым импульсом, при этом весь кабель используется в качестве одного канала связи, т.е. одновременная передача двух сигналов невозможна.

Первоначально последняя секция в названии спецификации предназначалась для отображения максимальной длины кабельного сегмента (без концентраторов и коммутаторов) в сотнях метров. Однако для удобства и более полного определения сути стандарта в его названии цифры были заменены буквами T и F, где T обозначает twisted pair – витую пару, а F обозначает fiber – волокно.

Таким образом, в настоящее время можно встретить сети, основанные на следующих спецификациях:

- 10 Base-2 – 10 MHz Ethernet на коаксиальном кабеле с сопротивлением 50 Ом, baseband. 10Base-2 известен как «тонкий Ethernet»;
- 10 Base-5 – 10 MHz Ethernet на стандартном (толстом) коаксиальном кабеле с сопротивлением 50 Ом, baseband;
- 10 Base-T – 10 MHz Ethernet по кабелю витая пара;
- 100 Base-TX – 100 MHz Ethernet по кабелю витая пара;
- 100 Base-FX – многомодовое оптоволокно, по которому может передаваться несколько оптических сигналов по одному волокну. Недостатком является сравнительно небольшая полоса пропускания;

- 100 Base-T4 – четырехпарная витая пара, в которой для передачи данных используется все четыре пары проводников, а не две;
- 1000 Base-SX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 550 м;
- 1000 Base-LX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 550 м. Оптимизирована для дальних расстояний при использовании одномодового волокна (до 40 км).

Весьма существенным преимуществом различных вариантов Ethernet является обоюдная совместимость, которая позволяет использовать их совместно в одной сети, в ряде случаев даже не изменяя существующую кабельную систему.

Стандарт технологии Fast Ethernet также включает в себя рекомендации относительно обеспечения возможности полнодуплексной работы (full-duplex mode) при подключении сетевого адаптера к коммутатору или же при непосредственном соединении коммутаторов между собой.

Суть полнодуплексного режима заключается в возможности одновременной передачи и приема данных по каналам Tx (канал от передатчика к приемнику) и Rx (канал от приемника к передатчику), при этом скорость передачи возрастает вдвое и достигает 200 Мбит/с. На данный момент практически все производители сетевого оборудования заявляют, что их устройства обеспечивают работу в полнодуплексном режиме, однако из-за разного толкования стандарта, в частности способов управления потоком кадров, не всегда удается добиться корректной работы этих устройств и хороших скоростных показателей.

Открытая модель межсетевого взаимодействия OSI/ISO

Разнообразие сетевых протоколов, технологий методов, средств и инструментария передачи данных между всеми участниками процесса межсетевого взаимодействия не могло не вызвать необходимость в строгой и четкой структуризации и формализации всех этапов взаимодействия. Это так называемая задача совместимости. Для нормального функционирования в сетях

среди разнообразия сетевых операционных систем, сетевого оборудования различных производителей, различных по сути протоколов прикладного уровня, необходимо, чтобы информационный пакет, отправленный с одного сетевого устройства, был доставлен на целевое сетевое устройство и, что очень важно, был верно интерпретирован этим устройством. Проще говоря, если вы отправили электронную почту с компьютера под управлением операционной системы Windows Vista на компьютер под управлением операционной системы Linux, вы должны быть уверены, что письмо дойдет до получателя. И не просто дойдет, но и будет открыто соответствующей программой, т.е. пользователь за компьютером-получателем откроет и прочтет это сообщение именно как электронное письмо, а не скажем, как фильм или электронную таблицу.

С развитием локальных сетей стало ясно, что необходима единая, стандартная модель, которой бы придерживались все производители сетевых продуктов, чтобы как минимум обеспечить совместимость своих новых разработок с уже существующими и работающими в компьютерной сети.

И такая модель была разработана. Над ее созданием в начале 80-х годов трудились ведущие организации по стандартизации – ISO, ITU-T и некоторые другие. Их труды принесли огромную пользу – была разработана модель протоколов передачи данных, которая сыграла значительную роль в развитии сетей. И до настоящего времени все, что касается сетевого взаимодействия, прямо или косвенно использует эту модель. Эталонная модель разработана Международной организацией по стандартизации (International Organization for Standardization, ISO) и получила название *Open System Interconnection Reference Model*, или модель *OSI*, как ее и называют сейчас.

Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 70-е годы. Полное описание этой модели занимает более 1000 страниц текста.

Модель OSI/ISO средства взаимодействия делят на семь уровней, каждый из которых выполняет свою, четко определенную роль:

- 7-й – прикладной (Application);
- 6-й – представительный (Presentation);

- 5-й – сеансовый (Session);
- 4-й – транспортный (Transport);
- 3-й – сетевой (Network);
- 2-й – канальный (Data Link);
- 1-й – физический (Physical).

Рассмотрим более детально каждый из уровней данной модели.

ФИЗИЧЕСКИЙ УРОВЕНЬ

Самый нижний уровень модели OSI. На этом уровне определяются такие характеристики сетевых компонентов: типы соединений сред передачи данных, физические топологии сети, способы передачи данных (с цифровым или аналоговым кодированием сигналов), виды синхронизации передаваемых данных, разделение каналов связи. Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение такие характеристики физических сред передачи данных, как полоса пропускания, помехозащищенность, волновое сопротивление и др. С физическим уровнем обычно ассоциируется подключение следующего сетевого оборудования: концентраторов, хабов и повторителей, регенерирующих электрические сигналы; соединительных разъемов среды передачи, обеспечивающих механический интерфейс для связи устройства со средой передачи; модемов и различных преобразующих устройств, выполняющих цифровые и аналоговые преобразования. Этот уровень модели определяет физические топологии в сети, которые строятся с использованием базового набора стандартных топологий. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

КАНАЛЬНЫЙ УРОВЕНЬ

Проверяет доступность среды передачи, а также реализует механизмы обнаружения и коррекции ошибок. Для работы на канальном уровне биты группируются в наборы. Эти наборы называются *кадрами* (*frame*). Канальный уровень обеспечивает корректность передачи каждого кадра. Для этого на канальном уровне используется метод подсчета контрольной суммы. Итак, если на физическом уровне единица информации – биты, то на канальном уровне – кадры. Специальная последовательность битов помещается в начало и конец каждого кадра для его выделения, а

также вычисляется контрольная сумма – все байты обрабатываются определенным способом и добавляется контрольная сумма к кадру. В таком виде кадр приходит по сети к получателю, где он снова вычисляет контрольную сумму полученных данных, сравнивает результат с контрольной суммой из кадра. Если они совпадают, то кадр правильный и получатель его принимает. Если же контрольные суммы не совпадают, то о дальнейшей его обработке никакой речи быть не может – фиксируется ошибка передачи.

Канальный уровень определяет:

- правила организации битов физического уровня (двоичные единицы и нули) в логические группы информации, называемые кадрами или фреймами (frame);
- правила обнаружения (и иногда исправления) ошибок при передаче;
- правила управления потоками данных (для устройств, работающих на этом уровне модели OSI, например мостов);
- правила идентификации компьютеров в сети по их физическим адресам.

С канальным уровнем обычно связаны следующие сетевые соединительные устройства:

- мосты;
- интеллектуальные концентраторы;
- коммутаторы;
- сетевые интерфейсные платы (сетевые интерфейсные карты, адаптеры и т.д.).

СЕТЕВОЙ УРОВЕНЬ

Служит для образования единой транспортной системы, объединяющей несколько сетей. При этом эти сети могут использовать абсолютно разные принципы передачи информации и быть организованными совершенно произвольно по структуре.

Как говорилось ранее, канальный уровень обеспечивает доставку данных между узлами сети только с соответствующей типовой топологией, например только в сети топологии «звезда». Данное ограничение не позволяет строить сети с развитой структурой, например сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых действуют избыточные связи между узлами.

Конечно, можно было бы усложнять средства канального уровня, чтобы они могли поддерживать избыточные связи, но

модель OSI предлагает другое решение – разделения обязанностей между уровнями. Так был создан новый уровень – сетевой. На этом уровне сам термин «сеть» наделяют специфическим значением. Здесь под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных средства канального уровня, строго определенные именно для этой топологии. Внутри каждой сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. На сетевом уровне единица информации представляется *пакетами*.

ТРАНСПОРТНЫЙ УРОВЕНЬ

Обеспечивает приложениям или верхним уровням модели OSI (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется.

СЕАНСОВЫЙ УРОВЕНЬ

Обеспечивает управление обменом информацией между двумя системами в сети (диалогом в сети): фиксирует, какая сторона сетевых «переговоров» является активной в настоящий момент, и предоставляет средства синхронизации. Эти средства позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке и не начинать все с начала. Сеансовый уровень отвечает за организацию и поддержку соединений между сессиями, администрирование и безопасность сети.

УРОВЕНЬ ПРЕДСТАВЛЕНИЯ

Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессию и т.п.) прикладного уровня в поток информации для транспортного уровня. Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC. На этом

уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб.

ПРИКЛАДНОЙ УРОВЕНЬ

Это в действительности просто набор разнообразных программных средств, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые веб-страницы, а также организуют свою совместную работу, например с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется *сообщением* (*message*). Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является копирование файлов, обмен почтовыми сообщениями и управление сетью.

Итак, мы рассмотрели все семь уровней модели OSI. Как можно заметить, в модели отделены программная и аппаратная часть структуры сети. Первые два уровня работают с аппаратными средствами сети и зависят от топологии сети и сетевого оборудования. Остальные верхние уровни очень мало зависят от технических особенностей построения сети. Если возникнет возможность перейти на другую сетевую технологию, это не потребует никаких изменений в программных средствах верхних уровней.

Порты

Существуют два типа межкомпьютерного обмена данными – датаграммы и сеансы. *Датаграмма* – это сообщение, которое не требует подтверждения о приеме от принимающей стороны, а если такое подтверждение необходимо, то адресат должен сам послать специальное сообщение. Для осуществления обмена данными таким способом принимающая и передающая стороны должны строго придерживаться определенного протокола во избежание потери информации. Каждая датаграмма является самостоятельным сообщением, и при наличии нескольких датаграмм в ЛВС их доставка адресату, вообще говоря, не гарантируется. При этом датаграмма обычно является частью какого-либо сообщения, и в большинстве ЛВС скорость передачи датаграмм гораздо выше, чем сообщений в сеансах.

В *сеансе* предполагается создание логической связи для обмена сообщениями между компьютерами и гарантируется получение сообщений. В то время как датаграммы могут передаваться в произвольные моменты времени, в сеансе перед передачей сообщения происходит открытие сеанса, а по окончании обмена данными сеанс должен быть закрыт.

Операционные системы большинства компьютеров поддерживают мультипрограммный режим, т.е. несколько программ выполняются одновременно (параллельно выполняется несколько процессов). С некоторой степенью точности можно говорить о том, что процесс – это и есть окончательное место назначения для сообщения. Однако в силу того, что процессы создаются и завершаются динамически, отправитель редко имеет информацию, достаточную для идентификации процесса на другом компьютере. Поэтому возникает необходимость в определении места назначения данных на основе выполняемых процессами функций при отсутствии каких-либо данных о тех процессах, которые реализуются этими функциями.

На практике вместо того, чтобы считать процесс конечным местом назначения, полагают, что каждый компьютер имеет набор некоторых точек назначения, называемых протокольными портами. Каждый порт идентифицируют целым положительным числом (от 0 до 65535). В этом случае операционная система обеспечивает механизм взаимодействия, используемый процессами для указания порта, на котором они работают, или порта, к которому нужен доступ. Обычно порты являются буферизированными, и данные, приходящие в конкретный порт до того, как процесс готов их получить, не будут потеряны: они будут помещены в очередь до тех пор, пока процесс не извлечет их.

Чтобы лучше понять технологию портов, представьте, что вы пришли в банк, чтобы сделать вклад. Для этого вам необходимо подойти к определенному окошку, где оператор оформит документы и вы откроете счет. В этом примере банк представляет собой компьютер, а операторы банка – программы, которые выполняют определенную работу. А вот окошки – это и есть порты, при этом каждое окошко в банке часто нумеруется (1, 2, 3 …). То же самое относится и к портам.

Следовательно, чтобы связаться с портом на другом компьютере, отправитель должен знать как IP-адрес компьютера-получателя, так и номер порта в компьютере. Каждое сообщение

содержит как номер порта компьютера, которому адресовано сообщение, так и номер порта-источника компьютера, которому должен прийти ответ. Таким образом реализуется возможность ответить отправителю для каждого процесса.

Порты с номерами от 0 до 1023 являются привилегированными и используются сетевыми службами, которые, в свою очередь, запущены с привилегиями администратора (суперпользователя). Например, служба доступа к файлам и папкам Windows использует порт 139, однако если она не запущена на компьютере, то при попытке обратиться к данной службе (т.е. к данному порту) будет получено сообщение об ошибке.

Порты с 1023 до 65535 являются непривилегированными и используются программами-клиентами для получения ответов от серверов. Например, веб-браузер пользователя, обращаясь к веб-серверу, использует порт 44587 своего компьютера, но обращается к 80 порту веб-сервера. Получив запрос, веб-сервер отправляет ответ на порт 44587, который используется веб-браузером.

Адресация в IP-сетях

Как уже говорилось ранее, каждое сетевое устройство должно иметь уникальный адрес, чтобы другие участники процесса межсетевого взаимодействия могли однозначно идентифицировать его и передать информацию. Идентификатором сетевых устройств в сетях является IP-адрес. Однако существуют также другие виды адресации в локальных сетях – они рассмотрены ниже.

АППАРАТНЫЕ (HARDWARE) АДРЕСА

Их еще называют MAC-адресами. Эти адреса предназначены для сети небольшого или среднего размера, поэтому они не имеют иерархической структуры. Типичным представителем адреса такого типа является адрес сетевого адаптера. MAC-адрес обычно используется только аппаратурой, поэтому его стараются сделать по возможности компактным и записывают в виде двоичного или шестнадцатеричного значения, например 0081005e24a8.

Аппаратные адреса не задаются вручную, они «вшиваются» в аппаратуру фирмой-изготовителем или генерируются случайным образом при каждом запуске оборудования (при таком способе уникальность адреса в пределах сети также обеспечивается оборудованием).

СИМВОЛЬНЫЕ АДРЕСА ИЛИ ИМЕНА

Такие адреса более удобны для запоминания людям, особенно если они несут определенный смысл. Символьные адреса легко использовать как в небольших, так и крупных сетях. Если это большая сеть, то символьное имя может иметь сложную иерархическую структуру. Например, адрес ftp.microsoft.com говорит о том, что данный компьютер поддерживает архив в сети корпорации Microsoft.

ЧИСЛОВЫЕ СОСТАВНЫЕ АДРЕСА

Символьные адреса, конечно, удобны для людей, но их использование создает много проблем в сети. Во-первых, символьные имена могут быть довольно большой длины. Во-вторых, символьные имена можно легко изменять, такое непостоянство и большая длина имени существенно затрудняет передачу их по сети. Поэтому в большинстве случаев в больших сетях для определения адресов узлов используют числовые составные адреса фиксированного и компактного форматов или, как их еще называют, IP-адреса.

IP-адрес – это основной адрес сетевого уровня модели OSI/ISO. Данный адрес однозначно идентифицирует сетевой объект в сети. IP-адрес разделяется на две части: номер сети и номер узла.

Номер сети может быть выбран администратором произвольно либо назначен по рекомендации специального подразделения сети Интернет (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Интернета. Обычно поставщики интернет-услуг получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами.

Рассмотрим структуру IP-адреса. IP-адрес имеет длину 4 байта, это дает в совокупности 32 бита доступной информации. 32-битовая разрядность IP-адреса приводит к тому, что числа получаются большими, даже если они представлены в десятичной форме исчисления. Поэтому, для удобства IP-адрес записывается в виде четырех чисел, разделенных точками:

- 128.10.2.30 – десятичная форма представления адреса – 4 числа, разделенных точками. Каждое из этих чисел называется октетом;
- 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

Классы IP-адресов

Как уже было сказано, IP-адрес состоит из двух логических частей: номера сети и номера узла в сети. Сразу возникает вопрос: как определить в одном адресе, где номер сети, а где номер узла? Можно условиться использовать, например, первые 8 или 16 бит адреса для номера сети, а остальные – для номеров узлов в этой сети. Но в таком случае адресация получается абсолютно не гибкой, мы будем иметь или много маленьких сетей и мало больших, или наоборот.

Для того чтобы более рационально определиться с величиной сети и при том разграничить, какая часть IP-адреса относится к номеру сети, а какая – к номеру узла, условились применять систему классов. Эта система использует значения первых битов адреса, которые являются признаками того, к какому классу относится тот или иной IP-адрес (рис. 2.4).

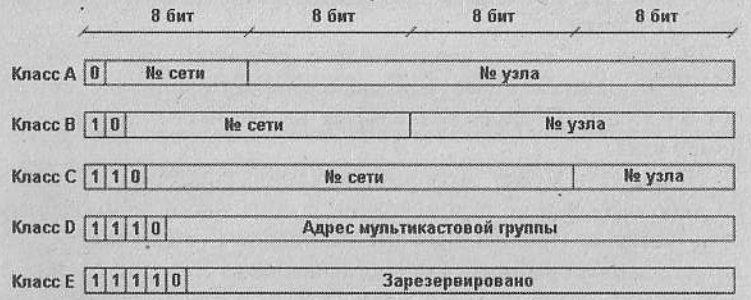


Рис. 2.4. Биты в IP-адресах

СЕТЬ КЛАССА A

Если адрес начинается с 0, то сеть относят к классу A. Номер сети класса A занимает один байт, остальные 3 байта отводятся для номеров узла в этой сети. Таким образом, сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.)

Исходя из сказанного ранее, самих сетей класса A может быть немного, но зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов. Например, IP-адрес 102.56.187.5 обозначает сеть с номером 102 и хост с номером 56.187.5.

СЕТЬ КЛАССА B

Если первый октет IP-адреса находится в диапазоне от 128 до 191, то сеть относится к классу B. В сетях класса B и под номер сети, и под номер узла одинаково отводится по 16 бит, т.е. по 2 байта. Например, IP-адрес 154.2.91.240 обозначает сеть с номером 154.2 и хост с номером 91.240.

Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов 2^{16}, что составляет 65 536 узлов.

СЕТЬ КЛАССА C

В сети класса C значение первого октета в IP-адресе находится в диапазоне от 192 до 223. В этом случае под номер сети отводится 24 бит, а под номер узла – 8 бит. Сети класса C имеют небольшое количество узлов 2^8, то есть 256. Надо отметить, что именно сети класса C являются наиболее распространенными.

СЕТЬ КЛАССА D

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес – multicast.

Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес. Ниже об этом будет рассказано подробнее.

СЕТЬ КЛАССА E

В сетях класса E адрес начинается с последовательности 11110. Адреса этого класса зарезервированы для будущих применений.

Диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей, приведены в табл. 2.2.

Таблица 2.2

Диапазоны номеров сетей

Класс	Первые биты	Наименьший адрес сети	Наибольший адрес сети	Максимальное количество узлов
A	0	1.0.0.0	126.0.0.0	224
B	10	128.0.0.0	191.255.0.0	216

Класс	Первые биты	Наименьший адрес сети	Наибольший адрес сети	Максимальное количество узлов
C	110	192.0.1.0	223.255.255.0	28
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	зарезервирован

ОСОБЫЕ IP-АДРЕСА

Существуют некоторые значения IP-адресов, зарезервированные для особых целей. Различают следующие типы специальных IP-адресов:

- 0.0.0.0 – может использоваться как адрес отправителя в IP-пакете. Это означает, что компьютер, отправивший пакет, не имеет IP-адреса. В таблице маршрутизации адрес сети 0.0.0.0 указывает на маршрут «по умолчанию» – он применяется при пересылке пакетов, которые не попадают под другие записи таблицы;
- Loopback (127.0.0.0 – 127.255.255.255) – так называемая «петля», или локальный интерфейс. Данный IP-адрес присутствует в любой сетевой операционной системе и предназначен для работы и самодиагностики программного обеспечения, требующего сетевого подключения. Даже если на компьютере нет сетевой карты, данный IP-адрес присутствует в любом случае;
- Fake (10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 и 192.168.0.0 – 192.168.255.255) – «серые», не маршрутизируемые IP-адреса – они предназначены только для работы внутри корпоративных сетей и не маршрутизируются в глобальной сети Интернет. В последнее время наблюдается острая нехватка адресного пространства, поэтому Fake-адреса используются компаниями для адресации внутри своих сетей: поскольку адреса не маршрутизируются в Интернете, они гарантированно не пересекаются и могут быть использованы произвольно;
- адреса для автоконфигурации (169.254.0.0 – 169.254.255.) – диапазон адресов для Zeroconf (технологии автоматической настройки сети, позволяющей хостам автоматически создавать работающую IP-сеть без специальной настройки). Выбирается DHCP-клиентами при недоступности DHCP-сервера;

Примечание. *DHCP (Dynamic Host Configuration Protocol*, протокол динамической конфигурации узла) – сетевой протокол, с помощью которого каждому компьютеру в IP-сети можно автоматически назначить динамический IP-адрес в заданном администратором диапазоне. Это позволяет избежать ручной настройки IP-адресов всех компьютеров сети.

- широковещательные адреса (255.255.255.255) – отправка пакета на этот адрес вызывает его доставку всем машинам в одной сети с отправителем;
- адрес, в котором бит адреса компьютера установлен в «0», обозначает адрес сети – например 192.168.1.0.

Конечно, существует значительно больше специальных зарезервированных IP-адресов. В данной главе рассматриваются лишь основные специализированные адреса, которые могут пригодиться при построении и диагностике локальной сети.

Для того чтобы соединить компьютеры в сеть, недостаточно только назначить им IP-адреса, необходимо также правильно назначить сетевую маску.

СЕТЕВЫЕ МАСКИ

Наиболее часто используемым классом сетей является класс C, вследствие того что достаточно мало компаний требуют выделения всей сети класса B или тем более – A.

Адресное пространство, выделенное для адресации компьютеров в сети, можно разбить на еще более мелкие структуры, которые называются *подсетями*. Разбиение единого адресного пространства на подсети необходимо для более экономного использования IP-адресов. Например, если в компании есть только 25 компьютеров, не имеет смысла покупать для себя блок сети класса C для 254 хостов (всего в сети класса C может быть 255 хостов, но 0 в бите хоста обозначает адрес сети, а значение 255 в последнем октете используется для широковещательной рассылки). Разделение IP-адресов на сети и подсети осуществляется с помощью так называемых *сетевых масок*.

Сетевая маска – это 32-битное число, которое накладывается на IP-адрес и позволяет однозначно идентифицировать адрес сети и адрес хоста в этой сети. Стандартные маски для сетей:

- класс A – 255.0.0.0;
- класс B – 255.255.0.0;
- класс C – 255.255.255.0.

Если представить маску сети не в десятичном виде (255.255.255.0), а в двоичном (11111111.11111111.11111111.00000000), то становится видно, что первые три октета содержат только «1», что соответствует адресу сети, а четвертый октет содержит «0», что соответствует адресу хоста.

Кроме стандартных масок, для классов сетей A, B и C имеются так называемые *маски переменной длины*, которые позволяют разбивать сети на еще более мелкие сегменты. Например, есть компания, в которой всего 10 компьютеров, и необходимо, чтобы все компьютеры имели реальные маршрутизируемые адреса. Как видно из количества компьютеров, покупать всю сеть класса C для использования всего 10 адресов нецелесообразно, в этом случае покупается так называемая *подсеть класса C*. Маска данной подсети рассчитывается по количеству компьютеров в сети.

Рассмотрим полную таблицу соответствия префиксов CIDR (Classless InterDomain Routing, бесклассовая адресация) количеству узлов и сетей (табл. 2.3).

Таблица 2.3
Диапазоны номеров сетей

Длина префикса CIDR	Теоретическое количество хостов	Маска сети
/1	2147483648	128.0.0.0
/2	1073741824	192.0.0.0
/3	536870912	224.0.0.0
/4	268435456	240.0.0.0
/5	134217728	248.0.0.0
/6	67108864	252.0.0.0
/7	33554432	254.0.0.0
/8	16777216	255.0.0.0
/9	8388608	255.128.0.0
/10	4194304	255.192.0.0
/11	2097152	255.224.0.0
/12	1048576	255.240.0.0

Длина префикса CIDR	Теоретическое количество хостов	Маска сети
/13	524288	255.248.0.0
/14	262144	255.252.0.0
/15	131072	255.254.0.0
/16	65536	255.255.0.0
/17	32768	255.255.128.0
/18	16384	255.255.192.0
/19	8192	255.255.224.0
/20	4096	255.255.240.0
/21	2048	255.255.248.0
/22	1024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224
/28	16	255.255.255.240
/29	8	255.255.255.248
/30	4	255.255.255.252
/31	2	255.255.255.254

В рассматриваемом примере наиболее приближенное число хостов к требуемым будет 16, так как 8 – это очень мало, а 32 – слишком много. Значит, можно предложить предприятию подсеть класса C с маской 255.255.255.240 или, как еще часто пишут, в формате CIDR, /28 по количеству единичных битов сети в маске.

Для того чтобы настроить передачу данных между компьютерами в пределах одной сети или подсети, вполне достаточно знать IP-адрес, маску и иметь сетевой кабель для соединения компьютеров. Но для того чтобы организовать пересылку пакетов

из одной подсети в другую, этого мало – необходимо также владеть хотя бы теоретическими знаниями о маршрутизации пакетов в сети.

Маршрутизация пакетов

Маршрутизацией называется процесс определения маршрута следования пакета от узла-отправителя к узлу-получателю через системы связи. Если узел-отправитель и узел-получатель пакета находятся в пределах одной подсети, то маршрутизация происходит на основе физических адресов, о которых было сказано ранее, и для маршрутизации задействуется протокол физического уровня модели OSI.

Принадлежность узлов к одной подсети определяется сетевой подсистемой операционной системы на базе масок. Рассмотрим простой пример (рис. 2.5):

узел-отправитель: IP 192.168.1.10, маска сети 255.255.255.0,
узел-получатель: IP 192.168.1.11, маска сети 255.255.255.0.

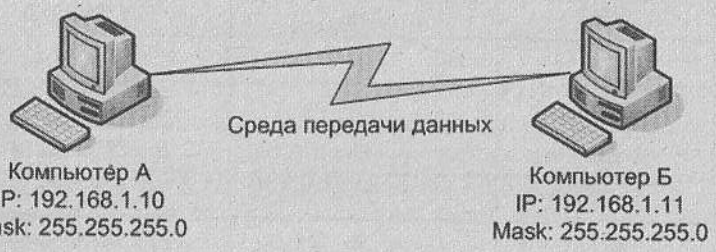


Рис. 2.5. Два хоста принадлежат одной сети

На каждом хосте есть локальная система маршрутизации со своей встроенной таблицей, просмотреть которую можно, набрав команду `route print` в командной строке операционной системы (рис. 2.6).

Сетевая подсистема накладывает на IP-адрес отправителя пакета и на IP-адрес получателя пакета маску подсети и анализирует адреса сетей, к которым принадлежат хосты. В данном случае адресами сетей будут являться 192.168.1.0 и для отправителя, и для получателя.

Так как хосты находятся в одной подсети, то для передачи пакетов между ними используются протоколы физического уровня.

Если же адреса подсетей различны, сетевая подсистема смотрит наличие маршрутов к подсети отправителя в своей таблице маршрутизации и, если не находит, отправляет по умолчанию по маршруту на так называемый *default gateway*. Таковым обычно является специальное сетевое устройство – *маршрутизатор*. Именно это устройство, которое может быть как аппаратным (т.е. функции маршрутизации выполняет специальная микросхема), так и программным (в этом случае это обычный компьютер со специальным программным обеспечением, которое и занимается маршрутизацией).

```
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза     Интерфейс  Метрика
          0.0.0.0          0.0.0.0    92.113.216.208  92.113.216.208     1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1    50
  92.113.216.208  255.255.255.255    92.113.216.208  92.113.216.208     1
  92.255.255.255  255.255.255.255        127.0.0.1       127.0.0.1    20
      192.168.1.0    255.255.255.0    192.168.1.2     192.168.1.2      20
      192.168.1.2  255.255.255.255        127.0.0.1       127.0.0.1    20
    192.168.1.255  255.255.255.255    192.168.1.2     192.168.1.2      1
        195.5.5.205  255.255.255.255    92.113.216.208  92.113.216.208   20
          224.0.0.0        240.0.0.0    192.168.1.2     192.168.1.2      1
          224.0.0.0        240.0.0.0    92.113.216.208  92.113.216.208   1
  255.255.255.255  255.255.255.255    92.113.216.208  92.113.216.208     1
  255.255.255.255  255.255.255.255    192.168.1.2     192.168.1.2      1
Основной шлюз:     92.113.216.208
```

Рис. 2.6. Локальная таблица маршрутизации

Маршрутизацией, приемом и передачей пакетов занимаются специальные подпрограммы на уровне ядра операционной системы. Пользовательский уровень находится выше уровня ядра, и для пользователя сети все эти процессы не представляют особого интереса. При работе в локальных сетях и в Интернете пользователь столкнется с протоколами прикладного уровня (см. ниже).

Имена компьютеров в сети

Как показала практика, пользователям значительно удобнее называть компьютеры не числами, а именами. При этом у одной машины может быть несколько имен, но одно и то же имя не может быть присвоено двум компьютерам. Основным вопросом при этом становится перевод имен в интернет-адреса. Таким переводом занимаются специальные программы, установленные на некоторых сетевых узлах.

Для упрощения обращения к компьютерам была введена *доменная система имен* (*Domain Name System*, *DNS*), представляю-

щая метод назначения имен путем возложения на группы пользователей ответственности за подмножества имен. В этой системе каждый уровень называется доменом и отделяется от других точками (например, pfu.edu.ru, рис. 2.7). Первый домен в имени (pfu) – имя реального компьютера. Второй (edu) – имя группы, создавшей и курирующей имя компьютера. Третий, домен верхнего уровня (ru) в данном случае обозначает Россию. Каждая группа может изменять находящиеся под ее контролем имена.

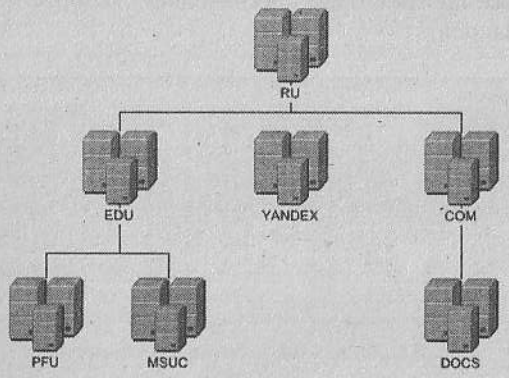


Рис. 2.7. Пример домена в системе DNS

Если все группы будут соблюдать правила и обеспечивать уникальность имен, то никакие два компьютера в Интернете не будут иметь одинаковых имен.

Организационные домены верхнего уровня были созданы, когда была изобретена доменная система. Изначально их было шесть (табл. 2.4).

Таблица 2.4

Первоначальные домены верхнего уровня

Домен	Использование
com	Коммерческие организации
edu	Учебные заведения
gov	Правительственные учреждения
mil	Военные учреждения

Домен	Использование
org	Прочие организации
net	Сетевые ресурсы

Когда сеть Интернет, зародившаяся в США, стала международной, возникла необходимость предоставить всем странам возможность контроля за именами систем, находящихся в них. Для этой цели был создан набор двухбуквенных доменов, которые соответствуют доменам высшего уровня для этих стран, например: ru – Россия, ua – Украина, kz – Казахстан и т. д.

Однако в США, которые тоже имеют свой собственный код страны, он широко не применяется – большинство систем пользуются организационными доменами (типа com), а не географическими (типа us). Следует отметить, что у компьютера могут быть имена обоих видов, а вот способа преобразования организационных имен в географические не существует.

Для того чтобы преобразовать имя в адрес, компьютер обращается к серверам DNS распределенной базы данных, призванной находить компьютеры и службы по понятным именам. Вначале он «опрашивает» локальные серверы DNS на наличие адреса. При этом существует три возможности:

- локальный сервер знает адрес, так как этот адрес находится в той части всемирной базы данных, которую курирует данный сервер;
- локальный сервер знает адрес, так как кто-то недавно уже спрашивал о нем. Когда кто-либо спрашивает об адресе, сервер DNS некоторое время помнит его на тот случай, если чуть позже о нем спросит кто-нибудь еще. Это значительно повышает эффективность работы системы;
- локальный сервер не знает адреса, но знает, как его определить.

Если ни один из этих вариантов не сработал, то адрес определяется следующим образом. Программное обеспечение локального сервера связывается с корневым сервером, который знает адреса серверов доменов высшего уровня (крайней правой части имени, например в случае адреса pfu.edu.ru это ru), и запрашивает у него адрес компьютера, отвечающего за домен ru. Получив информацию, он связывается с этим компьютером и запрашивает у него адрес сервера edu, и т.д.

Прикладные протоколы в сетях TCP/IP

К протоколам прикладного уровня модели OSI/ISO можно отнести следующие наиболее распространенные протоколы:

- HTTP (Hyper Text Transfer Protocol);
- FTP (File Transfer Protocol);
- SMTP (Simple Mail Transfer Protocol);
- POP3 (Post Office Protocol v.3)

Рассмотрим эти протоколы подробнее.

ПРОТОКОЛ HTTP

Основным назначением протокола HTTP является передача веб-страниц (текстовых файлов с разметкой HTML). Протокол HTTP – это протокол, основанный на принципе запрос – ответ, где запросы посылает клиентская сторона, а обработкой их и пересылкой веб-содержимого – сервер (рис. 2.8).

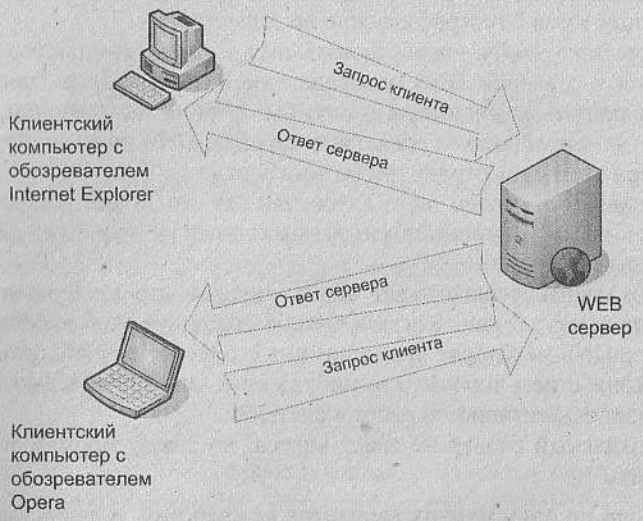


Рис. 2.8. Схема работы протокола HTTP

Протокол HTTP без преувеличения является в настоящее время наиболее распространенным протоколом прикладного уровня в Интернете. С его помощью пользователи Интернета просматривают любимые сайты, читают новости, смотрят клипы, скачивают музыку, общаются.

ПРОТОКОЛ FTP

Основным назначением протокола FTP является передача файлов между клиентом и сервером. Протокол FTP является на текущий момент основным протоколом для скачивания файлов с серверов в Интернете и закачки их на серверы.

FTP является сложным протоколом, при работе с ним создается два канала: управляющий (ftp-command) и канал данных (ftp-data) (рис. 2.9).

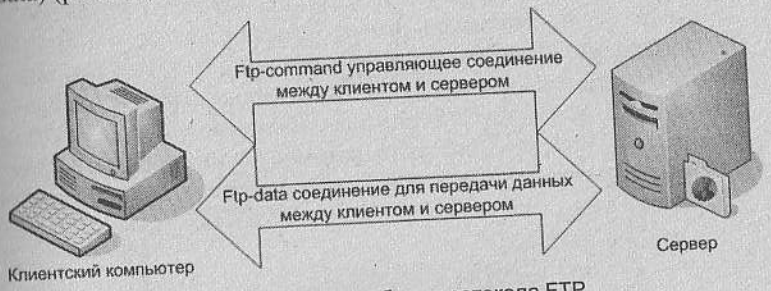


Рис. 2.9. Схема работы протокола FTP

Протокол FTP поддерживает два режима работы: активный и пассивный. Управляющее соединение одинаково для обоих режимов. Клиент инициирует TCP-соединение с динамического порта (1024 – 65535) к порту номер 21 на FTP-сервере и сообщает свои имя пользователя и пароль для подключения к серверу. Дальнейшие действия зависят от того, какой выбран режим FTP (активный или пассивный).

В активном режиме клиент инициирует сетевое соединение и сообщает серверу номер порта (из динамического диапазона 1024–65535) для того, чтобы сервер мог подключиться к клиенту, установить соединение и передать данные. FTP-сервер подключается к заданному номеру порта клиента, используя со своей стороны номер 20 TCP-порта для передачи данных.

В пассивном режиме, после того как клиент инициирует сетевое соединение, сервер сообщает клиенту номер TCP-порта (из динамического диапазона 1024–65535), к которому можно подключиться для установки соединения и передачи данных.

Главное отличие между активным и пассивным режимами FTP – это сторона, которая открывает соединение для передачи данных. В активном режиме клиент должен принять соединение от FTP-сервера, а в пассивном – соединение всегда инициирует клиент.

ПРОТОКОЛ SMTP

Основная задача протокола SMTP состоит в том, чтобы обеспечивать передачу электронных сообщений (электронную почту). Для работы через протокол SMTP клиент создает TCP-соединение с сервером через порт 25. Затем клиент и SMTP-сервер обмениваются информацией, пока соединение не будет закрыто или прервано (рис. 2.10).

Рис. 2.10. Схема работы протокола SMTP

ПРОТОКОЛ POP3

Основной задачей протокола POP3 является получение почтовых сообщений клиентом с сервера. Перед работой через протокол POP3 сервер прослушивает порт 110. Когда клиент хочет использовать этот протокол, он должен создать TCP-соединение с сервером. Когда соединение установлено, сервер отправляет приглашение. Затем клиент и POP3-сервер обмениваются информацией, пока соединение не будет закрыто или прервано.

Оборудование для построения локальных сетей

Для построения локальных сетей используется активное и пассивное сетевое оборудование. К активному сетевому оборудованию можно отнести сетевые карты, коммутаторы, концентраторы, повторители, маршрутизаторы, точки доступа. К пассивному оборудованию относятся сетевой кабель, разъемы, сетевые розетки. Рассмотрим оборудование, которое может понадобиться для построения простейшей локальной сети.

СЕТЕВАЯ КАРТА (СЕТЕВОЙ АДАПТЕР)

Предназначена для непосредственного соединения сетевого кабеля с компьютером (рис. 2.11). Очевидно, что сетевые адаптеры и кабели являются аппаратной основой организации локальной сети и их нормальная работа жизненно важна для сети. Функцией сетевого адаптера является передача и прием сигналов из кабеля. При передаче адаптер воспринимает команды и данные от операционной системы, преобразует эту информацию в один из стандартных форматов и передает ее в сеть через подключенный к адаптеру кабель. При приеме происходят аналогичные действия, только в обратном порядке.

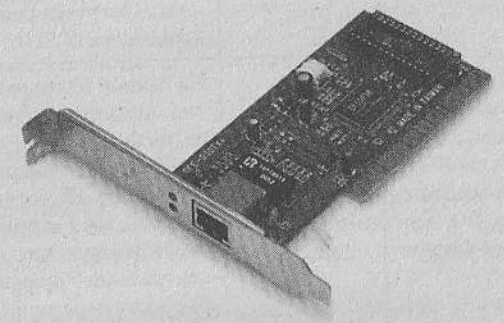


Рис. 2.11. D-Link 10/100Mbs Fast Ethernet

Приведем характеристики распространенных и хорошо зарекомендовавших себя сетевых адаптеров (табл. 2.5).

Таблица 2.5

Характеристики некоторых сетевых адаптеров

Наименование	Чип	Комментарий
D-Link DFE-528TX	D-Link DL10038C	Максимальная длина рабочей линии (сегмента) 400 м, P'n'P (Plug and Play). Технология

Наименование	Чип	Комментарий
		разработана компанией Microsoft и заключается в том, что при первой инсталляции устройства система сама его обнаруживает и пытается найти оптимальный драйвер к нему. Прекрасно работает на длинных сегментах
D-Link DFE-550TX	D-Link DL10050B	Хорошо выполненный чип, но без механизма адаптации к условиям конкретного кабельного окружения. Поддержка полнодуплексной связи (Full-duplex) и очень низкая загрузка центрального процессора (CPU)
3Com 3C905CX-TX-M	3Com 920-ST06	На данной плате расположен чип, поддерживающий технологии адаптации к условиям конкретного кабельного окружения. По сравнению с остальными картами имеет самую низкую загрузку центрального процессора. Скорость передачи 10 или 100 Мбит/с, поддерживается полнодуплексная связь, есть светодиодные индикаторы для 10/100 Мбит/с
Intel Pro/100 M Desktop Adapter	Intel 82551QM	Автоматическая настройка скорости 10 или 100 Мбит/с обеспечивает автоматическое соединение на максимально возможной скорости, что повышает общую производительность сети. Применяется адаптивная технология, неустойчивая связь на длинных сегментах, P'n'P

Наименование	Чип	Комментарий
InBusiness PRO/100+	Intel GD82559	Наиболее подходящая сетевая карта для рабочей станции начального уровня. Отличная поддержка режима Full-duplex и невысокая загрузка CPU. Низкая цена
LG LNIC-10/100Aw Planet ENW-9504 Surecom EP-320X-R	Realtek RTL8139D	Карты, построенные на этом чипсете, принадлежат бюджетному сегменту рынка и стоят очень дешево. Конечно, этот факт сказывается на их работе. Нестабильная работа в полнодуплексном режиме и большая загрузка центрального процессора не позволяют получить хорошие скоростные показатели
CompuShack Fastline II PCI UTP DEC-Chip Lantech FastLink/TX	Intel (DEC) 21143-PD	Старый чипсет. Высокая загрузка процессора, отсутствие поддержки режима Full Duplex. В сетях на основе концентраторов карты могут применяться, в противном случае их лучше не использовать

Конечно же, при выборе адаптера большое значение имеет тип используемого кабеля. Кроме того, каждый адаптер, устанавливаемый в компьютер, должен нормально работать с остальными устройствами компьютера, например с материнской платой.

СЕТЕВОЙ КАБЕЛЬ

Основой любой ЛВС является сетевой кабель, который обеспечивает канал связи компьютера с остальными компьютерами сети. В настоящее время в основном применяются такие типы кабеля, как витая пара и оптоволокно, однако до сих пор встречаются сети, построенные с использованием коаксиального кабеля.

КАБЕЛЬ ВИТАЯ ПАРА

Содержит четыре пары проводов, скрученных один с другим по всей длине кабеля (рис. 2.12). Скручивание позволяет повы-

сить помехоустойчивость кабеля и снизить влияние каждой пары на все остальные. Кроме этого, для повышения помехозащищенности был разработан *экранированный кабель*, проводники которого кроме внешней изоляции также заключены в оболочку из фольги, которая отражает магнитные помехи.

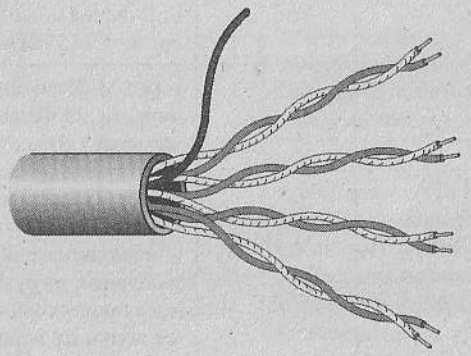


Рис. 2.12. Сечение кабеля витая пара

Следует иметь в виду, что из четырех скрученных пар в сетях, удовлетворяющих спецификациям 10 Base-T и 100 Base-TX (см. ниже), используются только 4 проводника (т.е. 2 пары), а максимальная длина сегмента не может превышать 100 м. Кабель разделен на классы, причем наиболее качественной считается витая пара 5-го класса (категории). Для соединения кабеля с компьютером или концентратором используется разъем типа RJ-45, внешний вид которого показан на рис. 2.13.

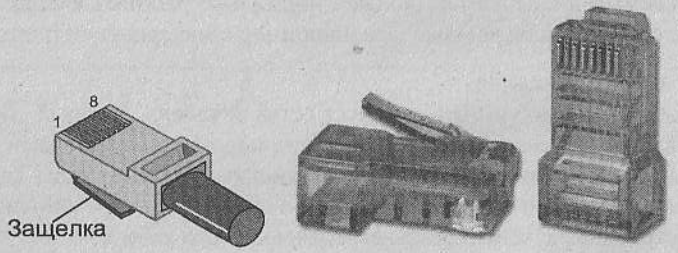


Рис. 2.13. Коннектор RJ-45

Характеристики кабеля витая пара приведены в табл. 2.6.

Таблица 2.6

Характеристики кабеля витая пара

Наименование	Стандарт разъема	Длина сегмента	Число витых пар
100 Base-TX	RJ-45	100 м	2
100 Base-T4	RJ-45	100 м	4

Необходимо отметить, что стоимость коаксиального кабеля в настоящее время выше стоимости витой пары (да и купить его практически невозможно), а по надежности и скорости передачи данных витая пара выигрывает у коаксиального кабеля. Кроме того, витая пара позволяет сделать сеть более надежной, а обрыв на линии легко локализуется и не влияет на работу других рабочих станций. Единственным оправданием использования коаксиального кабеля может быть необходимость соединения двух компьютеров или сетей, находящихся на расстоянии, превышающем 100 м, поскольку максимальная длина «тонкого» коаксиального кабеля достигает 180 м, а «толстого» – 500 м. И все же оборудование для использования коаксиального кабеля купить сейчас практически невозможно.

КОНЦЕНТРАТОР (HUB), ИЛИ РЕПИТЕР (REPEATER)

Представляет собой устройство, предназначенное для соединения компьютеров при использовании топологии «звезда». Концентратор является узловой точкой сети, к которой подключаются компьютеры и периферийные устройства с сетевым интерфейсом. Кроме этого, при передаче данных он усиливает сигнал, что позволяет увеличить длину сегмента.

При построении сетей важными факторами в выборе концентратора являются его стоимость, длина рабочего сегмента, надежность и универсальность. Концентраторы соединяют сегменты, использующие одинаковые или разные типы носителя; восстанавливают сигнал, увеличивая дальность передачи; передают данные в обоих направлениях. Таким образом, концентраторы – самый дешевый способ расширить сеть, построенную с использованием коаксиального кабеля или витой пары. Концентраторы расширяют возможности сети, разделяя ее на сегменты, уменьшая тем самым количество компьютеров на один сегмент. У этих

устройств состояние активности сети легко наблюдать с помощью световых индикаторов, которыми, как правило, снабжен каждый порт. Кроме того, часто присутствуют индикаторы для отображения информации о передаче неверных пакетов (jabber) и о возникновении в сети коллизии.

При выборе места для установки концентратора в целях уменьшения длин сегментов сети целесообразно расположить его вблизи геометрического центра сети. Такое расположение позволит минимизировать расход кабеля, причем длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 м. Чаще всего концентратор ставят на стол, закрепляют его на стене с помощью входящих в комплект концентратора скоб или монтируют в серверную стойку. При планировании сети не следует забывать о возможности наращивания (каскадирования) концентраторов путем соединения их в одном месте по несколько устройств с использованием портов расширения (рис. 2.14). В этом случае обратите внимание на возможность подвода электропитания для концентраторов, а также на тот факт, что расстояние между каскадируемыми концентраторами не должно превышать 5 м.

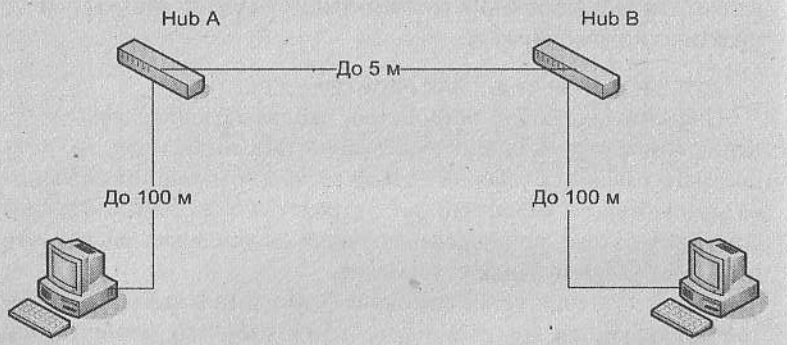


Рис. 2.14. Правила каскадирования сетевых концентраторов

Концентраторы позволяют использовать для объединения компьютеров в сеть стандартный кабель на основе витой пары. Для таких соединений предусмотрен стандарт 10 Base-T, обеспечивающий полную совместимость с сетевым оборудованием разных фирм и позволяющий организовать сеть на базе недорогих и простых в установке кабелей и разъемов. Для подключения устройств к сети используются модульные разъемы типа RJ-45.

КОММУТАТОР (SWITCH)

Является технически более сложным устройством, чем концентратор. Основным недостатком концентратора является тот факт, что при получении сигнала от какого-либо компьютера он усиливает его и передает на все остальные порты, тем самым создавая лишний трафик (поток информации), поскольку чаще всего передаваемый сигнал предназначен только для одного компьютера.

Коммутаторы позволяют направить поступивший в них сигнал только в тот порт, к которому подключен требуемый компьютер. Другими словами, коммутатор выполняет целенаправленную пересылку пакетов между двумя портами на основе физического (MAC) адреса получателя (рис. 2.15). Это возможно благодаря тому, что коммутатор обладает встроенным процессором и памятью и хранит таблицу соответствий MAC-адресов компьютеров и портов, к которым они подключены. Данное свойство коммутаторов позволяет существенно уменьшить сетевой трафик и тем самым повысить производительность сети.

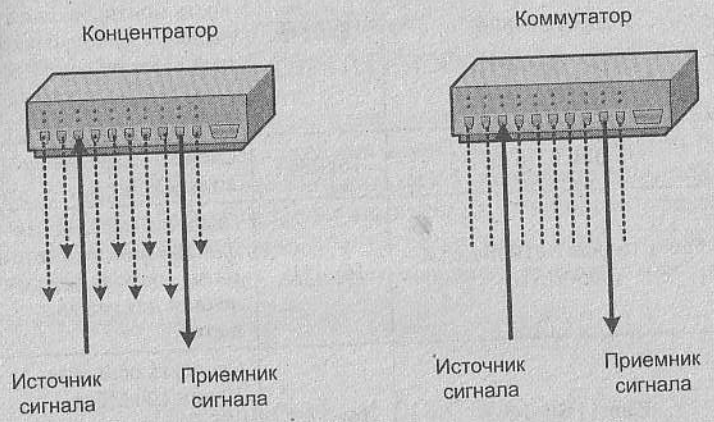


Рис. 2.15. Отличие концентратора от коммутатора

Вид коммутатора показан на рис. 2.16, а основные характеристики некоторых коммутаторов приведены в табл.2.7.

При построении одноранговых сетей обычно не используются подсети адресов, и поэтому маршрутизатор не нужен. Как уже говорилось выше, если компьютеры находятся в одном логическом сегменте, маршрутизация происходит на втором уровне модели OSI/ISO и осуществляется на базе коммутаторов второго уровня.

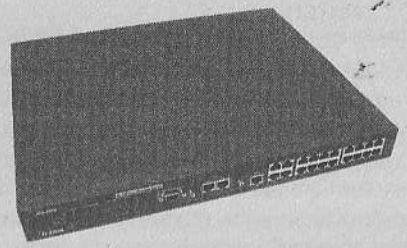


Рис. 2.16. Внешний вид сетевого коммутатора D-link

Таблица 2.7
Характеристики некоторых коммутаторов

Наименование	Порты	Комментарий
Planet FSD-803	8xRJ45	Скорость передачи до 100 Мбит/с. Возможность монтирования в стойку. Полнодуплексный режим. Память до 2000 MAC-адресов на порт
3COM 3C16751	16xRJ45	Скорость передачи до 100 Мбит/с
Focus 16-port 10/100BaseTX (065-9131i)	16xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта
Planet FSD-1603	16xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта
D-link DES 3624i	24xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта. Возможность ручной настройки каждого порта

И все же, какое оборудование из всего его многообразия на компьютерном рынке выбрать? Какими правилами руководствоваться? Решение в данном случае необходимо принимать, сравнивая реальные потребности в производительности и размере сети и материальные возможности. Для домашней локальной сети не принципиален вопрос мощной пропускной способности активного оборудования и его стопроцентная отказоустойчивость. При построении обычной домашней сети размером 3–10 компьютеров вполне подойдет 100-мегабитное активное сетевое оборудование таких фирм, как D-link и Planet, в ценовом диапазоне до 700 рублей и встроенные сетевые карты. Если же сетевого адаптера в компьютере нет, то вполне подойдут сетевые решения на базе чипа Realtek RTL8139D в ценовом диапазоне до 300 рублей.

Глава 3
Введение в беспроводные сети

В данной главе читатель ознакомится с технологиями построения беспроводных сетей, их функциями, принципами работы и назначением. Рассматриваются технологии, используемые для построения беспроводных сетей различного уровня, протоколы передачи данных в беспроводных сетях. Уделено внимание вопросам безопасности передачи данных в беспроводных сетях.

Технологии и протоколы беспроводных сетей

За последние годы рынок мобильных устройств, таких как PDA (Personal Digital Assistant, личный цифровой секретарь) и мобильные компьютеры, претерпел огромные изменения. Наблюдается четкая тенденция к развитию, а следовательно, и к повсеместному внедрению и удешевлению большинства устройств, бывших ранее в определенной степени элитными аксессуарами.

Портативные ноутбуки и PDA в настоящее время стали как повседневным рабочим инструментом, так и средством развлечения. С увеличением числа мобильных пользователей возникает острая необходимость в оперативном осуществлении коммуникаций между ними, в обмене данными, в быстром получении информации. Неудивительно, что происходит интенсивное развитие рынка технологий беспроводных коммуникаций. Особенно это актуально в отношении беспроводных сетей, или так называемых WLAN-сетей (Wireless Local Area Network).

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорости современных сетей довольно высоки (порядка 108 Мбит/с), что позволяет их использовать для очень широкого спектра задач;
- с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Специфика подобных сетей заключается в том, что при выборе оборудования факторы надежности, безопасности и масштабируемости отходят на второй план. Основными становятся вопросы стоимости оборудования и простоты настройки и обслуживания. Беспроводные сети все чаще и чаще используются для организации мелких офисных сетей с последующим подключением к глобальной сети Интернет с помощью технологии ADSL или тех же беспроводных технологий RadioEthernet или WiMAX.

В зависимости от способа подключения к Интернету центральным устройством такой беспроводной сети может стать ADSL-модем со встроенной точкой доступа или беспроводной маршрутизатор. В первом случае подразумевается, что подключение организовано по технологии ADSL. Второй вариант подойдет практически для любого другого способа подключения, лишь бы Интернет был доступен на выходе устройства с портом Ethernet (см. рис. 3.1, 3.2).

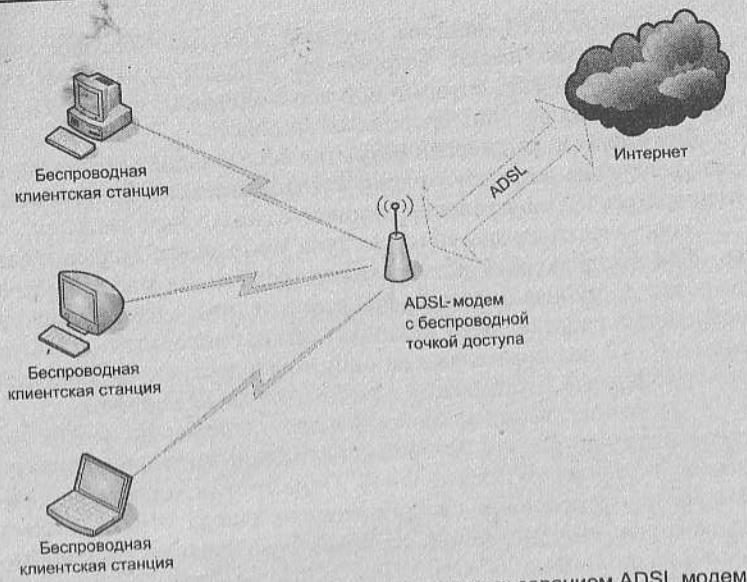


Рис. 3.1. Схема доступа к сети Интернет с использованием ADSL модема с беспроводной точной доступа

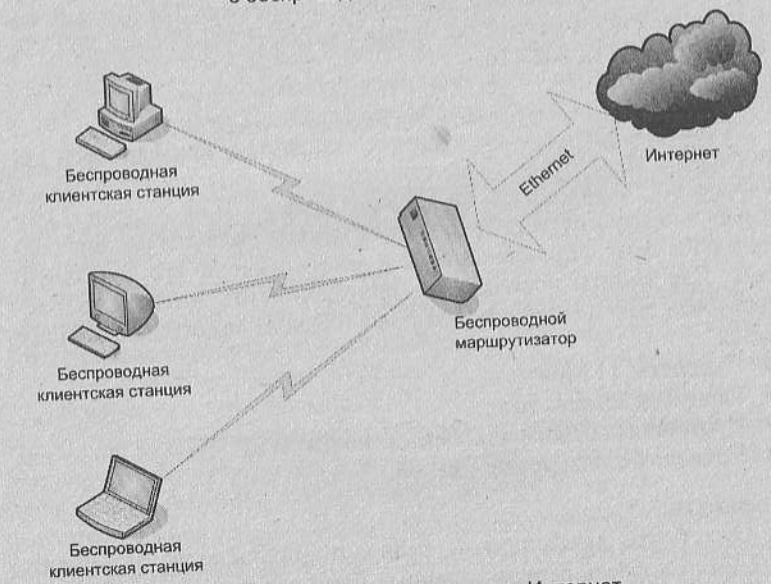


Рис. 3.2. Схема доступа к сети Интернет с использованием беспроводного маршрутизатора

Обычно и ADSL-модемы с точкой доступа, и беспроводные маршрутизаторы имеют встроенный Ethernet-коммутатор (как правило, на 4 порта), который при необходимости можно использовать для подключения проводных устройств.

Для увеличения площади покрытия беспроводной сети, а также для увеличения возможного количества пользователей сеть может расширяться путем установки дополнительных точек доступа.

Теоретически каждая точка доступа Wi-Fi может поддерживать до 2048 беспроводных клиентских устройств. На практике из-за того, что доступная полоса пропускания делится между всеми одновременно работающими пользователями, приходится ограничиваться 10–20 пользователями на одну точку доступа – в зависимости от конкретных требований к скорости обмена данными.

В настоящее время широкое распространение получили три технологии построения беспроводных сетей, а именно: технология RadioEthernet, WiMax и Wi-Fi. Однако если первые две ориентированы в основном на организацию канала подключения к провайдерам интернет-услуг, то Wi-Fi была изначально ориентирована на организацию SOHO (Small Office – Home Office) сетей.

Именно данной технологии и уделяется внимание в этой книге при рассмотрении беспроводных технологий. На данный момент существует четыре основных стандарта Wi-Fi – это 802.11b, 802.11g, 802.11i, 802.11n.

802.11B

Один из первых беспроводных стандартов, применяемый повсеместно до сих пор. Скорость передачи довольно невысокая, а безопасность находится на низком уровне. При желании злоумышленнику может потребоваться меньше часа для расшифровки ключа сети и проникновения в интересующую его локальную сеть. Для защиты используется протокол WEP, который охарактеризовал себя не с лучшей стороны и был взломан несколько лет назад.

- Скорость: 11 Мбит/с.
- Радиус действия: 50 м.
- Протоколы обеспечения безопасности: WEP.
- Уровень безопасности: низкий.

802.11G

Это более продвинутый стандарт, пришедший на смену 802.11b. Скорость передачи данных была увеличена почти в пять раз, и теперь она составляет 54 Мбит/с. При использовании оборудования, поддерживающего технологии superG или True MIMO, предел максимально достижимой скорости составляет 125 Мбит/с. Возрос и уровень защиты: при соблюдении всех необходимых условий при правильной настройке его можно оценить как высокий. Данный стандарт совместим с новыми протоколами шифрования WPA и WPA2.

- 54–125 Мбит/с.
- Радиус действия: 50 м.
- Протоколы обеспечения безопасности: WEP, WPA, WPA2.
- Уровень безопасности: высокий.

802.11I

Это новый стандарт, внедрение которого только начинается. В данном случае непосредственно в сам стандарт встроена поддержка самых современных технологий, таких как True MIMO и WPA2. Поэтому необходимость более тщательного выбора оборудования отпадает. Планируется, что это стандарт придет на смену 802.11g и сведет на нет все попытки взлома.

- Скорость: 125 Мбит/с.
- Радиус действия: 50 м.
- Протоколы обеспечения безопасности: WEP, WPA, WPA2.
- Уровень безопасности: высокий.

802.11N

Будущий стандарт, разработки которого ведутся в данный момент. Этот стандарт должен обеспечить большие расстояния охвата беспроводных сетей и более высокую скорость, вплоть до 540 Мбит/сек.

- Скорость: 540 Мбит/с.
- Радиус действия: неизвестно.
- Протоколы обеспечения безопасности: WEP, WPA, WPA2.
- Уровень безопасности: высокий.

Оборудование для построения беспроводных сетей

Рассмотрим оборудование, применяемое для построения беспроводных локальных сетей. Выбор оборудования напрямую зависит от сложности планируемой сети, количества хостов, метода

доступа к сети Интернет, требованиям к безопасности. В данном случае нас интересует оборудование, необходимое для следующих моделей беспроводных локальных сетей:

- сеть «точка – точка» – используется для объединения двух компьютеров друг с другом;
- сеть «точка доступа – клиенты» – используется для подключения нескольких клиентских компьютеров с использованием точки доступа.

Прежде всего, необходимо подобрать беспроводной сетевой адаптер. В настоящее время рынок активного сетевого оборудования предлагает достаточно широкий выбор беспроводных адаптеров. Все зависит от типа подключения адаптера (USB, PCMCI, PCI, PCI-e), от поддерживаемых стандартов, требуемых скоростей и расстояния между двумя компьютерами. Характеристики наиболее распространенных на рынке беспроводных сетевых адаптеров приведены в табл. 3.1.

Таблица 3.1

Характеристики беспроводных адаптеров

Наименование	Возможности
PCI-адаптер Edimax EW-7128g	Интерфейс: PCI 2.2 Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с IEEE 802.11g: до 54 Мбит/с
PCMCI Edimax EW-7108PCg	Интерфейс: PCMCI Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с IEEE 802.11g: до 54 Мбит/с
PCI-адаптер ZyXEL G-320H	Интерфейс: PCI 2.2 Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с IEEE 802.11g: до 54 Мбит/с
USB-адаптер ZyXEL G-202	Интерфейс: USB 2.0 Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с IEEE 802.11g: до 54 Мбит/с

Наименование	Возможности
PCI-адаптер ASUS WL-138gE	Интерфейс: PCI 2.2 Поддерживаемые скорости: до 54 Мбит/с
Адаптер DWL-G520	Интерфейс: PCI 2.2 Поддерживаемые скорости: 802.11b: 11Мбит/с IEEE 802.11g: до 54 Мбит/с

Приведем примеры конструктивного исполнения беспроводных адаптеров (рис. 3.3–3.5).

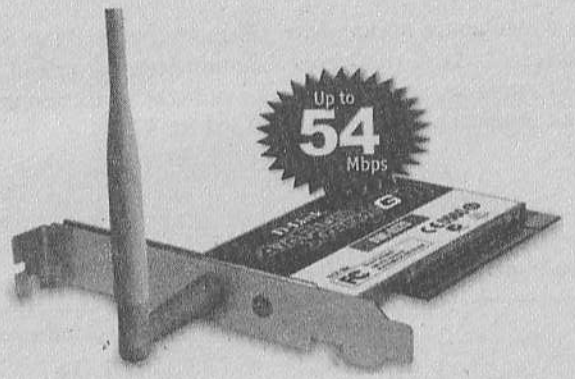


Рис. 3.3. Внешний вид PCI-адаптера DWL-G520

Рис. 3.4. Внешний вид адаптера ZyXEL G-202

Рис. 3.5. Внешний вид адаптера Edimax EW-7108PCg

Для соединения нескольких компьютеров в одну беспроводную локальную сеть требуется наличие хотя бы одной точки доступа. Краткие характеристики имеющихся в настоящий момент на рынке точек доступа приведены в табл. 3.2.

Таблица 3.2

Характеристики беспроводных точек доступа

Наименование	Возможности
ZyXEL G-3000 EE	Интерфейс: 10/100 Base-TX Ethernet Стандарт: Wi-Fi: IEEE 802.11g Поддерживаемые скорости: IEEE 802.11g: до 54 Мбит/с Зона покрытия: до 300 м вне помещения
D-Link DWL-2000AP	Интерфейс: 10/100 Base-TX Ethernet Стандарты: IEEE 802.11b/g WLAN, IEEE 802.3/u Ethernet. Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с IEEE 802.11g: до 108 Мбит/с в режиме турбо Зона покрытия: до 350 м вне помещения
ASUS WL-320g Encore	Интерфейс: 10/100 Base-TX Ethernet Стандарты: IEEE 802.11g, IEEE 802.11b. Поддерживаемые скорости: IEEE 802.11b: до 11 Мбит/с

Наименование	Возможности
	IEEE 802.11g: до 54 Мбит/с Зона покрытия: до 150 м вне помещения

Внешний вид беспроводных точек доступа различается как цветовой гаммой, так и инженерным исполнением корпуса, но в общем они имеют вид прямоугольной коробки с антенной (одной или более, в зависимости от поддерживаемых диапазонов) (рис. 3.6).

Рис. 3.6. Внешний вид беспроводной точки доступа

Вопросы безопасности в беспроводных сетях

В вопросах безопасности беспроводные сети имеют очень много общих граней с проводными сетями, однако имеются и существенные различия. Для того чтобы проникнуть в проводную сеть, злоумышленнику необходимо получить физический доступ к активному сетевому оборудованию для перехвата потока трафика. В случае с беспроводной сетью достаточно установить антенну в любом месте в зоне действия сети.

В настоящее время для защиты Wi-Fi-сетей применяются сложные алгоритмические модели аутентификации, шифрования

данных, контроля целостности их передачи. Но не всегда было так, на ранних стадиях развития технологий беспроводных сетей появлялись сообщения о том, что, даже не используя сложного оборудования и специальных программ, можно было подключиться к некоторым корпоративным сетям, просто проезжая мимо с ноутбуком.

Вот стандартный список того, что может осуществить злоумышленник в случае нелегитимного доступа к беспроводной сети:

- доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через нее — и к ресурсам LAN;
- прослушивание трафика и получение конфиденциальной информации;
- искажение проходящей информации;
- воровство интернет-трафика;
- атаку на ПК пользователей и серверы сети (например, Denial of Service или даже глушение радиосвязи);
- внедрение поддельной точки доступа.

В беспроводных сетях применяются следующие технологии защиты.

WEP

Данная технология была разработана специально для шифрования потока передаваемых данных в рамках локальной сети. Данные шифруются ключом с разрядностью от 40 до 104 бит. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Но оказалось, что взломать такую защиту можно — соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack). Основное ее слабое место — именно вектор инициализации.

IEEE 802.1X

Это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. 802.1X базируется на протоколе расширенной аутентификации Extensible Authentication Protocol (EAP), протоколе защиты транспортного уровня Transport Layer Security (TLS) и сервере доступа RADIUS (Remote Access Dial-in User Server). Плюс к этому стоит добавить новую организацию работы клиентов сети. После того как пользователь прошел

этап аутентификации, ему высылается секретный ключ в зашифрованном виде на определенное незначительное время — время действующего на данный момент сеанса. По завершении этого сеанса генерируется новый ключ и опять высылается пользователю. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

WPA

Это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

- WPA — технология защищенного доступа к беспроводным сетям (Wi-Fi Protected Access);
- EAP — протокол расширенной аутентификации (Extensible Authentication Protocol);
- TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol);
- MIC — технология проверки целостности сообщений (Message Integrity Check).

VPN

Технология виртуальных частных сетей Virtual Private Network (VPN) была предложена компанией Intel для обеспечения безопасного соединения клиентских систем с серверами по общедоступным интернет-каналам. VPN очень хорошо себя зарекомендовали с точки зрения шифрования и надежности аутентификации. Плюс технологии состоит и в том, что на протяжении более трех лет практического использования в индустрии данный протокол не получил никаких нареканий со стороны пользователей. Информации о его взломах не было.

Технологий шифрования в VPN применяется несколько, наиболее популярные из них описаны протоколами PPTP, L2TP и IPSec с алгоритмами шифрования DES, Triple DES, AES и MD5. IP Security (IPSec) используется примерно в 65—70% случаев. С его помощью обеспечивается практически максимальная безопасность линии связи.

И хотя технология VPN не предназначалась изначально именно для Wi-Fi, она может использоваться для любого типа сетей, и идея защитить с ее помощью их беспроводные варианты одна из лучших на сегодня.

Для VPN выпущено уже достаточно большое количество программного и аппаратного обеспечения. Поддержка VPN присутствует в системах Windows NT/2000/XP, Sun Solaris, Linux. Для реализации VPN-защиты в рамках сети необходимо установить специальный VPN-шлюз (программный или аппаратный), в котором создаются туннели, по одному на каждого пользователя. Например, для беспроводных сетей шлюз следует установить непосредственно перед точкой доступа. А пользователям сети необходимо установить специальные клиентские программы, которые в свою очередь также работают за рамками беспроводной сети и расшифровка выносится за ее пределы.

Глава 4
Домашняя сеть: шаг за шагом

В данной главе внимание уделяется пошаговому практическому алгоритму построения локальной сети в домашних условиях. Рассматривается построение сети из двух компьютеров без использования коммутатора, создание локальной сети из трех компьютеров с использованием коммутатора, использование общих папок и принтеров.

Общие рекомендации

При переходе от теории к практике построения сетей необходимо выработать определенный алгоритм последовательности действий при проектировании, построении и диагностике локальной сети. Ниже приведен список вопросов, на который необходимо ответить, чтобы грамотно спроектировать локальную сеть и найти компромиссное решение между качеством работы данной сети и затратами на монтаж и поддержку сети.

Перед тем как спланировать сеть, следует ответить на вопросы:

1. Какое количество компьютеров планируется в сети? От ответа на данный вопрос зависит топология сети.
2. Какой будет топология сети? Ответ повлияет на выбор активного сетевого оборудования.
3. Каково территориальное расположение всех объектов межсетевого взаимодействия? Ответ позволит определиться с количеством активного сетевого оборудования и с применяемыми сетевыми технологиями объединения сегментов сетей.

4. Каковы требования к надежности и пропускной способности локальной сети? Ответ позволит правильно выбрать модель и производителя сетевого оборудования, а также программно-аппаратные средства защиты, применяемые при построении данной сети.
5. Будет ли доступ к глобальной сети Интернет и как он будет организован? От ответа зависит выбор технологии подключения, управления трафиком и выбор каналообразующего оборудования.

Конечно, список вопросов не претендует на исчерпывающую полноту, однако, ответив даже на них, удастся избежать многих недочетов при построении и дальнейшем обслуживании локальной сети.

Одноранговая сеть из двух компьютеров

Итак, ответим на список вопросов при построении локальной сети из двух компьютеров, находящихся в одной квартире:

1. Количество компьютеров в сети – два.
2. Топология сети – «точка – точка».
3. Территориальное расположение всех объектов межсетевого взаимодействия – в пределах 20 м.
4. Требования к надежности и пропускной способности локальной сети – минимальные.
5. Доступ к Интернету в ближайшее время не планируется.

Поясним ряд деталей. Объединить два компьютера в локальную сеть можно и с помощью коммутатора (или концентратора), но это не рационально, если не планируется расширение сети. Дело в том, что два компьютера в сеть можно объединить одним кабелем, подключив его к портам сетевой карты на одном и на другом компьютере.

Приступим к созданию локальной сети из двух компьютеров без доступа к сети Интернет и без возможных вариантов подключения других компьютеров к этой локальной сети.

ОБЖИМ КАБЕЛЯ

Витая пара (UTP/STP, unshielded/shielded twisted pair) в настоящее время является наиболее распространенной средой передачи сигналов в локальных сетях. Кабели этого типа различаются

по категориям (в зависимости от полосы пропускания) и типа проводников. В кабеле 5-й категории находится восемь проводников, перевитых попарно (т.е. четыре пары).

Структурированная кабельная система, построенная на основе витой пары 5-й категории, имеет очень большую гибкость в использовании. Грамотное построение сети на ее основе должно базироваться на следующих принципах.

Для витой пары применяют коннектор RJ-45 (рис. 4.1) – восьмиконтактный разъем, использующийся обычно для подключения кабеля к сетевым платам Ethernet.

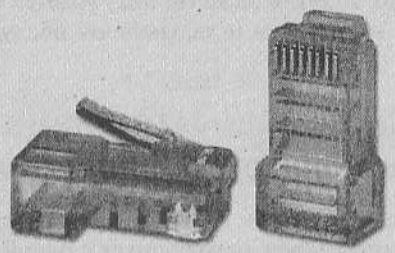


Рис. 4.1. Внешний вид коннектора RJ-45

Для монтажа коннекторов RJ-45 используются специальные обжимные приспособления, оснащенные лезвиями для снятия защитной оболочки и восемью ножами для фиксации.

Для обжима кабеля необходимо выполнить следующие действия:

1. Аккуратно обрезать конец кабеля. Проследить, чтобы торец кабеля был ровным.
2. Используя обжимной инструмент (рис. 4.2), аккуратно снять с кабеля внешнюю изоляцию на длину примерно 20 мм и обрезать нить, вмонтированную в кабель. Она предназначена для удобства снятия изоляции с кабеля на большую длину. Обратить внимание, что любые повреждения изоляции проводников недопустимы – именно поэтому желательно использовать специальный инструмент, лезвие резака которого выступает на толщину внешней изоляции.
3. Надеть на кабель защитный колпачок, который предназначен для защиты коннектора от повреждения и попадания пыли.
4. Аккуратно расплести и выровнять проводники в один ряд, при этом их следует расположить в порядке, указанном в табл. 4.1.

Проводники должны располагаться строго в один ряд, без нахлестов друг на друга.

Примечание. При соединении кабелем двух компьютеров используется так называемый «перекрестный» кабель (Crossover), в котором раскладка T568B используется для первого коннектора, а T568A – для второго.

Таблица 4.1

Стандартные разводки кабеля «витая пара»

Номер проводника	Разводка T568B	Разводка T568A
Первый	Бело-оранжевый	Бело-зеленый
Второй	Оранжевый	Зеленый
Третий	Бело-зеленый	Бело-оранжевый
Четвертый	Синий	Синий
Пятый	Бело-синий	Бело-синий
Шестой	Зеленый	Оранжевый
Седьмой	Бело-коричневый	Бело-коричневый
Восьмой	Коричневый	Коричневый

5. Обрезать проводники так, чтобы они выступали над внешней обмоткой на 8–10 мм.
6. Удерживая разъем защелкой от себя (защелка не должна быть видна), вставить кабель в коннектор. Каждый проводник должен попасть на свое место в разъеме и упереться во фронтальную стенку коннектора. Прежде чем обжимать коннектор, следует убедиться, что в расположении проводников нет ошибок (провода часто путаются, когда их вставляют в коннектор).
7. Вставить коннектор в гнездо на обжимных клещах и сжать его до упора-ограничителя на клещах – фиксатор на коннекторе встанет на свое место, удерживая кабель в разъеме неподвижным. Контактные ножи разъема врежутся каждый в свой проводник, обеспечивая надежный контакт.
8. Надеть колпачок на коннектор – кабель готов.

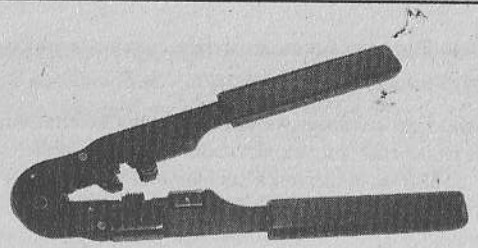


Рис. 4.2. Обжимной инструмент

После изготовления данного кабеля необходимо с помощью него соединить сетевые платы двух компьютеров, при этом получается полнофункциональное соединение на скорости, зависящей только от сетевых карт. Если это качественные карты от известных производителей, которые поддерживают полнодуплексный режим, то можно получить соединение на скорости, близкой к 200 Мбит/с.

ИНСТАЛЛЯЦИЯ СЕТЕВОГО АДАПТЕРА

В большинстве современных компьютеров сетевая карта уже является неотъемлемым элементом материнской платы. Разъем сетевой карты RJ45 выглядит следующим образом:

- на стационарном компьютере — рис. 4.3;
- на ноутбуке — рис. 4.4.

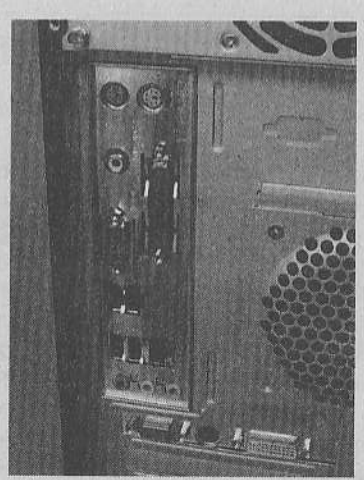


Рис. 4.3. Разъем RJ45 на стационарном компьютере

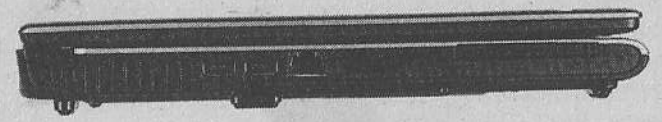


Рис. 4.4. Разъем RJ45 на на ноутбуке

Если же такого адаптера в компьютере нет, что, правда, для современного ПК маловероятно, существует ряд устройств как для стационарных компьютеров, так и для ноутбуков. Для стационарных – это обычные PCI-платы (рис. 4.5)

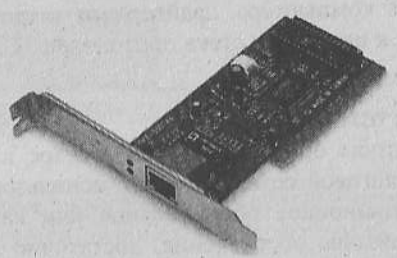


Рис. 4.5. Сетевая карта для настольного компьютера

Для ноутбуков, в которых по той или иной причине нет сетевой карты или же она не исправна, есть устройства формата PCMCIA (рис. 4.6).

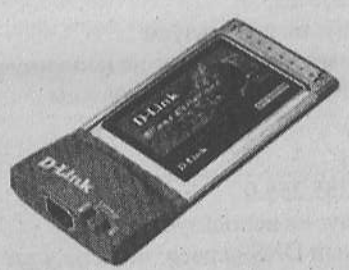


Рис. 4.6. Сетевая карта стандарта PCMCIA

Если же и PCMCIA-слот по каким-либо причинам не доступен, есть возможность использовать USB сетевые адаптеры, такие адаптеры являются универсальными как для настольных, так и для мобильных компьютеров (рис. 4.7).

Рис. 4.7. Сетевая карта стандарта USB

Итак, провод готов, сетевая карта инсталлирована в соответствующий порт компьютера, драйверы на устройство установлены, переходим к настройке стека протоколов TCP/IP для установки соединения.

НАСТРОЙКА TCP/IP

Для того чтобы организовать межсетевое взаимодействие в простой одноранговой сети, не нужно использовать дорогостоящее маршрутизационное оборудование или какое-то дополнительное программное обеспечение, достаточно лишь правильно настроить сетевой стек.

Для соединения двух компьютеров в единую сеть будем использовать следующие адреса:

- **Компьютер А**
  - IP 192.168.1.10
  - Netmask: 255.255.255.0
  - Default Gateway: не используем
  - Предпочитаемый DNS-сервер: не используем
  - Вторичный DNS-сервер: не используем
- **Компьютер Б**
  - IP 192.168.1.11
  - Netmask: 255.255.255.0
  - Default Gateway: не используем.
  - Предпочитаемый DNS-сервер: не используем
  - Вторичный DNS-сервер: не используем

Почему выбраны именно эти настройки? Как уже говорилось в главе 2, для построения частных локальных сетей необходимо использовать так называемые «серые» не маршрутизируемые сетевые адреса, поэтому класс сети был выбран самый малый из стандартных – класс С, маска 255.255.255.0. Важно помнить: для

того чтобы между компьютерами установилось подключение без использования дорогостоящего оборудования, надо, чтобы они находились в одной подсети (192.168.1.0). Для подключения двух и более компьютеров к одноранговой сети без выхода в глобальную сеть Интернет указывать основной шлюз и DNS-сервера не нужно. DNS-серверы служат для преобразования символьных имен в IP-адреса, и наоборот. Виды адресации в Интернете были рассмотрены ранее.

Рассмотрим пошагово, как настроить стек протоколов TCP/IP в Windows Vista.

1. Нажать кнопку *Пуск* и выбрать пункт меню *Сеть* (рис. 4.8).

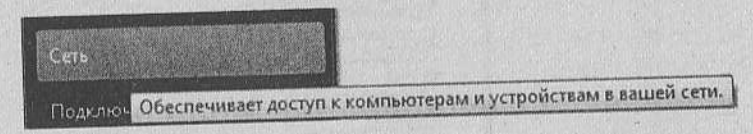


Рис. 4.8. Сеть

2. В открывшемся окне выбрать в верхней панели задач пункт *Центр управления сетями и общим доступом* (рис. 4.9).

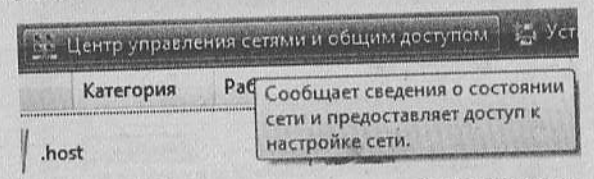


Рис. 4.9. Центр управления сетями и общим доступом

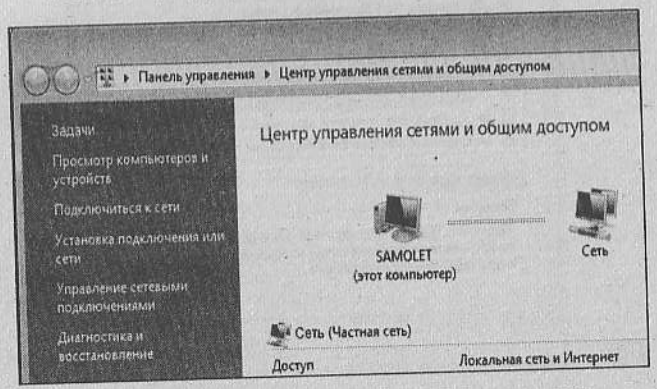


Рис. 4.10. Управление сетевыми подключениями

3. В левой панели щелкнуть на пункте *Управление сетевыми подключениями* (рис. 4.10).
4. Щелчком правой кнопки мыши вызвать контекстное меню соединения *Подключение по локальной сети* и выбрать *Свойства* (рис. 4.11).

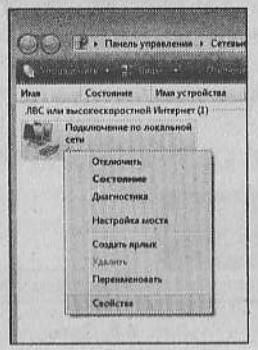


Рис. 4.11. Сетевые подключения

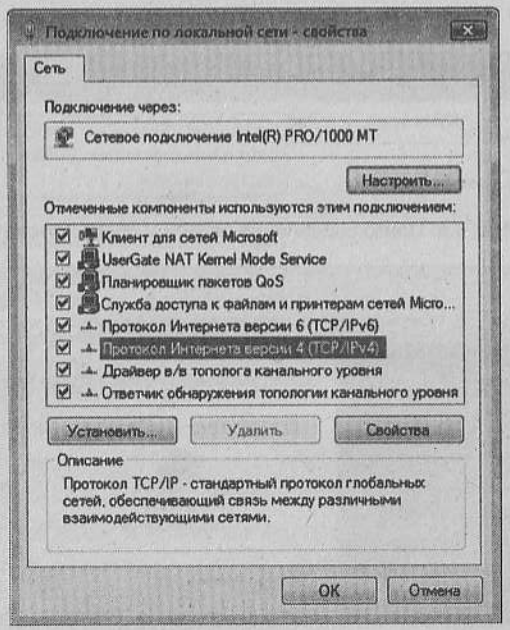


Рис. 4.12. Свойства подключения по локальной сети

5. На вкладке *Сеть* выбрать в списке пункт *Протокол Интернета версии 4* и нажать кнопку *Свойства* (рис. 4.12).
6. В появившемся окне ввести IP-адрес и маску сети (рис. 4.13).
7. Нажать кнопку *OK* и закрыть окно свойств подключения по локальной сети.

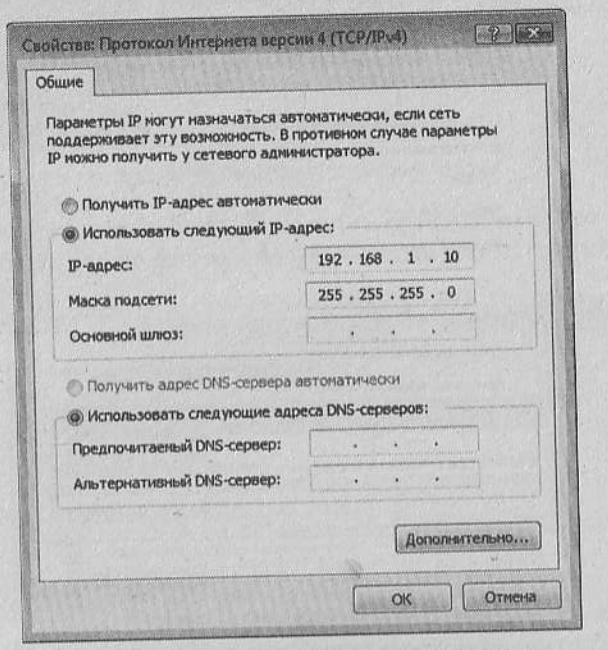


Рис. 4.13. Настройка TCP/IP на компьютере A

Те же самые манипуляции необходимо проделать и на втором компьютере, с одним лишь отличием: IP-адрес будет не 192.168.1.10, а 192.168.1.11 (рис. 4.14).

После назначения IP-адресов, для того чтобы не было никаких проблем с подключением между двумя компьютерами, следует отключить Windows Firewall.

Windows Firewall – это программа, контролирующая сетевые соединения и на основе прописанных в ней правил обработки пакетов принимает решение: блокировать пакет или пропустить его в систему. Более подробно о работе с Windows Firewall и о его настройках будет рассказано в части II, посвященной программам для работы в Интернете. В данном случае лучше его

отключить, так как сеть состоит всего из двух компьютеров и никто посторонний не может вмешаться в процесс межсетевого взаимодействия.

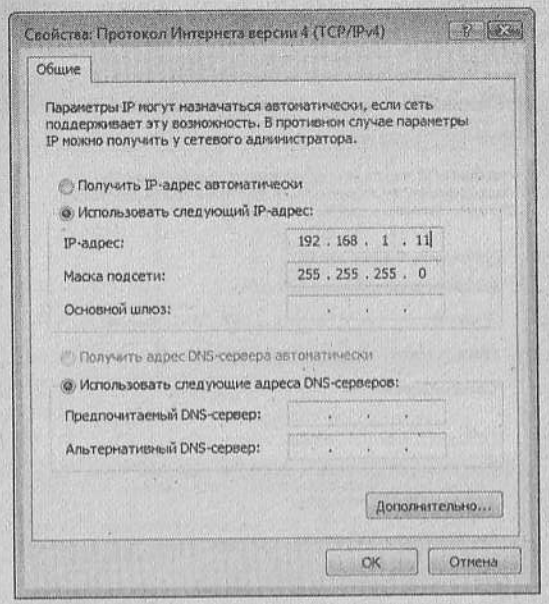


Рис. 4.14. Настройка TCP/IP на компьютере Б

Для отключения Windows Firewall нужно:

1. Открыть панель управления (рис. 4.15) и активизировать оснастку *Брандмауэр Windows*.

Рис. 4.15. Брандмауэр Windows в панели управления

2. Нажать в левой панели пункт *Включение и отключение брандмауэра* (рис. 4.16).

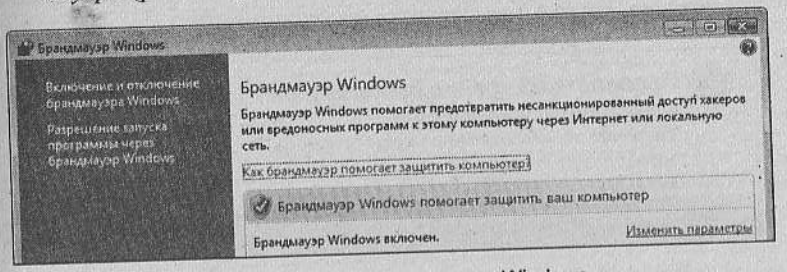


Рис. 4.16. Окно брандмауэра Windows

3. В открывшемся окне управления брандмауэром (рис. 4.17) выбрать опцию *Выключить (не рекомендуется)* и нажать *OK*.

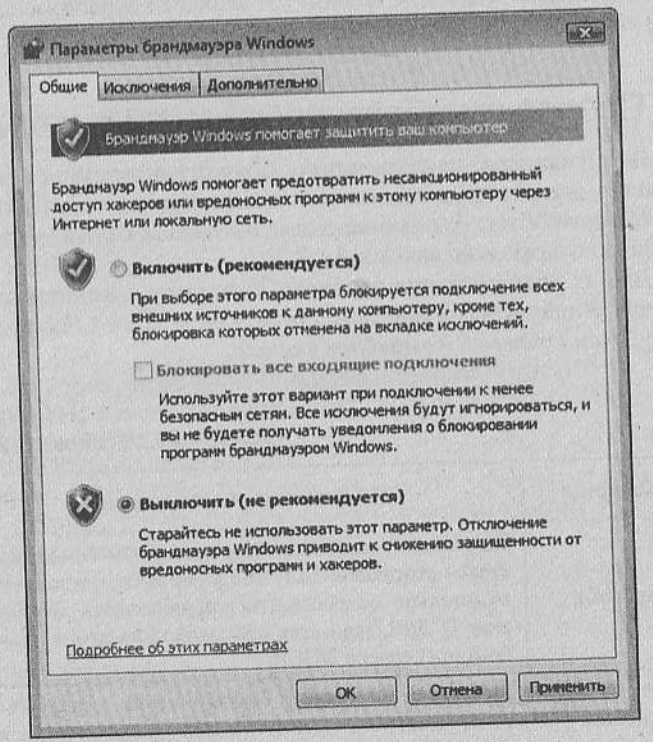


Рис. 4.17. Отключение брандмауэра Windows

4. Появится предупреждение о том, что брандмауэр выключен и предложение его включить (рис. 4.18). Это можно сделать позднее, когда в том появится необходимость.

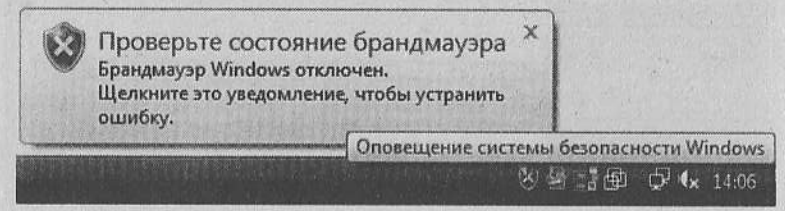


Рис. 4.18. Сообщение об отключении брандмауэра Windows

Теоретически данные между компьютерами уже могут передаваться. Однако требуется провести проверку всех настроек сетевого подключения для полной уверенности в работоспособности системы.

Проверка работоспособности системы

В большинстве случаев понять причину отсутствия связи позволяют специальные сетевые утилиты, которые входят в поставку Windows Vista. Для выполнения этой задачи служат несколько утилит, которые описаны в табл. 4.2.

Для их использования необходимо открыть окно консоли Microsoft Windows Vista при помощи команды *Пуск | Все программы | Стандартные | Командная строка*.

Таблица 4.2

Основные сетевые утилиты

Команда	Описание и назначение
ipconfig	Позволяет узнать параметры текущей конфигурации стека протоколов TCP/IP. Кроме того, позволяет принудительно освобождать или обновлять конфигурацию TCP/IP, если стек протоколов настраивается при помощи сервера DHCP
nbtstat	Выполняет проверку подключений через TCP/IP, отображает статистику подключений и настройки протокола TCP/IP, касающиеся протокола NetBIOS

Команда	Описание и назначение
netstat	Отображает статистику протокола TCP/IP и информацию о текущих соединениях
nslookup	Позволяет тестировать работу DNS-сервера, получать информацию о ресурсных записях, запрашивая DNS-серверы
ping	Проверяет правильность настройки стека протоколов TCP/IP и тестирует наличие физической связи с другими узлами
tracert	Применяется для трассировки маршрута IP-пакета от источника до получателя

Более подробную информацию об этих утилитах можно найти в справочной системе Windows. Далее будет рассмотрена работа двух утилит, которые используются наиболее часто (ipconfig и ping).

ПРОВЕРКА НАЛИЧИЯ СВЯЗИ

После настройки всех компьютеров, входящих в локальную сеть, нужно проверить наличие связи между ними и правильность настройки сетевых протоколов. При конфигурировании сети возможен ряд ошибок, которые приводят к тому, что компьютеры не могут взаимодействовать. К таким ошибкам относятся:

- некорректная установка драйверов сетевой карты;
- неправильная работа сетевых протоколов или их некорректная настройка;
- назначение ошибочного IP-адреса или маски подсети;
- физическое повреждение кабеля.

ПРОВЕРКА СЕТЕВОЙ КАРТЫ

Первое, что необходимо сделать, – это проверить правильность установки и настройки драйверов сетевой карты, для чего следует выполнить такие действия:

1. Открыть панель управления и выбрать пункт *Оборудование и звук*.
2. Нажать кнопку *Диспетчер устройств*, при этом будет открыто одноименное окно.
3. В окне *Диспетчер устройств* открыть пункт *Сетевые платы* и убедиться, что около платы не стоит значок с желтым восклицательным знаком .

4. Если значок присутствует, переустановить драйвер. Наиболее правильным решением является загрузка свежего драйвера с сайта производителя (это можно сделать в интернет-кафе или на любом доступном компьютере, подключенном к сети Интернет).

Если переустановка драйвера не помогла избавиться от ошибки, нужно заменить сетевую карту.

ПРОВЕРКА НАСТРОЙКИ TCP/IP

Для проверки настройки протокола TCP/IP необходимо выполнить следующие действия:

1. Открыть окно консоли Windows при помощи команды *Пуск* | *Все программы* | *Стандартные* | *Командная строка*.
2. Ввести команду ipconfig /all и нажать **Enter**. При выполнении команды будут показаны параметры текущей конфигурации TCP/IP (рис. 4.19).
3. Убедиться в правильности конфигурирования протокола TCP/IP путем сверки планируемых настроек с реальными.
4. Если настройки не совпадают, изменить их и выполнить процедуру проверки еще раз.

ПРОВЕРКА НАЛИЧИЯ ФИЗИЧЕСКОЙ СВЯЗИ

После проверки сетевых настроек компьютера, подключенного к сети, требуется проверить, корректно ли работают коммутаторы и кабели, т.е. существует ли физическая связь между компьютерами.

```
C:\Users\phant0m>ipconfig

Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::1c6c:7e17:aa65:4e17%8
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.11
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . :

Туннельный адаптер Подключение по локальной сети*:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::5efe:192.168.1.11%10
   Основной шлюз. . . . . . . . . . :

Туннельный адаптер Подключение по локальной сети* 2:

   Состояние носителя. . . . . . . . : Носитель отключен
   DNS-суффикс подключения . . . . . :

C:\Users\phant0m>_
```

Рис. 4.19. Использование утилиты Ipconfig

Для выполнения этой проверки следует использовать утилиту ping, которая проверяет правильность настройки TCP/IP и тестирует соединения с другими узлами. Ее принцип работы заключается в отправке небольших пакетов данных по указанному адресу. Существующие стандарты предполагают, что, получив такой пакет, любое сетевое устройство должно отправить ответ на адрес источника. Если в течение определенного времени ответ не пришел, считается, что между двумя устройствами линия связи отсутствует.

Для использования утилиты ping нужно выполнить следующие инструкции:

1. Включить компьютеры, с которыми нужно проверить связь.
2. Открыть окно консоли Windows.
3. Ввести команду ping 127.0.0.1, которая позволит протестировать корректность работы самой утилиты. Программа ping вернет результаты, похожие на те, что показаны на рис. 4.20.
4. Изменить адрес в команде на адрес компьютера, например ping 192.168.1.10, если запускать с компьютера А. Эта процедура еще раз проверит, насколько корректно работает сетевая карта.
5. Выполнить проверку целевого компьютера, например ping 192.168.1.10 с компьютера Б. Если ответ будет получен, то все в порядке, если же в качестве ответа будет возвращена строка «Превышен интервал ожидания для запроса», то это говорит о неисправности кабеля либо несоответствии настроек TCP/IP.

При использовании утилиты ping можно применять ключ -t (отделяется пробелом от команды ping), который позволяет отправлять в сеть неограниченное количество пакетов. Например, при выполнении команды ping -t 192.168.1.10 будет происходить постоянная отправка пакетов, и можно обнаружить ситуацию, при которой появляется (или пропадает) связь.

```
Обмен пакетами с  127.0.0.1 по 32 байт:

Ответ от  127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от  127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от  127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от  127.0.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для  127.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рис. 4.20. Использование утилиты ping

Теперь два компьютера могут обмениваться данными, но для того, чтобы объединить их в полноценную локальную сеть, этого недостаточно. Было бы крайне удобно, чтобы компьютеры находили друг друга в сетевом окружении как отдельные ресурсы. Для этого необходимо объединить их в одну группу и присвоить сетевые имена.

ИЗМЕНЕНИЕ ИМЕНИ И ГРУППОВОГО ИДЕНТИФИКАТОРА КОМПЬЮТЕРОВ

Для изменения сетевой идентификации компьютера (т.е. его имени) нужно выполнить следующие действия:

1. Открыть *Панель управления*, выбрать раздел *Система и ее обслуживание*, а в нем — раздел *Система*.
2. Воспользоваться ссылкой *Изменить параметры* и в появившемся окне *Свойства системы* на вкладке *Имя компьютера* нажать кнопку *Изменить*.
3. В появившемся окне *Изменение имени компьютера* (рис. 4.21) требуется ввести новое имя компьютера. Также нужно установить и принадлежность к рабочей группе (группа переключателей *Является членом*).
4. Нажать кнопку *OK*.
5. Перезагрузить компьютер, если операционная система не выполнила эту процедуру автоматически.

Для одноранговой сети из двух компьютеров в качестве примера назначим компьютерами имена HomeA и HomeB. Оба компьютера объединены в одну и ту же группу WORKGROUP.

При назначении группы необходимо следовать определенным правилам:

- имя рабочей группы не должно совпадать с именем компьютера;
- имя рабочей группы может содержать до 15 символов;
- запрещается использование таких символов: ; : " < > * + = \ | ?,.

Теперь оба компьютера можно увидеть в сетевом окружении. Это очень удобно при использовании *общих папок* — локальных ресурсов, предоставленных для общего доступа в сети.

В результате всех этих манипуляций получилась модель соединения двух компьютеров, представленная на рис. 4.22.

Теперь рассмотрим схему построения одноранговой сети с использованием трех и более компьютеров.

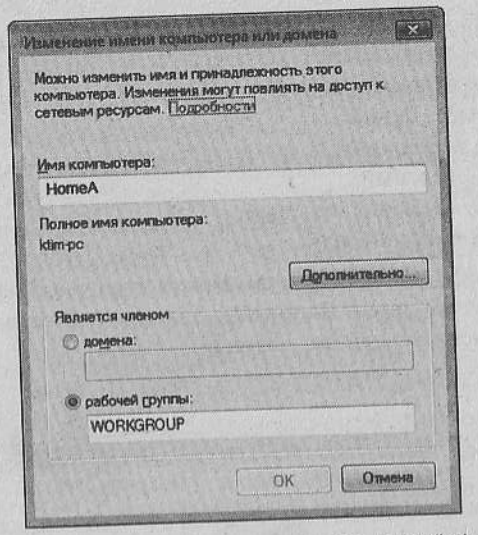


Рис. 4.21. Изменение имени компьютера в Windows

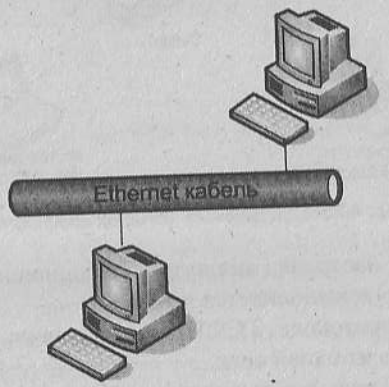


Рис. 4.22. Соединение двух компьютеров «точка – точка».

Соединение трех и более компьютеров без выделенного сервера

При соединении в сеть трех и более компьютеров с использованием коммутатора для всех компьютеров используется раскладка T568B (табл. 4.1), где:

- первый – бело-оранжевый;
- второй – оранжевый;
- третий – бело-зеленый;
- четвертый – синий;
- пятый – бело-синий;
- шестой – зеленый;
- седьмой – бело-коричневый;
- восьмой – коричневый.

Проводники должны располагаться строго в один ряд, без нахлестов друг на друга. Например, для четырех компьютеров схема подключения представлена на рис. 4.23.

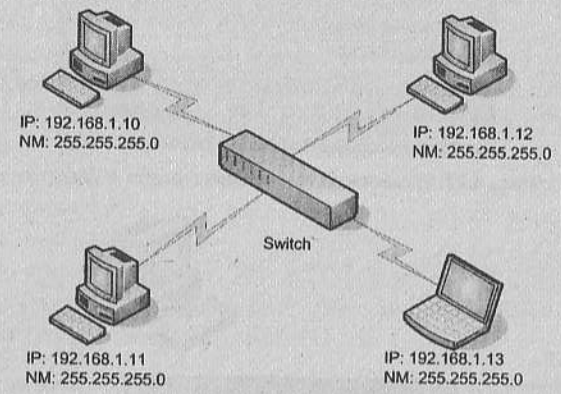


Рис. 4.23. Соединение четырех компьютеров

Дальнейшая настройка аналогична соединению двух компьютеров (см. выше) и выполняется по схеме:

1. Настройка протокола TCP/IP при условии, что все адреса должны быть из одной сети.
2. Назначение имен компьютерам и объединение их в единую группу.
3. Отключение брандмауэра Windows.
4. Проверка соединения при помощи утилиты ping.

Использование общих папок

В большинстве локальных сетей пользователи предпочитают обмениваться информацией посредством общих папок, которые

представляют собой специальные сетевые ресурсы, находящиеся на различных компьютерах, подключенных к локальной сети.

Для просмотра общих папок достаточно открыть Проводник и в области переходов выбрать элемент *Сеть*, в результате чего в поле списка файлов будут отображены компьютеры рабочей группы, к которой принадлежит компьютер пользователя. Выбрав какой-либо компьютер, пользователь может просмотреть список папок, которые открыты для общего доступа (рис. 4.24). Чтобы начать работу с общей папкой, достаточно сделать на ней двойной щелчок.

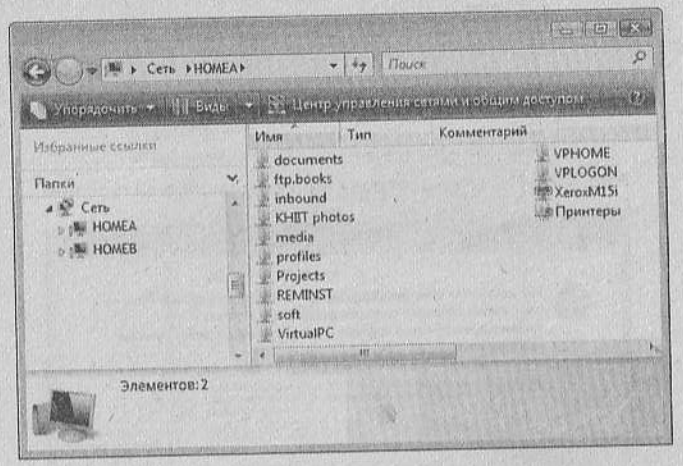


Рис. 4.24. Общие папки на сетевом ресурсе

Однако не все папки могут быть доступны пользователю. Например, одним пользователям будет разрешено только считывать информацию, другим доступ будет ограничен паролем. Связано это с назначенными разрешениями для общего ресурса, которые определил владелец компьютера.

Например, если для подключения к общей папке необходимо указать идентификационные данные, при попытке открыть папку система отобразит диалоговое окно *Подключение к* (рис. 4.25), в котором попросит указать имя пользователя и пароль. Если пароль указано верно – будет отображено содержимое папки, если нет – окно будет показано еще раз, при этом система сообщит, что введенные имя пользователи или пароль не совпадают с существующими в системе.

Если пользователь пытается подключиться к папке, для которой ему не назначены какие-либо права доступа, система отобразит окно с отказом в доступе (рис. 4.26).

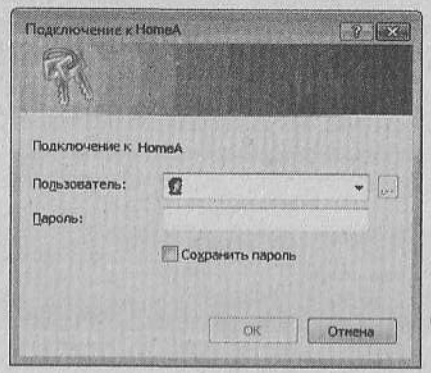


Рис. 4.25. Попытка доступа к папке, защищенной паролем

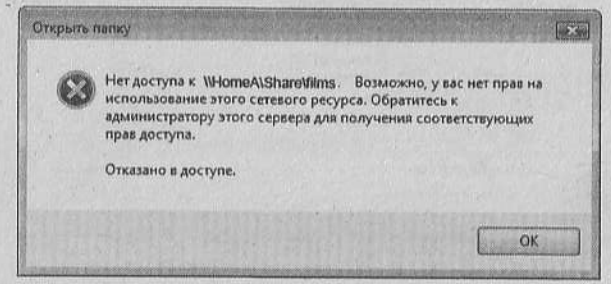


Рис. 4.26. Отказ в доступе к общей папке

В данном случае пользователь не может подключиться к ресурсу, и если доступ к нему все-таки требуется получить, необходимо обратиться к администратору компьютера, на котором расположен ресурс, с просьбой предоставить соответствующие разрешения.

Предоставление общего доступа к папкам

Основным назначением локальной сети является обеспечение информационного обмена между пользователями. Но так как вся информация представлена в файлах, необходимо уметь предоставлять доступ к файлам, которые нужны пользователям, и разделять права доступа.

Например, требуется создать каталог, в котором пользователи других компьютеров могли бы хранить свои файлы или хотя бы считывать уже имеющиеся. Для этого, в первую очередь, необходимо настроить *Центр управления сетями и общим доступом*, а также разрешить подключение пользователей к компьютеру путем создания исключения в брандмауэре для служб *Общий доступ к файлам и принтерам* и *Основы сетей*.

Затем нужно открыть Проводник, найти папку, к которой необходимо предоставить общий доступ, и, вызвав контекстное меню, выбрать команду *Свойства*, при выполнении которой будет отображено диалоговое окно параметров папки. Далее требуется перейти на вкладку *Доступ* (рис. 4.27) и нажать кнопку *Дополнительный доступ*.

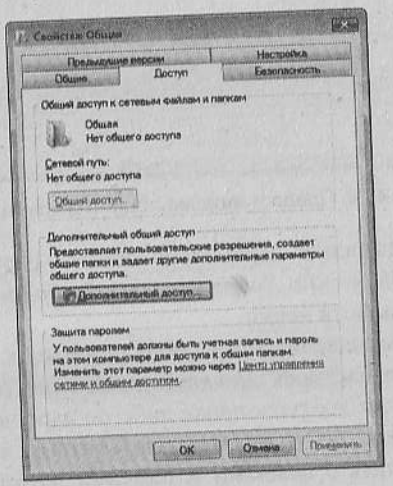


Рис. 4.27. Свойства папки. Вкладка *Доступ*

В результате будет открыто окно *Дополнительный общий доступ* (рис. 4.28), в котором следует:

- установить флажок *Открыть общий доступ к этой папке*;
- указать максимальное число подключений к данной папке (для этого используется регулятор *Ограничить число одновременных пользователей до*);
- написать комментарий к общему ресурсу в поле *Примечание*.

Примечание. Для несерверных систем максимальное число ограничено десятью подключениями, т.е. одновременно к ресурсу могут быть подключены не более десяти пользователей, даже если переключатель установлен в максимально возможное положение.

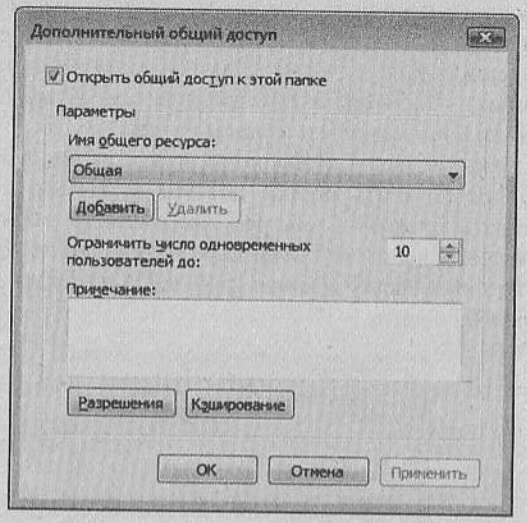


Рис. 4.28. Предоставление общего доступа к папке

После определения параметров общего ресурса следует нажать кнопку *ОК* в окне *Дополнительный общий доступ*, а также закрыть окно свойств папки.

Теперь пользователи смогут подключаться к компьютеру и в зависимости от настроек *Центра управления сетями и общим доступом* получат доступ к папке либо по паролю, либо без него.

В случае, если требуется определить, кто из пользователей сети может работать с файлами и папками, которые находятся в общем ресурсе, можно отредактировать список контроля доступа, который появляется при нажатии кнопки *Разрешения* в окне *Дополнительный общий доступ* (рис. 4.29).

По умолчанию все пользователи, подключающиеся к общему ресурсу, имеют право просматривать его содержимое, но не имеют возможности изменять файлы. Пользователь может переопределить эти разрешения или добавить в список другие группы и указать для них особые разрешения.

Применяются следующие типы разрешений доступа к общим папкам или дискам:

Чтение – назначается группе *Все* по умолчанию и позволяет:

- просматривать имена файлов и подкаталогов;
- просматривать данные в файлах;
- выполнять программные файлы.

Изменение – никогда не назначается группам по умолчанию. Включает все функции разрешения *Чтение*, а также позволяет:

- добавлять файлы и подпапки;
- изменять данные в файлах;
- удалять подпапки и файлы.

Полный доступ – по умолчанию назначается группе *Администраторы* на локальном компьютере. Разрешение *Полный доступ* включает разрешения *Изменение* и *Чтение*, а также позволяет изменять NTFS-разрешения для файлов и папок и назначать владельцев папок и файлов.

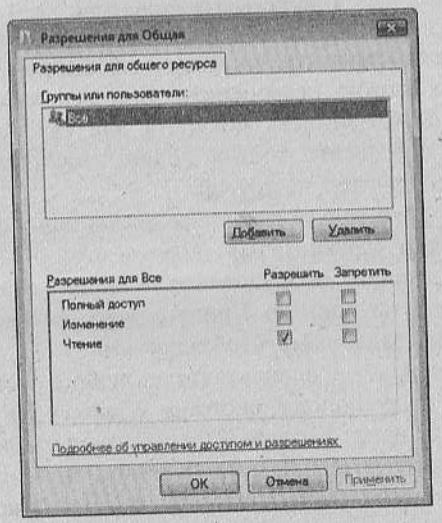


Рис. 4.29. Список разрешений для общего ресурса

В том случае, если общий каталог находится на NTFS-диске, пользователь кроме разрешений общего доступа может применять и NTFS-разрешения для более гибкой настройки прав других пользователей при работе с общим ресурсом. Если же логи-

ческий диск отформатирован с использованием FAT32, разрешения общего доступа являются единственным ограничением, поскольку они касаются только общих папок и не ограничивают пользователя, если он выполнил локальный вход в систему.

Если одновременно применяются и NTFS-разрешения, и разрешения общего доступа, то при работе пользователя с ресурсом они комбинируются, и в результате действуют наиболее ограничивающие разрешения. Например, если для каталога NTFS-разрешения установлены в *Полный доступ*, а разрешения общего доступа – в *Чтение*, то пользователь может только считывать данные этого каталога, но не изменять их.

Одним из несомненных преимуществ объединения компьютеров в локальную сеть является возможность использования одного принтера для печати документов с нескольких компьютеров, так называемая «сетевая печать».

Сетевая печать

Возможность печатать документы на сетевом принтере в домашней сети сложно переоценить. При использовании сетевой печати нет необходимости покупать для каждого компьютера принтер или переносить данные с одного компьютера, к которому подключен принтер, на другой.

Существует несколько вариантов организации сетевой печати. Первый вариант (сравнительно дорогостоящий) – это покупка специализированного оборудования – «принт-сервера», к которому подключается принтер. Принт-сервер – это небольшой компьютер с строго заданными возможностями.

Второй вариант – использование любого компьютера под управлением операционной системы Windows XP или Windows Vista в качестве принт-сервера. Рассмотрим его более подробно.

Прежде всего, необходимо подключить принтер к компьютеру, руководствуясь инструкцией пользователя, которая идет в комплекте с печатным устройством. Подключение происходит с помощью USB- или LPT-кабеля. В настоящее время, как правило, используется USB-кабель. Далее система попросит установить драйверы для данного устройства, они должны быть на CD-диске, входящем в комплект поставки принтера. После установки необходимых драйверов устройство должно появиться в системе.

Посмотреть установленные принтеры можно в меню *Пуск* | *Панель управления* | *Принтеры* (рис. 4.30).

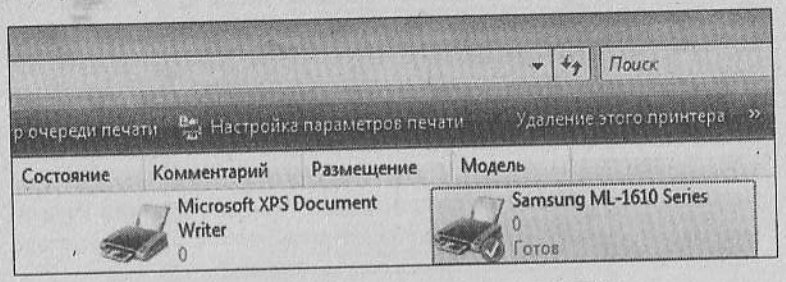


Рис. 4.30. Отображение принтера в системе

Принтер готов для локального использования, т.е. можно использовать его только с того компьютера, на который он установлен сейчас. Чтобы позволить всем пользователям сети использовать его в качестве общего принтера, необходимо предоставить к принтеру общий доступ. Для этого следует щелкнуть на ярлычке принтера правой кнопкой мыши и выбрать пункт *Общий доступ* (рис. 4.31).

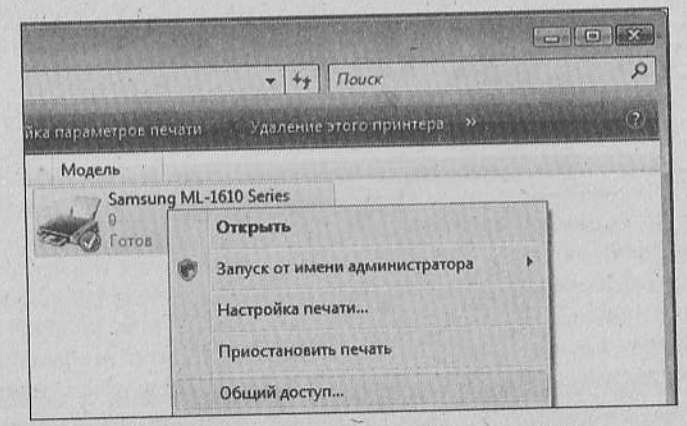


Рис. 4.31. Предоставление общего доступа

Для включения возможности использования данного принтера как общего, необходимо нажать на кнопку *Настройка общего доступа*. После этого станут доступны для выбора опции общего доступа (рис. 4.32).

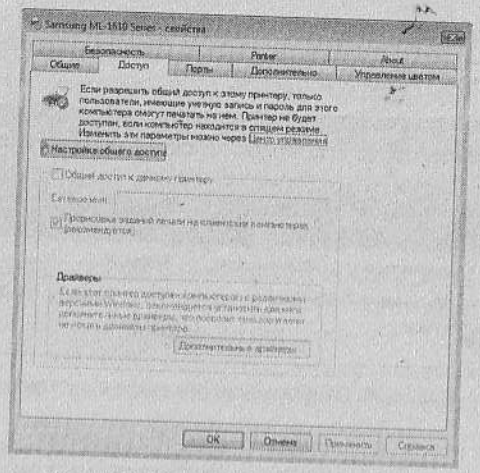


Рис. 4.32. Настройка общего доступа

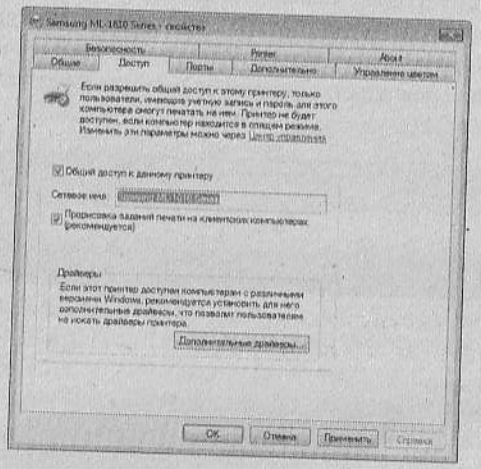


Рис. 4.33. Выбор сетевого имени

Следует установить оба флажка (*Общий доступ к данному принтеру* и *Прорисовка заданий печати на клиентских компьютерах*). Первая позволит предоставить общий доступ к принтеру по сети, а вторая даст возможность пользователям у себя на компьютерах следить за состоянием их заданий печати. Также необходимо задать сетевое имя для принтера – именно под этим именем его будут видеть все пользователи локальной сети (рис. 4.33).

На этом базовая настройка сетевой печати завершена. Теперь любой пользователь локальной сети сможет видеть данный принтер, однако есть исключение – все пользователи должны находиться в одной подсети с принтером. Для преодоления этих ограничений используются сложные сетевые технологии, такие как доменная структура. Их изучение выходит за рамки данной книги.

Теперь перейдем к настройке клиентского компьютера для использования сетевой печати. Прежде всего, необходимо перейти в *Панель управления* | *Принтеры* и щелкнуть на рабочем поле правой кнопкой мыши. Откроется меню, в котором нужно выбрать подменю *Установить принтер* (рис. 4.34).

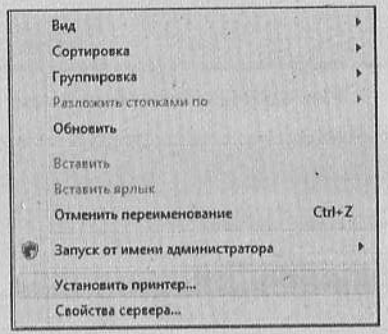


Рис. 4.34. Установка принтера на клиентском компьютере

Следующим шагом система предложит установить либо локальный принтер, который подключен непосредственно к локальному компьютеру, либо сетевой, беспроводной или Bluetooth принтер. Необходимо выбрать второй вариант (рис. 4.35).

Система автоматически выполнит поиск доступных в сети принтеров и предоставит список. Требуется выбрать тот принтер, который используется в качестве общего сетевого (рис. 4.36).

Даже если в системе, на которую устанавливается сетевой принтер, нет нужного драйвера для принтера, система автоматически по сети загрузит его с компьютера, к которому подключен принтер. Если же операционные системы на компьютере-сервере и компьютере-клиенте различаются, то необходимо запастись диском с драйверами под принтер для операционной системы, установленной на компьютере пользователя.

Следующим шагом система попросит задать имя для сетевого принтера (рис. 4.37).

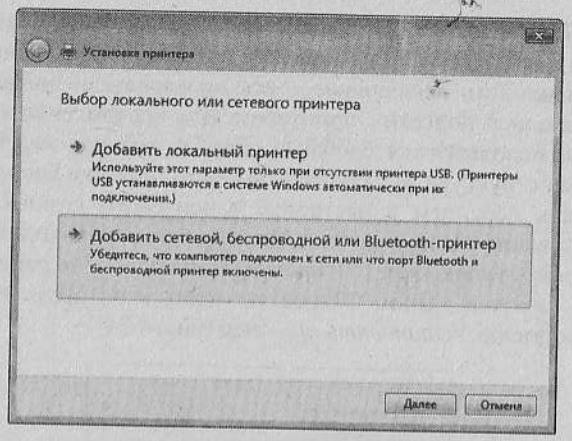


Рис. 4.35. Добавление принтера

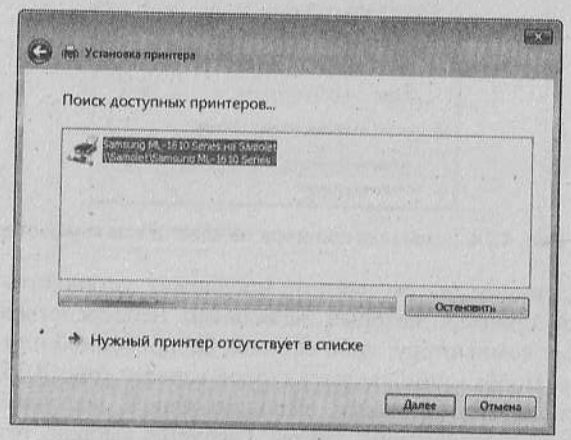


Рис. 4.36. Поиск и установка принтера

Следующий этап является завершающим в установке сетевого принтера на клиентском компьютере. Система предложит пользователю распечатать пробную страницу на сетевом принтере – и мастер установки завершит свою работу (рис. 4.38).

Заметим, что объединение двух настольных компьютеров по проводной сети ничем не отличается от соединения двух ноутбуков. Важно, чтобы на материнской плате каждого из них присутствовал разъем RJ45 и была установлена операционная система Windows Vista.

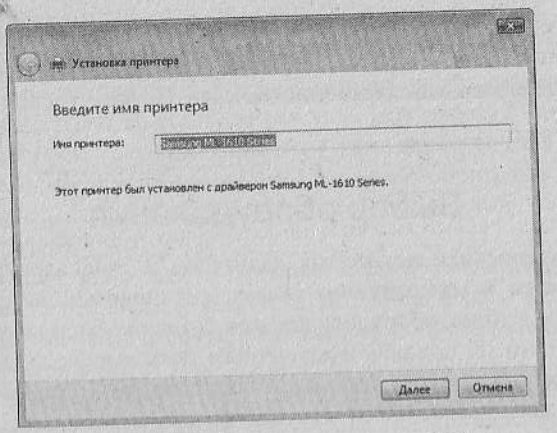


Рис. 4.37. Задание имени принтера

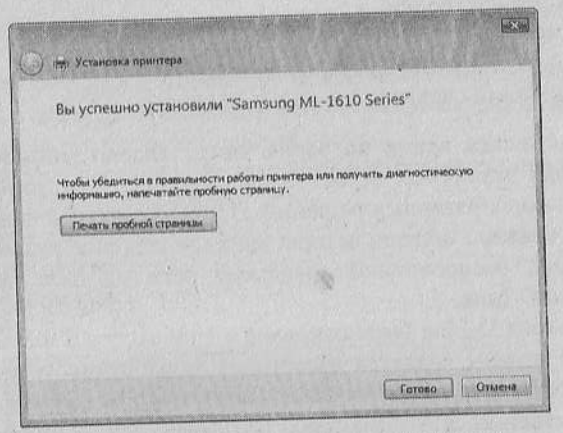


Рис. 4.38. Завершение установки принтера

Глава 5
Создание беспроводной локальной сети

В этой главе на практике рассматриваются вопросы выбора и настройки оборудования для создания беспроводной локальной сети. Рассматриваются два варианта подключения: «точка –точка» – подключение без выделенной точки доступа, с использованием

только беспроводных сетевых адаптеров и подключение «точка – многоточка» – с использованием выделенной точки доступа для объединения компьютеров в единую сеть. Начнем с выбора оборудования.

Выбор оборудования

Характеристики некоторых адаптеров и точек доступа были рассмотрены в предыдущих главах, остановимся на основных критериях выбора оборудования для создания беспроводной локальной сети. К основным критериям, которые должны учитываться при построении домашней беспроводной сети, можно отнести такие:

- поддерживаемые скорости передачи;
- простота настройки;
- стоимость оборудования;
- гибкость и простота подключения;
- доступность сервиса.

В настоящее время на рынке представлено множество устройств для различных областей применения — от домашних до крупных корпоративных решений. Проведя определенный анализ рынка и сравнив модели, авторы приняли решение рассматривать построение беспроводной локальной сети на базе продукции компании D-Link.

Компания D-Link была основана в 1986 году в Тайвани и в настоящий момент является известным разработчиком и производителем сетевого оборудования. Компания предлагает широкий выбор решений для домашних пользователей, корпоративного сегмента и провайдеров нтернет-услуг.

Для построения беспроводной сети в качестве точки доступа будем использовать беспроводной маршрутизатор DI-624+.

DI-624+ AirPlusXtremeG+ высокоскоростной 2.4ГГц 802.11g беспроводной широкополосный маршрутизатор со встроенным 4-портовым коммутатором Fast Ethernet. Маршрутизатор поддерживает скорость беспроводного соединения до 54 Мбит/с и позволяет легко и быстро настроить общий доступ к Интернету для проводной или беспроводной сети. Это устройство разрабатывалось для установки в помещениях и предоставляет расширенные функции, функции безопасности и качества обслуживания (QoS). Данная

технология позволяет приоритезировать потоки данных, выделяя под наиболее чувствительные к задержкам потоки лучшую полосу пропускания, встроенный Firewall позволяет создать надежную систему защиты от внешних вторжений. При работе в помещении дальность приема сигнала зависит от типа перекрытий в помещении и может варьироваться от 10–15 м (железобетонные перекрытия толщиной более 40 см) до 45–65 м (гипсокартон, тонкая кирпичная кладка).

В качестве клиентского сетевого адаптера используется беспроводной сетевой адаптер DWL-G122. DWL-G122 – это высокопроизводительный беспроводной адаптер USB стандарта 802.11g, который используется для соединения компьютера с высокоскоростной беспроводной сетью. Этот адаптер легко подключается к компьютеру через быстрый порт USB 2.0 и обеспечивает скорость беспроводного соединения до 54 Мбит/с.

Адаптер выбирался из соображений цены, поддерживаемых технологий и универсальности. Действительно, сейчас трудно найти компьютер, в котором нет поддержки стандарта USB. Поэтому этот адаптер может быть использован как для настольных компьютеров так и для мобильных систем.

В комплект поставки беспроводного маршрутизатора входят:

- диск с ПО и документацией;
- руководство пользователя;
- маршрутизатор;
- кабедь Ethernet;
- адаптер сети 220V;
- съемная штатная антенна.

В комплект поставки беспроводного адаптера DWL-G122 входят:

- беспроводной адаптер DWL-G122;
- диск с документацией;
- руководство по быстрой установке;
- USB-удлинитель.

Вначале рассмотрим настройку сетевого адаптера DWL-G122.

Настройка DWL-G122

Весь процесс конфигурирования адаптера можно разбить на несколько этапов:

- установка драйверов устройства;
- настройка беспроводного сетевого адаптера;
- проверка работоспособности.

Начнем с первого этапа:

1. Для начала необходимо подключить устройство DWL-G122 к свободному порту USB на передней или на задней панели компьютера.
2. Система обнаружит устройство и предложит несколько вариантов поиска и установки драйвера (рис. 5.1).

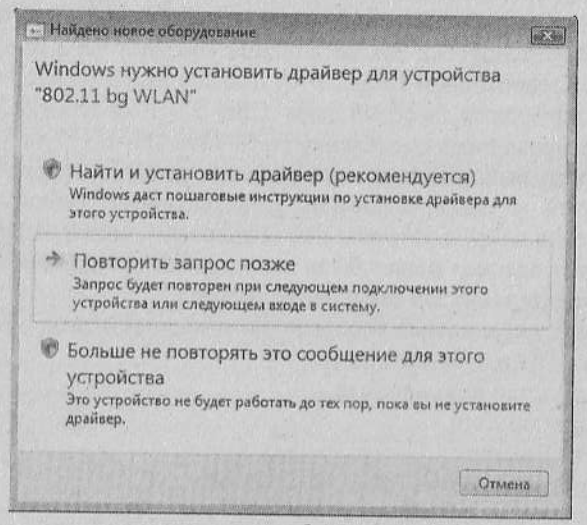


Рис. 5.1. Установка драйвера

Необходимо выбрать вариант Найти и установить драйвер. После этого система продолжит процесс установки драйверов для данного устройства.

3. Следующим шагом система предложит несколько вариантов поиска драйвера (рис. 5.2).

Если нет диска с драйверами, то, конечно, можно попытаться произвести поиск драйверов в Интернете на специализированном сайте компании Microsoft. Но как показывает опыт, система для таких специфических устройств на этом узле драйверов не находит. Следовательно, нужно выбрать пункт *Не выполнять поиск в Интернете*.

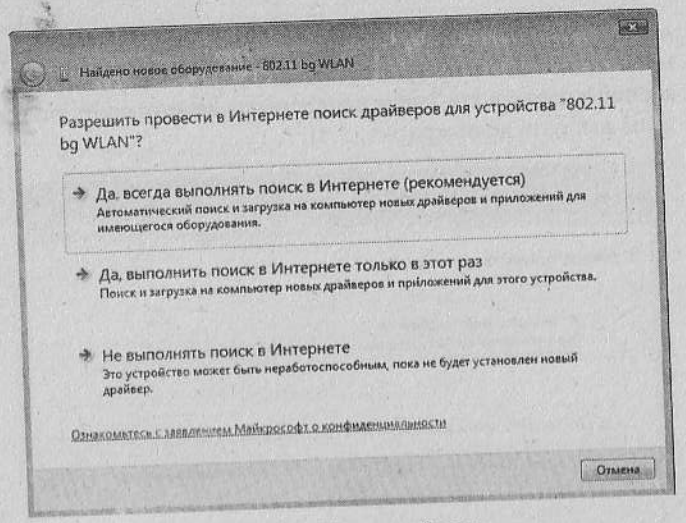


Рис. 5.2. Поиск драйвера

4. Далее система предложит вставить в оптический привод диск с драйверами. Если диск есть, его необходимо вставить, если нет, то следует выбрать пункт *Такого диска нет. Покажите другие возможности* (рис. 5.3).

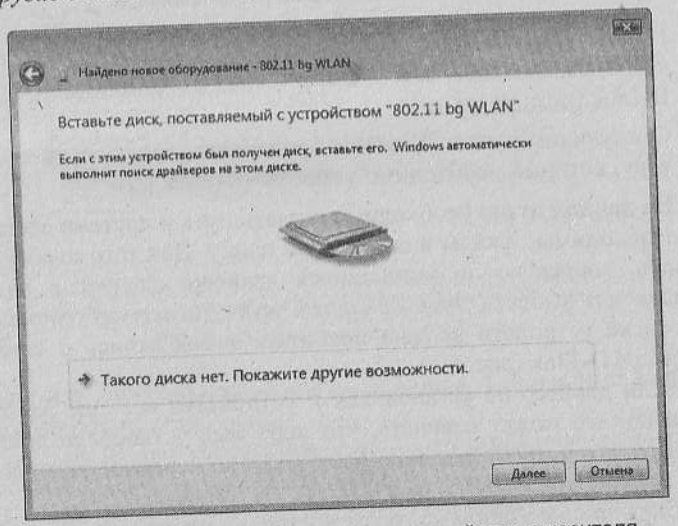


Рис. 5.3. Автоматическая установка драйвера с носителя

5. Если диска нет, система не сможет установить драйвер автоматически и либо предложит искать решение проблемы в базе знаний в Интернете, либо предоставит возможность пользователю выбрать драйвер (рис. 5.4).

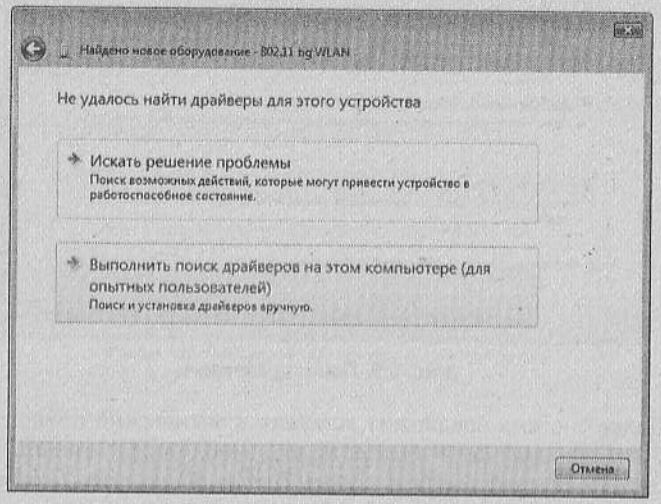


Рис. 5.4. Автоматический поиск драйвера

Настоятельно рекомендуется перед установкой скачать необходимые драйверы для Windows Vista с официального сайта D-Link (http://dlink.ru).

6. Следующим шагом Windows предложит указать путь к драйверу, который необходимо установить (рис. 5.5).

На данном этапе необходимо указать путь и система скопирует необходимые файлы в системную папку. Для того чтобы проверить, корректно ли установился драйвер, следует в панели управления выбрать *Оборудование и звук | Диспетчер устройств*. В списке устройств должна появиться новая запись о сетевом адаптере D-Link (рис. 5.6).

Если драйвер не установился и устройство все еще работает неверно, это может означать, что либо был установлен драйвер для другого устройства, либо было указано неверное расположение папки с драйвером.

Следующим этапом является настройка протокола IP для беспроводного адаптера.

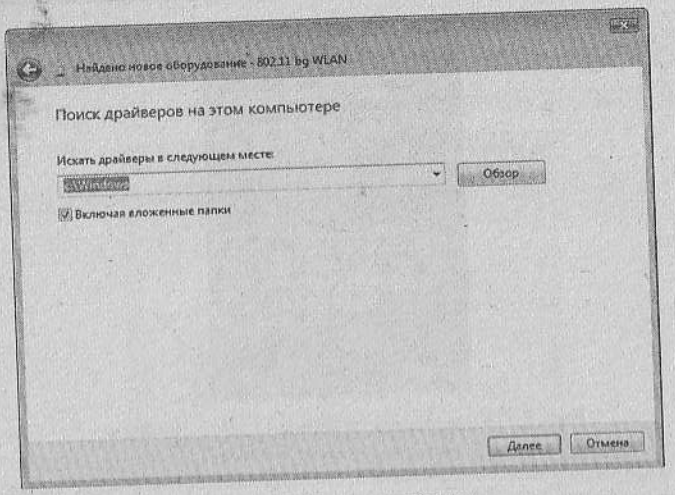


Рис. 5.5. Путь к драйверу

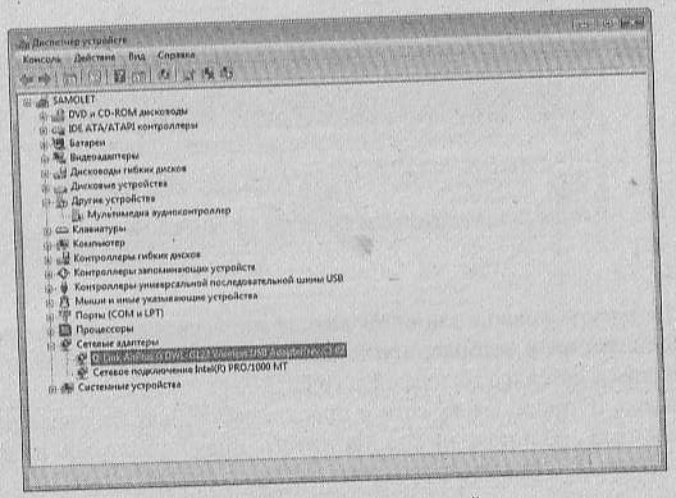


Рис. 5.6. Новое сетевое устройство

Как и в настройке проводного адаптера, необходимо выполнить следующие действия:

1. Открыть панель управления, выбрать пункт *Центр управления сетями*.
2. В левой части окна нужно выбрать *Управление сетевыми подключениями* (рис. 5.7).

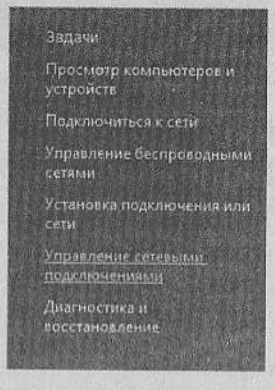


Рис. 5.7. Управление сетевыми подключениями

3. Откроется окно, в котором отображены все сетевые подключения (рис. 5.8).

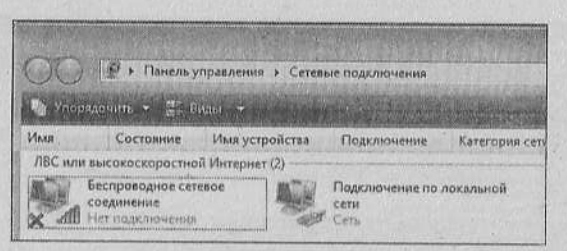


Рис. 5.8. Сетевые подключения

4. Щелкнуть правой кнопкой мыши на беспроводном сетевом соединении и выбрать пункт *Свойства*. Откроется меню настройки сетевого интерфейса (рис. 5.9).
5. Задать IP-адрес, маску сети и шлюз в настройках беспроводного адаптера. Шлюзом нужно назначить предполагаемый в дальнейшем IP-адрес беспроводного маршрутизатора (рис. 5.10).

Важно помнить, что диапазон IP-адресов для локальной сети необходимо выбрать из диапазона так называемых «серых» или немаршрутизируемых IP-адресов. Как уже говорилось в главе 2, эти адреса выделены для организации локальных сетей и могут быть использованы любое количество раз в разных локальных сетях. Кроме того, необходимо помнить, что и контроллер, и маршрутизатор должны находиться в одной подсети. Именно поэтому были выбраны IP-адреса 192.168.0.1 и 192.168.0.2 при

маске подсети 255.255.255.0. Что касается адреса DNS-сервера, то необходимо указать DNS-сервер интернет-провайдера либо, в случае определенных настроек точки доступа, адрес точки доступа.

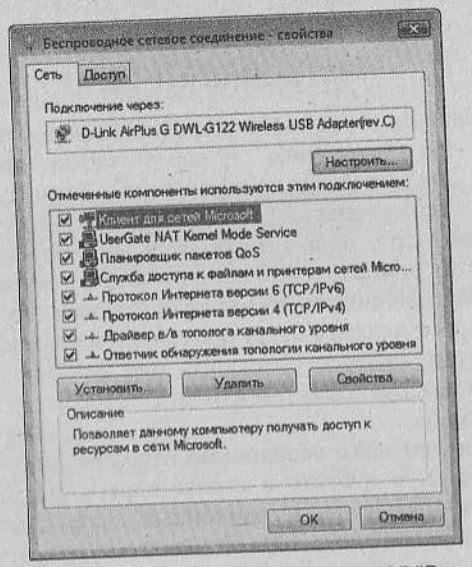


Рис. 5.9. Настройка протокола TCP/IP

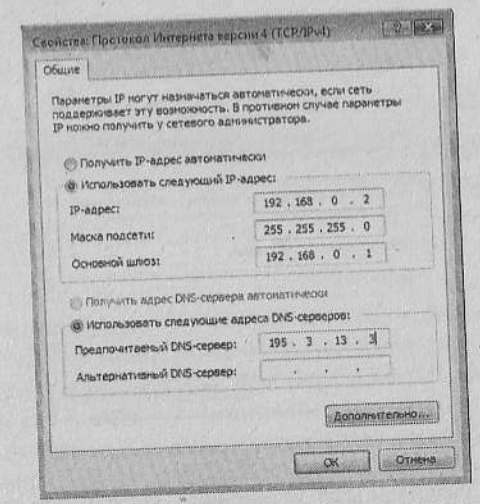


Рис. 5.10. Определение параметров протокола IP

На данном этапе конфигурирование беспроводного адаптера завершено, перейдем к конфигурированию беспроводного маршрутизатора.

Настройка DI-624+

Конфигурирование данного устройства происходит через веб-интерфейс. По умолчанию IP-адрес маршрутизатора будет 192.168.0.1. Для того чтобы подключиться к устройству через сеть, необходимо подключить маршрутизатор либо непосредственно к самому компьютеру. либо к порту Ethernet-коммутатора, подключенному к тому компьютеру, с которого будет производиться конфигурирование данной точки. В настройках сетевого подключения на компьютере, с которого будет производиться конфигурирование маршрутизатора, следует установить для сетевого адаптера IP-адрес из сети 192.168.0.0/24, например 192.168.0.2, и сетевую маску 255.255.255.0.

На следующем шаге необходимо открыть браузер, например Internet Explorer, и набрать в строке адреса http://192.168.0.1. Появится меню ввода регистрационных данных для доступа к веб-интерфейсу конфигуратора точки доступа. По умолчанию имя пользователя – admin, поле пароля – пустое (рис. 5.11).

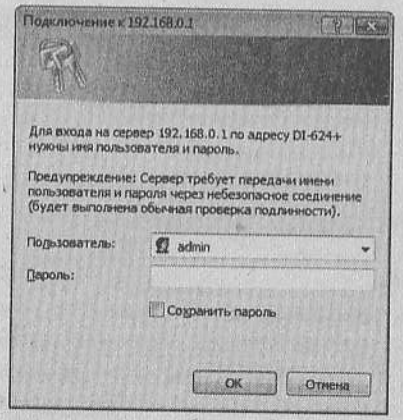


Рис. 5.11. Ввод регистрационных данных

Появится окно мастера установки. Эта утилита поможет быстро настроить точку доступа для работы. С ее помощью настраиваются только базовые функции, которые необходимы и достаточны для работы в стандартной конфигурации (рис. 5.12).

Необходимо нажать кнопку *Run Wizard*. Запустится мастер настройки подключения и проведет по всем этапам первичной настройки беспроводной сети. Настройка с помощью мастера не отличаются разнообразием либо гибкостью, но она необходима и достаточна для создания соединения между точкой доступа и беспроводным адаптером.

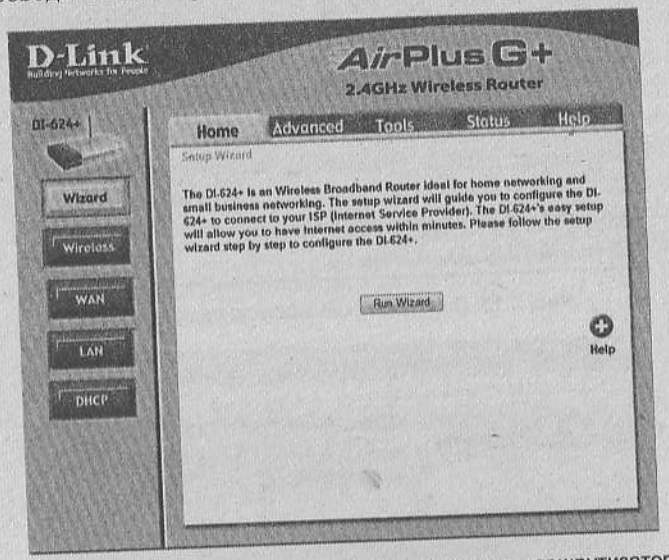


Рис. 5.12. Стартовая страница веб-конфигуратора маршрутизатора

В первом окне мастера перечислены все шаги, которые будут выполнены при настройке беспроводного сетевого подключения (рис. 5.13):

1. Первым шагом необходимо изменить пароль администратора для веб-конфигуратора маршрутизатора. Если этого не сделать, то он будет стандартным, а это значит, что любой человек из внутренней сети, а при определенных условиях и из внешней сети, сможет изменить настройки маршрутизатора. Этого допустить ни в коем случае нельзя (рис. 5.14).
2. Следующим шагом идет установка временной зоны. Это необходимо будет в дальнейшем для корректной работы сервера синхронизации времени на маршрутизаторе.

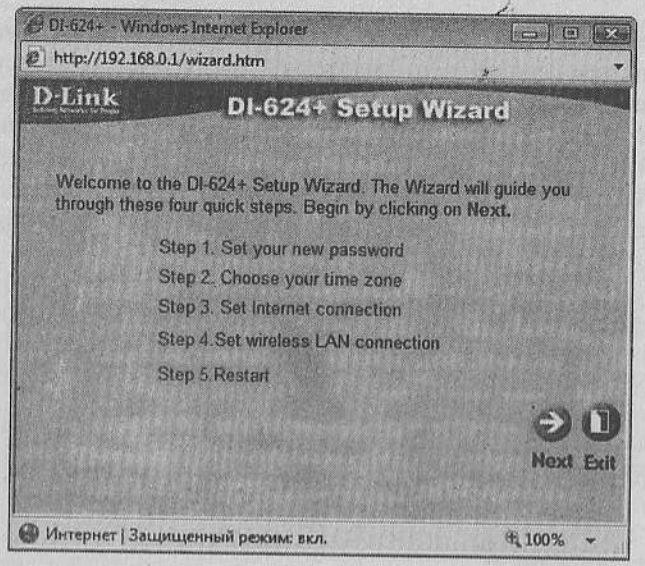


Рис. 5.13. Основное окно мастера подключения

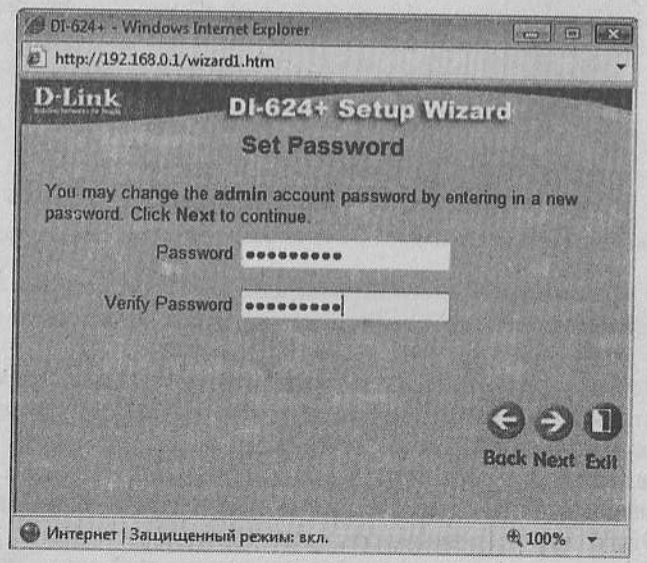


Рис. 5.14. Смена пароля

3. На следующем шаге мастера маршрутизатор опрашивает порт с надписью *WAN*, именно к нему должно быть подсоединено устройство для подключения к глобальной сети Интернет. В данном случае это ADSL-модем (о технологии ADSL более подробно см. в главе 6). Поэтому маршрутизатор диагностирует, что типом подключения является PPPoE, которое характерно для ADSL-провайдеров. После определения типа подключения мастер предлагает заполнить форму с учетной записью и паролем, который выдал ADSL-провайдер при подключении (рис. 5.15).
4. В следующем окне необходимо указать имя для SSID и номер радиоканала, на котором будет выполнятся передача данных. SSID – это идентификатор сети Wi-Fi, иначе говоря, название сети, который позволяет отделить одни сети от других и различать их. Сеть с одним идентификатором имеет, как правило, одни и те же параметры. SSID может быть произвольным, например HOMENET. А канал рекомендуется оставить по умолчанию (рис. 5.16).

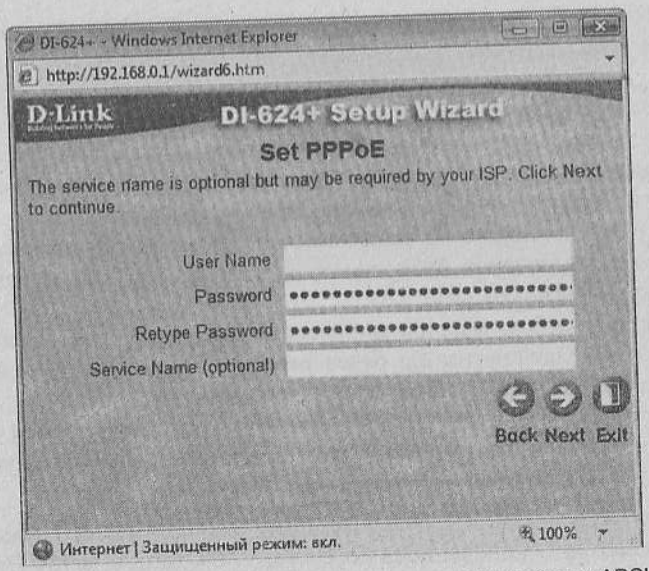


Рис. 5.15. Учетная запись для подключения к провайдеру ADSL

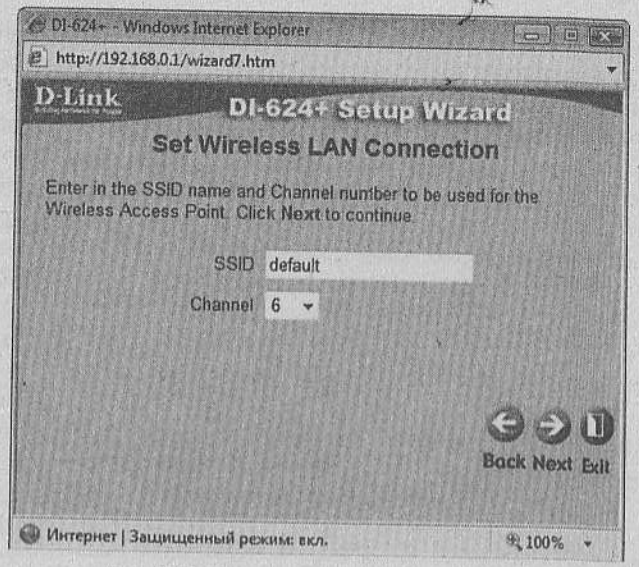


Рис. 5.16. Указание SSID и номера канала

5. Далее требуется задать вид шифрования и ключ-пароль. Можно выбрать шифрование по умолчанию WEP-64bit. В дальнейшем при настройке маршрутизатора можно будет изменить и тип шифрования, и ключ. Ключ задается в шестнадцатиричной системе исчисления, что предполагает использование букв от A(a) до F(f) и цифр от 0 до 9. Ключ можно сгенерировать, используя специальные программы, или задать в ручную. Важно не забыть его, потому что он потребуется для подключения беспроводного адаптера к беспроводному маршрутизатору (рис. 5.17).
6. На этом работа мастера закончена. Необходимо нажать кнопку *Restart*. Маршрутизатор будет перезагружен, и все изменения вступят в силу. Таким образом, работа с беспроводным маршрутизатором закончена. Для более детальной настройки маршрутизатора необходимо обратиться к официальной документации на сайте производителя (http://dlink.ru).

Для подключения к беспроводному маршрутизатору следует также настроить операционную систему. Выбираем меню *Пуск | Подключения*, после чего появится окно с указанием найденных сетей (рис. 5.18).

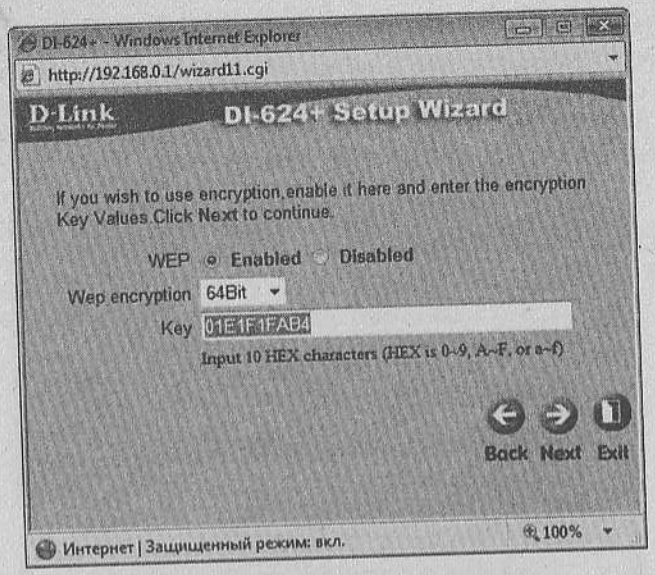


Рис. 5.17. Опции шифрования

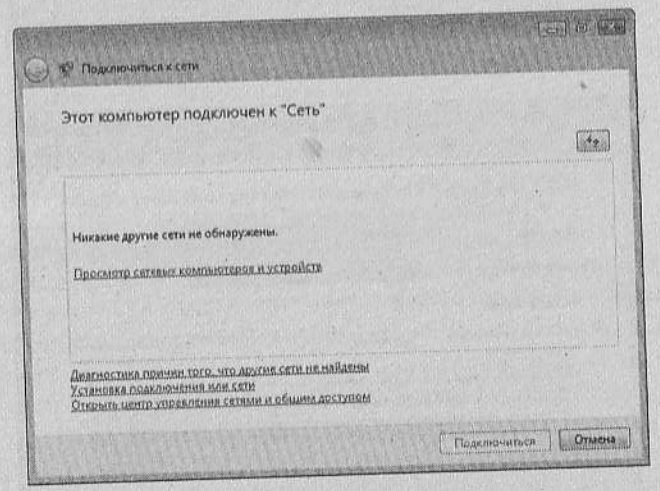


Рис. 5.18. Создание нового подключения

Если беспроводной маршрутизатор работает правильно, то откроется окно с обнаруженной только что настроенной сетью *Homenet*. Если же маршрутизатор в данный момент отключен, то

система не обнаружит ни одной сети. В этом случае следует выключить маршрутизатор и настроить подключение к беспроводной сети. Необходимо выбрать подменю *Установка подключения или сети*, после чего откроется окно выбора типа сети, к которой необходимо установить подключение (рис. 5.19).

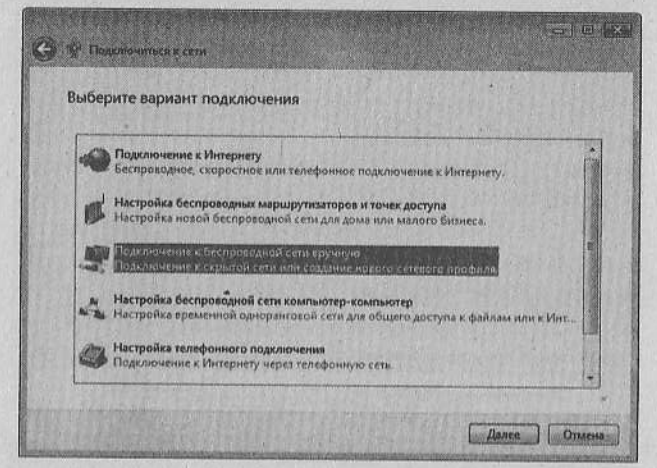


Рис. 5.19. Выбор варианта подключения

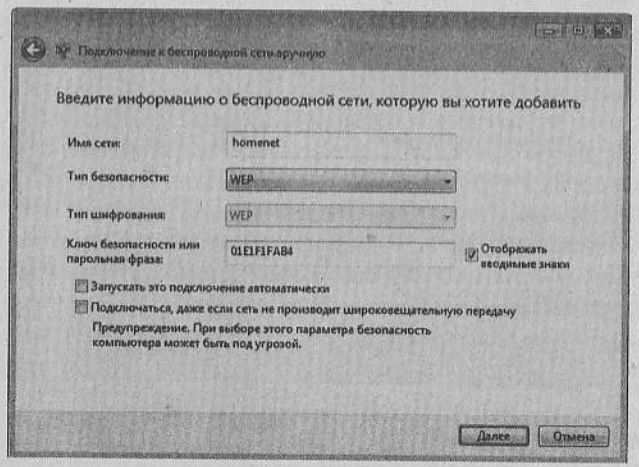


Рис. 5.20. Задание параметров подключения к сети

Далее мастер операционной системы предложит задать параметры, необходимые для создания подключения к беспроводной сети (рис. 5.20).

Следует заполнить все поля, в поле *Имя сети* вписать название SSID, которое задавалось при настройке беспроводного маршрутизатора, тип безопасности – такой же, как и при настройке маршрутизатора, и, главное, идентичный заданному ключ.

После заполнения всех необходимых полей и нажатия кнопки *Далее* появится предложение подключиться к созданной сети или изменить параметры доступа (рис. 5.21).

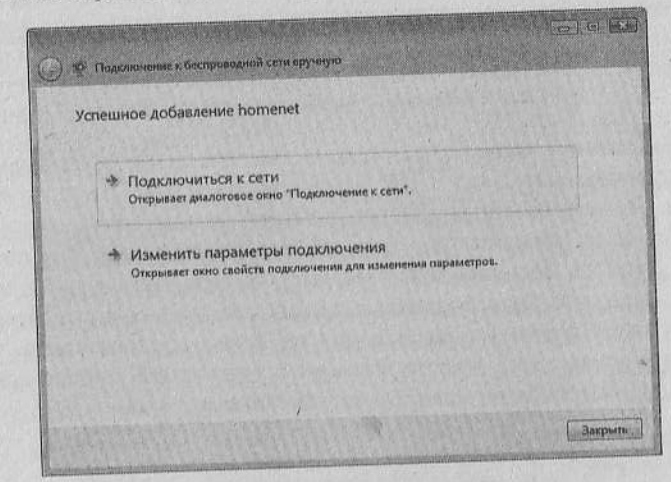


Рис. 5.21. Подключение к сети

Если все параметры указаны верно, точка доступа включена и сетевой адаптер настроен правильно, должно появиться сообщение об успешном подключении к беспроводной сети (рис. 5.22).

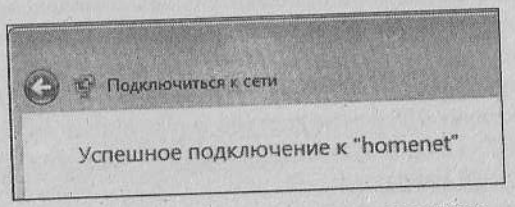


Рис. 5.22. Подключение успешно завершено

Обязательным шагом является проверка соединения путем пересылки ICMP-пакетов с помощью утилиты ping, о которой было рассказано в главе 4 (рис. 5.23).

```
C:\Users\phant@m>ping 192.168.0.1

Обмен пакетами с 192.168.0.1 по с 32 байт данных:

Ответ от 192.168.0.1: число байт=32 время=3мс TTL=127
Ответ от 192.168.0.1: число байт=32 время=3мс TTL=127
Ответ от 192.168.0.1: число байт=32 время=3мс TTL=127
Ответ от 192.168.0.1: число байт=32 время=3мс TTL=127

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 3 мсек, Среднее = 3 мсек

C:\Users\phant@m>_
```

Рис. 5.23. Результаты работы команды ping

На данном этапе было создано беспроводное подключение между пользовательским ПК и маршрутизатором. Аналогичные шаги необходимо предпринять для всех компьютеров, которые планируется объединить в единую беспроводную сеть с помощью данного беспроводного маршрутизатора. При этом нужно учитывать, что беспроводные адаптеры на других компьютерах могут быть других моделей и других фирм, следовательно, интерфейс управления и настройки могут отличаться, однако принцип соединения будет аналогичен описанному.

Публичные точки доступа Wi-Fi

Существует множество различных сетей Wi-Fi, однако наибольшее распространение получили публичные сети, или публичные точки доступа. Эти сети располагаются в аэропортах, ресторанах, кафе, барах и развлекательных комплексах.

В большинстве публичных точек доступа имеется возможность бесплатного использования Интернета. Наиболее распространена публичная бесплатная сеть *Яндекс.WiFi*. На данный момент существует 288 точек доступа в различных городах России и стран СНГ. Подробную информацию о сети можно узнать на сайте http://wifi.yandex.ru.

В Интернете существуют специализированные сайты, на которых пользователь может узнать о расположении публичных сетей Wi-Fi. Рассмотрим некоторые из них:

- http://www.wns.ru – сайт посвящен развитию Wi-Fi в Москве, содержит полный каталог публичных точек доступа Москвы с указание месторасположения и тарифов;
- http://wifi.cnews.ru – сайт-каталог публичных точек доступа в России и странах СНГ с указанием местоположения и тарифа, позволяет сортировать точки доступа по странам, городам и месту расположения.

ПОДКЛЮЧЕНИЕ К СУЩЕСТВУЮЩЕЙ СЕТИ WI-FI

Для подключения к сети Интернет с помощью Wi-Fi необходимо подключиться к существующей сети Wi-Fi, предоставляющей доступ к сети Интернет. Данное подключение аналогично подключению к одноранговой сети, которое уже было описано выше. При подключении операционная система (ОС) попросит ввести пароль доступа к сети, который будет указан администратором сети. После успешного подключения к сети Wi-Fi Windows предложит выбрать настройку сетевого размещения (рис. 5.24).

В данном окне необходимо указать место, где расположена Wi-Fi сеть. Существуют три места расположения сети: *Дома, На работе, Общественное место*. В соответствии с местом расположения сети Windows автоматически настроит параметры безопасности. Для сети, расположенной в общественном месте, ОС автоматически заблокирует доступ к сетевым папкам ноутбука.

После настройки работа в сети Wi-Fi полностью аналогична работе с проводной сетью.

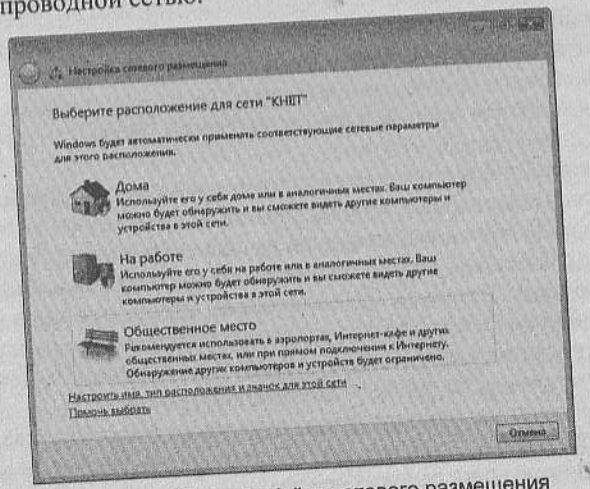


Рис. 5.24. Окно настройки сетевого размещения

Глава 6
Подключение к глобальной сети

В данной главе рассматриваются вопросы подключения к глобальной сети Интернет. Выполняется обзор существующих технологий подключения, рассказывается, как решается проблема «последней мили», рассматриваются критерии выбора провайдера и настройка ОС для работы через то или иное соединение.

Технологии подключения к сети Интернет

В настоящее время существует огромное количество различных технологий доступа к сети Интернет: это и Dial-Up, и различные варианты DSL-подключений, и беспроводные технологии. Рассмотрим наиболее распространенные из них и проведем краткую характеристику оборудования, применяемого при подключении к сети Интернет. Для начала обратимся к истории и посмотрим, как начинали свое развитие технологии подключения к Интернету.

Подавляющее большинство провайдеров интернет-услуг имеют иерархическую структуру (рис. 6.1). Существуют провайдеры высокого уровня, так называемые Top Level Providers, региональные провайдеры, городские провайдеры и их абоненты. Абоненты не могут получать данные непосредственно от провайдеров высокого уровня, они получают их от городских, максимум от региональных провайдеров, а те, в свою очередь, – от провайдеров более высокого уровня.

Основной задачей регионального, городского провайдера является покупка за как можно меньшую цену широкого канала доступа в Интернет у провайдера высшего уровня и продажа этого же канала своим абонентам за разумную, но как можно более высокую цену. При этом качество связи, скорость и цена должны быть конкурентоспособными на рынке информационных услуг.

Организация канала связи между провайдером и конечным потребителем и есть проблема «последней мили».

Существует много вариантов деления технологий «последней мили» на классы, наиболее распространенным является деление по типу приемо-передающей среды:

- передача данных по медным линиям;
- передача данных с помощью витой пары;
- передача данных по оптоволоконным каналам;
- передача данных по радиоканалам.

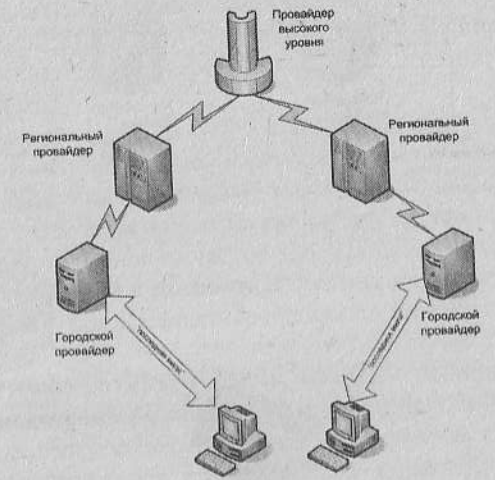


Рис. 6.1. Схема работы интернет-провайдеров

На основе каждого из видов приемо-передающей среды базируется несколько технологий передачи данных. Рассмотрим наиболее распространенные из них.

Dial-Up

Dial-Up – это одна из самых старых и низкоскоростных технологий подключения к Интернету. Для подключения используется обычная телефонная линия и специальное устройство, модем. Рассмотрим схему работы технологии Dial-Up (рис. 6.2).

Для работы по технологии Dial-Up требуется специализированное оборудование, такое как «модем». Это сокращение от термина «модулятор-демодулятор». Данное устройство преобразует (модулирует) сигнал с цифрового компьютерного в аналоговый, который может передаваться по телефонным проводам, и наоборот, преобразует сигнал с аналогового в цифровой, понятный компьютеру, т.е. демодулирует сигнал. Максимальные ско-

рости, которые достигаются при работе по данной технологии, – это 56 Кбит/с, или 7 Кбайт/с. Больших скоростей просто не предусмотрено протоколом v.92, который специфицирует работу данных устройств.

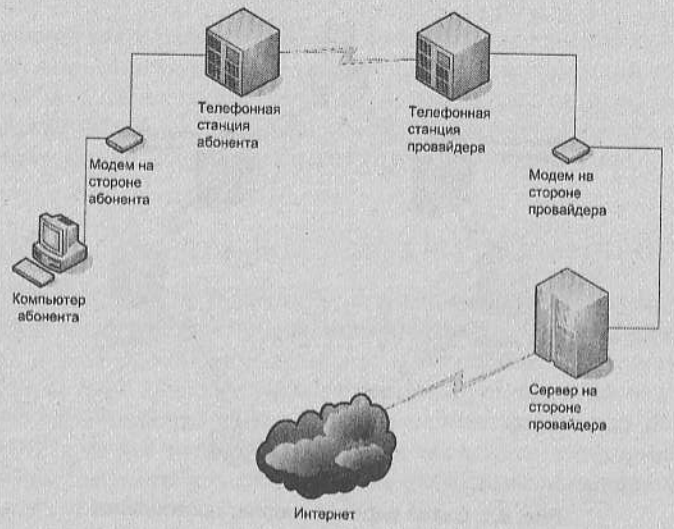


Рис. 6.2. Схема работы технологии Dial-Up

Необходимо отметить, что в силу своих многочисленных минусов, таких как постоянная занятость телефонной линии в момент соединения, низкая скорость обмена данными, нестабильная работа, данная технологий постепенно уходит в прошлое и вытесняется более современными и высокоскоростными технологиями.

Мобильные устройства и сети

Большинству пользователей ноутбуков необходим постоянный доступ к сети Интернет. Однако точки доступа сети Wi-Fi по-прежнему мало распространены, чтобы можно было мобильно подключиться к Интернету. Для мобильного доступа к сети Интернет можно использовать широко распространенные мобильные сети GSM- и CDMA-операторов. Для подключения к Интернету при помощи мобильных сетей необходим специальный модем или мобильный телефон. Скорость передачи данных в современных мобильных сетях третьего поколения может достигать значения в несколько мегабит в секунду.

ОБЗОР СОВРЕМЕННЫХ МОБИЛЬНЫХ СЕТЕЙ

На сегодняшний день наиболее распространены два стандарта цифровой мобильной связи: GSM и CDMA.

Стандарт *GSM* (Global System for Mobile Communications – глобальные системы для мобильных коммуникаций) был разработан в 1985 году.

К настоящему времени система GSM развилась в глобальный стандарт второго поколения, занимающий лидирующие позиции в мире как по площади покрытия, так и по числу абонентов.

Стандарт GSM предусматривает работу передатчиков в двух диапазонах частот: полоса частот 890–915 МГц используется для передачи сообщений с подвижной станции на базовую, а полоса 935–960 МГц – для передачи сообщений с базовой станции абоненту.

CDMA (Code Division Multiple Access) – технология сотовой системы подвижной радиосвязи, в которой используется множественный доступ с кодовым разделением каналов, была разработана и предложена для коммерческого применения компанией Qualcomm. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах или временных интервалах, сигналы CDMA распределены в непрерывном частотно-временном пространстве. Фактически метод манипулирует и частотой, и временем, и энергией.

Для увеличения скорости передачи данных в GSM-сетях и их конкуренции с CDMA-сетями были разработаны технологии пакетной передачи данных GPRS и EDGE.

GPRS (General Packet Radio Service) – это система, которая реализует и поддерживает протокол пакетной передачи информации в рамках сети GSM. Система GPRS обеспечивает мобильных пользователей высокой скоростью передачи данных и оптимально приспособлена для прерывистого трафика, характерного для сетей Интернет. На начальном этапе могут быть предложены скорости доступа от 14,4 Кбит/с (при использовании одного временного слота) до 115 Кбит/с (при объединении нескольких слотов).

EDGE была представлена в 1997 году в качестве эволюции существующего стандарта GSM. EDGE использует ту же полосу пропускания и структуру временных слотов, что и GSM. При ис-

пользовании нескольких временных слотов совместно с системой GPRS можно достичь скорости передачи 384 Кбит/с.

Бурное развитие сети Интернет привело к массовой потребности пользователей в мобильном подключении к Интернету. Для осуществления высокоскоростного мобильного подключения к сети Интернет были разработаны стандарты сотовой связи третьего поколения: W-CDMA и CDMA2000.

Согласно стандартам IMT-2000 мобильная связь третьего поколения – это интегрированная сеть, обеспечивающая скорость передачи данных: для абонентов, передвигающихся со скоростью до 120 км/ч, – не менее 144 Кбит/с, со скоростью до 3 км/ч – 384 Кбит/с, для неподвижных объектов – 2,048 Мбит/с.

Рассмотрим стандарты сотовой связи третьего поколения.

W-CDMA (другое название – UMTS, Universal Mobile Telecommunication System – универсальная система мобильной связи) – это стандарт, который принят в Европе и Японии. UMTS – это модернизация стандарта GSM. Теоретически он обеспечивает скорость передачи данных до 2 Мбит/с.

CDMA2000 – основной конкурент европейской версии UMTS. Несмотря на то что стандарты W-CDMA и CDMA2000 имеют общую аббревиатуру в своих названиях, это совершенно разные системы, использующие различные технологии. CDMA2000 имеет две фазы развития: 1XRTT, также известная как 1X, обеспечивает скорость передачи данных до 144 Кбит/с и может быть усовершенствована до второй фазы – 3XRTT (или 3X), где скорость достигает 2 Мбит/с.

Однако практическая реализация перечисленных выше стандартов связи не позволила реализовать скорости, указанные в стандарте IMT-2000. Для реализации высокоскоростного мобильного доступа к сети Интернет были разработаны специальные технологии надстройки над существующими сетями третьего поколения: для сетей CDMA2000 – EV-DO, для сетей UMTS – HSDPA.

HSDPA (High Speed Downlink Packet Access) – технология высокоскоростного пакетного доступа по входящему каналу. Стандарт позволяет увеличить скорость передачи данных в сетях 3G. Пиковая скорость передачи данных в сети HSDPA – 14,4 Мбит/с, тогда как средняя – 1–1,5 Мбит/с. Назначение HSDPA – обеспечение эффективного использования радиочастотного спектра при предоставлении услуг, требующих высокой скорости передачи

пакетных данных по нисходящим каналам, таких как доступ в Интернет и загрузка файлов. Эта технология хорошо адаптирована к условиям города и закрытых помещений. По сравнению с UMTS HSDPA можно передавать в три раза больше данных и поддерживать вдвое больше мобильных пользователей на одну соту.

Стандарт *CDMA2000 1xEV-DO* был принят TIA в октябре 2000 года. Он предусматривает следующую схему функционирования: аппарат одновременно производит поиск сети 1x и 1X EV-DO, передачу данных осуществляет с помощью 1X EV-DO, голоса – с помощью 1x. Уже разработаны четыре релиза технологии EV-DO: Revision Zero (Rev. 0), Revision A (Rev. A), Revision B (Rev. B) и Revision C (Rev.C).

Приведем реальную скорость передачи данных в мобильных сетях:

- GSM с использованием технологии GPRS: максимальная скорость загрузки данных – 115 Кбит/с, средняя — 48 Кбит/с;
- GSM с использованием технологии EDGE и GPRS: максимальная скорость загрузки данных – 207 Кбит/с, средняя – 144 Кбит/с;
- CDMA EV-DO обеспечивают максимальную скорость загрузки данных – 1 Мбит/с, среднюю –740 Кбит/с;
- UMTS HSDPA обеспечивают максимальную скорость загрузки данных – 1,8 Мбит/с, среднюю – 1,2 Мбит/с.

Примечание. Реальная скорость загрузки файлов будет уменьшаться по мере увеличения количества абонентов мобильной сети и может отличаться от приведенных выше скоростей.

Мобильное подключение к сети Интернет при помощи сетей третьего поколения позволяет комфортно использовать все приложения, с которыми пользователь привык работать, используя высокоскоростное проводное подключение. Недостаток GSM-подключения к сети Интернет не в том, что оно не в состоянии обеспечить достаточную скорость доступа к сети Интернет (100 – 200 Кбит/с для большинства задач вполне достаточно), а в том, что данное подключение не способно обеспечить приемлемое время отклика, которое даже в идеальных условиях превышает 400 мс.

ОБОРУДОВАНИЕ ДЛЯ ПЕРЕДАЧИ ДАННЫХ

Для того чтобы передавать данные при помощи мобильных сетей, пользователю необходимо специальное оборудование – GSM/CDMA-модем. Поскольку ни одна модель современного

ноутбука не обладает встроенным модемом GSM/CDMA, то его необходимо приобретать отдельно.

Проблему GSM/CDMA-модема легко решить, если пользователь использует услуги мобильной связи и у него есть мобильный телефон стандарта GSM или CDMA, поскольку все современные модели мобильных телефонов обладают встроенным модемом. Однако если у пользователя нет мобильного телефона или нужно подключиться к мобильной сети другого стандарта, то необходимо приобрести соответствующий мобильный телефон или специальный модем.

Если мобильная сеть требуется лишь для мобильного подключения к сети Интернет, то можно вместо мобильного телефона приобрести GSM/CDMA-модем, предназначенный только для передачи данных и отправки SMS-сообщений.

Современные GSM/CDMA-модемы могут подключаться к ноутбуку при помощи трех наиболее распространенных интерфейсов: USB, PCMCIA или ExpressCard.

Наиболее популярные модели модемов для ноутбуков выполнены в виде PCMCIA-карт расширения (рис. 6.3). Однако если пользователю необходим мобильный доступ к сети Интернет не только с ноутбука, но и со стационарного ПК, то наиболее выгодной будет покупка USB-модема (рис. 6.4).

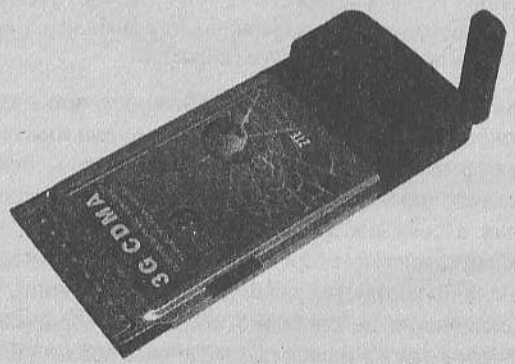


Рис. 6.3. CDMA PCMCIA-модем

Все чаще ноутбуки стали оснащаться новым высокоскоростным разъемом расширения ExpressCard, в продаже стали появляться ExpressCard-модемы (рис. 6.5).

Рис. 6.4. CDMA USB-модем

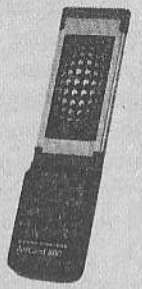


Рис. 6.5. UMTS HSDPA ExpressCard-модем

Модемы ExpressCard можно при помощи специального переходника (рис. 6.6) использовать в ноутбуках с разъемом PCMCIA. Таким образом, если пользователь планирует модернизировать свой ноутбук путем покупки нового, то наиболее выгодной будет покупка ExpressCard-модема, поскольку его можно будет использовать и в новых моделях ноутбуков.

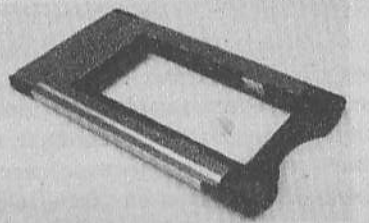


Рис. 6.6. Переходник PCMCIA – ExpressCard

G.SHDSL

Это технология из семейства xDSL (Digital Subscribe Line, цифровые абонентские линии), которое крайне привлекательно для провайдеров интернет-услуг в качестве решения проблемы «последней мили».

Семейство xDSL включает в себя множество протоколов, таких как ADSL, HDSL, SHDSL, G.SHDSL. В последнее время широкое распространение получили G.SHDSL и ADSL. Рассмотрим технологию G.SHDSL.

Данная технология позволяет передавать по обычной телефонной линии данные со скоростью до 2,3 Мбит/с (на сегодняшний день существуют так называемые Dual G.SHDSL-модемы, позволяющие объединять две физические медные линии в одну виртуальную и получать скорость до 4,6 Мбит/с). Данные передаются в синхронном режиме, т.е. и входящий, и исходящий поток передается с одинаковой скоростью. Эта технология рассчитана больше на корпоративный сектор использования, так как, во-первых, в домашнем обиходе синхронный канал не имеет большого значения, поскольку пользователей больше интересует скорость получения информации, а не скорость отправки, а во-вторых, влечет за собой существенные затраты на оборудование и организацию линии.

Схема работы технологии G.SHDS заключается в том, что на стороне провайдера и на стороне клиента устанавливаются специализированные модемы и между ними происходит организация информационного канала, причем телефонный аппарат к этой линии подключить уже нельзя. Эта телефонная линия будет использоваться только под услуги доступа к Интернету.

ADSL

ADSL расшифровывается как Asymmetric Digital Subscriber Line (Ассиметричная цифровая абонентская линия). В настоящий момент данная технология получает все большее и большее распространение. Благодаря ей обычная телефонная линия может превратиться в высокоскоростную цифровую линию передачи информации. На сегодняшний день максимальные скорости, которые могут достигаться по технологии ADSL – до 6 Мбит/с. Работа по технологии ADSL позволяет одновременно использовать и услуги телефонии, и услуги передачи доступа. Схема работы технологии ADSL достаточно проста (рис. 6.7): для разделения телефонной линии для услуг телефонии и ADSL используются частотные делители, или так называемые «сплитеры». К такому устройству подключается ADSL-модем и обычный телефонный аппарат, а оно, в свою очередь, включается в телефонную линию. На стороне провайдера тоже стоит сплитер, который разделяет сигнал на сервер данных и на телефонное оборудование.

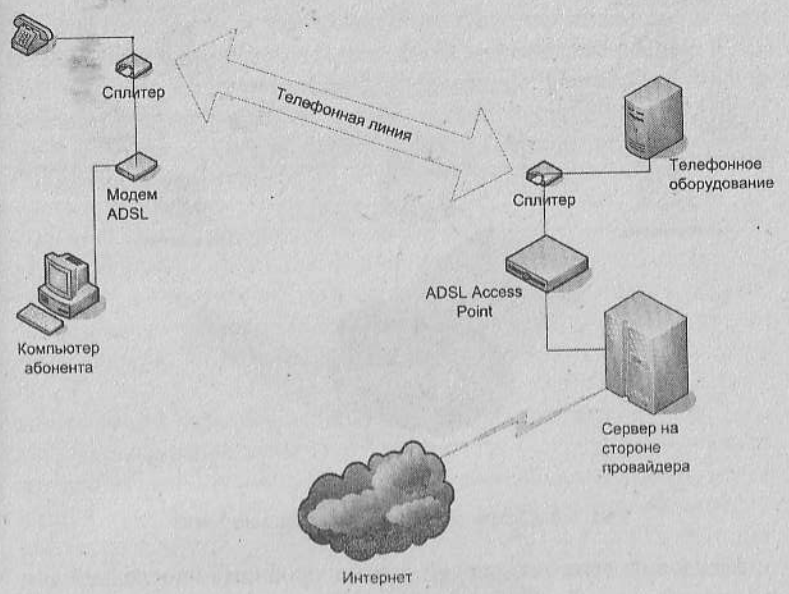


Рис. 6.7. Схема работы технологии ADSL

В настоящее время основным конкурентом технологии ADSL являются так называемые «домашние сети». Основным плюсом, который предоставляют домашние сети, является широкий спектр сетевых услуг и ресурсов, таких как множество музыки, фильмов, программ, которые внутри сети доступны для скачивания бесплатно и со скоростью гораздо более высокой, чем скорость доступа в Интернет. Различные чаты, форумы, порталы и тому подобное, разнообразие внутрисетевых сервисов зависит только от фантазии провайдера и его желания уделять этому время и средства.

Домашние сети

Данная технология подразумевает под собой подключение с помощью технологии Ethernet. Компьютеры пользователей связываются по технологии «звезда» с помощью обычной витой пары, объединяются в подсети и подключаются к одному глобальному узлу с широким каналом доступа к Интернету (рис. 6.8). Таким образом, пользователи могут беспрепятственно обмениваться информацией друг с другом, не используя при этом глобальную сеть.

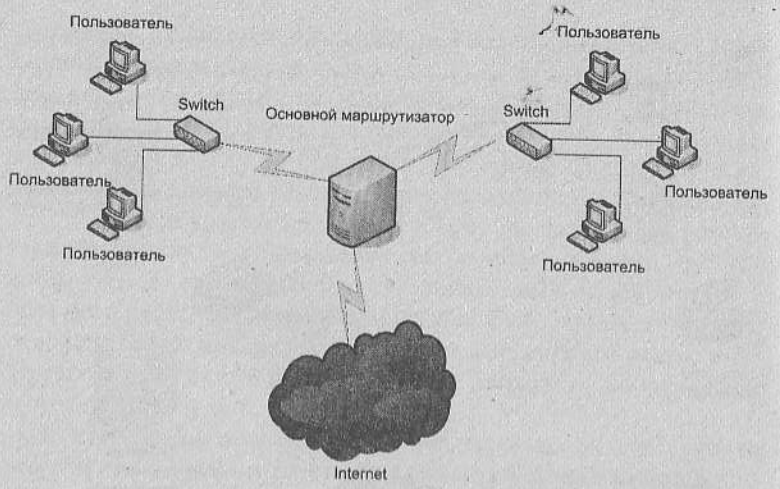


Рис. 6.8. Схема технологии «домашние сети»

Каждая из этих технологий решает проблему «последней мили» доступа от абонента к оборудованию провайдера для дальнейшего доступа к сети Интернет. В настоящий момент наиболее распространенными являются технологии ADSL и «домашние сети». В ряде случаев, когда подключение по иной технологии просто невозможно, используется технология Dial-Up.

Оборудование для подключения

Оборудование, которое используется для подключения к «домашней сети», уже было упомянуто. Со стороны пользователя – это обычная сетевая карта (рис. 6.9), к которой подключается кабель «витая пара». Со стороны провайдера кабель подключается к коммутационному сетевому устройству Hub или Switch, как было показано на рис. 6.8.

Для подключения с помощью технологии ADSL необходим ADSL-модем (рис. 6.10) и все та же сетевая карта. Модем с помощью порта Ethernet подключается к сетевой карте, а с помощью порта RJ-11 – к телефонной линии.

Для подключения по технологии Dial-Up используются или внешние аналоговые модемы (рис. 6.11), или внутренние (рис. 6.12). Как правило, внешние модемы применяются для подключения в условиях зашумленных АТС, где трудно достичь качественного сигнала в линии. Они на порядок дороже внутренних, но в то же время и надежнее.

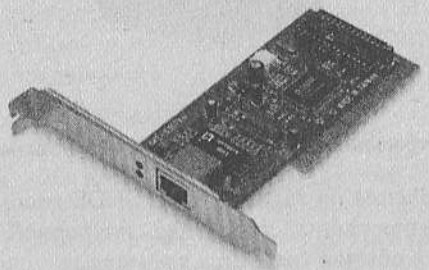


Рис. 6.9. Сетевая карта D-link

Рис. 6.10. ADSL-модем

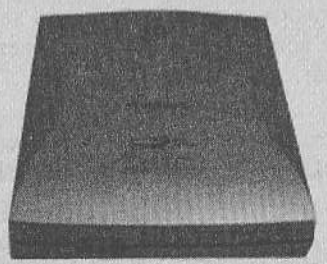


Рис. 6.11. Внешний модем для подключения по технологии Dial-Up

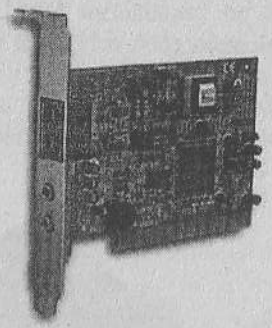


Рис. 6.12. Внутренний модем для подключения по технологии Dial-Up

Для подключения по технологии G.SHDS необходимо приобрести специализированный модем для синхронной передачи данных. Более того, обычно требуется два модема – для установки на стороне абонента и на стороне провайдера (рис. 6.13).

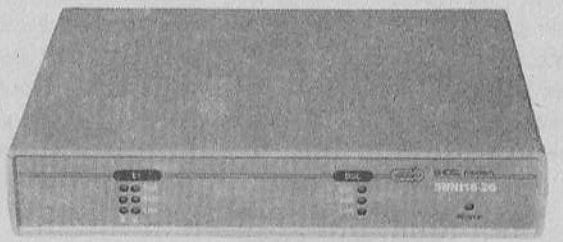


Рис. 6.13. G.SHDSL-модем

Какую же технологию выбрать, к какому именно провайдеру подключится, по каким критериям оценить качество работы провайдера? На такие вопросы необходимо ответить при подключении к сети Интернет.

Критерии выбора провайдера, предоставляющего услуги доступа к глобальной сети Интернет

Прежде всего, нужно определиться, по какой технологии выгоднее подключаться в каждом конкретном случае.

ADSL

Технология ADSL отличается следующими преимуществами:

- высокая скорость доступа к сети Интернет (от 64 Кбит/с до 6 Мбит/с);
- достаточно низкая стоимость безлимитного канала доступа (около 500 руб. за канал в 512 Кбит/с без учета трафика);
- незанятость телефонной линии;
- невысокая стоимость оборудования (около 700 руб. за модем);
- невысокая стоимость подключения (около 600 руб. первичный платеж за подключение).

Минусами данной технологии являются:

- отсутствие внутренних ресурсов, таких как фильмы, музыка, программы, – все ресурсы необходимо скачивать из Интернета;
- привязка строго к одному телефонному оператору, нельзя подключаться к разным операторам, как при технологии Dial-Up;
- стоимость оборудования выше, чем при подключении к «домашней сети»;
- негарантированная скорость передачи.

G.SHDSL

Технология G.SHDSL предоставляет следующие возможности:

- синхронная технология передачи данных;
- высокая скорость передачи данных – порядка 2 Мбит/с в обе стороны;
- стабильная гарантированная скорость передачи.

Из минусов данной технологии можно отметить:

- высокую стоимость оборудования – около 2500 руб. за модем;
- необходимость покупки двух модемов;
- необходимость отдельной выделенной линии;
- привязку строго к одному телефонному оператору, нельзя подключаться к разным операторам, как при технологии Dial-Up.

ДОМАШНИЕ СЕТИ

Технология «домашние сети» имеет следующие преимущества:

- высокую скорость передачи данных внутри сети;
- как правило, наличие развитой сетевой инфраструктуры с большим количеством ресурсов;
- низкую стоимость оборудования, так как обычно сетевые карты уже встроены в материнскую плату;
- не требуется телефонной линии.

К минусам этой технологии можно отнести следующие ограничения:

- высокую стоимость безлимитных каналов передачи данных (около 600–700 долларов за канал 64 Кбит);
- привязку к одному провайдеру.

DIAL-UP

Технология Dial-Up также имеет определенные плюсы:

- определенная мобильность, нет привязки к одному провайдеру;
- почасовая форма оплаты услуг;
- имеется возможность call-back (когда провайдер перезванивает абоненту для исключения оплаты за услуги телефонной связи);
- при использовании внутреннего модема – низкая стоимость оборудования.

Минусов же у этой технологии значительно больше:

- низкая скорость передачи данных (до 56 Кбит/с);
- нестабильность связи;
- зависимость от количества соединений к провайдеру: чем больше абонентов подсоединилось к провайдеру, тем ниже шансы дозвониться к нему;
- занятость телефонной линии;
- при использовании внешних модемов высокая стоимость оборудования;
- отсутствие внутренних ресурсов, таких как фильмы, музыка, программы, – все ресурсы необходимо скачивать с сети Интернет;
- даже если ресурсы и имеются, то скачать их проблематично в связи с низкой скоростью.

В табл. 6.1 приведены сравнительные характеристики каждой из технологий для облегчения выбора.

Таблица 6.1

Сравнительная характеристика различных технологий подключения к глобальной сети Интернет

Критерий	ADSL	Dial-Up	G.SHDSL	«Домашние сети»
Привязка к одному провайдеру	+	–	+	+

Критерий	ADSL	Dial-Up	G.SHDSL	«Домашние сети»
Высокая стоимость оборудования	–	–/+	+	–
Высокая скорость доступа к сети Интернет	+	–	+	+
Достаточно низкая стоимость безлимитного канала доступа	+	–	–	–
Незанятость телефонной линии	+	–	+/–	+
Невысокая стоимость подключения	+	+	–	+
Отсутствие внутренних ресурсов, таких как фильмы, музыка, программы	+	+/–	+/–	–
Негарантированная скорость передачи	+	+	–	–
Стабильная гарантированная скорость передачи	–	–	+	–
Необходимость покупки двух модемов	–	–	+	–
Необходимость отдельной выделенной линии	–	–	+	–
Не требуется телефонной линии	–	–	+/–	+

Критерий	ADSL	Dial-Up	G.SHDSL	«Домашние сети»
Нестабильность связи	–	+	–	–
Почасовая форма оплаты услуг	–	+	–	–
Имеется возможность call-back	–	+	–	–
Синхронная технология передачи данных	–	–	+	–

Для того чтобы выбрать провайдера, необходимо определиться, по какой технологии выгоднее подключаться. Проанализировав изложенный выше материал, можно сделать вывод, что наиболее привлекательными являются технологии ADSL и «домашние сети». После того как определились с выбором технологии, необходимо провести анализ рынка провайдеров для выбора оптимального. Обратить внимание необходимо на:

- стоимость подключения;
- стоимость услуг;
- разнообразие услуг;
- стабильность работы;
- как быстро реагирует провайдер на поломки.

Ну и конечно, следует выбирать из тех провайдеров, которые поддерживают ту технологию подключения, которая была выбрана как оптимальная.

Подключение по технологии ADSL

Прежде всего, необходимо выбрать провайдера, предоставляющего услугу ADSL и купить ADSL-модем. Настройки модема зависят от того, какие параметры соединения предоставляет провайдер. В рамках данной книги настройка непосредственно модема не рассматривается из-за широкого спектра настроек модемов в зависимости от их производителя и требований провайдера.

Необходимо только упомянуть, что модем может работать в двух режимах:

- режим «бридж»;
- режим «роутер».

В режиме «бридж» модем создает виртуальный канал между компьютером пользователя и сервером провайдера, для пользователя данный режим подразумевает полную «прозрачность» модема. Все функции по фильтрации трафика, ограничению пропускной способности, маршрутизации берет на себя компьютер пользователя. При данном режиме компьютер напрямую обращается к серверу, и именно сервер провайдера выдает IP-адрес компьютеру и является его шлюзом по умолчанию (рис. 6.14).

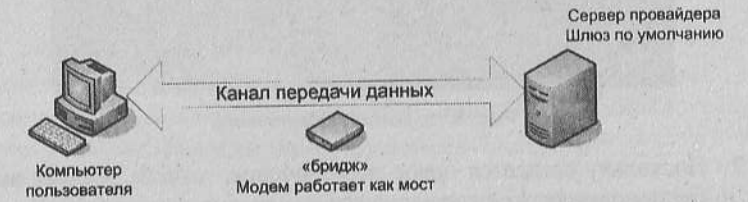


Рис. 6.14. Работа модема ADSL в режиме «бридж»

В режиме работы «роутер» ваш компьютер не открыт напрямую для доступа из Интернета, все общение происходит через модем, на него возложены функции маршрутизации и фильтрации трафика. В данном случае модем получает IP-адрес от провайдера, а адрес для вашего компьютера выбирается непосредственно вами из одной подсети с модемом (рис. 6.15).

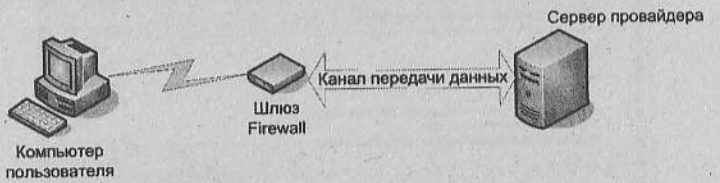


Рис. 6.15. Работа модема ADSL в режиме «роутера»

Рассмотрим настройку системы в случае, если модем работает в режиме «бридж».

Примечание. В режиме «роутер» настройка компьютера сводится к настройке сетевого соединения, что уже было рассмотрено.

5. После выбора варианта подключения отображается окно для ввода регистрационных данных, которые предоставил провайдер при заключении договора. (рис. 6.20).

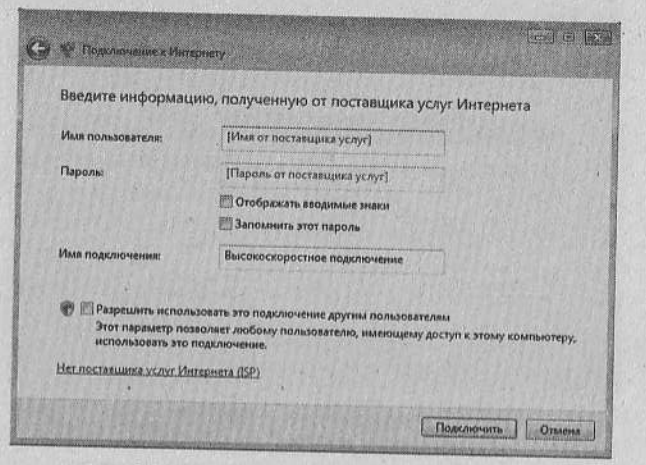


Рис. 6.20. Форма ввода регистрационных данных

Также предлагается отметить три опции:

- *Отображать вводимые знаки* – рекомендуется выбрать в первый раз, для того чтобы исключить ошибку при вводе регистрационных данных;

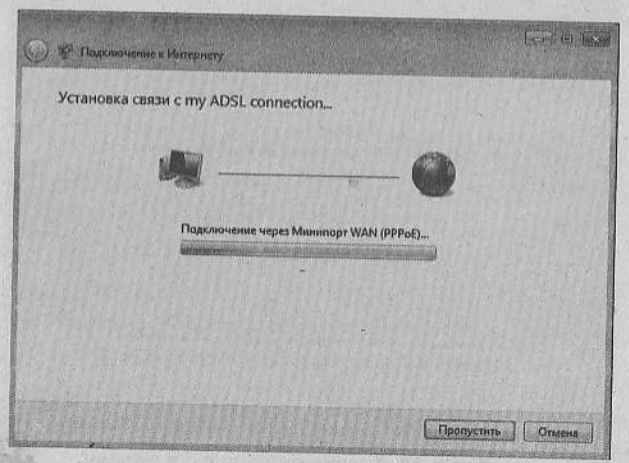


Рис. 6.21. Процесс подключения к Интернету

- *Запомнить этот пароль* – рекомендуется отметить, если нет каких-либо определенных ограничений на выход в Интернет для всех пользователей, работающих под данной учетной записью;
- *Разрешить использование этого подключения другим пользователям* – данный параметр позволяет сделать подключение доступным для всех пользователей этого компьютера.

6. После нажатия кнопки *Подключить* система попытается произвести соединение с Интернетом по созданному подключению (рис. 6.21).

Подключение по технологии Dial-Up

Рассмотрим подключение к Интернету с помощью технологии Dial-Up. Для настройки подключения необходимо выполнить следующие действия:

1. Открыть меню *Пуск* | *Подключения*, как и в случае с настройкой подключения с помощью технологии ADSL.
2. Выбрать пункт *Установка подключения или сети* (рис. 6.22).

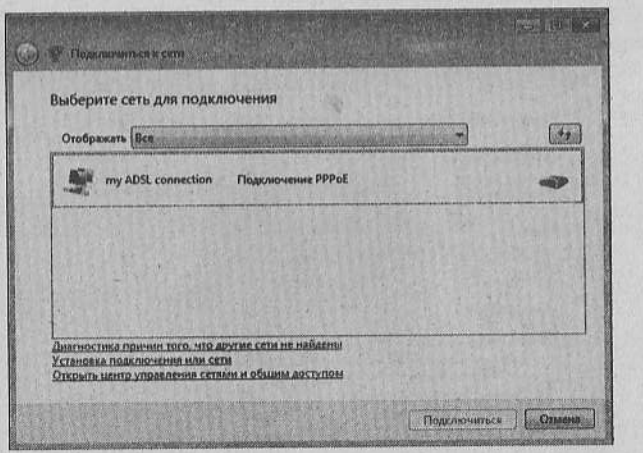


Рис. 6.22. Установка соединения или сети

3. Выбрать подменю *Варианты подключения*. При подключении по технологии Dial-Up нужно указать вариант *Настройка телефонного подключения* (рис. 6.23).

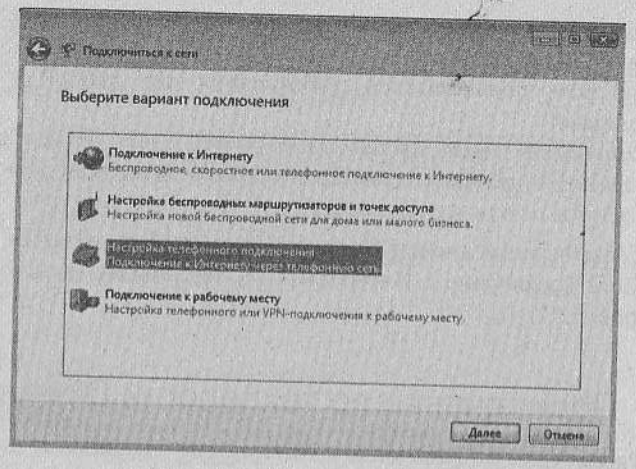


Рис. 6.23. Варианты подключения

4. Далее следует ввести регистрационные данные для этого подключения. Регистрационные данные, как и в случае с подключением по технологии ADSL, выдаются провайдером услуг подключения к Интернету (рис. 6.24).

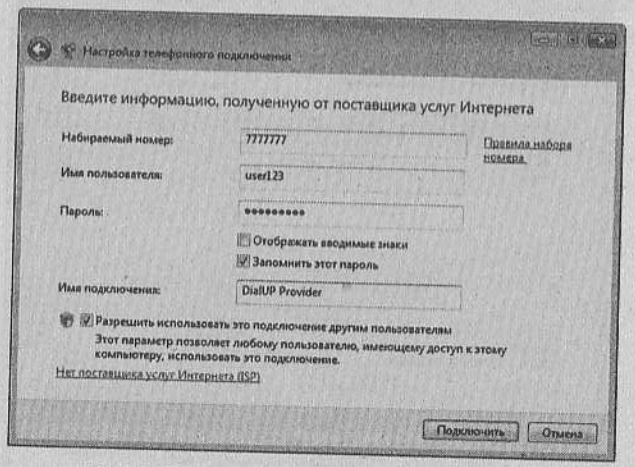


Рис. 6.24. Настройка регистрационных данных

После заполнения необходимых полей нужно нажать кнопку *Подключить*. Если все устройства подключены верно, регистрационные данные заполнены в соответствии с указанными провайдером, телефонный номер, на который происходит в данный момент дозвон, не занят, помехи на телефонной линии в пределах нормы, то произойдет подключение к сети Интернет по технологии Dial-Up.

Подключение по технологии GPRS

Настройка GPRS-соединения на компьютере пользователя по сути ничем не отличается от настройки обычного модемного соединения, поскольку телефон в данном случае и выступает в качестве GPRS-модема.

Рассмотрим подключение и настройку соединения GPRS для оператора МТС с использованием телефона Motorola C390 (данное устройство включает в себя GPRS-модем, который и необходим для организации такого доступа).

Итак, рассмотрим пошагово, что необходимо сделать, чтобы подключиться к Интернету с помощью мобильного телефона:

1. Загрузить операционную систему.
2. Подключить устройство с помощью специального интерфейсного кабеля (рис. 6.25) к порту USB на стационарном компьютере или ноутбуке.

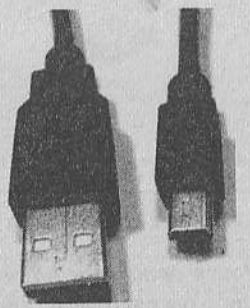


Рис. 6.25. Внешний вид интерфейсного кабеля miniUSB

3. Система обнаружит новое устройство и запустит мастер подключения нового оборудования, который предложит произвести поиск драйвера в Интернете. На этом шаге перейти к пункту *Не выполнять поиск в Интернете* (рис. 6.26).

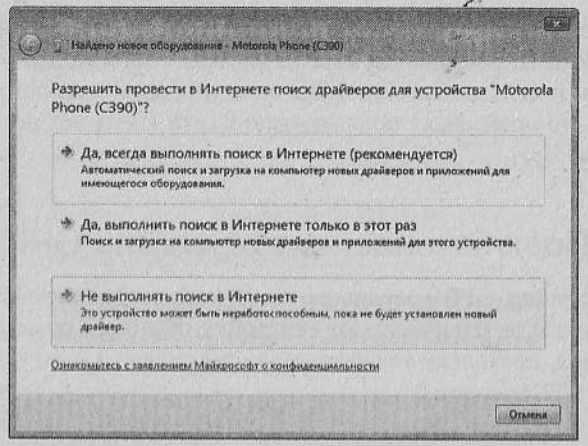


Рис. 6.26. Поиск драйверов в Интернете

4. На следующем шаге мастер предложит произвести поиск на этом компьютер, включая CD-диски. Если диск с драйверами есть, необходимо вставить его в CD/DVD привод – система выполнит поиск и инсталляцию драйвера, если нет – попросить показать другие возможности (рис. 6.27).

Рис. 6.27. Поиск драйверов на CD-диске

5. Выбрать пункт *Поиск драйверов на этом компьютере* и указать папку, куда распакованы драйверы для модема (рис. 6.28).
6. После установки драйверов отобразится сообщение об успешном завершении операции.
7. Проверить наличие модема в системе можно, открыв раздел *Модемы* в Диспетчере устройств (*Пуск* | *Панель управления* | *Диспетчер устройств* | *Модемы*, рис. 6.29).

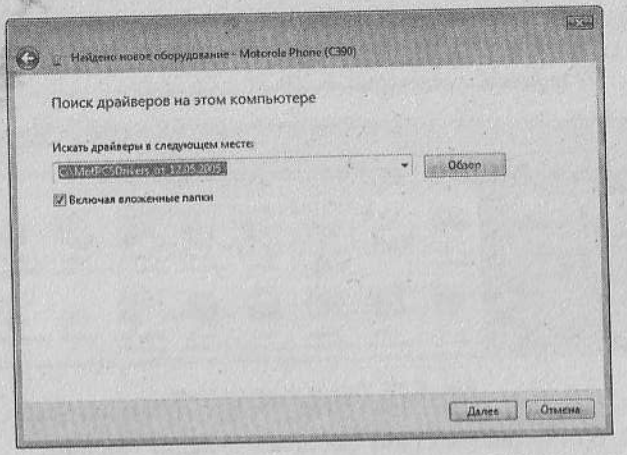


Рис. 6.28. Поиск драйверов на жестком диске

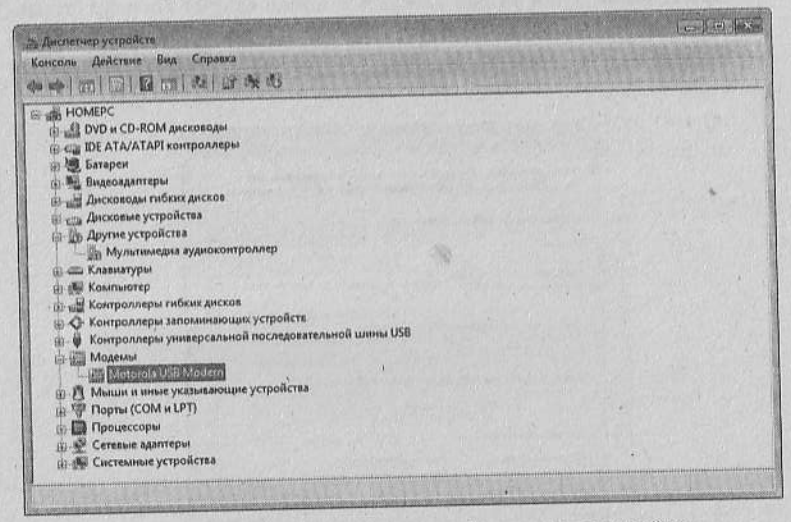


Рис. 6.29. Установленный модем в Диспетчере устройств

8. Теперь необходимо создать подключение к сети Интернет с использованием телефонного соединения, как и в случае с Dial-Up. Следует отметить, что есть некоторые тонкости в настройке параметров телефонов различных моделей. Информацию о конкретных настройках для каждой модели можно получить на сайте МТС http://mts.ru.

Следуем рекомендациям по настройке модема:

1.1. Открываем меню *Пуск* | *Настройка* | *Панель управления* | *Телефон и модем* (рис. 6.30).

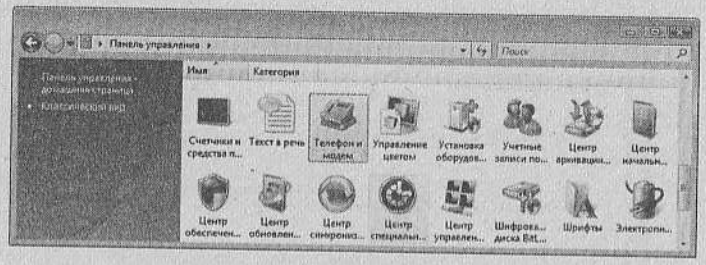


Рис. 6.30. Управление модемами

1.2. В открывшемся окне выбираем вкладку *Модемы*.

Примечание. Если раздел *Телефон и модем* открыт впервые, то может появиться окно *Сведения о местонахождении*. Необходимо ввести *Телефонный код города* (для Москвы – 495), выбрать *Тип набора номера* (тоновый набор) и нажать *ОК* (рис. 6.31).

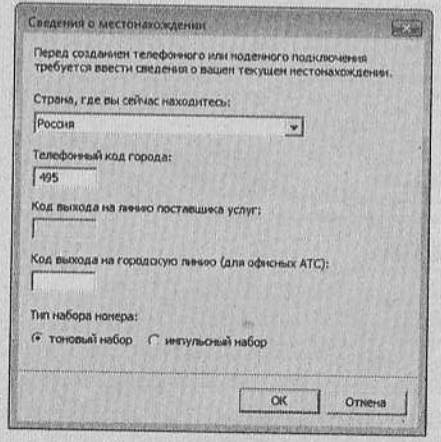


Рис. 6.31. Установка кода города и типа набора

1.3. Выбираем установленный модем и нажимаем кнопку *Свойства* (рис. 6.32).

1.4. В окне *Свойства модема* на вкладке *Общие* нажимаем кнопку *Изменить параметры*.

1.5. В появившемся окне переходим на вкладку *Дополнительные параметры связи* и вводим предоставленную оператором строку инициализации (рис. 6.33).

1.6. Нажимаем кнопку *ОК*. На этом настройка модема закончена.

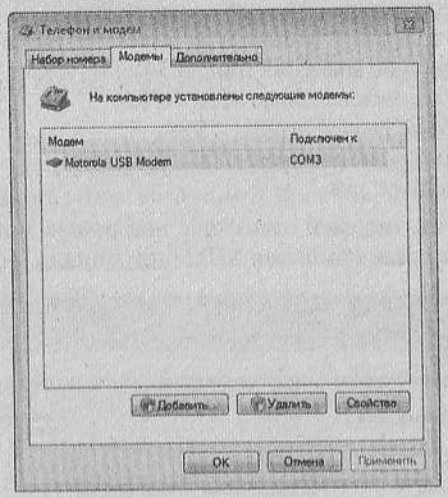


Рис. 6.32. Выбор модема

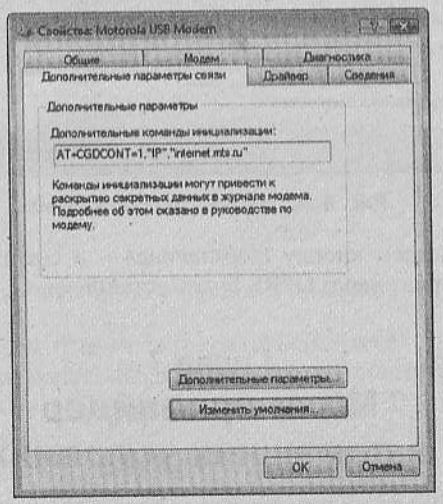


Рис. 6.33. Параметры инициализации модема

2. Далее необходимо настроить соединение (аналогична Dial-Up, отличие лишь в набираемом номере).
   2.1. Открываем *Пуск | Сеть | Центр управления сетями и общим доступом | Установка подключения или сети | Настройки телефонного соединения.*
   2.2. Для телефона Motorola в качестве параметров вводим следующие значения (рис. 6.34):
   - *Имя подключения*: MTS GPRS
   - *Набираемый номер*: *99#
   - *Имя пользователя*: mts
   - *Пароль*: mts

Для других моделей телефона настройки можно найти на официальном сайте компании МТС http://mts.ru.

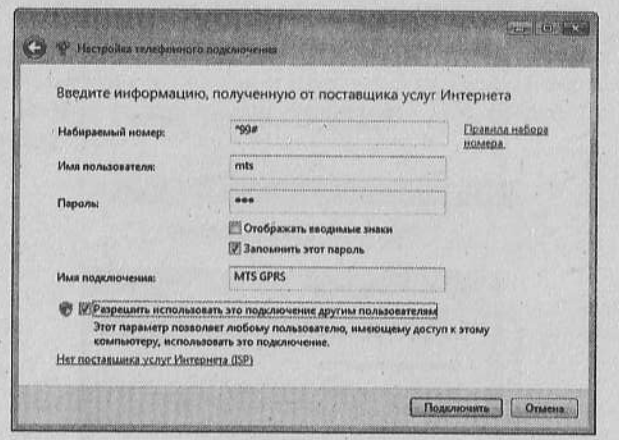


Рис. 6.34. Параметры подключения

2.3. Нажимаем кнопку *Подключить* – и соединение с сетью Интернет через GPRS будет установлено.

Глава 7
Мини-провайдер в домашних условиях

В этой главе рассматриваются вопросы предоставления общего доступа к сети Интернет для всех пользователей локальной сети. Распределение интернет-трафика между компьютерами рассматривается на примере использования специализированного программного обеспечения UserGate. Особое внимание уделяется настройке этой программы, нюансам и тонкостям работы различных сетевых технологий.

Варианты подключения сети к Интернету

Итак, сеть организована, соединения настроены, программы установлены. Что же еще можно полезного сделать, получив доступ к глобальной сети Интернет? Конечно, можно скачивать музыку, фильмы, программы, общаться с друзьями по всему миру, читать много полезных книг, статей, обзоров. Однако это далеко не весь перечень выгод, которые приносит подключение к Интернету.

Предположим, что сначала была организована одноранговая локальная сеть из пяти компьютеров (рис. 7.1)

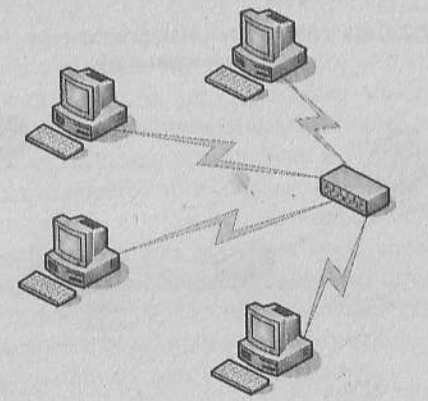


Рис. 7.1. Простая одноранговая сеть

В дальнейшем был приобретен ADSL-модем для подключения к сети Интернет. Подключить его к существующей сети можно по-разному. В первом случае (рис. 7.2) каждый пользователь сети будет иметь равноценный доступ к Интернету, не будет никаких ограничений, никакой тарификации.

Во втором же случае один компьютер будет выполнять роль своеобразного сервера, на котором будет установлено специализи-

рованное программное обеспечение для организации доступа, ограничения доступа, ограничения трафика, тарификации. Также на этом компьютере будет установлено две сетевые карты: одна – для связи с локальной сетью, а вторая – для выхода в Интернет (рис. 7.3).

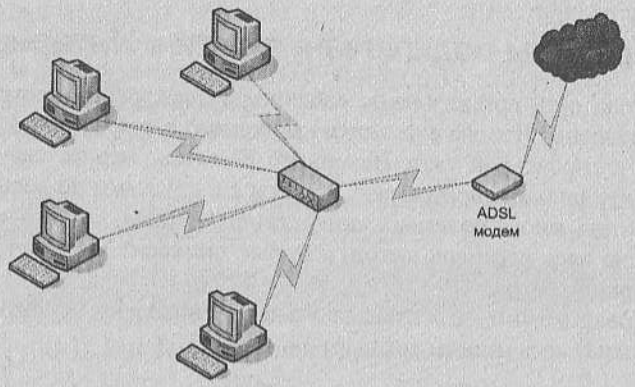


Рис. 7.2. Сеть с равноценным доступом к сети Интернет всех пользователей

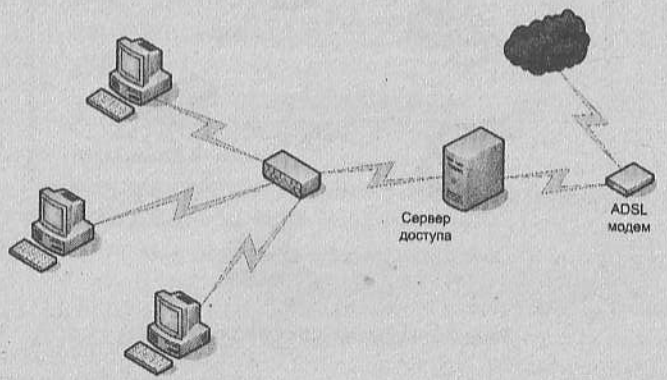


Рис. 7.3. Сеть с выделенным сервером

Данная схема подходит для организации так называемого «мини-провайдера». Организация сети по такой схеме имеет следующие плюсы:

- контроль доступа пользователей к ресурсам;
- контроль полосы пропускания для каждого пользователя;

- подсчет и экономия трафика;
- расширенные функции защиты;
- возможность предоставления услуг доступа к сети Интернет за определенную плату.

Конечно же, существуют и минусы, но их гораздо меньше:

- достаточная сложность настройки;
- необходим постоянно включенный сервер.

Таким образом, организация подобного провайдера при определнных условиях принесет много плюсов, начиная от колоссального опыта работы с различными сетевыми технологиями и заканчивая финансовой выгодой.

Прежде чем приступать к настройке программного обеспечения, рассмотрим используемые при организации мини-провайдера технологии.

Применяемые технологии

Proxy server (прокси-сервер) – это сервер-посредник между клиентским компьютером и Интернетом. Он выполняет функции обработки веб-содержимого, передаваемого между клиентом и сетью. Основными задачами прокси-сервера являются:

- обеспечение множественного доступа к Интернету с использованием одного внешнего IP-адреса;
- гибкое управление доступом пользователя к веб-содержимому и возможность ограничить доступ к определенным ресурсам как полностью, так и частично по заданным правилам;
- управление полосой пропускания для каждого пользователя;
- ускорение загрузки страниц за счет сохранения часто используемой информации на диск (кэширование).

Схема работы прокси-сервера достаточно проста (рис. 7.4).

Технология *NAT (Network Address Translation, трансляция сетевых адресов)* предназначена для предоставления множественного доступа к сети Интернет с помощью одного IP-адреса. Схема работы напоминает работу прокси-сервера, однако в более ограниченном варианте. NAT позволяет преобразовывать адреса, но не позволяет контролировать трафик (рис. 7.5).

Firewall (Брандмауэр, межсетевой экран) – данная технология позволяет защитить как отдельные компьютеры, так и всю

сеть от вредоносных действий злоумышленников. Правильно настроенный межсетевой экран позволит наряду с антивирусом и постоянными обновлениями программного обеспечения (ПО) свести риск успешной атаки на сеть или на отдельный компьютер к минимуму.

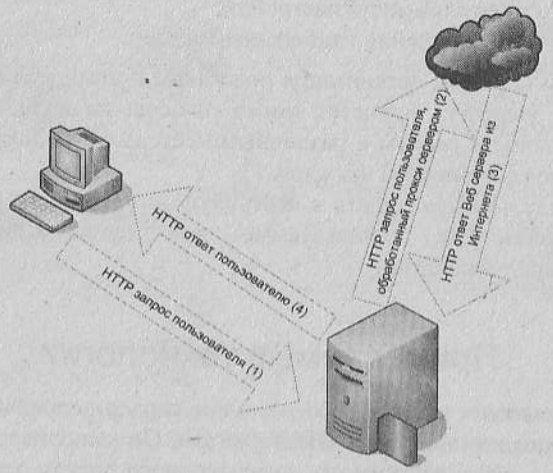


Рис. 7.4. Схема работы прокси-сервера

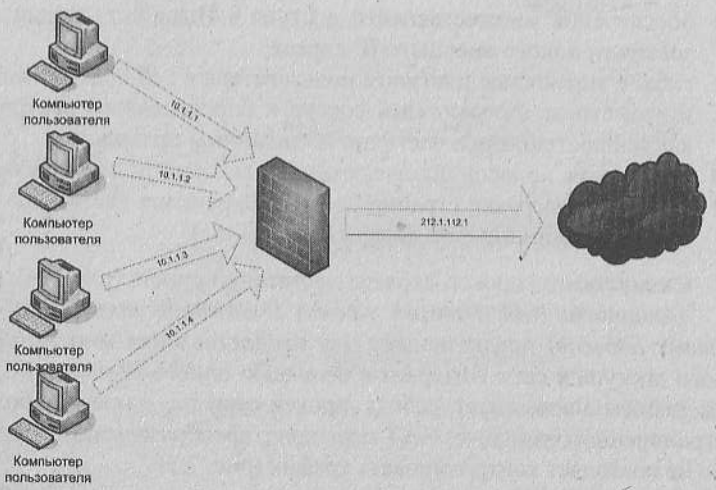


Рис. 7.5. Схема работы технологии NAT

Схема работы брандмауэра проста. Он стоит как бы на входе в сеть и сверяет все приходящие пакеты по сети с правилами, которые настроены заранее, и в соответствии с этими правилами либо блокирует пакеты, либо пропускает их в сеть, либо применяет иные действия (более подробно о брандмауэрах будет рассказано во второй части этой книги).

Таков краткий перечень технологий, применяемый при организации мини-провайдера. Теперь необходимо выбрать программное обеспечение, удовлетворяющее всем потребностям будущего провайдера. Прежде чем приступать к выбору и настройке ПО, нужно определиться, какими функциями должна обладать система управления мини-провайдером:

- предоставление общего доступа к Интернету;
- подсчет трафика;
- индивидуальное ограничение полосы пропускания;
- функции прокси-сервера;
- сбор и обработка статистики по каждому пользователю;
- возможность указания каждому пользователю индивидуального тарифного плана;
- авторизация пользователей.

Программа UserGate

UserGate – это комплексная программа для предоставления множественного доступа пользователей к сети Интернет с использованием одного IP-адреса. Программа поддерживает NAT для обеспечения правильной работы тех протоколов, которые не может обработать прокси-сервер. В программу встроен брандмауэр для защиты сети от вторжений и модуль подсчета трафика для детального подсчета трафика индивидуально для каждого пользователя.

UserGate используется для контроля и мониторинга интернет-соединений, учета трафика, контроля трафика, установки различных ограничений и правил работы для пользователей и просмотра статистики работы.

Отличительными особенностями UserGate является гибкое управление ограничениями по каждому пользователю, удобные средства мониторинга сети, встроенная система подсчета трафика и ряд дополнительных сервисов для администратора сети.

Рассмотрим функциональные возможности данной программы более подробно:

- кэширование – сохранение загруженных из Интернета файлов в общей кэш-памяти;
- защита сервера от интернет-атак (встроенный брандмауэр);
- авторизация пользователей по различным критериям;
- гибкая система ограничений трафика для каждого пользователя и группы пользователей, при превышении которых доступ в Интернет для пользователя автоматически закрывается;
- индивидуальные ограничения скорости доступа;
- фильтры веб-содержимого;
- каскадное подключение к нескольким прокси с возможностью авторизации;
- автоматическая и ручная рассылка пользователям информации по электронной почте об их трафике;
- мониторинг и учет трафика (NAT) в режиме реального времени;
- автоматический расчет стоимости работы пользователя в Интернете, исходя из индивидуально заданной цены времени и/или объема трафика;
- гибкий генератор отчетов;
- поддержка протоколов HTTP, FTP, POP3, SMTP, IMAP4, Telnet, IRC, NNTP, ICQ и многие другие.

УСТАНОВКА USERGATE

Прежде всего, рассмотрим этапы установки данного программного обеспечения. Получить 30-дневную ознакомительную версию можно на сайте продукта http://www.usergate.ru. Там же можно получить необходимую техническую поддержку по установке и конфигурированию программного продукта.

Приступим к установке программного продукта. Распаковываем архив с программой и запускаем программу setup.exe. Следующим шагом выбираем язык установки, по умолчанию – русский. Соглашаемся с условиями лицензионного договора, иначе программа просто не продолжит свою установку, и выбираем компоненты, которые необходимы для работы. Остановимся на них подробнее:

- *Сервер UserGate* – непосредственно сама программа;
- *Драйвер NAT* – драйвер, реализующий функцию преобразования сетевых адресов, о которой было сказано выше;

- *Утилита статистики* – предназначена для просмотра статистики работы пользователей и содержит информацию о параметрах соединений всех пользователей, такую как время соединения, длительность соединения, потраченные денежные средства, адреса, к которым обращался пользователь, количество полученной и переданной информации из сети;
- *Клиент авторизации* – это клиентская программа для UserGate, которая позволяет пользователю применять альтернативные способы авторизации. Дело в том, что в UserGate предусмотрено несколько способов авторизации: по IP, по MAC и IP, по диапазону IP, через веб-интерфейс и через клиент. Более подробно каждый способ авторизации будет рассмотрен ниже. Кроме того, клиентская программа позволяет пользователю ознакомиться со своим счетом, количеством полученных/отправленных Мбайт при подключении к серверу;
- *Утилита администрирования* – является средством управления сервером UserGate. С его помощью осуществляется настройка сервера в соответствии с необходимыми требованиями;
- *UserGate Agent* – данная утилита предназначена для мониторинга работы прокси-сервера.

Рекомендуется выбирать все компоненты для установки, поскольку они понадобятся в дальнейшей работе с прокси-сервером (рис. 7.6).

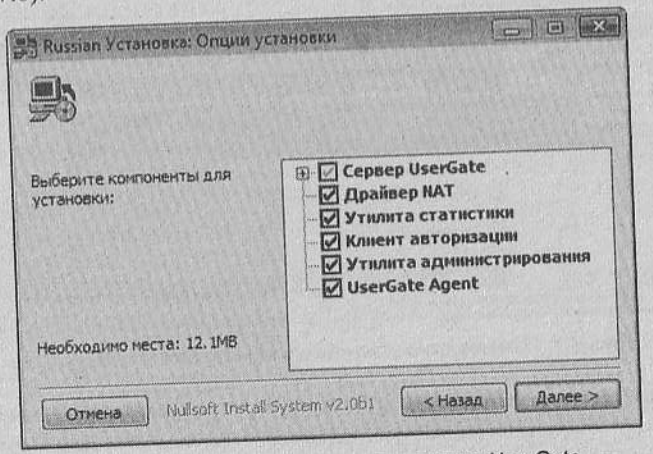


Рис. 7.6. Выбор компонентов установки UserGate

Далее программа установки предложит выбрать место, куда будет установлен данный программный продукт, по умолчанию C:\Program Files\UserGate4. Если это необходимо, выбираем альтернативный путь для установки и нажимаем кнопку *Установить*. После установки система потребует перезагрузки. На этом этапе установка приложения закончена.

КОНФИГУРИРОВАНИЕ USERGATE

После перезагрузки рекомендуется установить UserGate как сервис. Это необходимо для того, чтобы каждый раз после перезагрузки системы прокси-сервер запускался автоматически в фоновом режиме. Для этого следует выполнить команду меню *Пуск | Программы | UserGate4 | Install Service*. Теперь UserGate появится в списке сервисов системы. Перейдем непосредственно к конфигурированию UserGate.

Для того чтобы попасть в программу администрирования UserGate, необходимо щелкнуть правой кнопкой мыши по значку *UserGate Agent* в панели задач и выбрать *Start UserGate Administrator* (рис. 7.7). Откроется главное окно утилиты администратора UserGate.

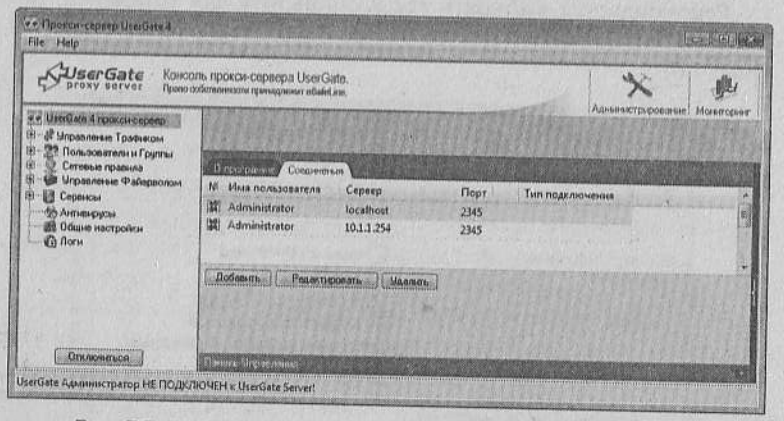


Рис. 7.7. Главное окно утилиты администрирования UserGate

Данная утилита предназначена для управления любым сервером UserGate, а не только установленным локально. Для того чтобы управлять удаленно несколькими серверами UserGate, следует знать их IP-адрес, порт, на котором установлен сервер, имя и пароль администратора. Имея всю необходимую информацию,

нужно лишь добавить новый сервер в список, нажав на кнопку *Добавить* в главном окне конфигуратора и заполнить соответствующую форму (рис. 7.8).

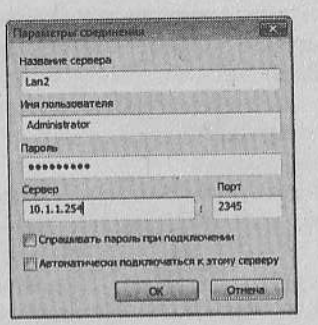


Рис. 7.8. Добавление нового сервера UserGate

В данном случае требуется настроить локальный сервер. Для этого нужно выбрать его в списке серверов и нажать кнопку *Подключиться*. После выполнения данных действий утилита подключится к серверу и отобразит уже существующие настройки, но поскольку сервер только что установлен – настраивать его нужно будет с самого начала под нужды конкретной сети.

Прежде всего, необходимо создать определенные тарифы, по которым будет считаться трафик пользователей, подключенных к Интернету через этот сервер. Это можно сделать в меню *Управление трафиком* (подменю *Тарифы*, рис. 7.9).

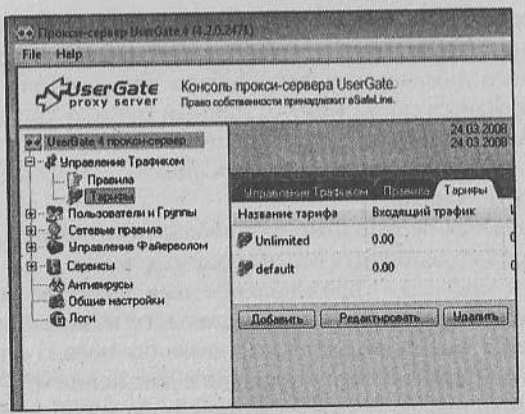


Рис. 7.9. Окно управления тарифами UserGate

При инсталляции программы по умолчанию создается тариф *default*. В нашем случае уже дополнительно создан тариф *Unlimited*. Создадим свой новый тариф. Для этого следует нажать кнопку *Добавить* внизу страницы. Откроется окно создания нового тарифа – нужно заполнить необходимые поля и нажать кнопку *ОК* (рис. 7.10).

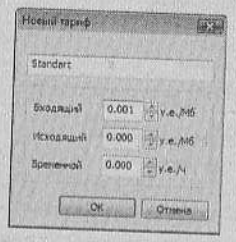


Рис. 7.10. Добавление нового тарифа UserGate

Кроме тарифов по количеству мегабайт или по времени использования Интернета, можно создавать так называемые пакетные тарифы. В эти пакеты включено определенное количество трафика в месяц/день/неделю, и пользователь по достижении этого лимита отключает либо включает ограничение по скорости доступа к Интернету. Создать такое правило можно в меню *Управление трафиком | Правила*. Таким образом можно создавать гибкие правила тарификации, смены тарифов, ограничений скоростей и многое другое, однако рассмотрение данного вопроса выходит за рамки этой книги.

В качестве примера рассмотрим простейшее создание пакетного плана с ограничением в 4000 Мбайт в месяц, при достижении данного лимита скорость доступа пользователя к сети Интернет снижается до 64 Кбит/с. Данный пример лишь иллюстрирует возможности UserGate в этой области.

1. Выбрать меню *Управление трафиком | Правила* и нажать кнопку *Добавить*.
2. Открывается первое окно для добавления правила, в котором необходимо заполнить все имеющиеся поля:
   - *Имя правила* – произвольное имя правила, по которому администратор будет определять его назначение. Рекомендуется давать осмысленные названия правил для более понятной идентификации правил в дальнейшем;
   - *Логика правил И/ИЛИ* – логика, по которой будут действовать все условия правил: логическое *И* объединяет все условия, логическое *ИЛИ* предоставляет выбор. Иначе говоря, если выбрать логическое *И* – то для срабатывания правил необходимо выполнение всех условий, при выборе логического *ИЛИ* – любого из них;
   - *Объект* – объект, над которым будет производиться действие. Можно выбрать либо *Трафик* – в этом случае при достижении определенных условий трафик считаться не будет, либо *Скорость* – при достижении определенных условий наступит ограничение скорости, либо *Тариф* – в этом случае при достижении условий произойдет смена тарифа, либо *Соединение* – при определенном условии соединение будет закрыто;
   - *Действие* – действие, производимое над объектом при достижении определенных условий. Действие зависит от объекта.

В данном примере при создании правила необходимо задать: имя *Ограничение - 64*, тип логики *И*, тип объекта *Скорость*, действие – *Установить*, значение 8 КБ/с (т.е 64 Кбит/с). Это делается для того, чтобы создать ограничение скорости для пользователей при превышении лимита трафика в месяц. После выбора условий следует нажать кнопку *Далее* (рис. 7.11).

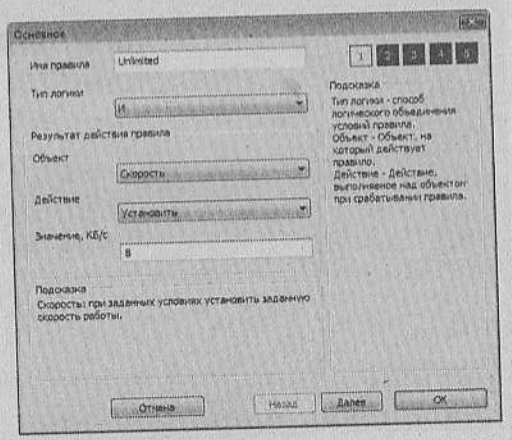


Рис. 7.11. Добавление нового правила UserGate

3. Открывается окно *Протоколы*, в котором можно выбрать применимость правил к определенным протоколам. Рекомендуется выбрать все протоколы и нажать кнопку *Далее* (рис. 7.12).

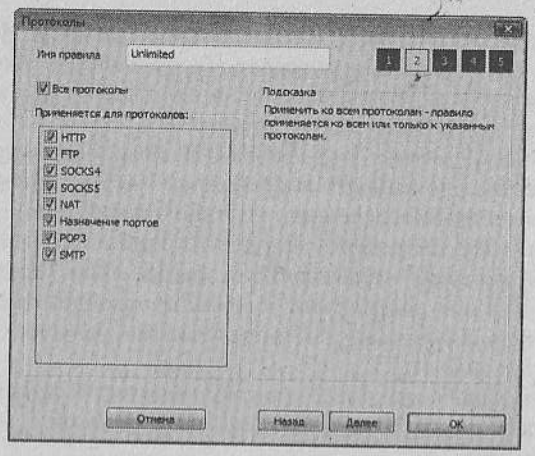


Рис. 7.12. Добавление нового правила UserGate – протоколы

4. В окне *Время и праздники* можно задать применимость данного правила для определенного времени суток и дней недели. Если требуется использовать правило без уточнения времени, следует оставить таблицу незаполненной (рис. 7.13).

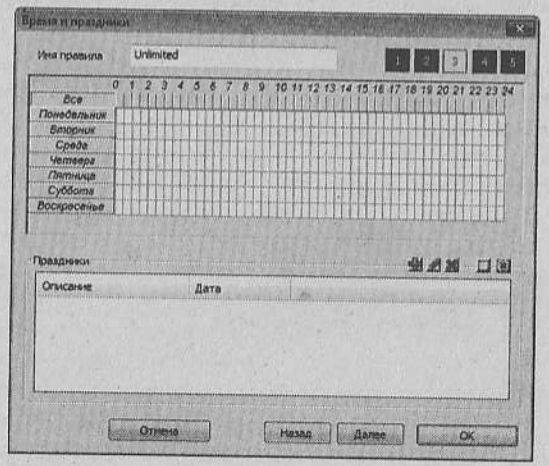


Рис. 7.13. Добавление нового правила UserGate – время и праздники

5. На странице *Лимиты* следует выбрать вкладку *В месяц*, ввести необходимый лимит Мбайт в месяц, при достижении которого включается правило, ограничивающее пропускную способность канала, и нажать кнопку *Далее* (рис. 7.14).

6. На странице *Фильтры* можно установить IP-адрес или диапазон адресов, с которых правило будет действительно, либо URL, при обращении на который данное правило будет срабатывать. В данном примере следует оставить эту страницу незаполненной и нажать кнопку *ОК*. На этом создание правила закончено (рис. 7.15).

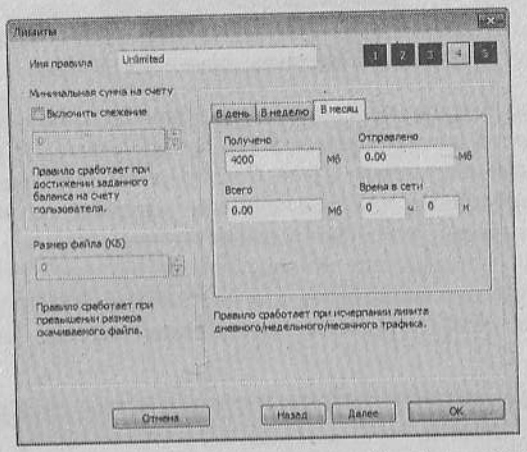


Рис. 7.14. Добавление нового правила UserGate – лимиты

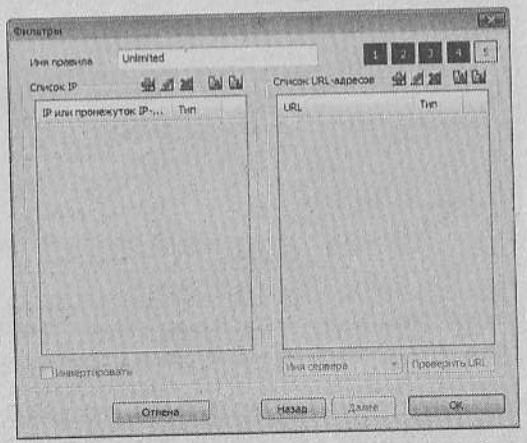


Рис. 7.15. Добавление нового правила UserGate – фильтры

7. На вопрос системы, применить ли данное правило для всех групп пользователей, надо ответить *НЕТ*.

   Примечание. Для сохранения всех изменений следует всегда нажимать кнопку *Сохранить изменения* в верхней части окна системы управления сервером (рис. 7.16).

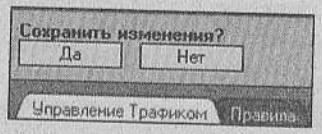


Рис. 7.16. Сохранение изменений в UserGate

8. Следующим шагом нужно создать группы пользователей для тарифного плана *Unlimited (Неограниченный)*. Сделать это возможно с помощью меню *Пользователи и группы | Группы*. Это необходимо для дальнейшего создания пользователей и более гибкого конфигурирования их возможностей. Создание группы – достаточно тривиальная задача: требуется вписать название группы, выбрать для нее тарифный план и отметить правила NAT и правила ограничения трафика для группы (рис. 7.17).

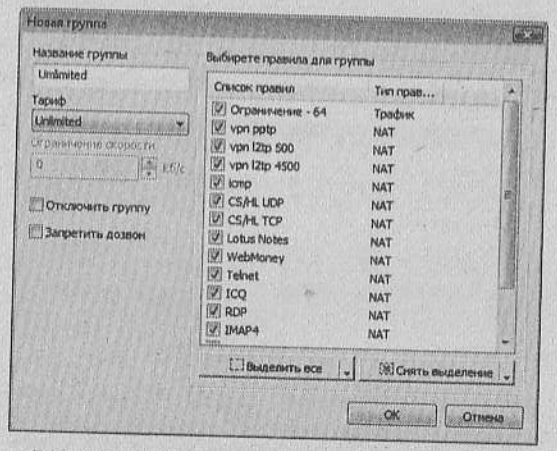


Рис. 7.17. Добавление новой группы в UserGate

Далее необходимо создать пользователей, который будут иметь возможность подключения к Интернету через данный сервер. Для этого следует перейти в меню *Пользователи и группы | Пользователи* и нажать кнопку *Добавить*. Появится окно создания нового пользователя (рис. 7.18), в котором нужно заполнить поля, требуемые для авторизации пользователя в системе.

Приведем пример, когда пользователь будет авторизироваться в системе с помощью специального клиентского ПО, позволяющего, кроме всего прочего, следить за балансом пользователя в системе. Рассмотрим заполняемые поля подробнее:

- *Имя* – имя пользователя, под которым он будет виден в системе администратору;
- *Эл. почта* – электронная почта пользователя, используется для рассылки статистики, желательно указывать существующий e-mail;
- *Тип авторизации* – UserGate поддерживает несколько типов авторизации пользователей. Типы авторизации будут рассмотрены ниже;
- *Ограничение скорости* – ограничение скорости соединения для данного пользователя, в Кбит/с (0 – отсутствие ограничения);

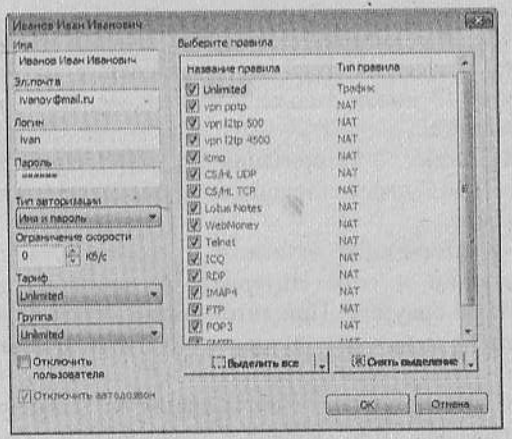


Рис. 7.18. Добавление нового пользователя в UserGate

- *Тариф* – тарифный план, применяемый по умолчанию ко всем соединениям данного пользователя. Можно указать любой тариф, имеющийся в системе, либо тариф группы, в которую входит пользователь;
- *Группа* – имя группы, в которую входит пользователь;
- *Отключить автодозвон* – опция, с помощью которой можно запретить пользователю инициировать Dial-Up соединение.

Эта опция имеет смысл, поскольку подключение к серверу с UserGate осуществляется по локальной сети;

- *Отключить пользователя* – опция, позволяющая отключить данного пользователя, не удаляя его из системы;
- *Выберите правила* – список правил, которые будут применяться для данного пользователя. Правила, применяемые для группы, в которую входит пользователь, всегда активны, и их нельзя отменить;
- *Выделить все* – опция, с помощью которой можно применить для пользователя все действующие правила трафика или правила NAT (для этого нужно выбрать стрелочку справа);
- *Снять выделения* – опция, с помощью которой можно отменить для пользователя все действующие правила трафика или правила NAT (выбрать стрелочку справа).

Типы авторизации, применяемые в UserGate:

- *IP-адрес* – авторизация по IP-адресу. Необходимо указать IP-адрес компьютера, с которого будет работать данный пользователь;
- *Диапазон IP* – авторизация одного клиента из диапазона IP-адресов. Создавать двух пользователей с авторизацией по диапазону IP можно только в том случае, если диапазоны не пересекаются;
- *IP+MAC адрес* – авторизация по комбинации IP- и MAC-адресов. MAC-адрес сетевой карты определяется при нажатии кнопки *mac*;
- *HTTP* – авторизация по имени и паролю, указываемые при подключении к сети Интернет. Авторизация выполняется средствами браузера. При авторизации таким способом пользователь не может использовать NAT и функцию назначения портов;
- *IP+MAC (абонемент)* – авторизация по комбинации IP- и MAC-адресов. При создании пользователя администратор UserGate задает логин и пароль, которые пользователь должен ввести в браузере при запросе на HTTP-авторизацию. Если пользователь планирует использовать какие-либо протоколы, кроме HTTP, тогда необходимо на странице регистрации (http://usergate/register.html) ввести логин и пароль. Привязка к IP- и MAC-адресу осуществляется в момент регистрации. В дальнейшем авторизация пользователя в UserGate осуществляется автоматически;

- *Windows login* – авторизация через логин, совпадающий с именем, под которым пользователь зарегистрирован в операционной системе на своем компьютере. В клиентской части нужно выбрать *Windows login*. Тогда UserGate Authentication Client передаст серверу UserGate имя пользователя, зарегистрированного в операционной системе. Предполагается, что пользователь успешно прошел авторизацию при входе в ОС Windows;
- *Имя и пароль* – авторизация осуществляется по логину и паролю, заданным администратором UserGate при создании пользователя. В модуле клиентской авторизации, установленном на машине пользователя, необходимо выбрать *Name and Password*, в поле *User name* указать логин, заданный при создании пользователя, нажать кнопку *Set PWD* и ввести пароль;
- *Active Directory* – авторизация через *AD*. Данный тип авторизации в домашних условиях не используется.

Заполнив необходимые поля, следует нажать кнопку *OK* – пользователь с заданными параметрами появится в системе. Просмотреть список пользователей можно на основной странице в меню *Пользователи и группы* | *Пользователи* (рис. 7.19).

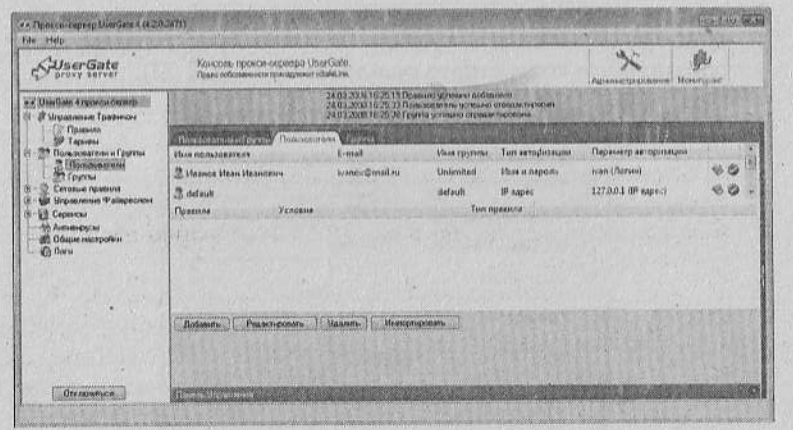


Рис. 7.19. Окно просмотра пользователей в UserGate

Программа также позволяет управлять пользователями в реальном режиме времени на этой же странице, достаточно лишь щелкнуть правой кнопкой мыши на пользователе (рис. 7.20).

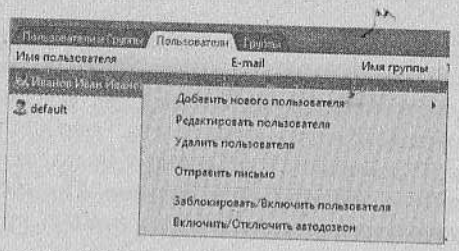


Рис. 7.20. Управление пользователем в UserGate

Теперь необходимо скопировать на компьютер пользователя клиент авторизации UGClient.exe и запустить его. Он позволит пользователю авторизироваться на сервере и получить доступ к сети Интернет. При первом запуске клиент попросит ввести IP-адрес сервера, на котором установлен UserGate (рис. 7.21).

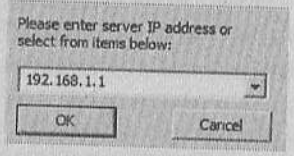


Рис. 7.21. Ввод IP-адреса сервера UserGate в клиенте авторизации

После подключения к серверу появится окно с параметрами авторизации для конкретного пользователя (рис. 7.22).

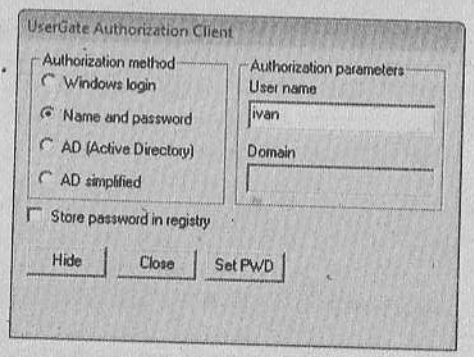


Рис. 7.22. Ввод учетных данных пользователя в клиенте авторизации

В данном случае выбираем тип авторизации *Name and Password*, в поле *User name* вводим логин пользователя и нажимаем кнопку *SetPWD* – появится окно, в котором вводим пароль (рис. 7.23).

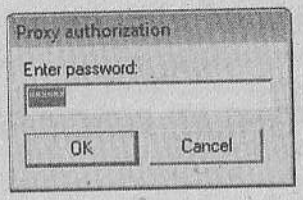


Рис. 7.23. Ввод пароля пользователя в клиенте авторизации

Для того чтобы получить доступ к сети Интернет, пользователь должен настроить некоторые параметры своего браузера. Возьмем для примера браузер Internet Explorer. Чтобы настроить браузер для обращения к прокси-серверу, следует выбрать меню *Сервис* | *Свойства Обозревателя* | *Подключения* | *Настройка сети* – откроется окно *Настройка параметров локальной сети* (рис. 7.24).

В области *Прокси-сервер* устанавливаем два флажка, в поле адреса вводим IP-адрес прокси-сервера (т.е. адрес, назначенный внутренней сетевой карте), а в поле *Порт* – 8080 (порт, который задан по умолчанию в настройках UserGate). Этих настроек достаточно для предоставления пользователю доступа к Интернету.

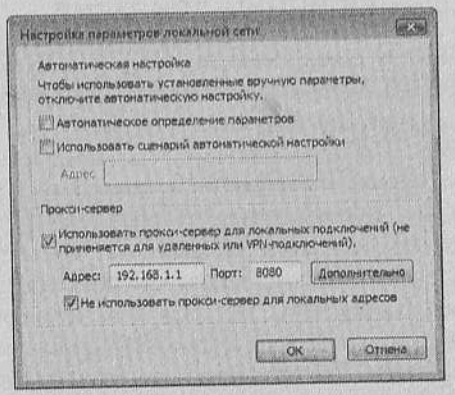


Рис. 7.24. Настройки Internet Explorer для работы через UserGate

Рассмотреть все возможности этой мощной и функциональной программы невозможно в рамках данного издания – это тема для отдельной книги.

Во второй части будут рассмотрены популярные программы и сервисы для работы в Интернете.

Часть II
Полезные программы

Глава 8
Обмен файлами в сетях

В последнее время широкое распространение получили локальные компьютерные сети. Существует большое количество программ, предназначенных для обмена в них информацией. В данной главе рассмотрены самые распространенные и удобные программы.

Принцип действия

Файлообменная сеть – сеть, в которой допускается возможность совместного использования файлов. Чаще всего такие сети бывают *одноранговыми*, что означает равноправие узлов (компьютеров сети) в обмене файлами, т.е. компьютеры этой сети одновременно являются серверами и клиентами. Существует три типа организации файлообменных сетей:

- *централизованная* – хоть каждый узел является сервером и клиентом, существует необходимость объединения клиентов в определенную структуру. Эту задачу выполняют серверы, которые хранят и используют служебную информацию о каждом компьютере сети. Эти сети легко программируются, служебная информация занимает небольшой объем, но из-за возможных технических проблем сервера, что может привести к полной недееспособности, данный тип сетей является ненадежным;
- *децентрализованные* – в отличие от предыдущего типа эти сети функционируют без сервера, а объем передаваемой служебной информации в них гораздо больше; надежность данного типа сетей очень высокая;

- *гибридные* – сочетают в себе скорость передачи данных в централизованных и надежность работы в децентрализованных сетях. Используются независимые серверы, которые синхронизируют служебную информацию между собой. Таким образом, при выходе из строя одного из них сеть продолжает функционировать.

µTorrent

Данная программа является бесплатным BitTorrent-клиентом для Windows с поддержкой загрузки нескольких файлов одновременно. Несмотря на небольшой размер, программа имеет большое количество различных функций. Предназначена для обмена файлами в Интернете. В данной программе имеется возможность ограничивать скорости отдачи и скачивания в зависимости от времени, настройки интерфейса, большое количество языков, а также подключение через прокси-сервер. Быстро восстанавливает прерванные загрузки и занимает маленький объем памяти.

Главное окно µTorrent состоит из меню, кнопок быстрого доступа, области с информацией о загрузке файлов и списка групп для сортировки этих загрузок (рис. 8.1).

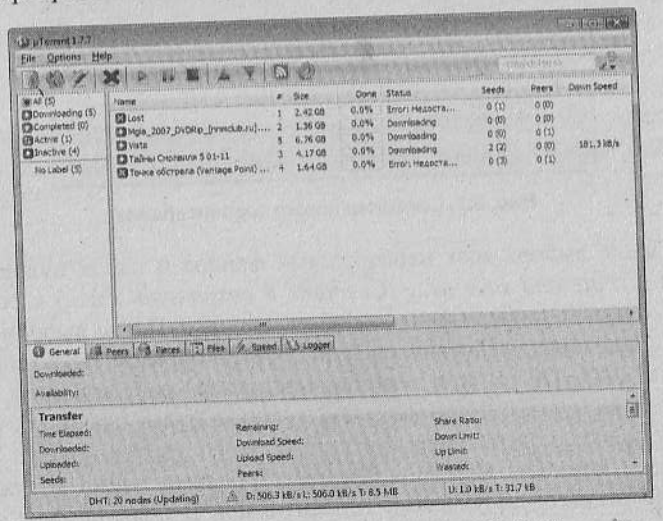


Рис. 8.1. Главное окно программы µTorrent

Для передачи файлов по Интернету через данную программу отправитель должен создать файл, содержащий список всех отправляемых файлов. Для этого необходимо в меню *File (Файл)* выбрать команду *Create New Torrent (Создать новый торрент)*. В появившемся окне посредством нажатия кнопок *Add file (Добавить файл)* и *Add directory (Добавить каталог)* нужно выбрать файлы и папки, которые пользователь желает отправить (рис. 8.2). Есть возможность добавить описание и изменить некоторые опции.

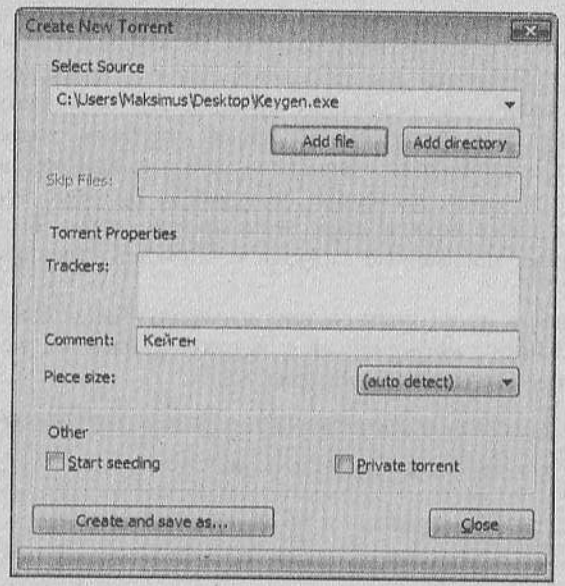


Рис. 8.2. Создание нового торрент-файла

После выбора всех необходимых файлов и папок нужно нажать *Create and save as... (Создать и сохранить как...)* и сохранить данный торрент-файл в любом каталоге. После выполнения всех описанных действий следует любым образом (электронная почта, ICQ, DC++, при помощи носителей) передать этот торрент-файл другим пользователям, которые будут скачивать файлы и папки, содержащиеся в списке этого торрент-файла. При помощи команды *Add New Torrent (Добавить новый торрент)* нужно открыть полученный торрент-файл. В появившемся окне будет отображена информация о данном торрент-файле (рис. 8.3).

Здесь также можно выбрать из списка файлы для скачивания и путь, по которому будут сохранены эти файлы. Для продолжение операции надо нажать *OK*.

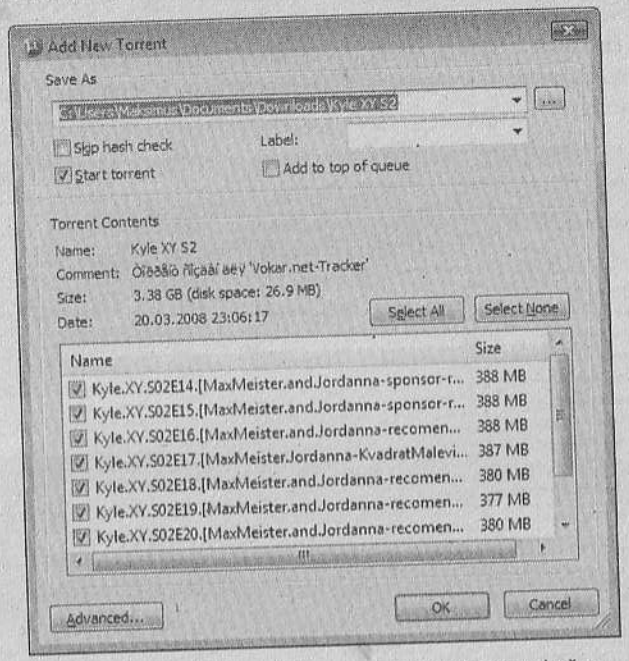


Рис. 8.3. Скачивание файлов из списка торрент-файла

В результате в главном окне будет отображаться информация о скачивании данных файлов так же, как и при скачивании файлов по URL.

DC++

DC++ – широко распространенная программа, которую применяют большинство пользователей локальных сетей для общения и обмена файлами.

Главное окно этой программы (рис. 8.4) состоит из трех областей. Главная область, занимающая бóльшую часть окна, содержит список всех пользователей, находящихся на данном хабе (отдельный узел какой-либо сети, к которому присоединяются пользова-

тели). При помощи нажатий на заголовки столбцов таблицы можно упорядочить список пользователей по нику (компьютерный псевдоним), объему доступной для скачивания информации, IP, описанию и др. Область, находящаяся в левой части окна, является чатом. Нижняя область окна отображает прогресс скачивания или отдачи файлов, показывая ник пользователя, скорость, оставшееся время и др.

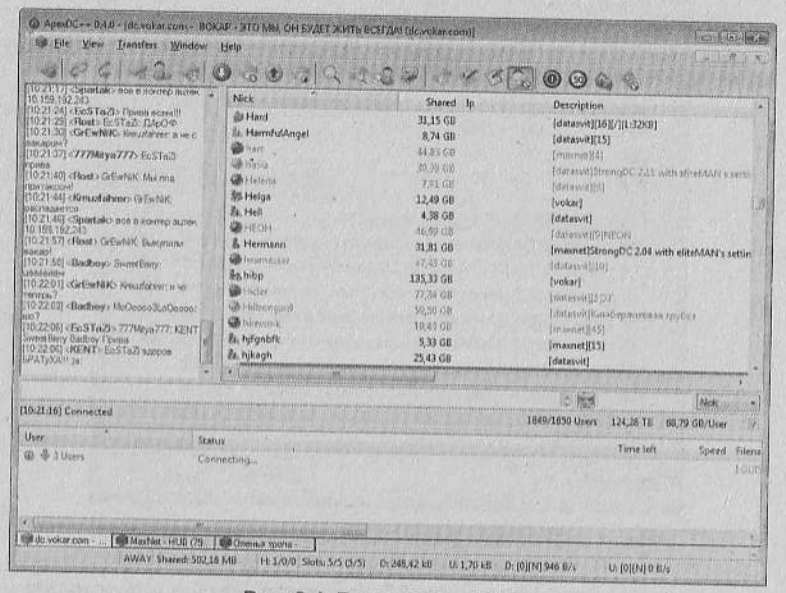


Рис. 8.4. Главное окно DC++

Для настройки программы необходимо выбрать в меню *File* (*Файл*) команду *Settings* (*Настройки*). Все настройки для облегчения работы с программой разделены на несколько групп. Отобразившееся окно (рис. 8.5) дает возможность изменить любые настройки программы: ник, скорость отдачи, соединение, путь для помещения временных и скаченных файлов, внешний вид программы и др.

Для того чтобы сделать доступными для скачивания другим пользователям какие-либо файлы, необходимо щелкнуть по группе *Sharing* (*Общий доступ*) и в области *Shared directories* (*Доступные для скачивания папки*) отметить необходимые папки с файлами (рис. 8.6). После этого программа предложит ввести

будущее название для этой папки, которое будут видеть другие пользователи. Затем следует нажать кнопку *OK*.

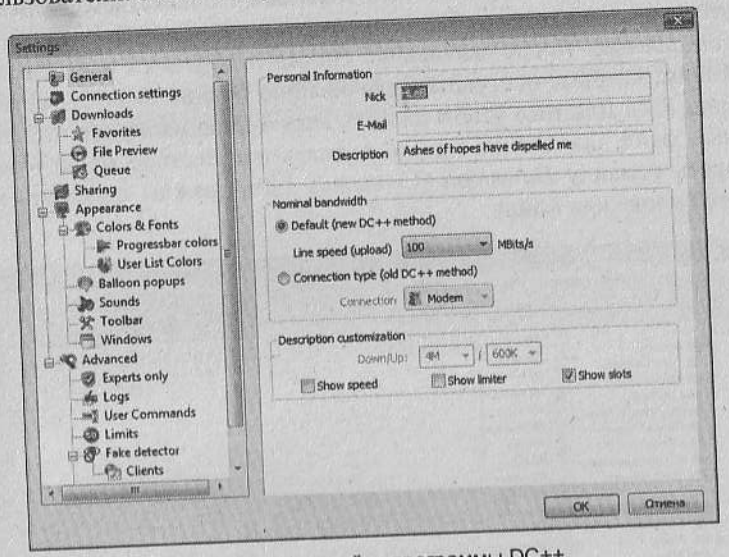


Рис. 8.5. Настройки программы DC++

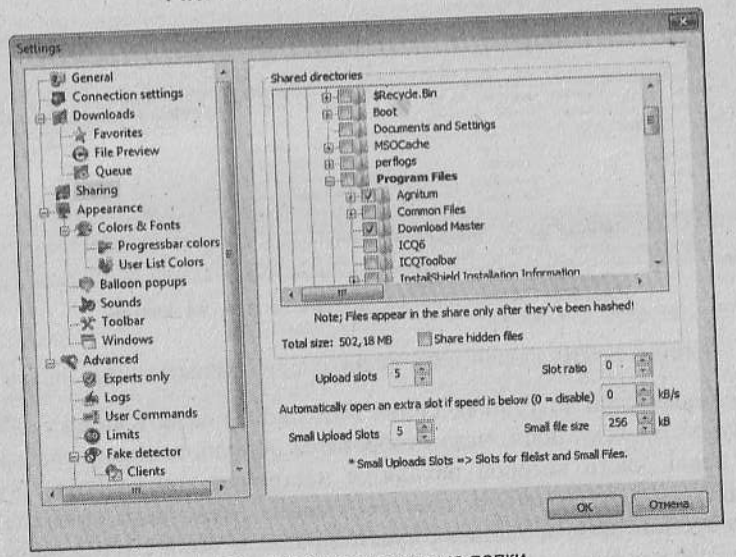


Рис. 8.6. Расшаренные папки

Для того чтобы скачать какие-нибудь файлы у пользователя, необходимо в контекстном меню, вызванном нажатием на имени этого пользователя, выбрать команду *Get file list* (*Получить список файлов*). После скачивания списка отобразятся все папки и файлы, которые доступны к скачиванию у данного пользователя (рис. 8.7). Для того чтобы скачать какую-либо папку или отдельный файл, достаточно просто вызвать контекстное меню и выбрать команду *Download* (*Скачать*) либо дважды щелкнуть по этой папке или файлу.

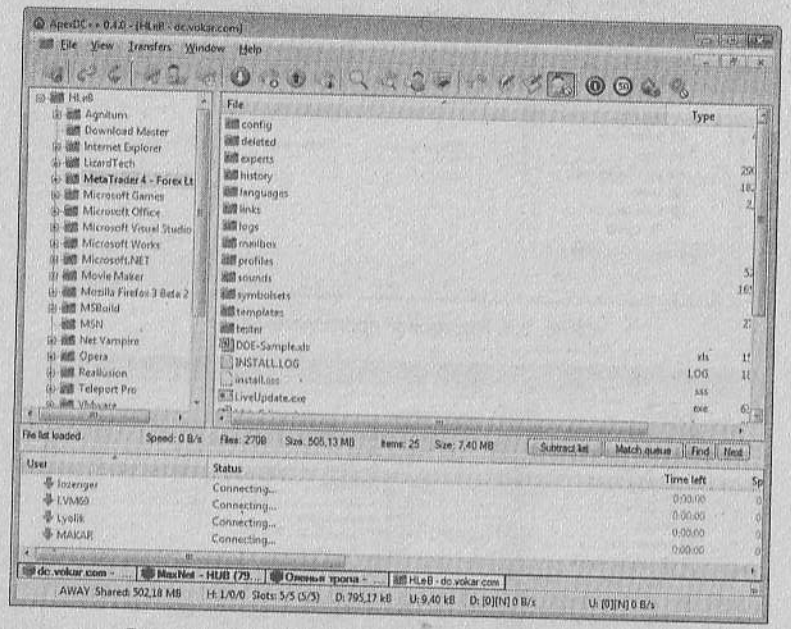


Рис. 8.7. Список файлов, доступных для скачивания

Чтобы найти какой-либо файл среди открытых для других пользователей доступных хабов, необходимо нажать кнопку  *Search (Поиск)*, после чего отобразится дополнительная вкладка, в левой части которой находятся настройки поиска (рис. 8.8). Здесь есть возможность ввести название (или часть названия) требуемого файла, указать диапазон размера файла, тип и хабы, на которых будет произведен поиск.

После указания всех параметров поиска следует нажать кнопку *Search* (*Поиск*) либо клавишу **Enter**. В результате в главной области данной вкладки отобразятся все файлы, удовлетворяющие критериям поиска (рис. 8.9). Чтобы скачать найденный файл, нужно дважды щелкнуть по нему или в контекстном меню выбрать команду *Download* (*Скачать*).

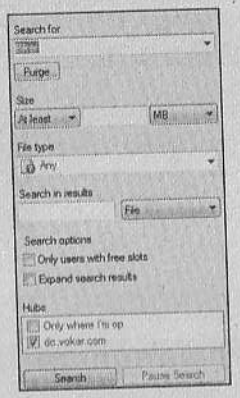


Рис. 8.8. Настройки поиска информации

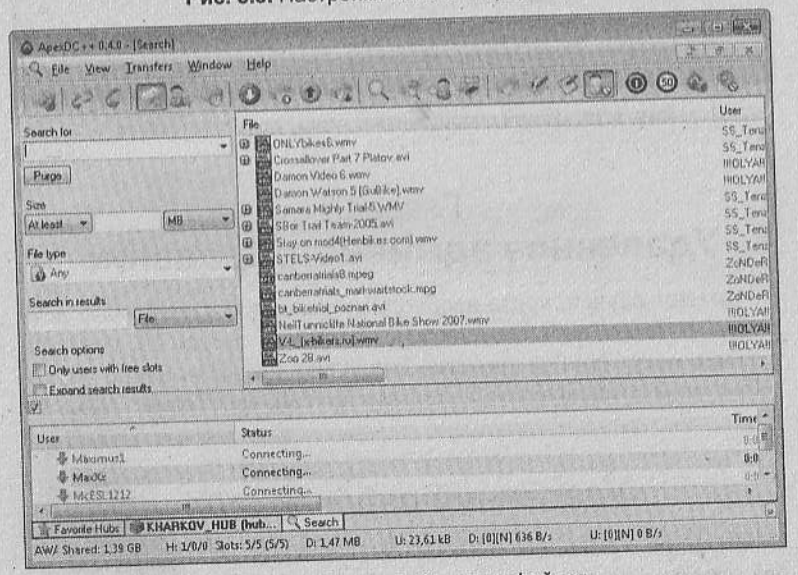


Рис. 8.9. Список найденных файлов

Для обмена текстовыми сообщениями при помощи этой программы нужно в контекстном меню пользователя выбрать команду *Send private message (Отправить личное сообщение)*. Затем в нижней строчке отобразившейся вкладки необходимо ввести сообщение и нажать **Enter** (рис. 8.10).

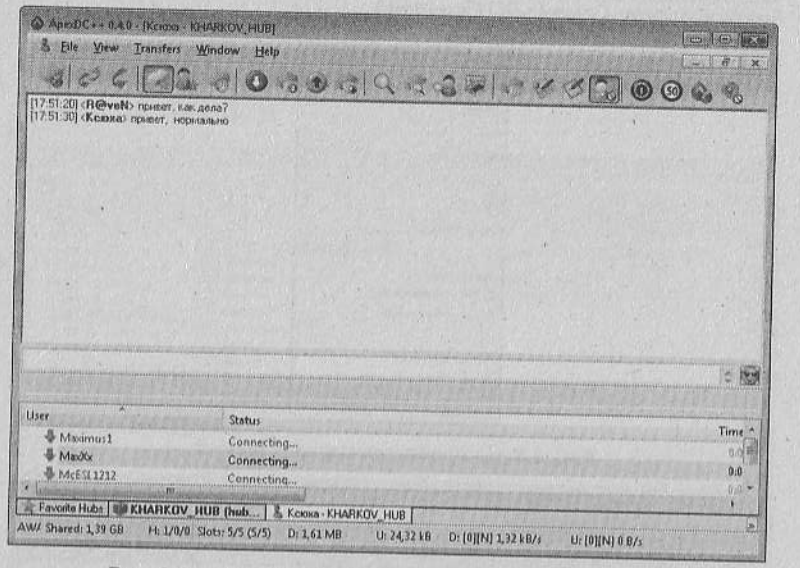


Рис. 8.10. Обмен сообщениями между пользователями

Глава 9
Удаленное администрирование

Бывают случаи, когда необходимо выполнить некоторые действия на каком-либо компьютере, находясь далеко от него. На помощь могут прийти средства, позволяющие полноценно управлять одним компьютером, используя другой, через сеть.

Удаленный рабочий стол

Функция *Удаленный рабочий стол* в Windows Vista позволяет без проблем получить доступ к рабочему столу любого другого

компьютера. Это дает возможность работать с файлами, сетевыми ресурсами, программами, т.е. делать все, что можно делать непосредственно на этом компьютере.

Для включения удаленного доступа к компьютеру (по умолчанию эта опция отключена) нужно открыть окно *Система* (категория *Система и ее обслуживание* в панели управления), в котором выбрать пункт *Настройка удаленного доступа* (рис. 9.1).

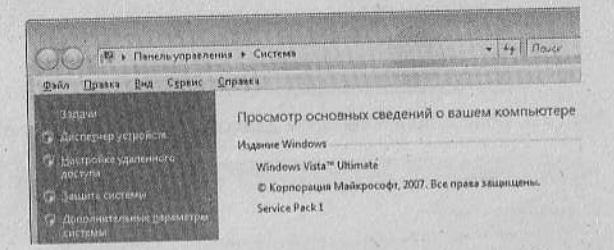


Рис. 9.1. Вызов настройки удаленного доступа в окне *Система*

После нажатия появится следующее окно, где на вкладке *Удаленное использование* нужно включить опцию *Разрешить подключения от компьютеров с любой версией удаленного рабочего стола* (рис. 9.2).

После этого необходимо выбрать компьютеры, с которых будет возможен доступ. Для этого надо нажать кнопку *Выбрать пользователей*, после чего отобразится окно, в котором будет указан список пользователей, имеющих удаленный доступ к данному компьютеру (рис. 9.3).

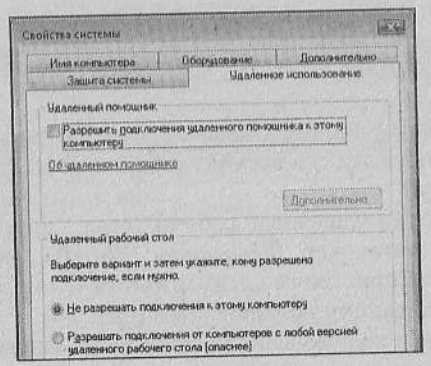


Рис. 9.2. Вкладка *Удаленные сеансы*

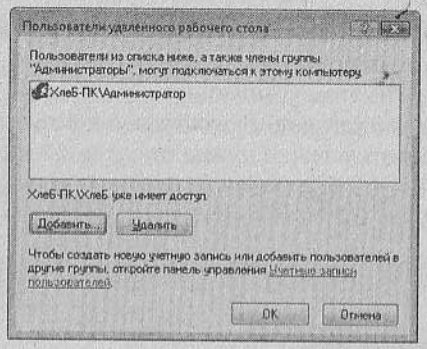


Рис. 9.3. Список пользователей удаленного рабочего стола

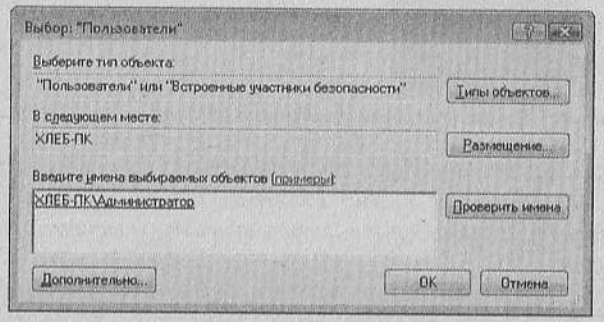


Рис. 9.4. Добавление пользователя в список

Добавить в список нового пользователя можно при помощи нажатия кнопки *Добавить*. Затем следует нажать кнопку *Дополнительно* (рис. 9.4).

В появившемся окне (рис. 9.5) нужно нажать *Поиск*, а затем выбрать пользователя из списка найденных. После выбора следует нажать *ОК*.

После нажатия кнопки *ОК* на всех оставшихся окнах будет открыт удаленный доступ всех пользователей из списка к данному компьютеру.

Чтобы зайти на удаленный рабочий стол с другого компьютера, нужно вызвать окно *Выполнить* (**Win+R**), ввести команду mstsc и нажать **Enter**. Затем следует ввести IP-адрес компьютера, к которому необходимо подключиться (рис. 9.6).

Для настройки подключения можно нажать кнопку *Параметры*. После нажатия окно раздвинется, предоставляя большое количество

опций для настройки соединения (рис. 9.7). Здесь можно настроить размер удаленного рабочего стола, цветовую палитру и др.

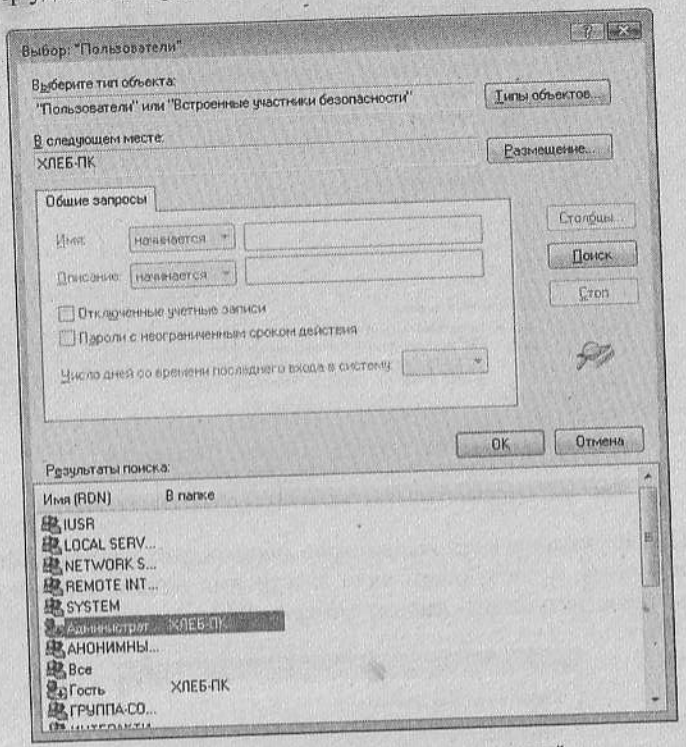


Рис. 9.5. Поиск доступных пользователей

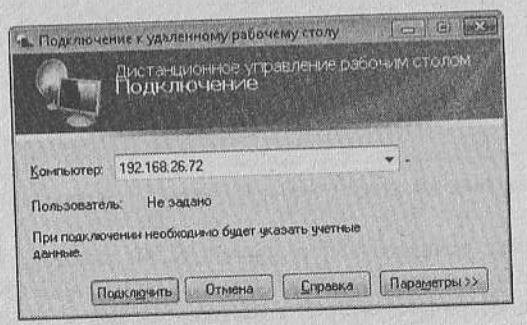


Рис. 9.6. Подключение к удаленному рабочему столу

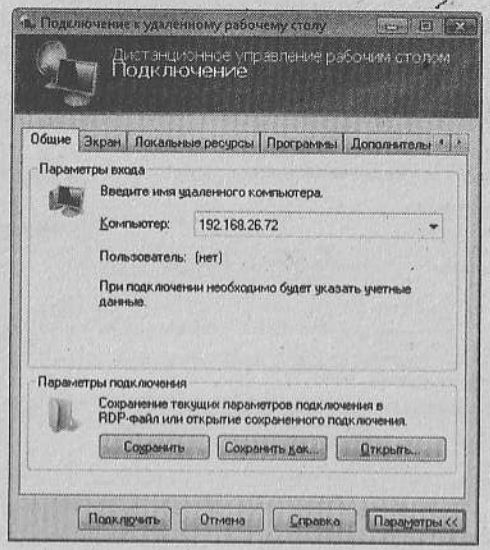


Рис. 9.7. Дополнительные параметры для подключения

После указания всех параметров необходимо нажать кнопку *Подключить*, в следующем окне ввести имя пользователя и пароль, после чего нажать кнопку *OK* (рис. 9.8).

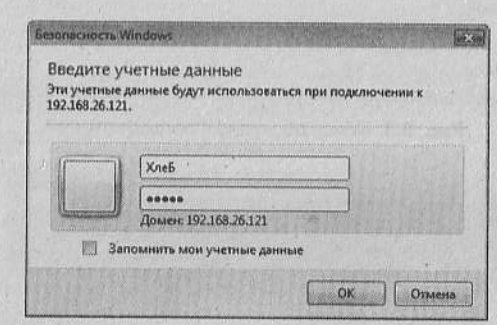


Рис. 9.8. Запрос имени пользователя и пароля

Если имя пользователя и пароль были введены правильно, появится окно, в котором будет изображен рабочий стол удаленного компьютера (рис. 9.9). В этом окне можно осуществлять все действия, которые допустимы при непосредственной работе на этом компьютере.

Рис. 9.9. Окно с рабочим столом удаленного компьютера

Remote Administrator (Radmin)

Radmin – быстрая, легкая в использовании, надежная программа, позволяющая управлять удаленным компьютером. При подключении к какому-либо узлу можно производить любые действия, доступные для этого компьютера.

После установки этой программы будет предложено ввести пароль для подключения к серверу на данном компьютере (рис. 9.10). После ввода пароля необходимо нажать *OK*.

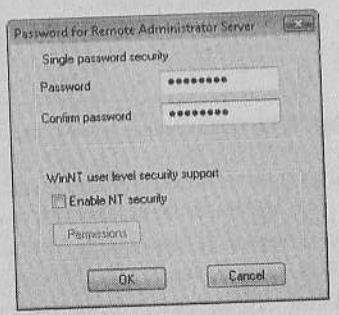


Рис. 9.10. Задание пароля для доступа к серверу

Главное окно программы содержит меню, кнопки быстрого доступа и область, в которой находится список серверов (рис. 9.11).

Если необходимо добавить в список новый сервер, то нужно в меню *Connection* (*Соединение*) выбрать команду *New* (*Новое*). После нажатия отобразится окно, в котором надо ввести название сервера и его IP-адрес, здесь также есть возможность настроить другие параметры соединения (рис. 9.12). После ввода всех нужных данных следует нажать кнопку *OK*, после чего данный сервер добавится в список.

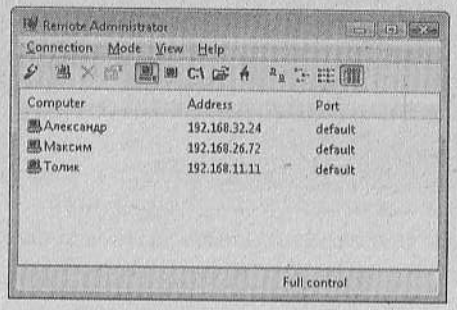


Рис. 9.11. Главное окно программы Radmin

Рис. 9.12. Добавление нового сервера

Эти параметры в дальнейшем можно будет изменить, выбрав команду *Properties* (*Свойства*) контекстного меню этого сервера и открыв вкладку *General* (*Основные*). На вкладке *Remote control/view* (*Удаленный контроль/просмотр*) можно настроить цветовой формат, способ отображения и частоту обновления кадров данного удаленного рабочего стола.

Для изменения параметров сервера нужно в каталоге, в котором установлена данная программа, запустить программу *Settings for Remote Administrator server* (*Настройки для сервера Radmin*). После запуска данного приложения отобразится окно, представленное на рис. 9.13.

Кнопка *Startup mode* (*Способ запуска*) дает возможность настроить автоматический или ручной способ запуска сервера. При нажатии кнопки *Set password* (*Установить пароль*) отображается окно, в котором можно изменить пароль для подключения к данному серверу. Нажатие кнопки *Options* (*Опции*) откроет окно, в котором можно изменить такие свойства, как IP-фильтр, порт и др.

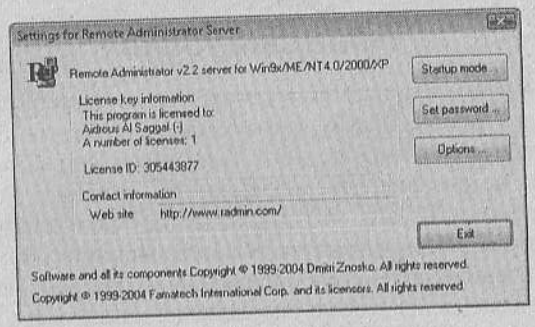


Рис. 9.13. Настройки сервера

Для подключения к какому-либо компьютеру можно либо дважды щелкнуть на названии сервера в главном окне, либо нажать кнопку  *Connect to address* (*Соединиться по адресу*), после чего в отобразившемся окне ввести IP-адрес сервера и нажать кнопку *Connect* (*Соединиться*) (рис. 9.14).

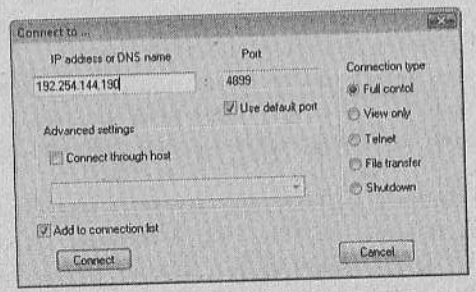


Рис. 9.14. Соединение с удаленным компьютером

После этого появится небольшое окно, в котором необходимо ввести пароль для доступа к данному серверу. Если пароль был введен корректно, то спустя некоторое время появится окно, в котором отобразится рабочий стол удаленного компьютера. В этом окне можно производить любые действия, доступные при работе на этом компьютере.

Для работы программы на удаленном компьютере должен быть инсталлирован и запущен сервер Radmin. При его установке будет предложено ввести пароль для доступа к данному компьютеру.

Глава 10
Брандмауэры

Подключение компьютера к сети Интернет позволяет не только получать необходимую информацию, общаться с другими пользователями сети и т. п., но и несет в себе определенную угрозу. Из-за несовершенства операционных систем и сетей существует вероятность того, что к компьютеру пользователя, который находится в сети, может быть подключен другой компьютер и злоумышленник, используя определенное программное обеспечение, произведет некоторые операции на компьютере пользователя. Это могут быть действия, направленные на похищение информации, которая хранится на компьютере пользователя, либо просто вызванные интересом злоумышленника. В любом случае несанкционированное подключение или взлом компьютера пользователя является не самым приятным событием для него.

Для защиты компьютеров, которые подключены к сети, используются специальные средства – как программные, так и физические, позволяющие производить контроль над данными, которые поступают или покидают компьютер пользователя. Такие средства называются *брандмауэрами* (*firewall*).

Брандмауэр может значительно повысить сетевую безопасность и уменьшить для компьютера риск нахождения в сети путем фильтрации небезопасных по своей природе информационных пакетов.

Принцип защиты компьютера, который является частью локальной сети, показан на рис. 10.1 В отличие от компьютеров, подключенных к локальной сети и защищенных корпоративным брандмауэром, компьютеры рядовых пользователей, которые

подключены непосредственно к сети с помощью коммутируемого доступа или выделенной линии, не имеют отдельного физического блока, который защищал бы их от атак извне. В связи с этим было создано большое число программных брандмауэров, среди которых лидирующие позиции занимают программы Agnitum Outpost Firewall Pro, ZoneLabs ZoneAlarm Pro и Norton Personal Firewall.

Рис. 10.1. Использование брандмауэра

Брандмауэр Windows

Учитывая рост сети Интернет, компания Microsoft пришла к решению включить в операционную систему Windows XP брандмауэр, позволяющий защитить подключение к сети. В Windows Vista эта программа стала еще более надежной, была снабжена удобными инструментами управления и дополнительными возможностями фильтрации и мониторинга сетевых соединений.

Брандмауэр Windows пропускает на компьютер информацию только в том случае, если обмен данными был начат с данного компьютера, а не из сети.

Брандмауэр не отображает пользователю какие-либо сообщения, поскольку их было бы очень много и они очень отвлекали бы от работы. Вместо этого брандмауэр Windows ведет запись всех попыток соединений в специальной системе мониторинга. Для просмотра событий брандмауэра следует открыть консоль *Брандмауэр Windows в режиме повышенной безопасности*, которая находится в *Панели управления* | *Система и ее обслуживание* | *Администрирование*.

Таким образом, брандмауэр Windows является хорошим средством для защиты компьютера, подключенного к сети Интернет, например домашнего ПК. Он позволяет отразить большое число сетевых атак, таких как сканирование портов (а ведь практически любая атака начинается с этого), однако он не защитит компьютер, если пользователь сам инициировал подключение к вражеской системе.

Примечание. При некорректной настройке брандмауэра Windows возможны проблемы при использовании общего доступа к файлам и принтерам локальной сети, а также при работе в Интернете.

Для того чтобы включить брандмауэр Windows, необходимо открыть панель управления, перейти в раздел *Безопасность* и щелкнуть по надписи *Брандмауэр Windows* – откроется окно, показанное на рис. 10.2. Здесь пользователь может просмотреть текущее состояние брандмауэра, а также, используя команды боковой панели или ссылку *Изменить параметры*, открыть окно конфигурирования программы.

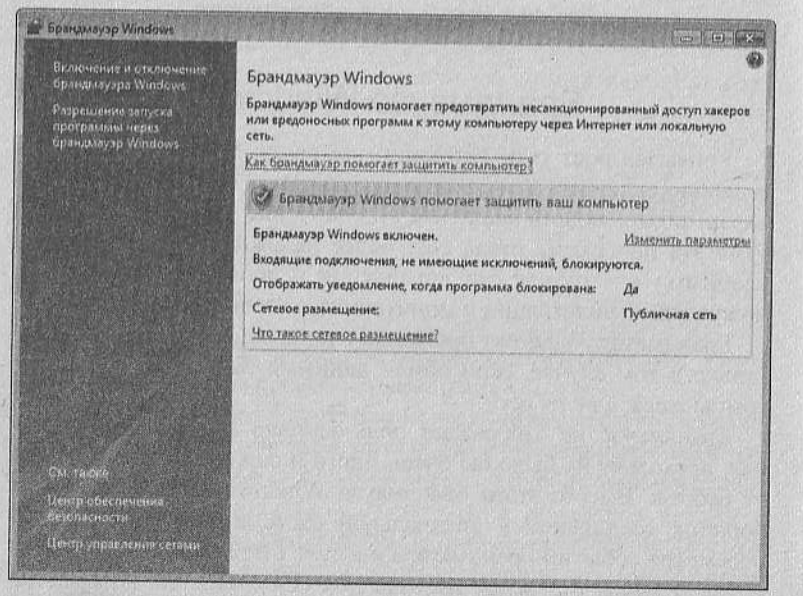


Рис. 10.2. Просмотр состояния брандмауэра Windows

Окно свойств брандмауэра показано на рис. 10.3. На первой вкладке – *Общие* – пользователь может включить или отключить брандмауэр путем установки переключателя в соответствующее положение. Если компьютер находится в публичной сети (Интернет или неконтролируемая локальная сеть), рекомендуется установить флажок *Блокировать все входящие поключения*, что заставит брандмауэр отклонять все незапрошенные информационные пакеты, приходящие на компьютер пользователя. После установки этого флажка пользователь будет иметь возможность работать в сети, однако другие пользователи подключиться к его компьютеру не смогут.

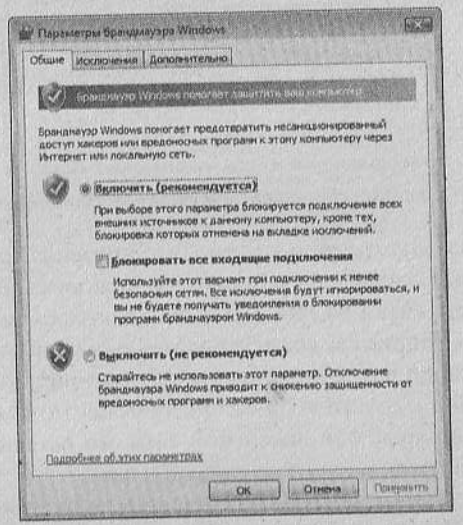


Рис. 10.3. Параметры брандмауэра Windows. Вкладка *Общие*

Вкладка *Исключения* (рис. 10.4) позволяет указать программу, которая даже при включенном брандмауэре сможет принимать входящие подключения. Таким образом, пользователи локальной сети смогут первыми инициировать соединение с защищаемым компьютером.

Если компьютер подключен к локальной сети, то на этой вкладке можно установить флажок *Общий доступ к файлам и принтерам*, что позволит пользователям других компьютеров обращаться к открытым папкам защищаемого ПК.

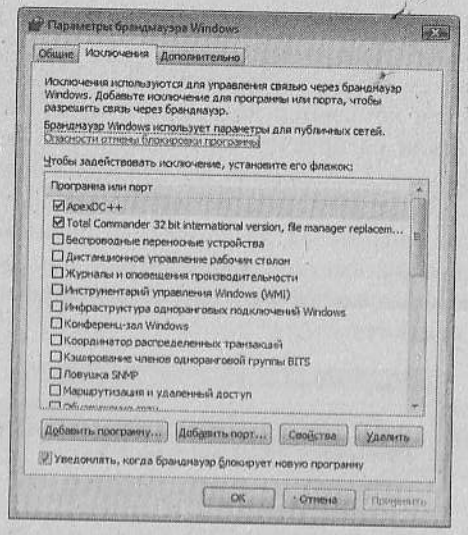


Рис. 10.4. Параметры брандмауэра Windows. Вкладка *Исключения*

На вкладке *Дополнительно* (рис. 10.5) перечислены все соединения, которые созданы на компьютере пользователя. Здесь можно определить, какие из них будут защищаться брандмауэром, а какие – нет. Например, если у пользователя дома имеются несколько компьютеров, объединенных локальной сетью, и один из них подключен к сети Интернет при помощи модема, можно отключить брандмауэр для локальной сети, но оставить его включенным для защиты модемного подключения.

Когда какая-либо программа пытается использовать компьютерную сеть и принимать подключения, инициированные удаленными пользователями, брандмауэр Windows отображает диалоговое окно (рис. 10.6), в котором пользователь может указать, допускаются ли входящие сетевые подключения к программе или нет. Если пользователь выбирает вариант *Продолжать блокировать*, клиенты локальной сети не смогут самостоятельно подключиться к программе, работающей на защищаемом компьютере. В случае если выбран вариант *Разблокировать*, программа заносится в список исключений и для нее разрешаются входящие подключения.

Если же пользователь случайно заблокировал работу какой-либо программы, он может добавить ее в список исключений.

Для этого необходимо открыть окно параметров брандмауэра Windows, перейти на вкладку *Исключения* и нажать кнопку *Добавить программу* (рис. 10.4). Система отобразит диалоговое окно *Добавление программы* (рис. 10.7). В нем нужно указать исполняемый файл программы, для которой должны быть разрешены входящие подключения. После нажатия на кнопку *OK* программа попадет в список исключений, и брандмауэр больше не будет блокировать подключения клиентов сети к этой программе.

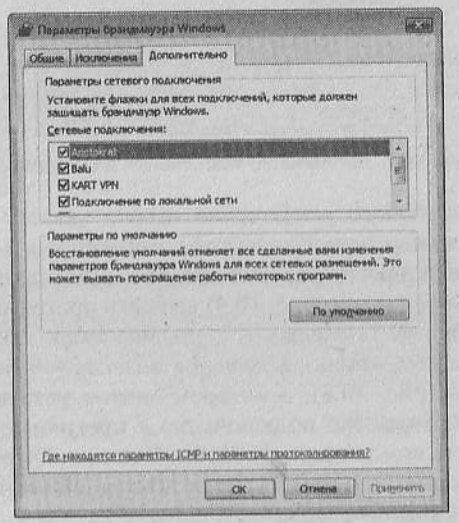


Рис. 10.5. Параметры брандмауэра Windows. Вкладка *Дополнительно*

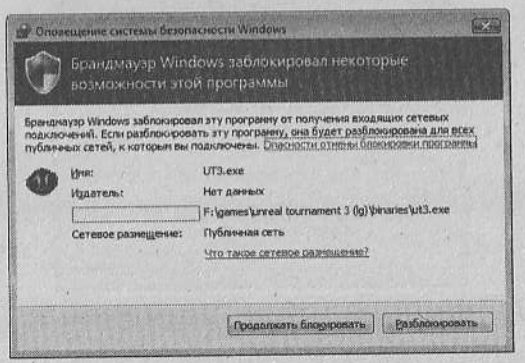


Рис. 10.6. Предупреждение о блокировании программы брандмауэром

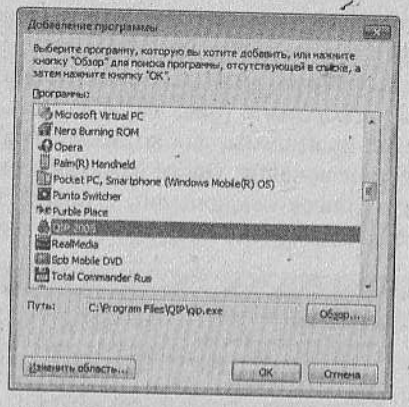


Рис. 10.7. Добавление исключения в брандмауэр

Также для любого исключения можно указать область, т.е. диапазон и/или перечень IP-адресов компьютеров, которые могут подключаться к программе или службе. Для этого следует на вкладке *Исключения* (см. рис. 10.4) выбрать программу или службу, нажать кнопку *Свойства* и в появившемся окне *Изменение программы* нажать кнопку *Изменить область* – откроется одноименное окно (рис. 10.8), в котором можно указать, для каких компьютеров разрешено подключение к программе или службе. Это могут быть компьютеры локальной сети, любые компьютеры (даже те, которые не принадлежат к локальной сети) или список определенных компьютеров.

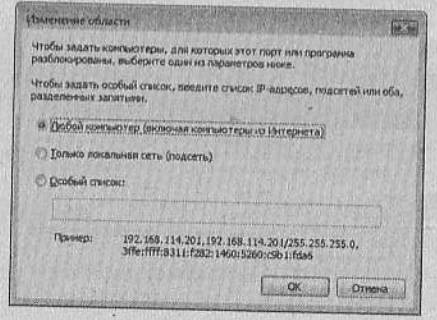


Рис. 10.8. Изменение области действия исключения

Таким образом, брандмауэр Windows является хорошей альтернативой другим программным пакетам, особенно для начинающих пользователей. Он не требует выполнения каких-либо настроек, что сводит к минимуму возможность неправильного конфигурирования. Его также можно использовать для настройки ограничений, регулирующих обмен данными между Интернетом и домашней или небольшой офисной сетью.

ZoneAlarm Pro

Данная программа представляет собой систему защиты от несанкционированного доступа из внешней глобальной сети в персональный компьютер или во внутреннюю сеть (интрасеть). К особенностям программы следует отнести высокую степень защиты компьютера, гибкость настройки, понятный интерфейс и простоту в использовании.

Окно программы показано на рис. 10.9. Оно содержит несколько панелей (кнопки для перемещения по ним расположены слева), а также несколько кнопок вверху окна программы.

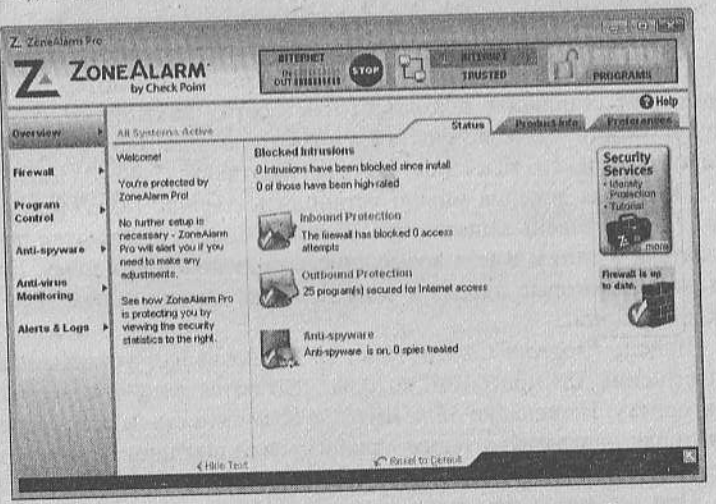


Рис. 10.9. Брандмауэр ZoneAlarm Pro. Панель *Overview*

Каждая панель отображает определенную информацию либо позволяет изменять настройки программы.

Панель *Overview* содержит три вкладки: *Status*, *Product info*, *Preferences*.

На вкладке *Status* отображается текущее состояние системы: количество попыток подключения к компьютеру пользователя; число программ, которые имеют доступ в Интернет, и служба проверки электронной почты.

Вкладка *Product info* содержит информацию о версии программы, лицензии, а также позволяет получить техническую поддержку разработчиков программы.

Вкладка *Preferences* позволяет настроить автоматическое обновление (группа *Check for updates*) и параметры соединения с разработчиками (можно запретить передачу IP-адреса компьютера и заставить программу сообщать пользователю о начале соединения с разработчиками). Также на данной вкладке можно установить пароль к программе. Это позволит запретить другим пользователям менять настройки программы и даже завершать ее работу.

Панель *Firewall* (рис. 10.10) содержит две основные вкладки: *Main* и *Zones*. На вкладке *Main* можно установить, используя «бегунки», уровень защиты для каждой из трех зон – зоны Интернета (*Internet Zone Security*), зоны доверия (*Trusted Zone Security*) и блокированной зоны (*Blocked Zone Security*).

Для зоны Интернета рекомендуется устанавливать *высокий* (*High*) уровень защиты, что позволит скрыть компьютер пользователя от остальных пользователей в сети. Фактически, они не будут видеть его; все попытки доступа к компьютеру будут блокироваться и, что важно, оставаться без ответа.

Для зоны доверия можно установить *средний* (*Med*) или *низкий* (*Low*) уровень защиты, что позволит видеть компьютер пользователя в сети и иметь возможность подключения к нему. Компьютеры, которые входят в зону доверия, можно определить на вкладке *Zones*.

Панель *Program Control* (рис. 10.11) позволяет устанавливать разрешения для программ, которые пытаются получить доступ к Интернету. На вкладке *Main* имеется возможность задать уровень контроля программ, а также включить или выключить автоматическую блокировку соединения.

При установке бегунка в положение *High* все программы, которые потребуют доступа в сеть, должны получить разрешение (также для определения разрешений используется вкладка *Programs*). Если бегунок установлен в положение *Med*, ZoneAlarm будет «изучать» программы, которые требуют доступа в Интернет, и, руководствуясь указаниями пользователя, либо разрешать

программам подключаться к сети, либо запрещать. После цикла вопросов ZoneAlarm будет самостоятельно управлять доступом программ в Интернет.

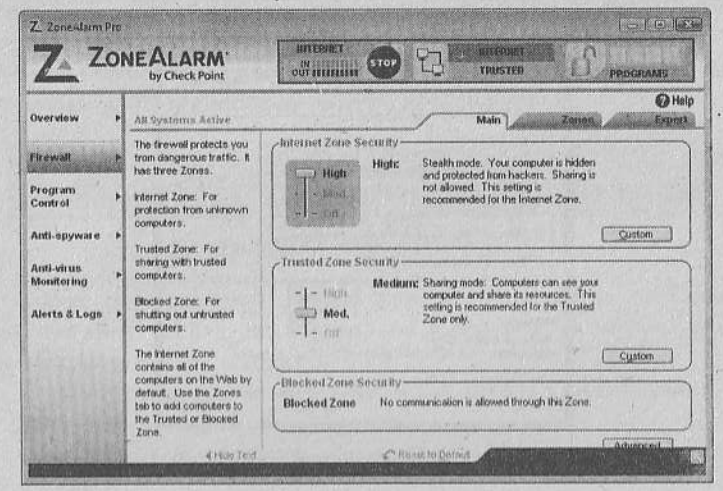


Рис. 10.10. Панель *Firewall*

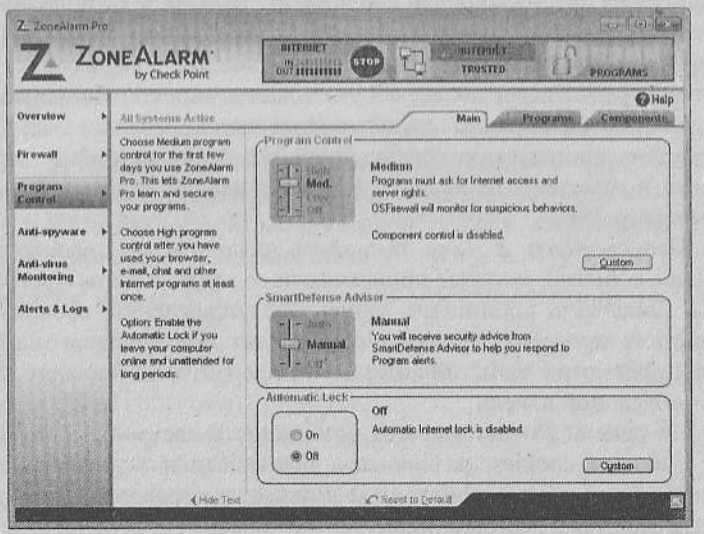


Рис. 10.11. Панель *Program Control*

Также на данной панели можно включить или выключить автоматическую блокировку соединения. Для настройки автоблокировки следует использовать окно *Custom Lock Settings*, которое открывается при нажатии на кнопку *Custom* (вкладка *Main*).

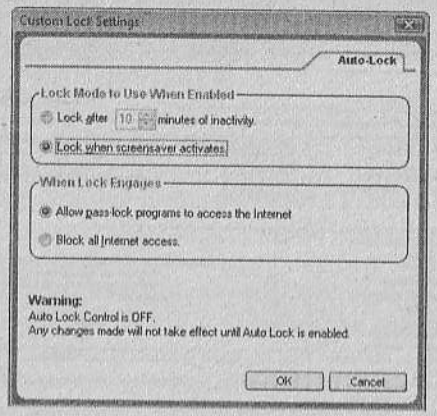


Рис. 10.12. Настройка автоматической блокировки соединения

В данном окне (рис. 10.12) можно установить параметры включения автоблокировки соединения: включать автоблокировку тогда, когда включается хранитель экрана, или по истечении определенного времени после начала простоя компьютера. Во второй группе переключателей указывается характер блокировки: полностью блокировать доступ в Интернет или блокировать доступ всех программ, за исключением тех, которые имеют привилегии и отмечены на вкладке *Programs* панели *Program Control* символом .

Панель *Alerts & Logs* позволяет включить или выключить запись событий, которые происходили во время работы программы. ZoneAlarm производит запись предупреждений, событий и действий программ, которые используют подключение к сети. Для просмотра событий достаточно перейти на вкладку *Log Viewer* данной панели.

На панели *Privacy* имеется возможность настройки контроля за файлами cookies, различными баннерами и всплывающими окнами, а также за скриптами и другими программами, которые встраиваются в веб-страницы.

Панель *E-mail Protection* предназначена для включения и настройки функции проверки электронной почты *MailSafe*. Данная функция проверяет электронные письма, получаемые пользователем, и блокирует все подозрительные скрипты, которые могут быть встроены в электронное письмо. Также *MailSafe* проверяет вложения электронных писем на наличие вирусов и в случае обнаружения вируса сообщает об этом пользователю.

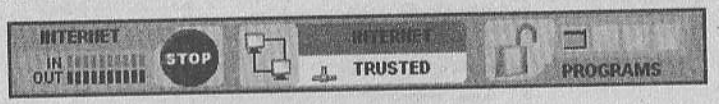


Рис. 10.13. Верхняя панель

Кроме перечисленных выше панелей, программа снабжена панелью (рис. 10.13), расположенной в верхней части окна программы, на которой находятся:

- индикаторы интернет-активности (*IN* и *OUT*), показывающие входящий и исходящий трафики;
- кнопка *STOP*, которая полностью блокирует интернет-активность;
- кнопка *INTERNET / TRUSTED*, позволяющая быстро открыть вкладку *Zones* панели *Firewall*.

Также на данной панели находится кнопка с изображением замка, позволяющая блокировать доступ всех программ к сети, за исключением тех, которые имеют привилегии и отмечены на вкладке *Programs* панели *Program Control* символом .

Когда программа запущена и пользователь начинает работу в Интернете, ZoneAlarm отображается в *System Tray* (*Область уведомлений*) в виде одной из двух иконок. Если передача данных между компьютером пользователя и сервером отсутствует, отображается иконка . Если же происходит передача данных, то выводится иконка ; при этом красный столбец показывает информацию, которая передается на сервер, а зеленый – информацию, которая поступает с сервера.

Кроме этого, во время работы программы могут появляться сообщения трех типов:

- сообщения об обнаружении новой сети (*New Network alerts*);
- сообщения программ (*New Program alerts*);
- сообщения брандмауэра (*Firewall alerts*).

New Network alerts (рис. 10.14) появляется тогда, когда пользователь дозванивается к провайдеру и получает IP-адрес. Это сообщение носит информативный характер и сообщает пользователю, что программа ZoneAlarm обнаружила сеть провайдера.

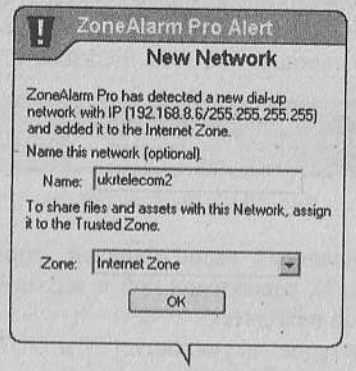


Рис. 10.14. Сообщение *New Network alerts*

New Program alerts (рис. 10.15) появляется в том случае, когда какая-либо программа пытается подключиться к Интернету. Используя данное окно, можно либо разрешить программе доступ в Интернет (кнопка *Yes*), либо запретить (кнопка *No*). Таким образом,

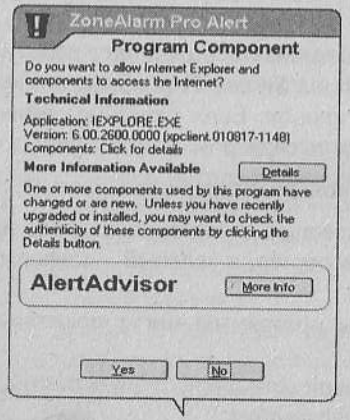


Рис. 10.15. Сообщение New Program alerts

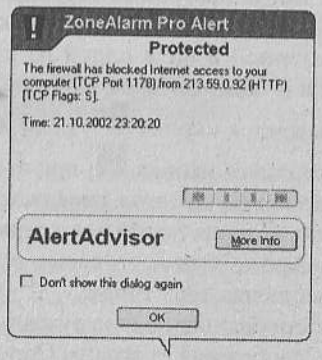


Рис. 10.16. Сообщение *Firewall alerts*

имеется возможность контролировать программы, которые получают доступ в Интернет. Также контроль за программами можно осуществлять на панели *Program Control* (вкладка *Programs*).

Firewall alerts (рис. 10.16) появляется тогда, когда брандмауэр блокирует нежелательный входящий или исходящий трафик. Данное сообщение, так же как и *New Network alerts*, носит информативный характер.

Таким образом, брандмауэр ZoneAlarm Pro является прекрасным инструментом, сочетающим в себе простоту в использовании и надежность, который способен полностью защитить компьютер пользователя от атак из сети.

Norton Internet Security 2008

Norton Internet Security 2008 – комплект программ, предназначенных для полной защиты от вирусов, «троянов», червей, хакерских атак. Включает в себя брандмауэр, модуль по поиску шпионских программ, антифишинговый фильтр. Программа дает возможность сделать полное сканирование компьютера на наличие всевозможных угроз, способствует безопасной работе в Интернете.

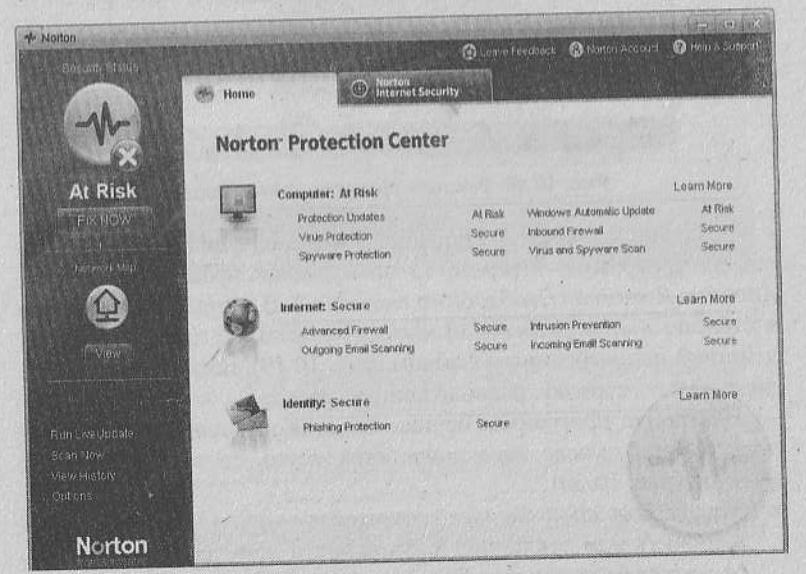


Рис. 10.17. Главное окно Norton Internet Security 2008

Главное окно программы изображено на рис. 10.17. Две вкладки содержат информацию о работе всех методов защиты. В левой нижней части окна находятся кнопки, с помощью которых можно просмотреть историю работы данной программы, просканировать компьютер, настроить какие-либо опции.

Для сканирования компьютера нужно нажать *Scan Now* (*Сканировать сейчас*). После нажатия появится окно, в котором будет отображаться информация о текущей проверке компьютера. На вкладке *Results Summary* (*Резюме результатов*) (рис. 10.18) можно увидеть общее количество проверенных файлов, количество файлов, представляющих угрозу безопасности и др.

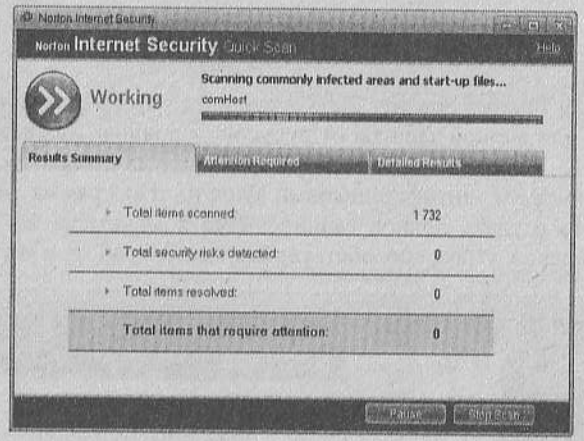


Рис. 10.18. Быстрая проверка компьютера

Если при проверке будет обнаружен какой-либо вирус, шпионская программа, «троян», то он будет отображен на вкладке *Attention Required* (*Необходимо внимание*). В выпадающем списке в столбце *Action* (*Действие*) можно выбрать одно из доступных действий над выбранным файлом (рис. 10.19), после чего необходимо нажать стрелку, расположенную рядом.

Настройка программы осуществляется нажатием кнопки *Options* (*Опции*), после чего появляется меню, состоящее из двух пунктов (рис. 10.20):

- *Norton Protection Center* – открывает окно, в котором можно включить или отключить возможность получения сообщений от центра безопасности Windows (рис. 10.21);

- *Norton Internet Security* – открывает окно, представленное на рис. 10.22. Здесь можно настроить общие настройки программы, защиту брандмауэра, автоматическое обновление и др.

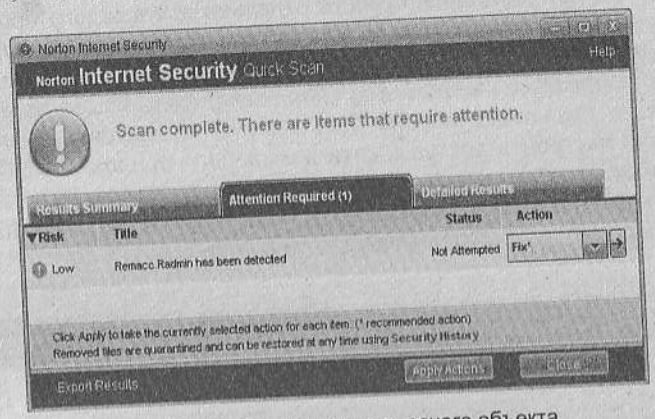


Рис. 10.19. Обнаружение опасного объекта

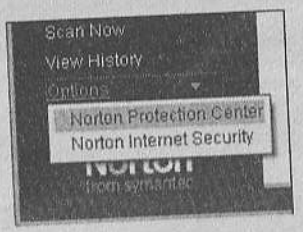


Рис. 10.20. Команды для настройки программы

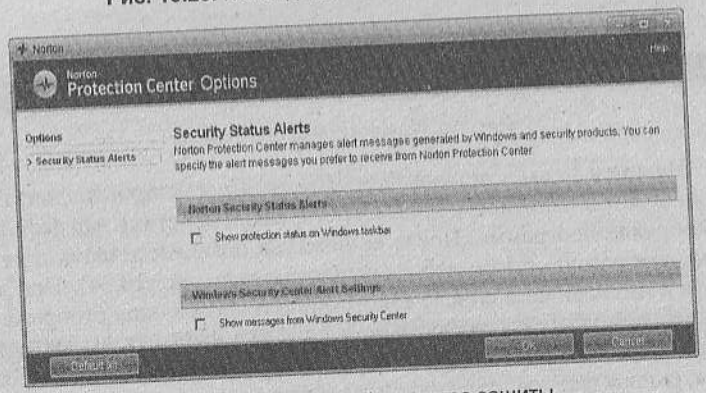


Рис. 10.21. Настройки центра защиты

Для настройки сетевых правил для каждого приложения отдельно нужно нажать в этом же окне надпись *Program Control* (*Контроль программ*) в группе *Personal Firewall* (*Персональный брандмауэр*). Есть возможность отдельно для каждого приложения полностью разрешить или запретить доступ в Интернет. Для добавления в список какого-либо другого приложения нужно воспользоваться кнопкой *Add* (*Добавить*) (рис. 10.23), затем выбрать в появившемся окне необходимое приложение. Здесь же можно настроить доступ к сети для любого приложения. Если в столбце *Access* указать значение *Allow*, то соответствующему приложению будут разрешены любые обращения к сети, при *Block* они будут блокированы.

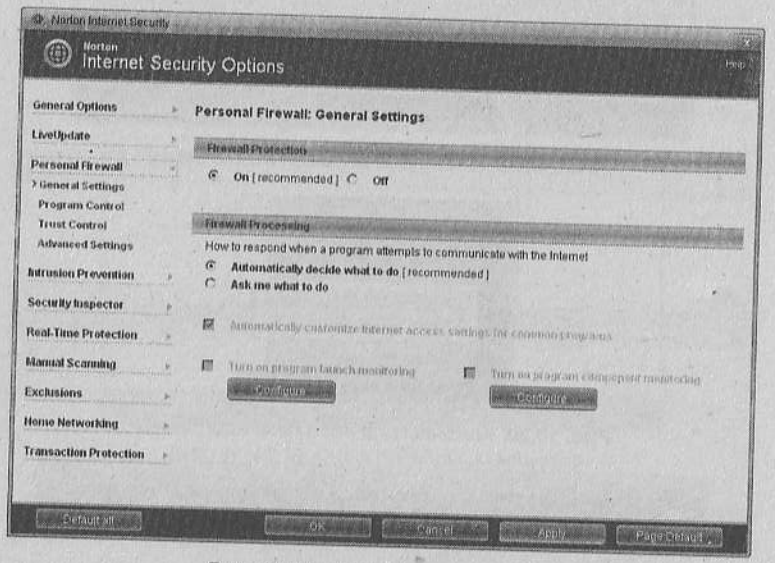


Рис. 10.22. Настройки программы

Надпись в главном окне *View History* (*Просмотр истории*) предоставляет возможность просмотреть, какие действия над файлами выполняла программа. После ее нажатия появляется окно, в котором изображен список действий программы (рис. 10.24). При выборе в выпадающем списке какого-либо пункта в окне отображается соответствующая информация. Есть возможность выбрать для просмотра историю действий программы, результаты сканирования, список файлов, попавших в карантин, и др.

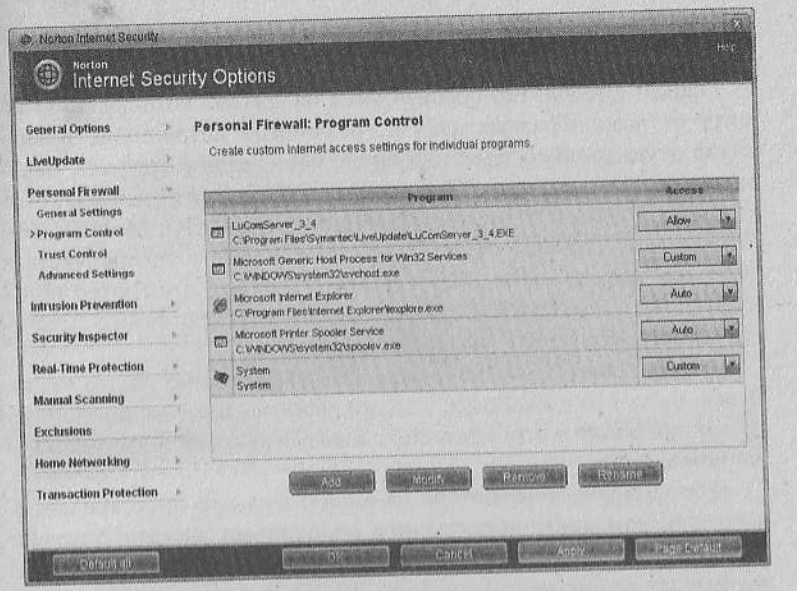


Рис. 10.23. Сетевые правила для различных приложений

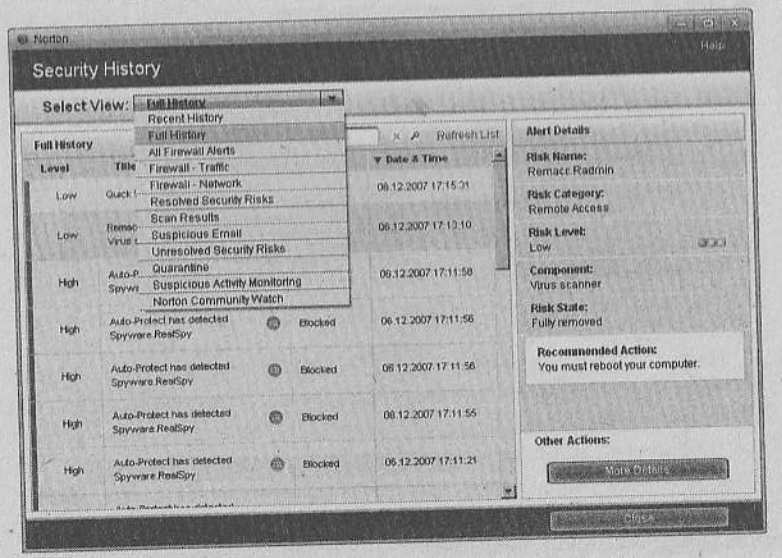


Рис. 10.24. Просмотр истории работы программы

Agnitum Outpost Firewall Pro 2008

Outpost Firewall Pro обеспечивает надежную комплексную защиту от разнообразных атак из различных источников. Брандмауэр осуществляет двухстороннюю фильтрацию трафика, определяет источник атаки. Компонент *Anti-Spyware* защищает от «троянов», червей и других видов шпионского ПО. Модуль *Host Protection* обеспечивает защиту от наиболее часто употребляемых хакерами методов атак. *Web Control* оберегает компьютер пользователя от посещений зараженных сайтов. В программе присутствует автоматическая настройка защиты.

Главное окно программы (рис. 10.25) разделено на две части. Левая часть отображает все модули защиты. Щелчок по любому из них приводит к отображению соответствующей информации о данном модуле.

Для проверки компьютера на наличие какого-либо вредоносного программного обеспечения необходимо нажать *Scan for Spyware* (*Сканировать на наличие шпионских программ*), после чего будет отображено окно (рис. 10.26), в котором следует выбрать способ проверки компьютера:

- *Quick system scan (Быстрая проверка системы)* – позволяет проверить области, в которых чаще всего находятся шпионские программы;

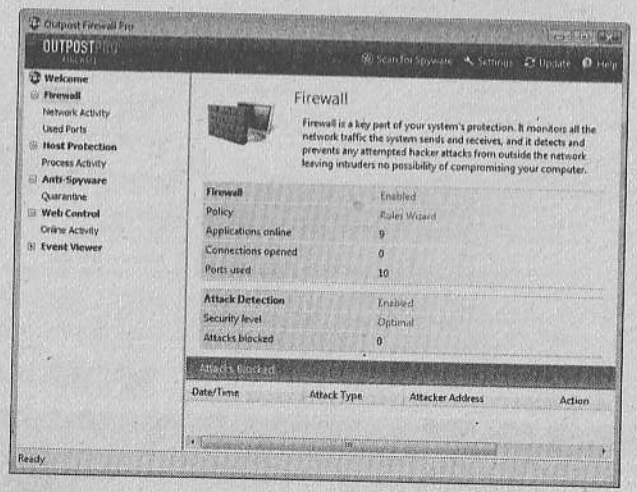


Рис. 10.25. Главное окно Outpost Firewall Pro 2008

- *Full system scan (Полная проверка системы)* – полностью проверяет компьютер;
- *Custom scan (Выборочная проверка)* – позволяет выбрать объекты для сканирования.

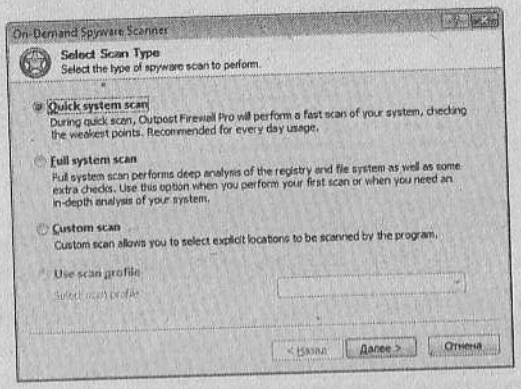


Рис. 10.26. Выбор метода проверки компьютера

При выборе метода *Custom scan* есть возможность выбрать области для проверки по своему усмотрению (рис. 10.27). Нажатие кнопки *Add (Добавить)* дает возможность добавить в список проверяемых объектов любые папки.

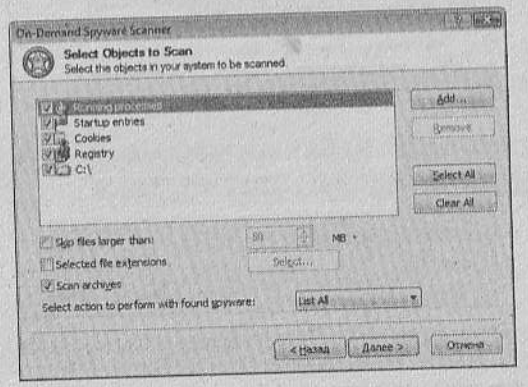


Рис. 10.27. Выбор областей для проверки

После выбора метода проверки необходимо нажать кнопку *Далее*. Появившееся окно будет отображать всю информацию о текущей проверке (рис. 10.28).

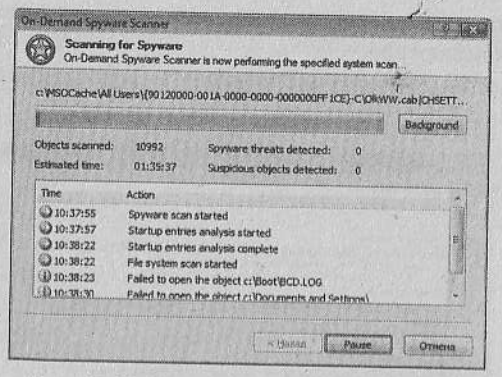


Рис. 10.28. Проверка выбранных областей

В этом окне будет показано количество проверенных, подозрительных и опасных файлов, а также время, затраченное на проверку. Кнопки, находящиеся в данном окне, дают возможность при необходимости приостановить и отменить текущую проверку. Если будет обнаружен вредоносный объект, то программа предложит выбрать одно из доступных действий (поместить в карантин, пропустить или удалить) (рис. 10.29).

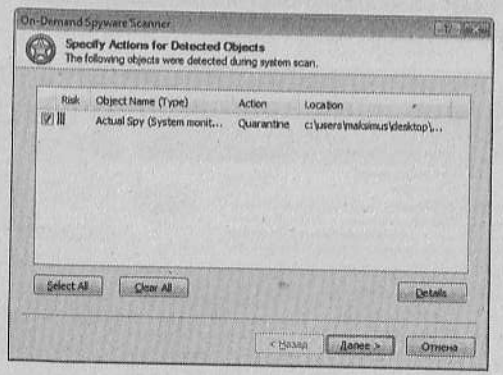


Рис. 10.29. Обнаружение вредоносного объекта

После завершения проверки будет представлен отчет о выполненной работе (рис. 10.30). Здесь будет отображено количество обнаруженных вредоносных и подозрительных программ, вылеченных, пропущенных и удаленных объектов, общее количество проверенных файлов, папок, процессов в памяти, ключей реестра и др.

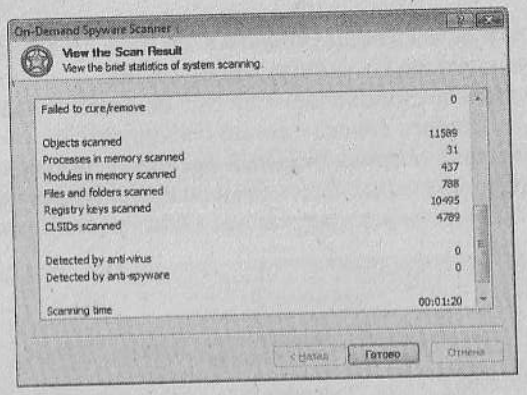


Рис. 10.30. Отчет о выполненной проверке

Для просмотра списка помещенных в карантин объектов нужно нажать на *Quarantine* (*Карантин*) (рис. 10.31). При помощи соответствующих кнопок можно удалить или восстановить любые объекты, находящиеся в данном списке.

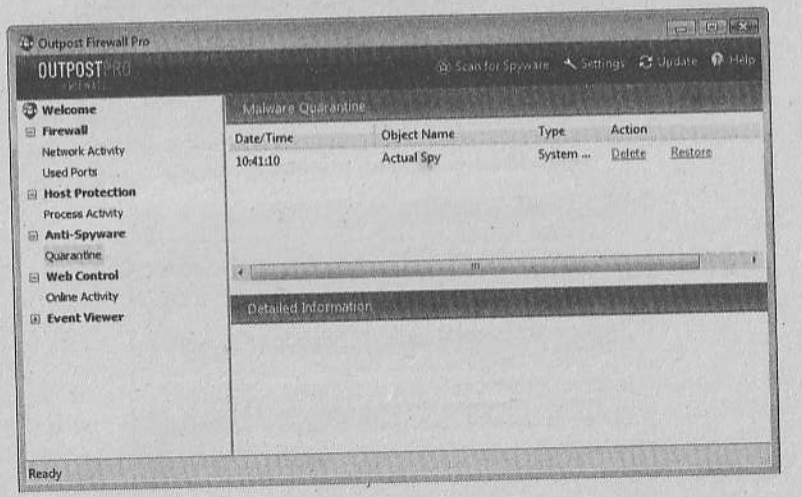


Рис. 10.31. Список помещенных в карантин объектов

В Outpost Firewall Pro имеется возможность настроить правила разрешения доступа любых программ к сети. Нажав кнопку *Settings* (*Настройки*) нужно выбрать *Network Rules* (*Сетевые*

правила) в группе *Firewall* (*Брандмауэр*) (рис. 10.32). Затем необходимо щелкнуть по соответствующей группе:

- *Blocked* (*Заблокированные*) – любые попытки соединения программ из данного списка с сетью блокируются;
- *Custom access* (*Индивидуальный доступ*) – позволяет выбрать условия, при которых будет разрешен доступ к сети;
- *Trusted* (*Доверенные*) – разрешены любые попытки соединения

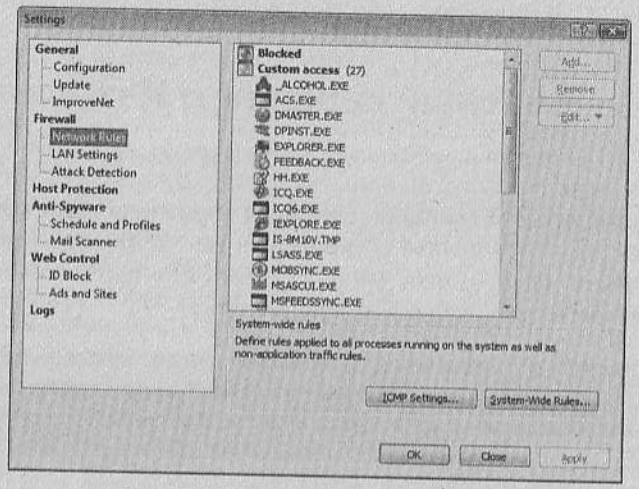


Рис. 10.32. Настройка сетевых правил

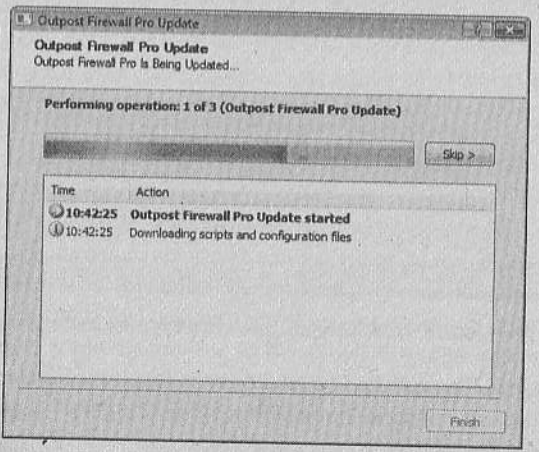


Рис. 10.33. Обновление баз

После щелчка по нужной группе необходимо нажать кнопку *Add* (*Добавить*), затем выбрать программу. Для удаления из данного списка нужно выбрать объект и нажать кнопку *Remove* (*Удалить*).

При помощи кнопки *Update* (*Обновить*) можно обновить базы данной программы. После нажатия на эту кнопку откроется окно с информацией о процессе обновления (рис. 10.33).

Глава 11
Безопасный серфинг в Интернете

При посещении веб-страниц пользователь может столкнуться с различного рода трудностями. Например, на компьютер могут проникнуть вирусы, которые распространяются по http-протоколу, повредить операционную систему и в дальнейшем создавать проблемы при работе с компьютером. Всплывающие окна, на которых кнопка *Закрыть* неочевидна или появляется спустя некоторое время, отвлекают от работы. Баннеры с flash-анимацией часто встречаются на веб-страницах и значительно влияют на скорость загрузки страниц и на объем интернет-трафика. Многие сайты пытаются привлечь внимание пользователя, используя средства раскрутки. При поиске в поисковых системах создается впечатление, что интернет-ресурс содержит нужную информацию, а на деле оказывается порно-сайтом или др.

Используя возможности браузеров, можно в некоторой степени обезопасить работу в Интернете. Рассмотрим подробнее некоторые браузеры.

Internet Explorer

Internet Explorer – наиболее популярный браузер, поскольку он входит в комплект стандартной поставки Windows. Внешний вид последней, седьмой, версии этого браузера представлен на рис. 11.1.

По сравнению с предыдущей версией в Internet Explorer 7 произошли радикальные изменения интерфейса. Прежде всего, веб-страницы ныне открываются в виде вкладок в одном и том же окне (между ними очень удобно переключаться). Таким образом, теперь у любителей Internet Explorer панель задач Windows не будет, как в прежние времена, полностью загромождена открытыми окнами этого браузера. Актуальность и удобство данно-

го нововведения очевидны, неясно лишь, почему оно появилось только в седьмой версии.

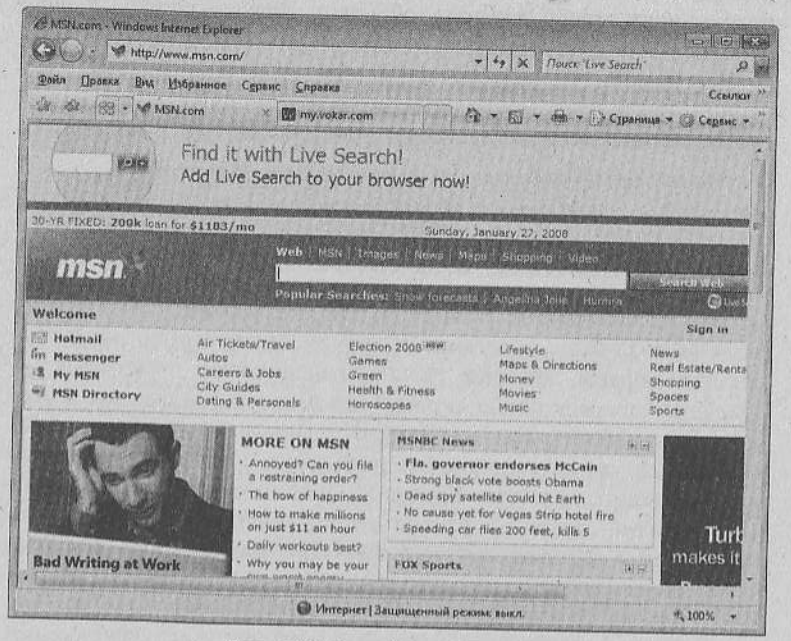


Рис. 11.1. Окно Internet Explorer

В седьмой версии Internet Explorer также добавлена возможность масштабирования веб-страницы (для этого нужно прокручивать колесико мыши, удерживая нажатой клавишу **Ctrl**).

Обратим внимание и на такое изменение интерфейса, как отсутствие строки главного меню. По умолчанию она отключена, и чтобы ее активировать, нужно щелчком правой кнопки мыши в области панели инструментов вызвать контекстное меню и выбрать в нем пункт *Строка меню*.

На рис. 11.2 показаны панели инструментов и строка меню Internet Explorer.

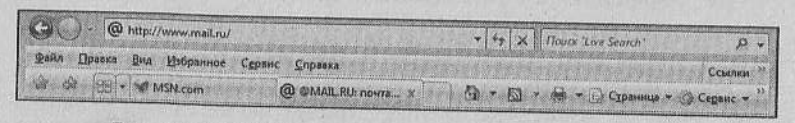


Рис. 11.2. Меню и панели инструментов Internet Explorer

Особое внимание разработчики уделили безопасности работы с веб-ресурсами в Internet Explorer 7: реализован механизм защиты от фишинга, появился защитный режим просмотра веб-страниц.

COOKIE

Cookie – это файлы, в которых веб-сайты сохраняют на компьютере пользователя некоторую информацию, что способствует более удобной и быстрой работе с данным ресурсом. Например, для входа на какой-нибудь веб-сайт необходимо ввести имя пользователя и пароль. После первого ввода и при условии, что хранение cookie разрешено, эти данные будут сохранены на компьютере пользователя, а при следующем посещении данного сайта эти данные будут введены автоматически.

Для настройки cookie необходимо в меню *Сервис* выбрать команду *Свойства обозревателя*. В появившемся окне нужно щелкнуть по вкладке *Конфиденциальность*. Перетаскивая бегунок, можно менять настройки файлов cookie. Шесть его различных положений соответствуют шести различным способам обработки файлов cookie (рис. 11.3).

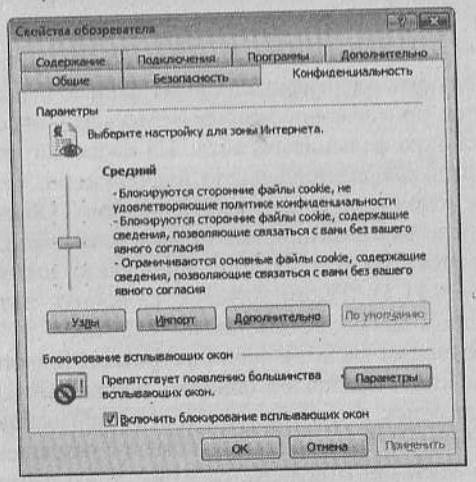


Рис. 11.3. Настройка для зоны Интернета

Для дополнительной настройки cookie нужно нажать кнопку *Дополнительно*. После этого появится окно, в котором можно настроить способ обработки файлов cookie. Есть возможность

настроить различные варианты действий с основными и сторонними файлами cookie (рис. 11.4), если поставить флажок *Перекрыть автоматическую обработку файлов "cookie"*. При включенной данной опции можно включить прием, блокировку или запрос для основных и сторонних файлов cookie.

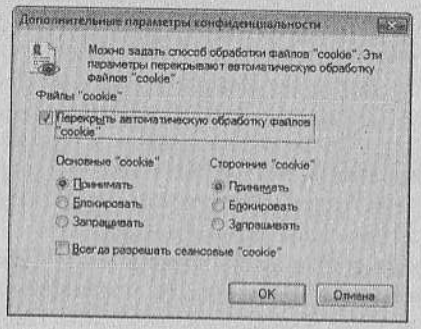


Рис. 11.4. Дополнительные параметры для файлов cookie

Путь, по которому сохраняются файлы cookies: C:\Documents and Settings\User\Cookies.

ФИШИНГ

Фишинг – вид интернет-мошенничества, при котором хакеры пытаются получить идентификационные данные пользователя. Этого добиваются при помощи массовой рассылки писем, в которых указаны ссылки на фальшивые сайты. На таких сайтах пользователь может оставить конфиденциальную информацию, которая будет в дальнейшем использована злоумышленниками. Обычно интернет-фишинг начинается с электронного письма со ссылкой.

После запуска Internet Explorer предложит настроить фильтр фишинга (рис. 11.5). Рекомендуется включить автоматический фильтр фишинга для более безопасной работы.

При включенном фильтре фишинга Internet Explorer сравнивает адреса посещаемых сайтов со списком подлинных сайтов. Также браузер ведет поиск в посещаемых сайтах признаков поддельных узлов. При обнаружении поддельного сайта с разрешения пользователя на сайт Microsoft отправляется адрес этого сайта, где в дальнейшем он проверяется и вносится в список фальшивых. При посещении такого рода сайтов будет отображено предупреждение.

Для включения или выключения фильтра фишинга нужно в меню *Сервис* выбрать команду *Свойства обозревателя*, в одноименном окне перейти на вкладку *Дополнительно* и установить переключатель *Включить автоматическую проверку веб-узлов* (рис. 11.6).

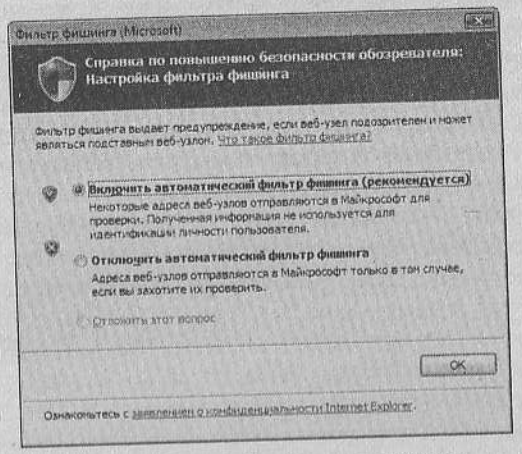


Рис. 11.5. Настройка фильтра фишинга

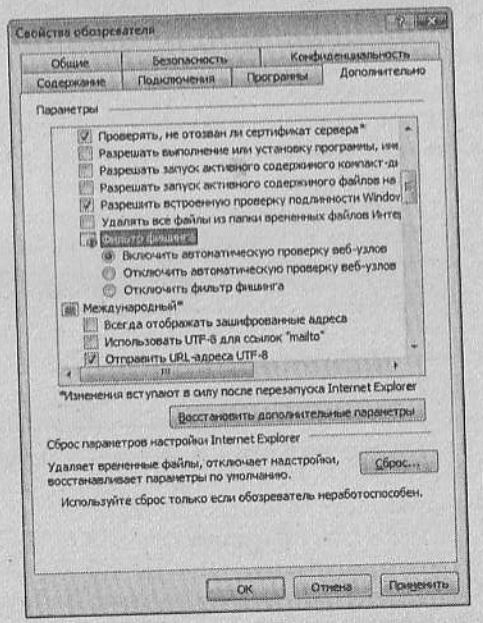


Рис. 11.6. Настройки фильтра на вкладке *Дополнительно*

ВСПЛЫВАЮЩИЕ ОКНА

Всплывающие окна – это небольшие окна, которые появляются поверх просматриваемой страницы. Чаще всего они содержат какую-нибудь рекламу. Так как это мешает работе и приводит к потреблению лишнего трафика, разработчики предусмотрели блокировку этих окон. Чтобы включить или выключить блокировку всплывающих окон, нужно в меню *Сервис | Блокирование всплывающих окон* выбрать команду *Выключить блокирование всплывающих окон* или *Включить блокирование всплывающих окон*. Для более подробной настройки следует в том же меню выбрать команду *Параметры блокирования всплывающих окон*. В появившемся окне можно добавить в список адреса узлов, получивших разрешение на всплывающие окна (рис. 11.7). Для этого надо ввести адрес узла в строку и нажать кнопку *Добавить*. Здесь же можно настроить некоторые другие параметры, например подачу звукового сигнала при блокировании всплывающего окна. При помощи выпадающего списка можно настроить уровень фильтра.

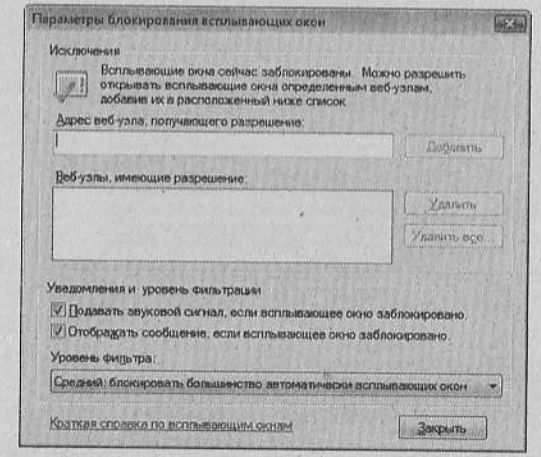


Рис. 11.7. Параметры блокирования всплывающих окон

Opera

Браузер Opera (рис. 11.8) компании Opera Software – достойный конкурент Internet Explorer (IE) и Netscape Navigator (NN). Он получил большое признание у пользователей. В отличие от

браузеров IE и NN, использующих исходные коды браузера Mozilla, Opera была написана с нуля на языке C++. Версия браузера 9 претерпела большие изменения по сравнению с предыдущими выпусками и стала действительно качественным продуктом, который поддерживает все стандартные функции и имеет улучшенную систему кэширования по сравнению с браузером Internet Explorer. Следует отметить, что важной особенностью текущей версии браузера Opera является его бесплатность. Также Opera отличается довольно быстрой загрузкой страниц и приятным дизайном. В браузере реализован MDI-интерфейс, контроль загрузки изображений отдельно для каждой открытой веб-страницы и многие другие полезные функции.

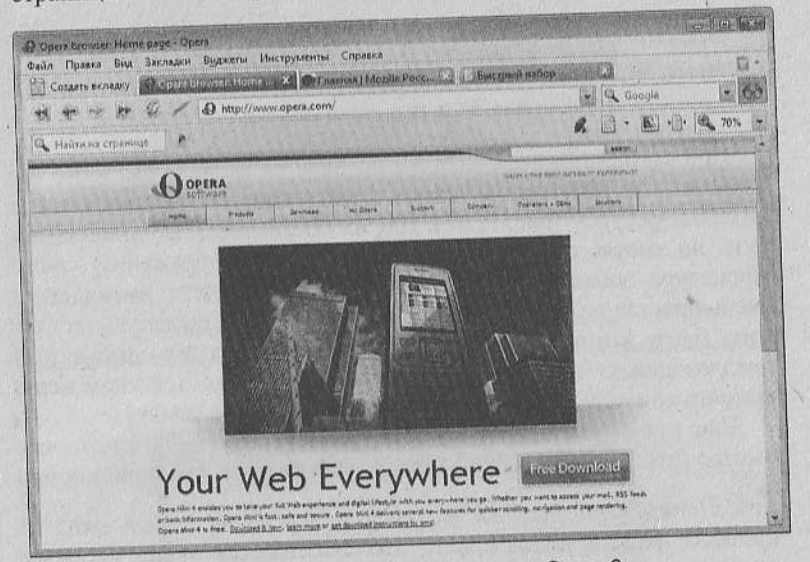


Рис. 11.8. Главное окно браузера Opera 9

Одной из особенностей Opera является наличие прекрасного менеджера закачек, что позволяет осуществлять контроль загрузки различных файлов из сети.

В Opera реализована поддержка подключаемых модулей, в частности Java 2 и Macromedia Flash Player, которые можно загрузить из Интернета или взять из дистрибутива NN, поскольку Opera поддерживает большое количество Netscape-совместимых подключаемых модулей. Кроме того, Opera поддерживает технологию

ShockWave и может воспроизводить звуковые файлы MID и WAV, показывать AVI-видео (при наличии соответствующих Plug-in).

Таким образом, браузер Opera благодаря своей компактности, быстроте и возможности тонкой настройки даже превосходит по некоторым параметрам своих конкурентов – Internet Explorer и Netscape Navigator.

Также, как и другие браузеры, Opera поддерживает работу со вкладками (рис. 11.9). Это дает возможность в одном окне работать одновременно с несколькими веб-страницами. Данный браузер обладает отличительной способностью поддерживать большое количество открытых вкладок с различными веб-страницами без заметного понижения скорости работы.

Рис. 11.9. Вкладки в Opera 9

При открытии новой вкладки появляется вкладка быстрого набора, на которой можно указать девять адресов на локальные и интернет-ресурсы (рис. 11.10). Для их посещения надо лишь щелкнуть по соответствующему уменьшенному изображению сайта. Процедура добавления нового адреса и изменения имеющегося очень простая и быстрая. Для добавления нужно щелкнуть по пустому месту и в появившейся форме ввести адрес или выбрать из предложенных. Чтобы изменить адрес, нужно в контекстном меню выбрать команду *Изменить* и также ввести новую ссылку.

Еще одна отличительная черта браузера Opera – возможность быстро отключать отображение рисунков при помощи кнопки *Показывать рисунки*, которая вынесена на панель окна. В процессе работы в Интернете это оказывается очень удобным инструментом, когда, например, при низкой скорости работы сайта отключение изображений заметно уменьшает трафик и сильно ускоряет процесс загрузки страницы. Отключение рисунков в других браузерах возможно лишь в настройках, что занимает относительно много времени.

Чтобы открыть окно настроек программы, нужно в меню *Инструменты* выбрать команду *Настройки*. В появившемся окне все опции распределены по пяти вкладкам (рис. 11.11). На первой вкладке *Общие* можно настроить некоторые функции, среди которых нужно отметить способ управления всплывающими окна-

ми. Есть возможность выбрать блокировку, открытие всех всплывающих окон, открытие их в фоновом режиме и блокировку незапрашиваемых окон.

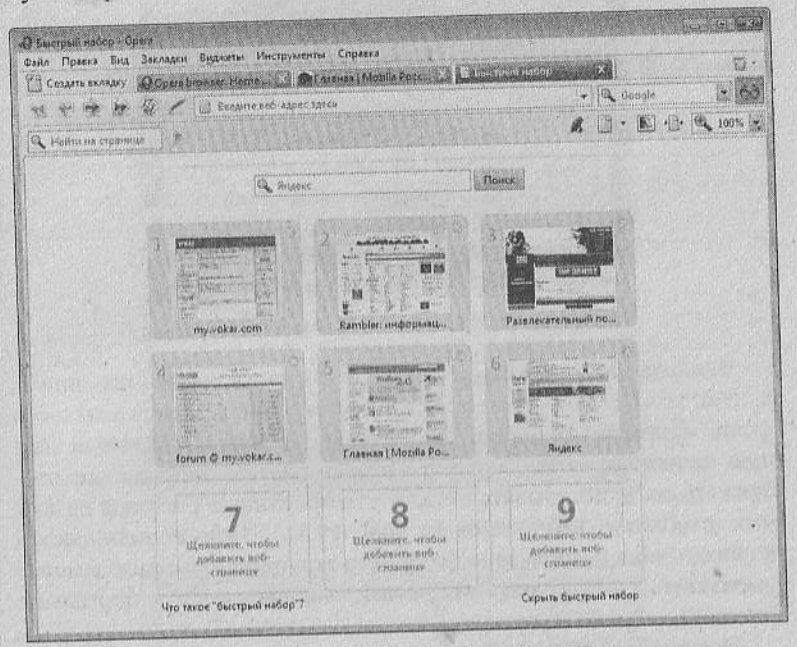


Рис. 11.10. Быстрый набор в Opera 9

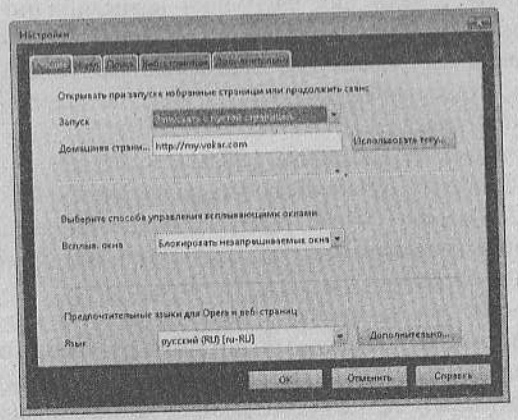


Рис. 11.11. Общие настройки в Opera

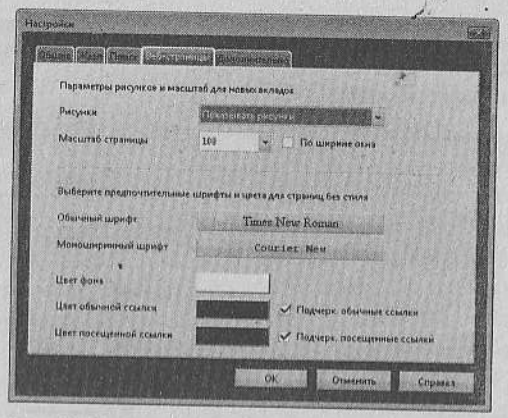


Рис. 11.12. Настройка отображения веб-страниц

Вкладка *Веб-страницы* дает возможность настроить шрифт и цвет текста, отображаемого на веб-страницах, цвета ссылок и фона, масштаб страницы. Также здесь можно настроить полезную функцию, позволяющую отображать все рисунки, не отображать их и показывать только кэшированные рисунки на любых открытых веб-страницах (рис. 11.12). При использовании дорогостоящего доступа к Интернету эта опция помогает заметно уменьшить расход трафика. Кстати, данная опция в программе Internet Explorer отсутствует.

Последняя вкладка *Дополнительно* содержит большое количество опций. Среди них настройки навигации по страницам, уведомлений, шрифтов, сохранения истории. В группе *Безопасность* находится управление сертификатами. Здесь же можно настроить «горячие» клавиши и управление браузером при помощи голоса (рис. 11.13).

Opera позволяет настроить файлы cookies для каждого сайта отдельно. Для этого нужно щелкнуть по группе *Cookies*, после чего выбрать *Принимать cookies* и другие опции по своему усмотрению. После выбора всех необходимых опций следует нажать кнопку *Управление cookies*.

После нажатия на кнопку откроется окно, в котором будет отображен список посещенных интернет-ресурсов, которые сохранили на компьютере пользователя файлы cookies. Любые из них можно удалить при помощи кнопки *Удалить*. Для настройки параметров этих файлов нужно нажать кнопку *Добавить*, после

чего в появившемся окне ввести адрес веб-узла, параметры файлов cookies и некоторые другие опции. После окончания необходимо нажать *OK*. После этого данный веб-узел будет добавлен в список и при его посещении будут выполняться все действия в соответствии с указанными настройками (рис. 11.14).

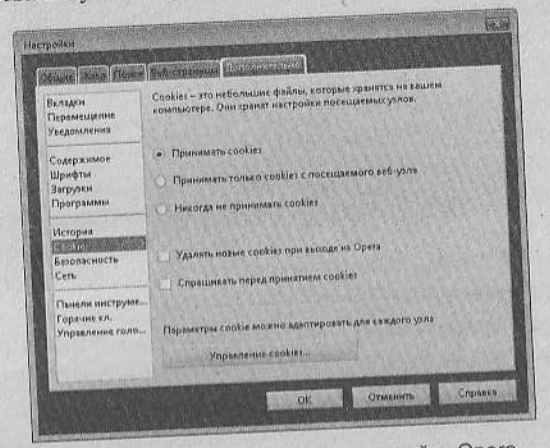


Рис. 11.13. Дополнительные настройки Opera

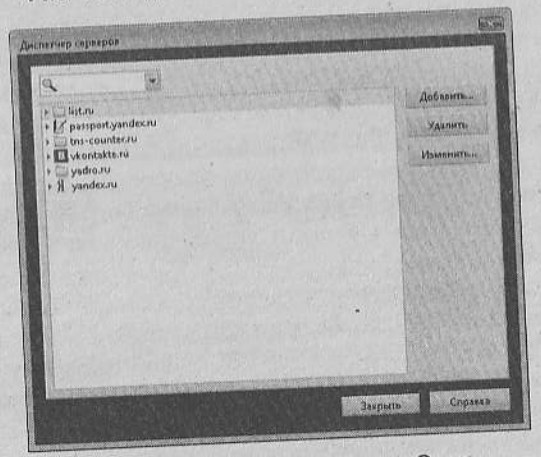


Рис. 11.14. Диспетчер серверов Opera

Недостатком браузера Opera можно считать отсутствие некоторых русских кодировок в английских версиях программы. Еще один существенный недостаток – ненадежная работа со скриптами.

Mozilla Firefox

Причина высокой популярности браузера Mozilla Firefox – простота его освоения. Действительно, интерфейс Firefox лаконичен, в нем есть пять основных кнопок на панели инструментов, за пределами которых лежит непознанная бесконечность – пользователю не нужно метаться в муравейнике значков, пунктов меню и панели настроек.

В этом браузере (рис. 11.15), как и в рассмотренных ранее, пользователю предоставляется возможность работать сразу с несколькими веб-страницами в пределах одного окна. Следует отметить работу со всплывающими окнами, открывающимися при работе со многими сайтами. Пользователь может самостоятельно указывать, с каких сайтов разрешать открытие всплывающих окон, а с каких нет.

Рядом со строкой ввода находится панель поиска. При поиске реализована возможность использования множества поисковых серверов.

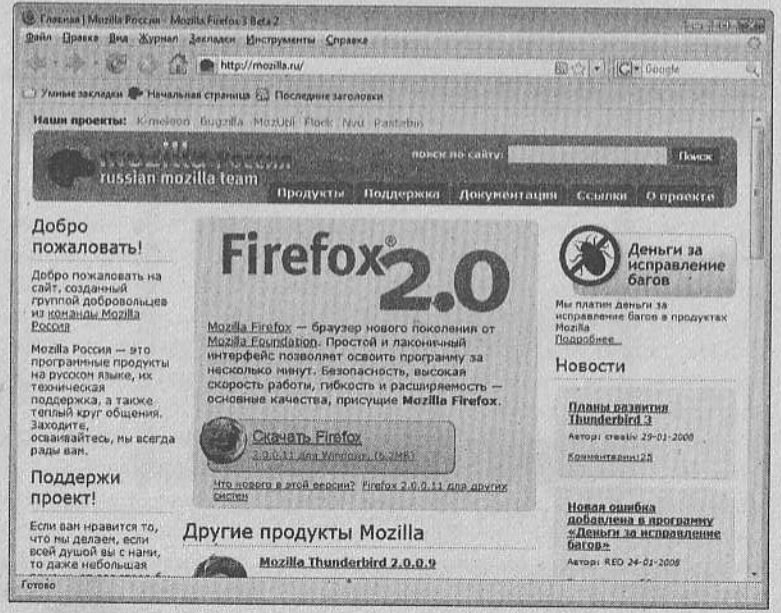


Рис. 11.15. Главное окно браузера Mozilla Firefox

По сравнению со своими аналогами данный браузер наиболее расширяемый и гибко настраиваемый. Пользователь может отображать панели инструментов, ставить дополнительные модули расширения и темы оформления. Mozilla Firefox подобно телескопической удочке может превращаться из маленького компактного браузера в удивительно многофункциональный инструмент для путешествий по всемирной сети.

В правом верхнем углу главного окна браузера находится поиск, в котором можно выбрать поисковую систему при помощи кнопки. В строчку, находящуюся рядом, нужно вводить слова или выражения, по которым будет происходить поиск (рис. 11.16). Можно скачать дополнительные поисковые плагины, нажав *Управление поисковыми плагинами* и выбрав в появившемся окне *Установить другие поисковые плагины*.

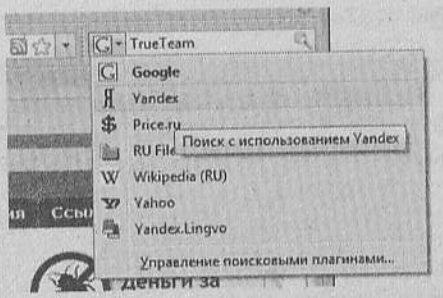


Рис. 11.16. Поиск в Mozilla Firefox

Настройка параметров для безопасной работы в Интернете выполняется в окне, открываемом при помощи вызова команды *Настройки* в меню *Инструменты*. Здесь все опции также разделены на несколько вкладок для ускорения поиска.

На первой вкладке *Основные* можно выбрать домашнюю страницу, путь для сохранения файлов, а также настроить данную программу как браузер по умолчанию (рис. 11.17).

Вкладка *Содержимое* дает возможность выбрать шрифт, его размер и цвет, которым будет отображаться содержимое веб-страниц, активировать блокировку всплывающих окон, автоматическую загрузку рисунков, а также использование Java и JavaScript. Есть возможность выбрать исключения. Здесь же можно выбрать предпочтительный язык для отображения страниц (рис. 11.18).

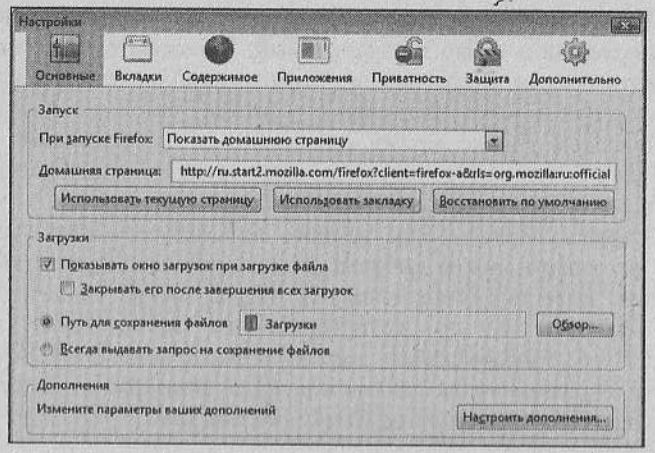


Рис. 11.17. Основные настройки Mozilla Firefox

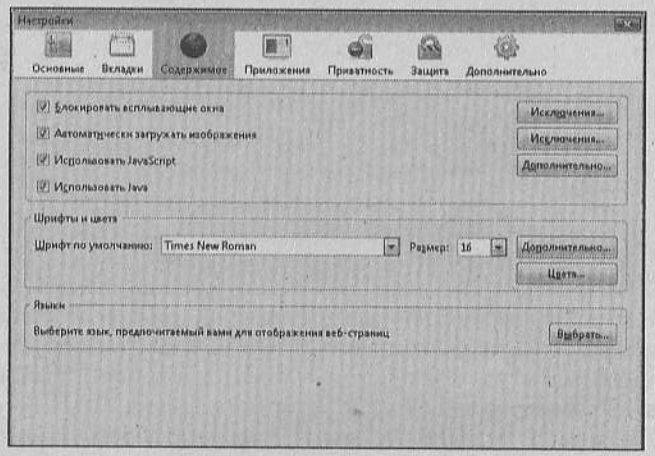


Рис. 11.18. Настройка отображения содержимого веб-страниц

На вкладке *Приватность* (рис. 11.19) можно настроить опции журнала посещений, сохранение адреса посещенных веб-страниц. При помощи кнопки *Показать cookies* можно просмотреть файлы cookie, но отсутствует возможность настроить их для каждого сайта отдельно. Можно удалять файлы cookie отдельно или все сразу. Присутствует функция поиска среди этих файлов.

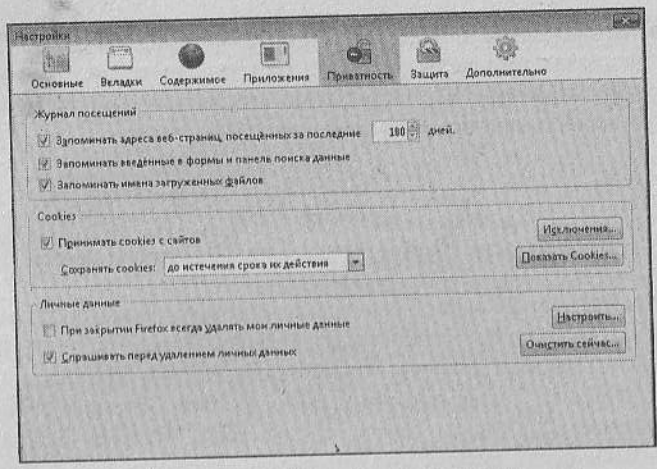


Рис. 11.19. Настройки приватности

На вкладке *Защита* (рис. 11.20) можно активировать или отключить антифишинговую проверку посещаемых веб-узлов, настроить его, включить запоминание паролей, предупреждения при попытках сайтов установить дополнения и др.

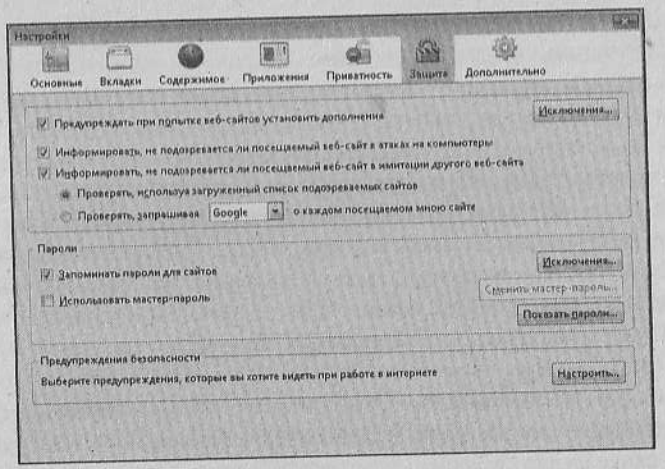


Рис. 11.20. Настройка защиты Firefox

Недостатками данного браузера являются невозможность добавления кнопки отключения изображений на панель главного

окна (отключается только в настройках), замедление работы во всех вкладках при загрузке одной из них. Также при случайном закрытии страницы ее необходимо открывать заново (в Opera можно вернуть при помощи команды *Undo*).

Глава 12
Закачка файлов из Интернета

Рассмотренные выше браузеры имеют возможность сохранять только открытую веб-страницу, но бывают моменты, когда пользователю нужно сохранить большое количество страниц или даже целый сайт. Также при скачивании файлов больших размеров из Интернета браузеры часто теряют связь, поэтому эффективность и скорость скачивания снижается. Для решения этих проблем существуют специальные программы, которые и описываются в данной главе.

Teleport Pro

При работе в сети Интернет у пользователя нередко возникают ситуации, когда необходимо сохранить ту или иную веб-страницу, а иногда и полностью портал на внешнем носителе. При этом можно воспользоваться возможностями браузера, который позволяет сохранить содержимое необходимой страницы, но это недопустимо, например, в случае сохранения некоторого раздела сайта. Для решения такого рода задач может оказаться очень полезной утилита *Teleport Pro* (рис. 12.1). Эта программа позволяет полностью загрузить требуемый раздел сайта, изменяя при этом содержимое HTML-кода, т.е. меняя ссылки, рисунки и т.д.

Программа Teleport Pro является полностью автоматическим, многопотоковым, перемещающимся по ссылкам и принимающим файлы «роботом-пауком». Это означает, что вся иерархия сайта будет сохранена на диске пользователя, а в ссылки на загруженном сайте будут добавлены соответствующие изменения.

Помимо этого, Teleport Pro может просматривать сайт, проверяя наличие файлов определенного типа и размера, искать страницы на сайте по ключевым словам, создавать список всех страниц и файлов сайта.

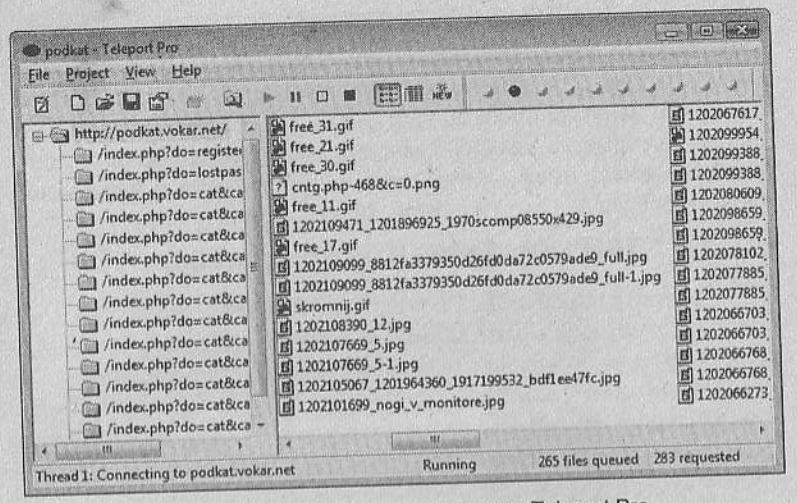


Рис. 12.1. Диалоговое окно утилиты Teleport Pro

Для того чтобы задать программе необходимые условия закачки сайта, следует воспользоваться кнопкой *New Project Wizard*, расположенной в левом верхнем углу. После нажатия этой кнопки появится окно (рис. 12.2), в котором пользователь должен определиться с выбором желаемых действий:

- *Create a browsable copy of a website on my hard drive* – создание копии сайта на жесткий диск компьютера с учетом сохранения целостности ссылок;
- *Duplicate a website, including directory structure* – копирование содержимого сайта с учетом структуры каталогов (в первом случае системой не поддерживается копирование древовидной структуры каталогов);
- *Search a website for files of certain type* – поиск на сайте файлов определенного типа;
- *Explore every site linked from a central site* – копирование всех сайтов, на которые ссылается центральный сайт;
- *Retrieve one or more files at known addresses* – поиск и загрузка файлов по определенному адресу;
- *Search a website for keywords* – поиск по ключевому слову на выбранном сайте.

Если вдруг программа обнаружит некорректную ссылку и не сможет скачать нужный файл, Teleport Pro сообщит об этом поль-

зователю. В этом случае можно сохранить проект и впоследствии запустить его еще раз на обработку. При этом Teleport Pro будет скачивать только те файлы, которые изменились со времени предыдущего запуска проекта, или снова попытается загрузить те файлы, которые не удалось скачать ранее. Таким образом, пользователь может иметь самую актуальную и полную версию интернет-ресурса на своем жестком диске.

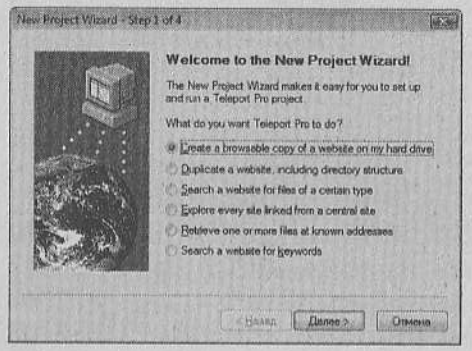


Рис. 12.2. Настройка мастера создания нового проекта

Рассмотрим использование утилиты Teleport Pro на примере создания копии раздела некого сайта. Для этого следует выбрать в диалоговом окне (рис. 12.2) опцию *Create a browsable copy of a website on my hard drive* и нажать кнопку *Далее*. Следующий шаг работы мастера – установка начальной страницы загрузки и названия, которое можно будет определить для копии начальной страницы. Затем с помощью мастера будет осуществлена установка следующих параметров загрузки (рис. 12.3):

- *Just text* – загрузка только текста;
- *Text and graphics* – загрузка текста и графических объектов;
- *Text, graphic, and sound* – загрузка текста, графических объектов и звука;
- *Everything* – загрузка всех объектов данного раздела сайта.

Если для доступа к этому разделу сайта требуется ввести имя пользователя и пароль, то в полях *Account* и *Password* необходимо указать соответствующую информацию.

Последний шаг работы мастера – сохранение проекта на компьютере, после чего необходимо будет воспользоваться кнопкой  *Start* для начала процесса загрузки.

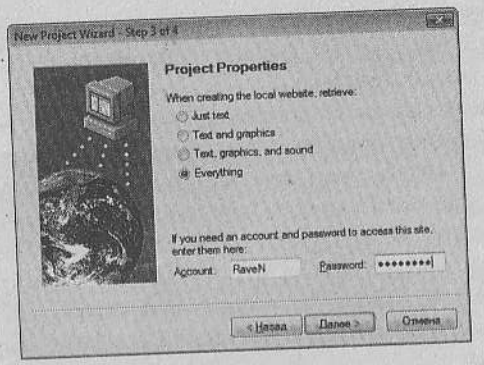


Рис. 12.3. Настройка параметров загрузки элементов сайта

ReGet

При работе в сети Интернет загрузка файлов осуществляется штатными методами браузеров. Главным недостатком этого процесса является отсутствие сохранения промежуточных данных. Иными словами, только по завершении загрузки необходимого файла из Интернета программы-браузеры производят его запись на диск. При этом часто возникает ситуация, когда в процессе загрузки файла происходит сбой связи, что может привести к потере уже загруженной его части. Для решения таких проблем используются специальные утилиты.

ReGet – одна из наиболее популярных программ в этом списке; она отличается высокой надежностью и удобством использования. Кроме того, она совершенствует процедуру загрузки файлов из Интернета. Как уже отмечалось, распространенной проблемой при загрузке файла при использовании стандартных средств различных браузеров (не только Internet Explorer) является то, что при обрыве связи или сбое компьютера повторную загрузку приходится осуществлять с самого начала файла, теряя таким образом всю загруженную ранее часть. Программа ReGet позволяет решить эту проблему, возобновляя загрузку с того места, где она прервалась, т.е. даже при плохом качестве связи можно добиться полной загрузки файла. Вместе с тем программа обладает рядом дополнительных возможностей, включая автодозвон и выключение компьютера по окончании загрузки файлов, что позволяет составить расписание самостоятельной работы

утилиты. Здесь можно также установить специальное время для дозвона, чтобы загрузка файлов проходила в то время, когда связь наиболее оптимальна.

Для начала работы с программой пользователю не нужно производить никаких настроек программы – автоматическая настройка всех параметров производится вместе с установкой и рассчитана на оптимальное использование. Все необходимые установки, которые приходится указывать в остальных программах загрузки файлов, ReGet отыскивает в настройках браузера. Это означает, что после установки программа сканирует реестр Windows и использует те же настройки и параметры соединения, что и браузер.

Обычно один и тот же файл в сети Интернет можно загрузить с нескольких серверов. Чаще всего процедура поиска и загрузки файла происходит в два этапа:

- первоначальный поиск серверов, на которых можно произвести загрузку;
- выбор наиболее удобного сервера, с помощью которого загрузка файла будет быстрее, надежнее и т.д.

В утилите ReGet находится встроенный перечень «зеркальных» серверов самых популярных сайтов и FTP-серверов, что позволяет ей самостоятельно определять наиболее удобный адрес для загрузки файла. При неудачной загрузке файла система может воспользоваться встроенным поиском для нахождения других источников для загрузки.

ReGet позволяет продолжить прерванный процесс загрузки файла после любых сбоев, если только возможность продления загрузки поддерживается сервером. Следует заметить, что популярное хранилище файлов RapidShare продление загрузки, так называемую докачку, не поддерживает. Если причиной разрыва соединения было прекращение связи с сервером, утилита повторит попытку соединения с ним через некоторое время. Эта функция также может быть полезна в ситуации, когда нужно соединиться с занятым сервером. При обрыве модемного соединения ReGet сумеет перезвонить провайдеру и восстановить связь. Даже в случае зависания или перезагрузки компьютера, а также аварийного завершения ReGet уже загруженная часть файла будет сохранена.

ReGet дает возможность загружать несколько файлов одновременно. Для каждого файла можно установить приоритет загрузки, чтобы он занимал бóльшую или меньшую долю отведенной пропускной способности канала связи. При этом можно создать расписание загрузки.

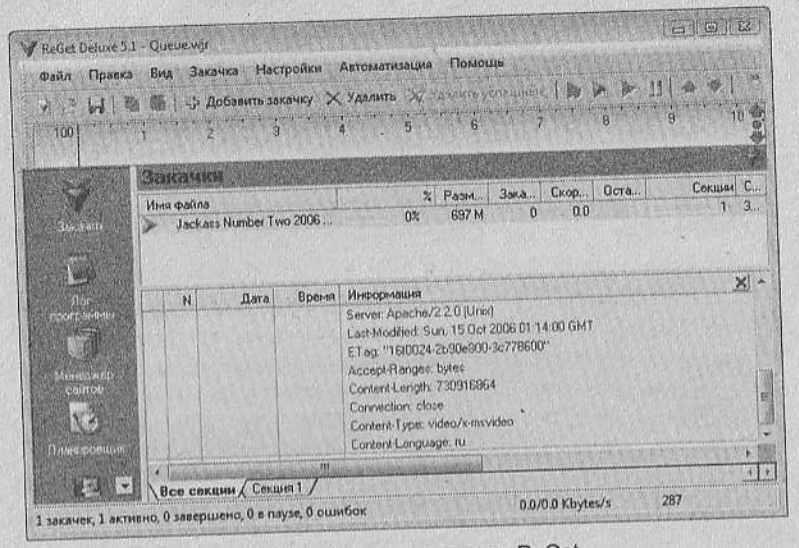


Рис. 12.4. Окно программы ReGet

В главном окне программы (рис. 12.4) отображается вся информация о текущих загрузках файлов (в терминах программы – *закачках*), а также информация о скорости соединения.

Одним из достоинств данного продукта является то, что в инсталляционный пакет программы входят различные языковые модули, в том числе и модуль русского языка (что не удивительно, поскольку разработчиками программы являются российские программисты). Сразу же после инсталляции пользователь имеет возможность установить язык интерфейса программы. Например, для установки русского языка необходимо в меню *View* (*Вид*) выбрать команду *Language* | *Russian*.

Интерфейс программы состоит из главного окна и нескольких панелей. Информация главного окна является контекстнозависимой, поскольку в нем отображается информация соответствующего раздела. Слева от главного окна расположена *Панель ReGet*, на ней находятся кнопки, описание которых представлено в табл. 12.1.

Таблица 12.1
Кнопки панели ReGet

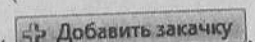
Кнопка	Название	Описание
	*Закачки*	Позволяет открыть окно закачек, в котором отображаются все запланированные закачки
	*Лог программы*	Открывает окно, в котором отображаются все события, которые происходили в процессе работы программы, номер события, дата и время, когда оно произошло, и его описание
	*Менеджер сайтов*	Менеджер сайтов является средством программы, позволяющим настроить параметры подключения к каждому из серверов, с которых происходит загрузка. Обычно настраиваются такие параметры, как логин и пароль, необходимые для подключения к сайту, а также максимальное число подключений к сайту
	*Планировщик*	Данное средство позволяет составить расписание работы программы. Пользователь имеет возможность автоматизировать такие действия: запуск антивирусной программы после загрузки файла; установку соединения с провайдером в заданные моменты времени; завершение работы программы при определенных условиях; выключение компьютера
	*История*	Данное окно содержит информацию об уже загруженных файлах. В нем отображается имя файла, его адрес, размер и время завершения закачки
	*Поиск*	Это средство позволяет осуществлять поиск файлов, используя большое количество поисковых систем. При задании критериев поиска и нажатии на кнопку *Поиск* ReGet отправляет запросы на поисковые системы, а затем отображает результаты поиска в окне.

Кнопка	Название	Описание
		При этом происходит фильтрация результатов для выявления дублирующихся файлов. Также ReGet осуществляет проверку найденных серверов на возможность загрузки требуемых файлов
	*FTP Explorer*	Данное средство программы является браузером, который позволяет просматривать сайты, используя протокол FTP

Процедура передачи утилите адреса файла, требующего загрузки, может выполняться одним из следующих способов:

- ручным вводом нужной ссылки;
- копированием необходимой ссылки через буфер обмена, который также находится под контролем утилиты;
- отслеживанием нажатий на ссылки в наиболее популярных браузерах, при этом происходит проверка их на присутствие файла для закачки (например, по расширению файла: ZIP, EXE и т.д.). После этого автоматически начинается процесс загрузки требуемого файла;
- перетаскиванием ссылки на иконку утилиты ReGet, которая обычно находится поверх остальных окон .

Для ручного ввода адреса ссылки необходимо выполнить одно из таких действий:

- нажать на кнопку  , которая находится на панели инструментов программы;
- выбрать в меню *Закачка* команду *Добавить закачку*;
- нажать на клавишу **Insert**.

При любом способе указания адреса загружаемого файла будет открыто окно *Свойства* (рис. 12.5).

В поле *URL* указывается адрес загружаемого файла. При ручном вводе адреса это поле будет пустым, а во всех остальных случаях программа автоматически подставит адрес.

В поле *Описание закачки* можно добавить информацию о загружаемом файле. Это полезно в том случае, когда в очереди закачки находится большое количество файлов и, как это часто бывает, их имена не очень понятны.

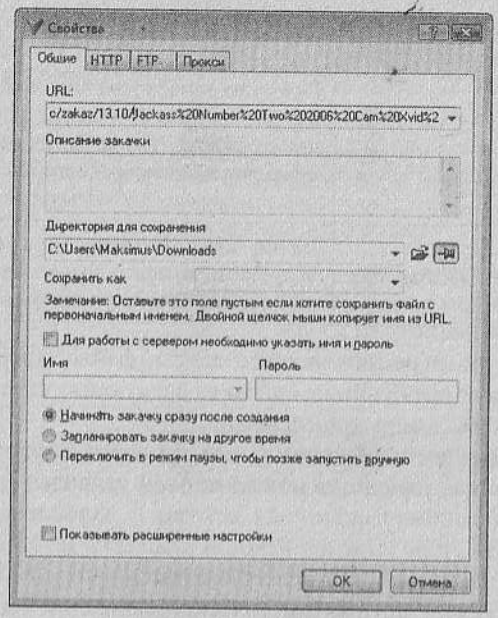


Рис. 12.5. Окно свойств закачки файла

В поле *Директория для сохранения* указывается каталог, в котором будет сохранен загруженный файл. По умолчанию программа создает каталог *My Downloads*, однако его легко можно изменить, нажав на кнопку  *Выбор папки* и указав любой другой каталог. Если же после выбора каталога нажать на кнопку  , данный каталог станет каталогом по умолчанию, т.е. все последующие файлы будут сохраняться в нем.

Если имя загружаемого файла непонятно и возникает необходимость его переименования, нужно использовать поле *Сохранить как*, в котором можно указать новое имя файла. Данная опция очень удобна, однако нужно внимательно следить за указываемым типом, поскольку он должен совпадать с типом загружаемого файла.

Когда для доступа к серверу, на котором находится загружаемый файл, требуется указать пароль, следует поставить соответствующий флажок, а также заполнить поля *Имя* и *Пароль*.

Также в окне можно указать время начала закачки файла.

Download Master

В завершение обзора программ для закачки файлов из Интернета рассмотрим программу Download Master. Эта программа, хотя и рассматривается последней, пожалуй, является эталоном для пользователя, который никогда не сталкивался с «качалками». Интуитивно понятный интерфейс делает работу комфортной и непринужденной, а наличие русскоязычного меню добавляет еще бóльшую привлекательность данному продукту. Программа обладает большим количеством различных настроек. Download Master способна быстрее обычных браузеров производить закачки, используя специальную технологию. При наличии всех необходимых функций для закачки файлов, при стабильной работе и постоянном обновлении программа Download Master является бесплатной. Рассмотрим поподробнее способы и тонкости работы в этой высокоэффективной программе.

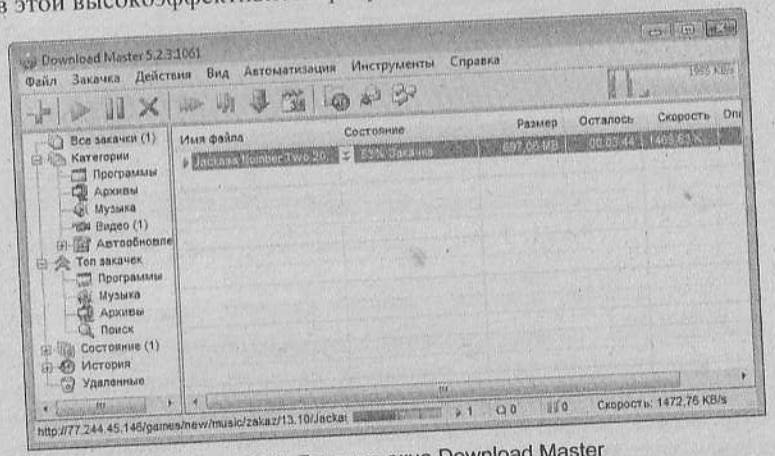


Рис. 12.6. Главное окно Download Master

Главное окно изображено на рис. 12.6. В самом верху окна располагается меню, содержащее все функции, доступные в программе: действия с текущими закачками, настройки вида окон, автоматические действия, а также настройки соединения, закачки, расписания и др.

Под строкой меню располагаются кнопки быстрого доступа к наиболее важным функциям программы: добавление, приостанов-

ка, удаление закачки, возобновление всех приостановленных, остановка всех текущих закачек, ограничение скорости скачивания.

Чтобы добавить закачку, можно воспользоваться кнопкой *Добавить закачку*. После этого появится окно, в котором требуется ввести URL-адрес необходимого файла (рис. 12.7). В следующих полях можно выбрать категорию скачиваемого файла и ввести его описание.

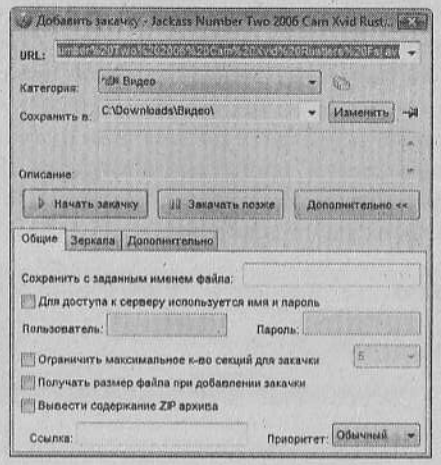


Рис. 12.7. Настройка скачиваемого файла

Для начала закачки файла следует нажать кнопку Начать закачку – откроется окно, в котором будут отображаться имя скачиваемого файла, описание, скорость скачивания, прошедшее и оставшееся время данной закачки, адрес, по которому сохраняется данный файл, а также графическое отображение скаченных секторов (рис. 12.8).

При необходимости приостановить закачку файла, нужно выделить ее в главном окне и нажать кнопку *Приостановить закачку*. Для продолжения загрузки файла можно воспользоваться кнопкой *Проверить обновление*. Если по текущему адресу расположена новая версия установщика программы или какой-либо другой файл, программа начнет его скачивать. Чтобы удалить закачку, следует воспользоваться кнопкой *Удалить закачку* или нажать клавишу **Delete**.

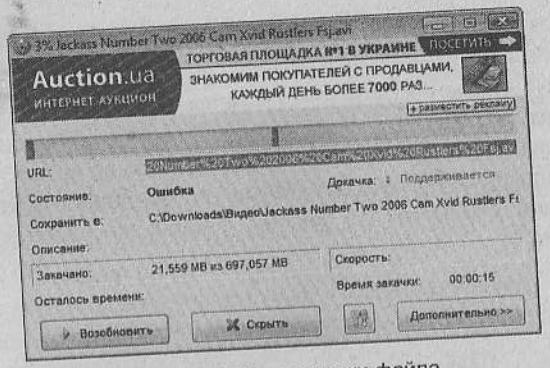


Рис. 12.8. Окно закачки файла

Для настройки данной программы надо выбрать команду *Настройка* в меню *Инструменты*. Появившееся окно содержит древовидную структуру, в которой распределены все настройки по группам, поэтому любую настройку можно быстро найти и изменить требуемым образом (рис. 12.9).

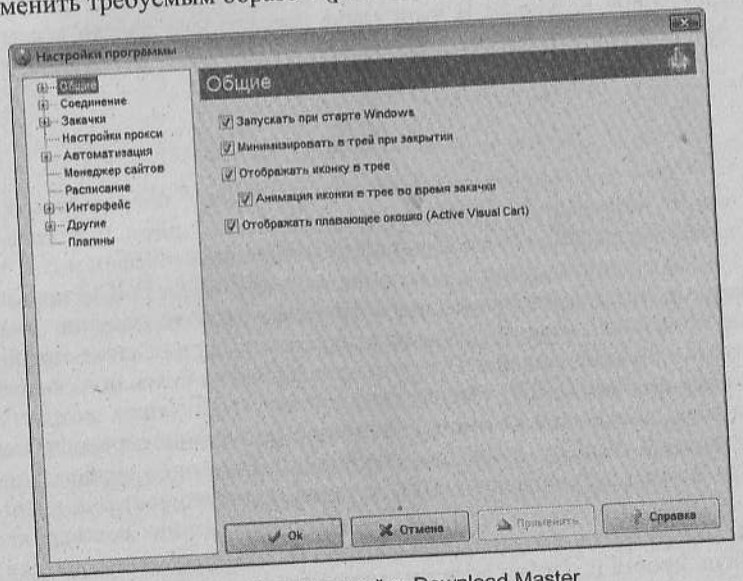


Рис. 12.9. Настройки Download Master

Download Master поддерживает подключаемые модули, что дает возможность расширить функциональность программы, бы-

стро проверить наличие новой версии данной программы, содержит несколько языков интерфейса, оптимальные настройки для различных типов соединения. Наличие истории закачек, поиска, возможности работы с командной строкой и способность прослушать и просмотреть аудио- и видеофайлы во время их закачек делает программу Download Master очень мощной многофункциональной утилитой для закачек файлов из локальной сети и Интернета.

Глава 13
Общение в Интернете

Интернет предоставил пользователям новый вид общения при помощи отправки друг другу текстовых сообщений. Даже находясь в разных точках Земного шара, сообщения доходят за несколько секунд. Существующие для этого программы занимают мало места на жестком диске и используют очень мало трафика и системных ресурсов. В этой главе рассмотрена работа в самых распространенных клиентах.

ICQ

ICQ – это своеобразный интернет-пейджер, посредством которого допускается общение пользователей, прием и отправка почты, отправка SMS-сообщения на мобильный телефон и т. д.

Это средство создала компания Mirabilis LTD. В ICQ пользователи, предварительно зарегистрировавшись и получив свой персональный номер (UIN), могут общаться как в режиме онлайн, так и в режиме офлайн. Программа позволяет искать пользователя по номеру (UIN), имени, псевдониму (NickName), возрасту, интересам и т.д. ICQ имеет обширную сеть своих серверов, что повышает скорость передачи сообщений. Еще одна особенность программы заключается в том, что она поддерживает ряд внешних интернет-приложений, т.е. интернет-телефонию, сетевые игры, почту и т.д. «Аська», как ласково ее именуют пользователи, очень проста и удобна в своих системных настройках. О ее популярности свидетельствует тот факт, что к началу 2000 года количество пользователей ICQ составляло около 60 млн, а к концу 2002 года – уже около 180 млн.

При обмене сообщениями в режиме онлайн ICQ соединяет компьютеры пользователей напрямую, без использования промежуточных серверов. А значит, общение происходит в реальном времени. Программа позволяет обмениваться не только сообщениями, но и любыми файлами, а также общаться при помощи микрофона и веб-камеры.

Даже если собеседник не подключен к сети, ему можно отправить текстовое сообщение – оно будет храниться на сервере и адресат получит его при выходе в сеть.

Для запуска программы ее нужно проинсталлировать, предварительно скачав установочный архив с http://icq.com/download. Устанавливается программа достаточно просто, безо всяких хитростей. На первом шаге появится экранная форма (рис. 13.1), на которой представлены общие сведения об устанавливаемом программном продукте. Можно изменить путь, по которому будет выполнена инсталляция. Для того чтобы изменить название папки или весь путь для установки, используют кнопку *Change (Изменить)*.

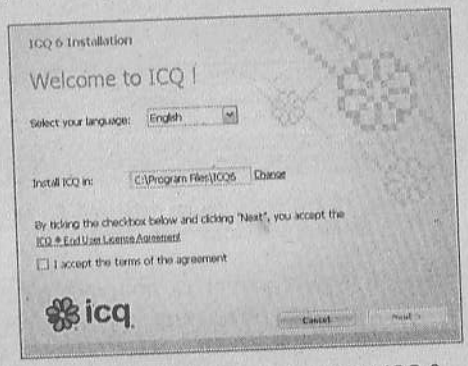


Рис. 13.1. Первый шаг установки ICQ 6

После нажатия кнопки *Next* появится экранная форма с лицензионным соглашением. Затем произойдет распаковка файлов, их копирование в папку установки, и после этого можно будет считать, что программа установлена. Однако это еще не все.

Для работы с программой необходимо зарегистрировать пользователя. Процесс регистрации пользователя запускается при нажатии на кнопку *Get a new account*.

При регистрации вначале появится лицензионное соглашение. После нажатия кнопки *Next* появится экранная форма (рис. 13.2),

в которой необходимо указать информацию об имени пользователя, его псевдониме (Nickname), адресе электронной почты и пароле доступа. Последний является обязательным атрибутом и необходим для того, чтобы UIN абонента не смог использовать другой человек.

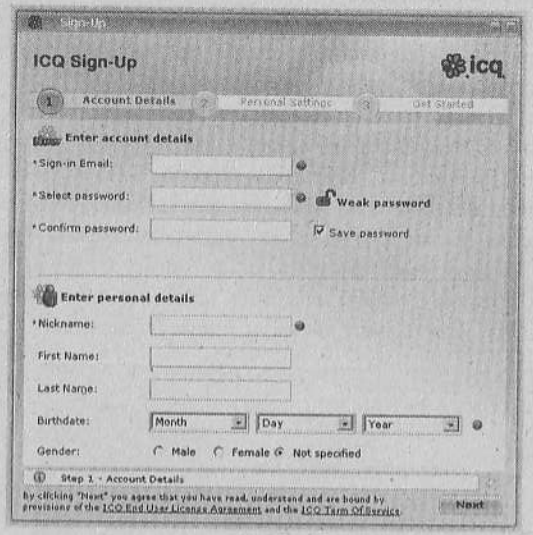


Рис. 13.2. Форма ввода первичных данных пользователя ICQ 6

На этой экранной форме вводится дополнительная информация о пользователе: пол, дата рождения, страна и город проживания, языки, на которых пользователь может общаться, и т.п.

После этого происходит процесс регистрации нового пользователя. Следует иметь в виду, что это занимает определенное время. При этом пользователь получает свой UIN и имеет возможность указать режим работы ICQ, когда другие пользователи могут с ним общаться либо беспрепятственно, не требуя разрешения (авторизации), либо только после авторизации со стороны пользователя. По мнению авторов, последний режим более предпочтительный. На последнем шаге регистрации пользователю предлагается воспользоваться несколькими сервисами, которые существуют в ICQ: поиск друзей в ICQ, установка в качестве главной веб-страницы браузера домашней страницы компании Mirabilis, подключение к

системе общения в реальном масштабе времени (ICQ-чат) и возможность включения в отправляемые электронные письма сигнатуры с указанием текущего статуса пользователя в сети.

После этого, собственно, и произойдет запуск программы, где необходимо будет ввести свой пароль. Напомним, что вместе с UIN для пользователя создается своя ICQ-страница в Интернете по адресу www.icq.com/<UIN пользователя>, с которой можно послать сообщение, даже не имея ICQ. Еще существует возможность посылать так называемый EmailExpress – для этого достаточно написать обычное электронное сообщение по адресу <UIN пользователя>@pager.mirabilis.com, и оно почти сразу придет на ICQ-пейджер.

Для комфортной работы следует немного настроить программу. Когда пользователь находится в режиме онлайн, в системном лотке (System Tray) (справа внизу на панели задач) ICQ покажет значок зеленого цвета (рис. 13.3а). Если же пользователь некоторое время на компьютере не работает, значок изменится и станет таким, как это показано на рис. 13.3б.

а б

Рис. 13.3. Системный значок ICQ:
а – режим онлайн; б – режим офлайн

Для работы ICQ использует специальные серверы. Можно добавить альтернативные серверы ICQ, чтобы программа работала быстрее – ведь главный сервер часто бывает очень перегружен. Поэтому в свойствах программы можно указать такие серверы:

icq3.mirabilis.com, icq4.mirabilis.com, icq5.mirabilis.com.

ICQ стандартно использует для соединения порт 4000, однако при работе на компьютерах, защищенных брандмауэрами, ICQ может автоматически определить прокси-настройки Интернета.

После регистрации на экране компьютера появится рабочее окно программы. Однако для начала следует включить в так называемый список контактов тех, с кем вам необходимо общаться. Для этого в рабочем окне нужно нажать кнопку *Add* – появится диалог, представленный на рис. 13.4.

Искать будущих корреспондентов можно по электронному адресу (E-Mail), сетевому псевдониму (Nickname), имени и фами-

лии (First/Last Name), личному номеру пользователя ICQ (UIN), по возрасту и интересам и т.д. Если будущий собеседник обнаружен по заданным параметрам поиска и есть желание добавить его в базу данных корреспондентов, его ник появляется в списке, отображаемом в рабочем окне программы.

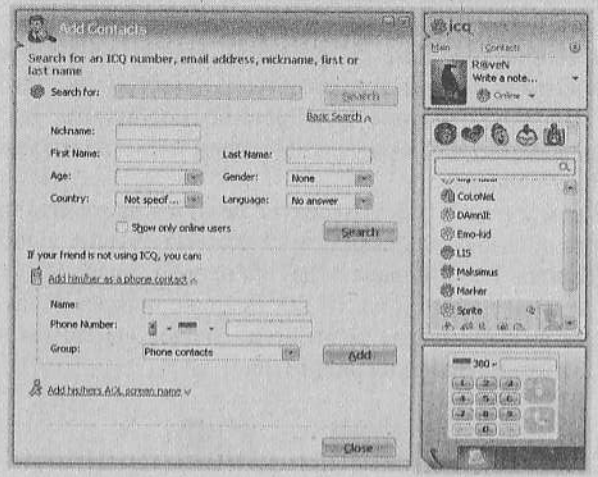


Рис. 13.4. Окна поиска контактов и рабочее окно

Если пользователь в данный момент не подключен к Интернету, его псевдоним находится в подразделе офлайн. Если же корреспондент оказался подключенным к Интернету и не стремится скрыть этот факт, его псевдоним находится в подразделе онлайн. При этом корреспондент также немедленно узнает в сети всех своих собеседников.

Таким образом, основное окно ICQ отображает состояние списка контактов и позволяет работать с другими пользователями. Следовательно, любое действие может начинаться в основном окне. При однократном щелчке левой кнопки мыши по псевдониму пользователя в списке контактов появляется меню, основные команды которого следующие:

- *Send Message (Передача сообщений)* – средство отправки коротких сообщений;
- *Send / Get File... (Передача / прием файлов)* – специальное встроенное средство для передачи пакетов файлов на компьютер другого пользователя;

- *Send EMail... (Электронная почта)* – возможность подготовки и отправки электронного письма с помощью любой почтовой программы, установленной на компьютере;
- *Send Web Page Adress (URL) (Передача URL-адресов)* – автоматическое включение посланного URL-адреса в систему закладок корреспондента или вызов его в окне работающего браузера;
- *Send / Start ICQ Chat (Прямая передача беседы)* – встроенная система поддержки сетевых конференций (как построчная, так и оконная) без ограничения числа пользователей;
- *Send SMS Message (Посылка коротких сообщений на телефон)* – средство, позволяющее осуществлять отправку SMS-сообщений на мобильный телефон;
- *Voice Message (Голосовые сообщения)* – система передачи голосовых сообщений собеседнику;
- *Message History (Архив сообщений)* – просмотр истории общения с выбранным корреспондентом (рис. 13.5).

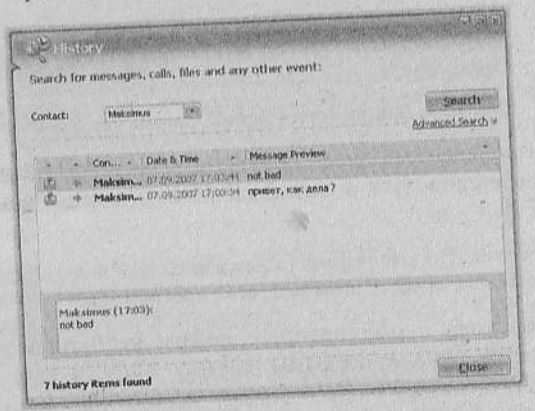


Рис. 13.5. Диалог *Message History*

Users Details / Address Book (Информация о пользователе) – важный пункт меню, позволяющий просмотреть регистрационную информацию собеседника. Диалог *Users Details* (рис. 13.6) в левой части содержит список доступной информации о корреспонденте в определенном тематическом порядке.

В режиме *General* можно увидеть в кратком виде основную информацию о собеседнике – начиная с UIN и заканчивая контактным телефоном и возрастом. Разумеется, эта информация

доступна только в случае, если она была предварительно введена при регистрации или указана при настройке программы. Остальные режимы позволяют более детально ознакомиться с информацией о собеседнике по той или иной тематике.

Рис. 13.6. Диалог *Users Details*, режим *Info Summary*

Если приведенный выше перечень возможностей недоступен, следует переключиться в *Advanced Mode (Расширенный режим)* работы ICQ.

Примечание. По умолчанию (в режиме *Simple mode*) будет доступна очень небольшая часть возможностей программы.

Для перехода в расширенный режим необходимо нажать в нижней части окна программы кнопку *Main*, а затем выбрать средство *To advanced mode* – теперь можно пользоваться всеми возможностями ICQ.

Для отправки сообщения, как уже было отмечено выше, достаточно в контекстном меню для указанного адресата выбрать пункт *Send Message*. После этого появляется окно (рис. 13.7), в нижнюю часть которого нужно вписать необходимый текст и нажать кнопку *Send (Отправить)*. Если текст доставлен адресату, он появляется в верхней части окна, где ведется своеобразный протокол беседы.

В этом же окне имеется возможность управлять внешним видом сообщений, т.е. изменять цвет текста, его размер и т.п. Кроме

того, в сообщениях допускается использовать *смайлики* – средство выражения эмоций с помощью некоторых символов.

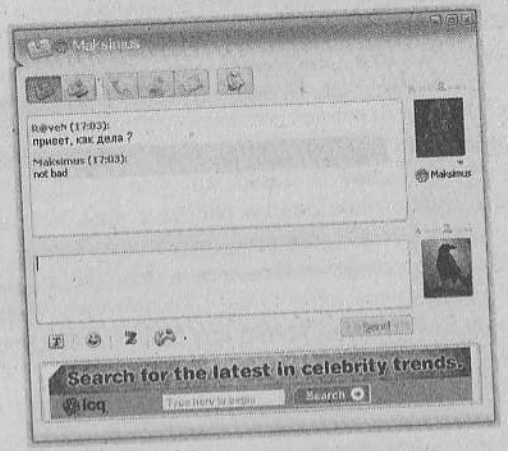


Рис. 13.7. Окно *Message Session*

Смайлики можно набирать непосредственно в окне сообщения с клавиатуры или воспользоваться специальным меню, где смайлики представлены в виде изображений забавных лиц.

ICQ может также передать файл другому пользователю. При этом не стоит забывать, что такая передача может быть осуществлена только в расширенном режиме работы. Обратите внимание и на то, что составлять запрос, чтобы передать файл, можно и в режиме автономной работы программы. Запрос будет сохранен и послан тогда, когда и отправитель, и получатель будут подключены к сети.

Итак, для передачи одного или нескольких файлов выбирают в контекстном меню адресата пункт *Send / Get File...*, а далее – *Send File*. В появившемся окне необходимо выбрать один или несколько файлов, которые следует переслать, после чего будет отображаться прогресс отправки файлов *Send Online File* (рис. 13.8). У пользователя, которому отправляются эти файлы, отобразится диалог запроса, в котором будет указано имя или количество файлов, а также их размер. Затем следует нажать кнопку *Send*, чтобы послать запрос на передачу файла, и, если получатель согласится, начнется передача файла.

Кратко рассмотрим возможности настройки самой программы.

Рис. 13.8. Отображение передачи файла

Для того чтобы откорректировать информацию о пользователе, введенную при регистрации, необходимо выбрать пункт *View / Change My Details* в меню, которое вызывается нажатием кнопки *Main*. Диалоговое окно и работа с ним полностью аналогичны окну *Users Details*, уже рассмотренному выше.

Настройки программы находятся в том же меню, в пункте *Preferences*. Диалоговое окно *Owner Preferences*, открывающееся при этом (рис. 13.9), традиционно для ICQ состоит из нескольких режимов, выбираемых в списке слева.

В частности, настройка списка контактов (*Contact List*) позволяет установить следующие его параметры:

- возможность автоматического открытия списка контактов при получении любого сообщения ICQ;
- включение режима *Поверх всех окон*, за исключением случая, когда основное окно ICQ свернуто;
- возможность создания списка контактов для избранных корреспондентов непосредственно на рабочем столе Windows;

  Примечание. Такие контакты называют *всплывающими*. Для этих собеседников можно установить возможность видеть их статус в режиме *Поверх всех окон*, остальные контакты видны не будут.

- возможность выбрать режим размещения последнего корреспондента, с которым общался пользователь, в начало списка контактов;
- средство минимизации диалогового окна отправки сообщения после того, как текст доставлен получателю;
- сворачивание окна ICQ через интервал времени, который укажет пользователь.

В диалоговом окне *Owner Preferences* очень важным является режим *Connections* (рис. 13.10) – настройки, предусмотренные здесь, влияют на работу программы в целом.

На вкладке *General* устанавливают Dial-Up-соединение с помощью модема (*Modem*) или постоянное через локальную вычислительную сеть (*Permanent*). В группе переключателей *Launch* можно определить, будет ли запускаться ICQ автоматически при включении компьютера. Группа *Firewall IP Setting* позволяет указать способ использования Firewall-сервера. Здесь рекомендуется вариант, когда программа сама автоматически определит нужную конфигурацию (*ICQ will determine IP Automatically*).

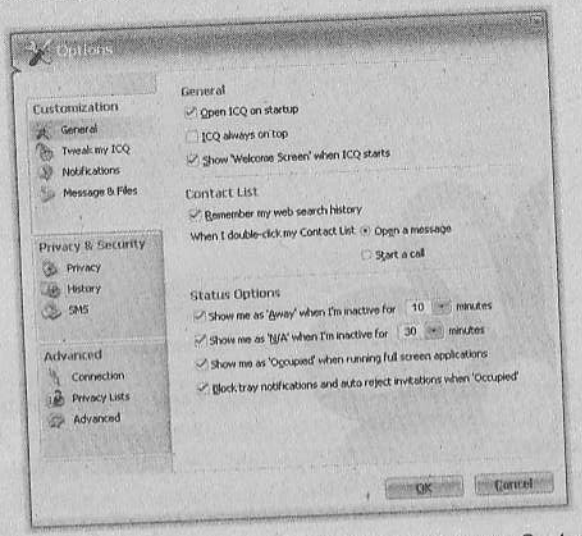


Рис. 13.9. Диалоговое окно *Owner Preferences*, режим *Contact List*

Вкладка *Connection* этого же диалога позволяет указать сервер системы, через который идет общение.

В поле *Host* указывается имя сервера, который обеспечивает работоспособность программы, а в поле *Port* – номер соответствующего порта. Разработчики программы предусмотрели средство автоматического определения настроек подключения к серверу. Для выбора этого режима достаточно нажать кнопку *Auto Configure*. На этой же вкладке необходимо определить параметры использования прокси-сервера сети, если таковой существует. Уточнение этих параметров осуществляется на оставшихся вкладках диалога – *Firewall* и *User*. Настройки, которые там расположены, во многом зависят от специфики подключения пользователя к Интернету, и в случае некорректности работы рекомендуется проконсультироваться с администратором сети.

Рис. 13.10. Вкладка *Connection*

На этом общее знакомство с основными навыками работы и настройки ICQ можно закончить. Для начала работы этого вполне достаточно. Рассмотрим лишь еще полезные ссылки, связанные с работой этой программы:

http://web.icq.com – основной сайт ICQ (рис. 13.11): описание программы и ее возможностей, а также дополнительных модулей к ней; служба поддержки и сервисные службы; система поиска собеседников по странам и интересам; множество различных сервисов, включая возможность загрузки самых свежих дополнений к ICQ;

http://icqcity.holm.ru – список пользователей ICQ по всем городам России и ближнего зарубежья. Интересно найти свой город и пользователей ICQ, которые в нем проживают;

http://www.icqfoto.ru – фотогалерея ICQ. Очень популярный сайт. Здесь пользователи ICQ могут разместить свои фотографии, поискать друзей, узнать много полезной информации о программе;

http://www.icqinfo.ru – страница, содержащая техническую информацию об ICQ: статьи по сетевой защите; возможность загрузки программ для общения и исправлений; информация об используемых в ICQ протоколах; предложения по продаже номеров знакомств обладателей ICQ;

Рис. 13.11. Главная страница сайта web.icq.com

http://www.icqguards.ru – клуб ICQ: лист пользователей; обзор интернет-ресурсов, посвященных ICQ. Здесь можно найти новых друзей или встретиться со своими старыми знакомыми.

QIP

QIP – бесплатная программа с закрытым кодом, позволяющая общаться в реальном времени через Интернет. Она является альтернативным клиентом ICQ, входит в список самых распространенных интернет-пейджеров, которым пользуются миллионы пользователей. QIP легко можно освоить благодаря несложному интерфейсу, разнообразные настройки могут приспособить программу под любого пользователя. Кроме отправления текстовых сообщений программа поддерживает передачу любых файлов.

После запуска программы появится окно (рис. 13.12), в котором необходимо ввести свой номер (ICQ#) и пароль (Password), а затем нажать кнопку Open / Login.

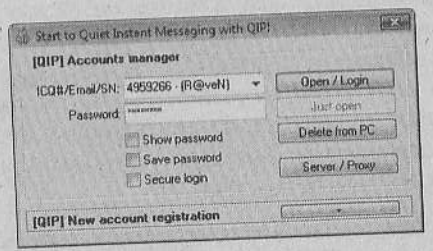


Рис. 13.12. Ввод номера ICQ и пароля для входа

Если у пользователя нет зарегистрированного номера, необходимо нажать кнопку [ ] – отобразится дополнительная часть окна (рис. 13.13). Для регистрации нового номера нужно выполнить следующие действия:

1. Ввести пароль для доступа к своему номеру в строку *New ICQ# Password (Новый пароль для ICQ#)*.

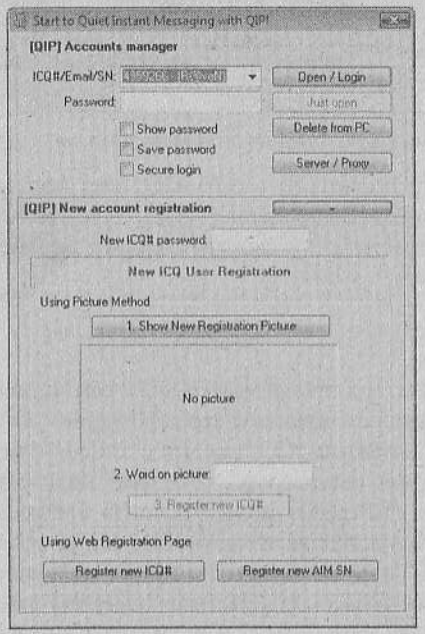


Рис. 13.13. Регистрация нового ICQ#

2. Нажать кнопку *Show New Registration Picture (Показать новую регистрационную картинку)* – загрузится картинка с некоторыми буквами и цифрами.
3. Набрать в поле *Word on picture (Слово на картинке)* слово, изображенное на рисунке, и нажать кнопку *Register new ICQ# (Зарегистрировать новый ICQ#)* – отобразится новый ICQ# и пароль, необходимый для доступа.

Для настройки соединения программы с сервером необходимо нажать кнопку *Server / Proxy (Сервер / Прокси)* – появится окно *Connection Settings (Настройки соединения)* (рис. 13.14). В этом

окне можно изменить все доступные настройки для наиболее быстрой и продуктивной работы.

Для подключения к серверу нужно нажать кнопку *Open / Login* (см. рис. 13.12) после ввода своего ICQ-номера и пароля. Если все настройки подключения корректны, а пароль правильный, откроется окно, содержащее список контактов (если они есть) и различные кнопки (рис. 13.15).

Рис. 13.14. Настройки подключения

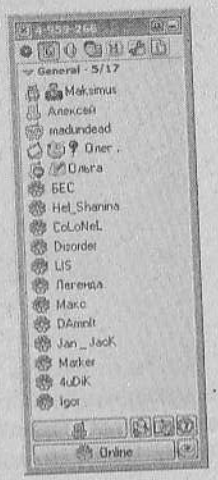


Рис. 13.15. Главное окно QIP

Для добавления контакта в список пользователя следует нажать кнопку [ ] *Main Menu (Главное меню)* и в списке команд выбрать *Add/Find Users (Добавить/Найти пользователей)*. После этого отобразится окно, представленное на рис. 13.16.

Если номер нужного контакта известен, то его надо ввести в строку *AIM SN / ICQ UIN* и нажать кнопку *Add (Добавить)*, расположенную правее. Далее программа предложит ввести имя контакта и выбрать группу.

Для поиска пользователя необходимо знать о нем какие-либо данные. Во вкладке *Simple Search (Простой поиск)* можно искать по ICQ-номеру, электронной почте, псевдониму, имени и фамилии. Если выбрать вкладку *Global Directory (Глобальный каталог)*, можно искать пользователя по полу, возрасту, стране и городу проживания, профессии и многому другому.

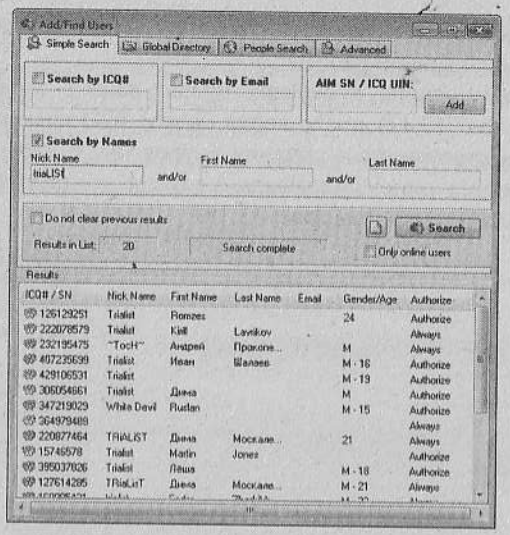


Рис. 13.16. Добавление и поиск контактов

Чтобы отправить текстовое сообщение пользователю, необходимо выполнить двойной щелчок по имени пользователя в списке контактов – откроется окно обмена сообщениями между пользователями (рис. 13.17). В нижней области надо ввести текстовое сообщение и нажать кнопку Send *(Отправить)* или клавишу **Enter**.

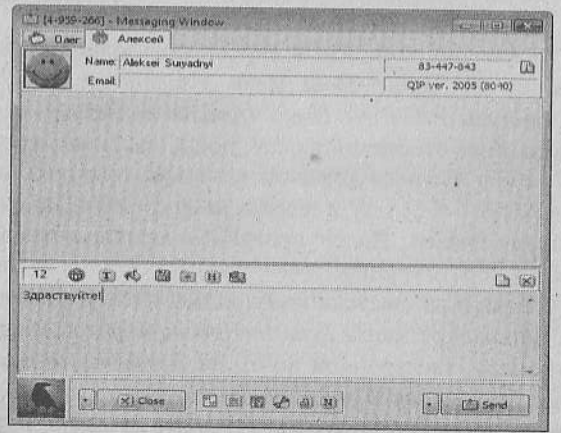


Рис. 13.17. Окно обмена сообщениями

Для просмотра информации о пользователе нужно нажать кнопку в окне обмена сообщениями или выбрать команду *User Details (Данные пользователя)* в контекстном меню, вызванном щелчком по имени контакта в главном окне (рис. 13.18). Здесь отображаются псевдоним, имя, фамилия, домашний и рабочий адреса, возраст, день рождения, интересы контакта и др., если пользователь ввел эти данные.

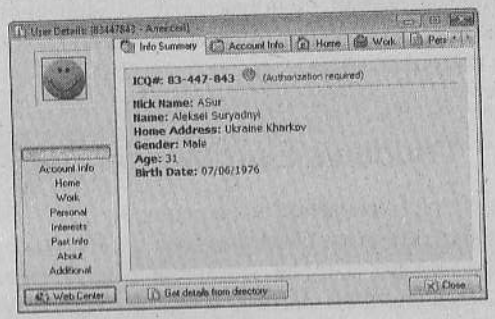


Рис. 13.18. Личные данные пользователя

Для настройки программы необходимо нажать кнопку . В отобразившемся окне (рис. 13.19) можно изменить такие параметры: автоматическую проверку наличия новой версии, сортировку списка контактов, различные настройки интерфейса, автоматическое подключение после разрыва, настройки звукового сопровождения и «горячих» клавиш.

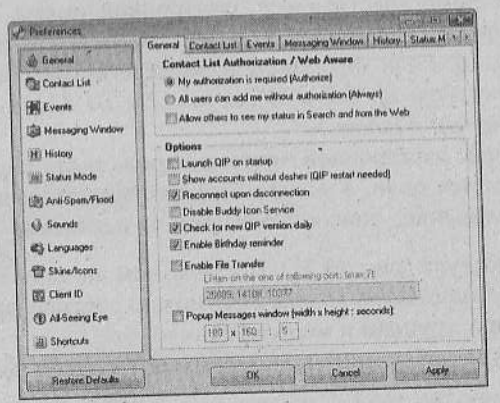


Рис. 13.19. Настройки QIP

QIP, так же как и ICQ, поддерживает смайлики, способен сохранять историю сообщений, обладает способностью добавлять другие языки интерфейса и др. Главный минус QIP – отсутствие поддержки подключаемых модулей для расширения функциональности. Но этот минус компенсируется следующими полезными функциями, которых нет в ICQ: просмотр IP-адреса клиента, времени входа пользователя в систему, удаление своего номера из списка контактов других пользователей, добавление контактов в свой список без авторизации, отправление сообщений, зашифрованных при помощи пароля.

Windows Live Messenger

Существует ряд программ, позволяющих обмениваться мгновенными сообщениями с собеседниками в сети Интернет. Среди них есть программа, которая входит в стандартный комплект программ в операционной системе Windows Vista – Windows Live Messenger. Эта программа широко распространилась благодаря большому количеству доступных языков. Windows Live Messenger предназначена для общения и работы в сети Интернет, в которую можно войти со многих современных устройств. Программа позволяет делать звонки с одного ПК на другой, а также на обычные телефоны за небольшую плату. Есть возможность общаться, используя веб-камеры.

После запуска программы появится окно (рис. 13.20), в котором необходимо ввести адрес электронной почты, на которую зарегистрирован пользователь и пароль, затем нажать кнопку *Sign in (Вход)*. Если пользователь не зарегистрирован, надо нажать ссылку *Sign up for a Windows Live ID (Зарегистрируйте идентификатор Windows)*.

Если адрес электронной почты и пароль были корректно введены, откроется окно, в котором можно увидеть свою картинку, личное сообщение, список контактов и несколько кнопок для быстрого доступа (рис. 13.21). Посредством кнопки  *Sort your contacts (Организовать контакты)* можно сортировать контакты по состоянию, группам и модулям.

Процедура добавления пользователей в список контактов напоминает ICQ: необходимо нажать кнопку  *Add a contact (Добавить контакт)*, затем в отобразившемся окне (рис. 13.22) следует ввести адрес электронной почты и многие другие настройки, такие как номер мобильного телефона, псевдоним, имя, фамилию, домашний и рабочий адрес и др.

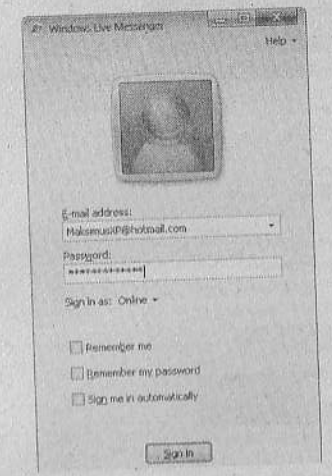


Рис. 13.20. Окно входа в программу Windows Live Messenger

Рис. 13.21. Главное окно Windows Live Messenger

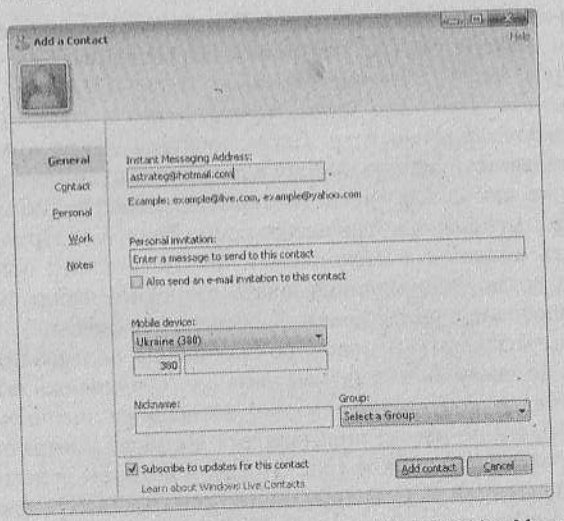


Рис. 13.22. Добавление новых контактов Windows Live Messenger

При помощи кнопки Maks (Online), расположенной рядом с картинкой пользователя, можно изменить свой статус, картинку, список контактов и др. (рис. 13.23).

Рис. 13.23. Изменение статуса

При выборе команды *Options (Параметры)* появляется окно, в котором находятся все настройки, разделенные на несколько групп (рис. 13.24): *Personal (Личные), General (Общие), Messages (Сообщения), Alerts and Sounds (Оповещения и звуки), File Transfer (Передача файлов)* и др. Переключаться между ними можно, нажав соответствующую кнопку в левой части данного окна.

Так же как и все другие интернет-пейджеры, Windows Live Messenger мгновенно отправляет сообщения, поддерживает возможность общения с несколькими пользователями одновременно, дает возможность использовать широкий выбор смайликов, вести голосовое и видеообщение, пересылать файлы.

Чтобы отправить мгновенное сообщение пользователю, надо выбрать команду *Send a instant message (Отправить мгновенное сообщение)* в контекстном меню, вызванном щелчком правой кнопки мыши по имени пользователя в списке контактов. После нажатия отобразится окно (рис. 13.25), в котором ведется беседа. Окно, аналогично ICQ и другим интернет-пейджерам, содержит область для ввода сообщения и область, в которой отображаются

все отправленные и полученные сообщения. Для отправки сообщения достаточно нажать клавишу **Enter**.

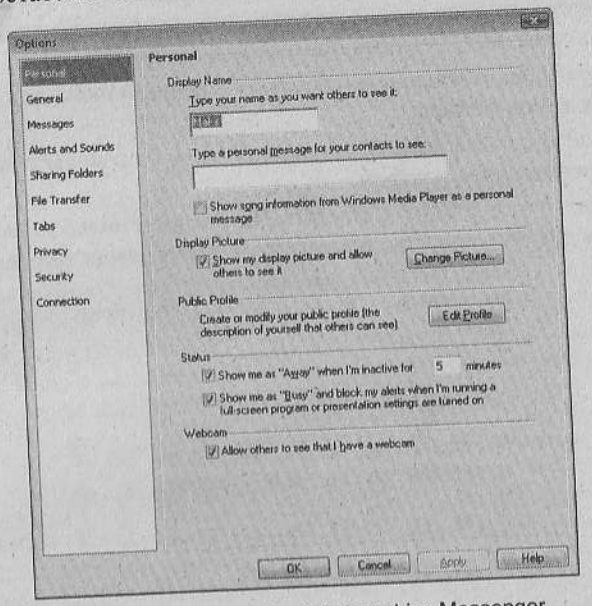


Рис. 13.24. Настройки Windows Live Messenger

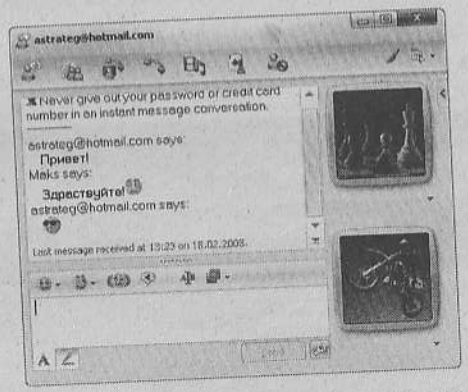


Рис. 13.25. Общение в Windows Live Messenger

Windows Live Messenger поддерживает смайлики, которые можно выбрать, нажав кнопку . После нажатия на эту кнопку

отобразится дополнительная форма (рис. 13.26), на которой можно выбрать смайлик, щелкнув по нему мышью.

В этом же окне можно увидеть кнопки, предназначенные для других полезных функций программы, например:

Send Files (Отправить файлы) – предназначена для отправки любых типов файлов;

Call a contact (Позвонить контакту) – позволяет начать беседу, используя микрофон;

Start or stop a Video Call (Начать или завершить видеовызов) – служит для общения с пользователями при помощи веб-камеры.

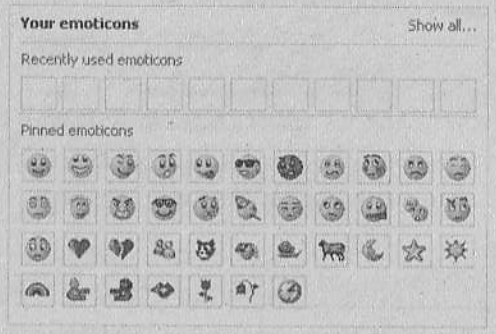


Рис. 13.26. Смайлики в Windows Live Messenge

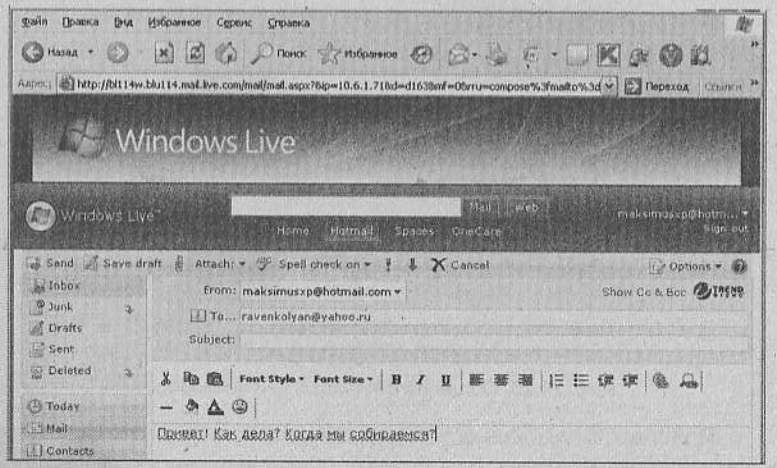


Рис. 13.27. Отправление сообщения в Windows Live Messenger

Для отправки электронной почты пользователю необходимо выбрать команду *E-mail (Электронная почта)* контекстного меню (рис. 13.27). В нижней части окна нужно набрать сообщение и нажать кнопку Send (*Отправить*).

Глава 14
Веб-камеры и Skype

В предыдущей главе были рассмотрены клиенты, предназначенные для обмена текстовыми сообщениями. Но при помощи камеры, подключаемой к компьютеру, можно увидеть своего собеседника, даже если он находится на другом континенте. В этой главе описывается такая камера, программа Skype, предназначенная для общения, и приведены несколько ссылок на интернет-ресурсы.

Описание устройства

Современная *веб-камера* (рис. 14.1) способна снимать видео, оцифровывать и сжимать его. Среди множества возможностей камеры следует отметить ее способность делать фотографии, серии фотографий, отслеживать положение лица, записывать видео со звуком при помощи встроенного микрофона. Большинство камер подключаются к компьютеру через интерфейс USB.

Посредством веб-камеры пользователь может разговаривать с человеком, находящимся в другой точке планеты, и видеть его, а также проводить видеоконференции.

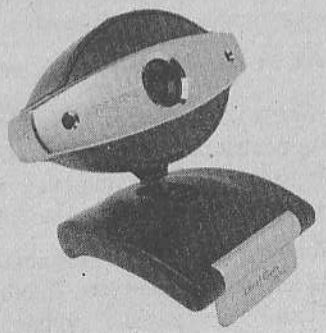


Рис. 14.1. Веб-камера Creative

Срок службы веб-камер почти неограничен, а цена такого устройства небольшая – от 16 долларов, так как нет смысла оснащать их дорогими матрицами.

Перед подключением веб-камеры к компьютеру для корректной работы устройства сначала необходимо установить программное обеспечение, которое, как правило, можно найти на компакт-диске, поставляемом в комплекте с веб-камерой, или загрузить с интернет-сайта производителя устройства. В конце процесса установки драйверов веб-камеры пользователю будет предложено подключить устройство к компьютеру, для того чтобы система произвела автоматическое конфигурирование. После автоматического конфигурирования будет отображено окно конфигурирования веб-камеры (рис. 14.2).

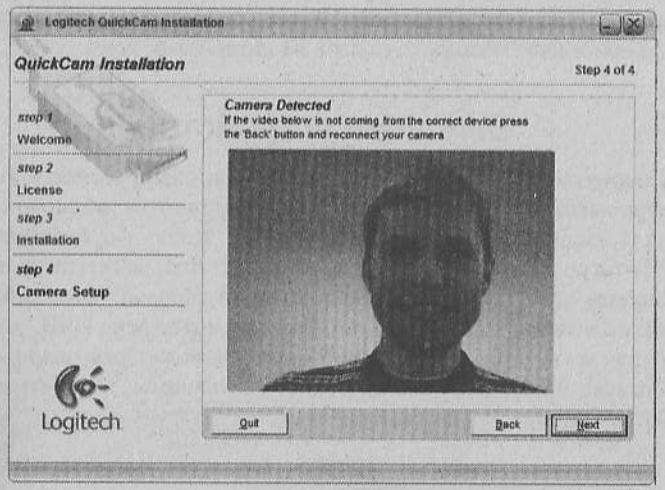


Рис. 14.2. Окно конфигурирования веб-камеры

В данном окне будут отображены видеоданные, получаемые с веб-камеры. Если видеоизображение нечеткое, размытое, то необходимо вручную настроить фокусировку веб-камеры, вращая кольцо фокусировки, которое размещено вокруг ее объектива.

По наличию иконки в области уведомлений можно определить, подключена веб-камера или нет. Двойной щелчок по этой иконке вызовет окно программы управления веб-камерой (рис. 14.3).

В этом окне пользователю доступны следующие функции:

- запись видео и фото с веб-камеры;
- выбор и настройка видеоэффектов, которые будут применяться при съемке видео;
- настройка приватной шторки – изображение, которое будет показываться вместо видео, полученного с веб-камеры для обеспечения приватности общения;
- параметры работы веб-камеры (рис. 14.4). Пользователь может настроить следующие параметры работы веб-камеры: яркость, контрастность, интенсивность цвета и баланс белого.

Рис. 14.3. Окно программы управления веб-камерой

Для записи видео- или фотоснимков необходимо нажать кнопку – откроется окно *Quick-Capture (Быстрый захват)*, изображенное на рис. 14.5. В данном окне пользователь может настроить разрешение видеоизображения (640×480 или 320×240), а также произвести запись видео, нажав кнопку *Record Video (Запись видео)*, или сделать фотоснимок, нажав кнопку *Take Foto (Получить фотографию)*.

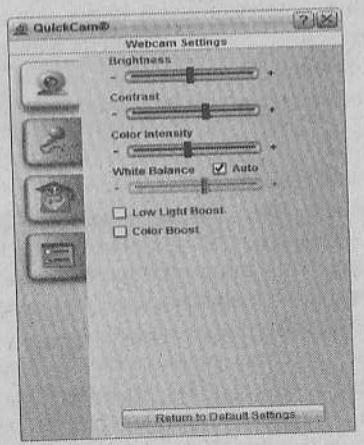


Рис. 14.4. Окно настройки веб-камеры

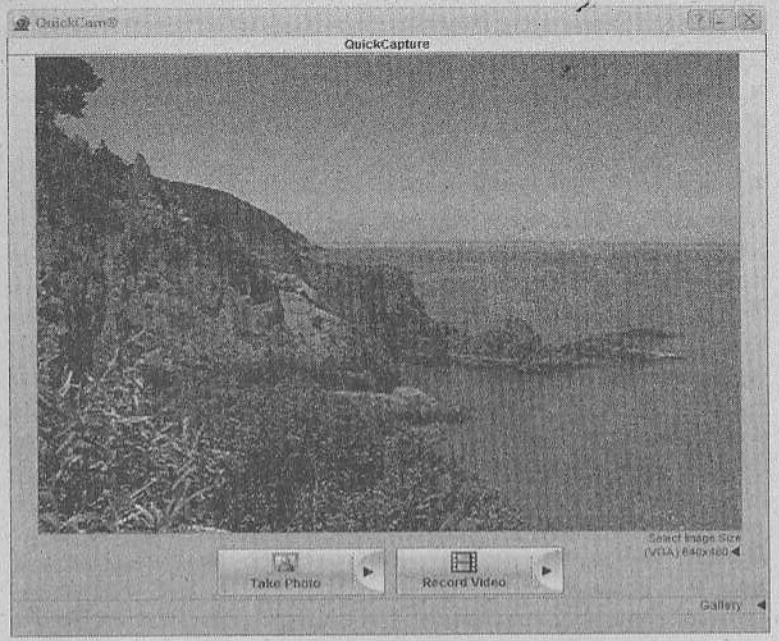


Рис. 14.5. Окно *QickCapture (Быстрый захват)*

После установки программного обеспечения и настройки веб-камеры она полностью готова к работе и может использоваться для осуществления видеозвонков в таких приложениях, как ICQ, Windows Live Messenger, Skype, и других менее популярных программах IP-телефонии. Подробнее возможности использования веб-камеры для осуществления видеозвонков рассмотрены в следующем разделе.

Интернет-телефония Skype

Телефония через Интернет – относительно новый вид связи, который обладает рядом преимуществ, что делает ее, бесспорно, перспективной. Эта технология позволяет использовать любую IP-сеть в качестве средства организации телефонных переговоров. Использование IP-телефонии позволяет значительно снизить стоимость звонка, а следовательно, сократить расходы на междугородную и международную связь.

Принцип действия IP-телефонии – это конвертация голосовой связи в пакеты данных. Функцию телефонного аппарата может выполнять как персональный компьютер, так и специальный IP-телефон, подключенный к Интернету.

В сравнении с первыми версиями решений IP-телефонии, которые допускали искажение и прерывание речи, качество связи в наше время значительно улучшилось. Достигнуто это было за счет совершенствования кодирования голоса и восстановления потерянных пакетов.

Известно, что для человека задержка до 250 мс практически незаметна. Существующие на сегодняшний день решения IP-телефонии превышают этот предел, так что разговор похож на мобильную связь по обычной телефонной сети через спутник, которую обычно оценивают как связь вполне удовлетворительного качества, требующую лишь некоторого привыкания, после которого задержки для пользователя становятся неощутимы. Сейчас достигнут такой уровень качества, когда речь передается настолько хорошо, что собеседники порой не догадываются, что соединение происходит по технологии IP-телефонии.

ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ SKYPE

http://skype.com

Skype – простая бесплатная программа, позволяющая бесплатно звонить абонентам Skype по всему миру. В данное время этой программой пользуются около 200 млн человек.

Персональные компьютеры абонентов Skype должны иметь разъем для подключения наушников и микрофона, т.е. атрибуты обычной телефонной трубки.

Сеть Skype базируется на прогрессивной P2P (peer-to-peer) технологии и обладает высоким качеством передачи голоса. Создатели программы специально консультировались со специалистами по акустике, как сделать искажения голоса менее заметными. Причем задействовать высокоскоростное интернет-соединение для беседы совсем не обязательно, достаточно обычного модема. Хотя, конечно, чем выше скорость, тем лучше качество.

Все общение между клиентами Skype зашифровано и не может быть перехвачено.

Skype имеет встроенный клиент обмена короткими сообщениями, но позволяет проводить чаты с участием не двух, а 100 и более человек одновременно. Если какой-то чат содержит осо-

бенно важную для пользователя информацию, то имеется возможность отметить его закладкой, для того чтобы потом быстро найти. Это может быть очень полезно при общении с членами семьи и деловыми партнерами.

В программе Skype есть возможность проводить видеоконференции. Изображение собеседника появляется в рабочем окне программы в отдельном окне.

РЕГИСТРАЦИЯ И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА SKYPE

После установки программы Skype и ее первого запуска пользователю сразу же будет предложено зарегистрироваться (рис. 14.6). Рекомендуется заполнить личную информацию, по которой другие пользователи Skype смогут вас идентифицировать.

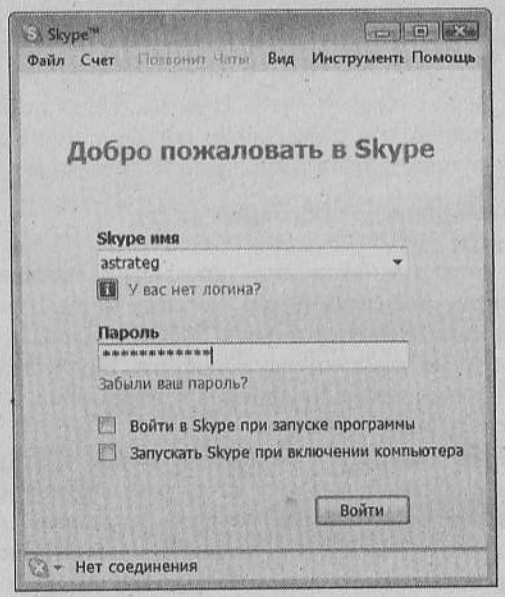


Рис. 14.6. Стартовое окно программы Skype

После запуска программы в области уведомлений можно будет увидеть значок , который сообщает, что программа работает в данное время. Щелкнув по нему, можно получить быстрый доступ к некоторым функциям программы.

Щелчок по своему имени в верхней части окна сворачивает или разворачивает область персонализации. Здесь можно написать текст, который будет сопровождать имя в списках контактов других пользователей (рис. 14.7).

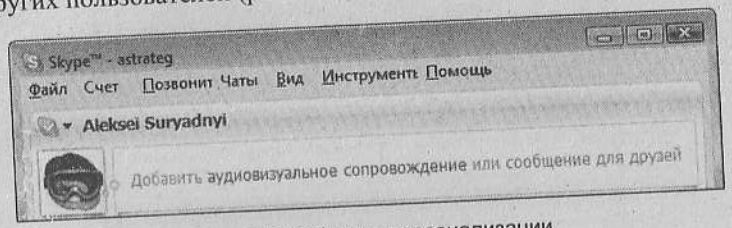


Рис. 14.7. Область персонализации

В этой же области можно выбрать себе «портрет» – для этого надо лишь щелкнуть по нему мышью. После этого программа предложит несколько стандартных картинок, можно также загрузить свою с жесткого диска или установить картинку, сделав скриншот из какого-либо видеофайла (рис. 14.8).

Рис. 14.8. Выбор картинки

ЗВОНКИ И КОНТАКТЫ

При разработке программы ее производители руководствовались тем, что программное обеспечение должно помогать работать, а не создавать дополнительные трудности. Поэтому интерфейс Skype максимально упрощен, и каждый, кто знает Windows и умеет пользоваться телефоном, сможет освоить эту программу (рис. 14.9).

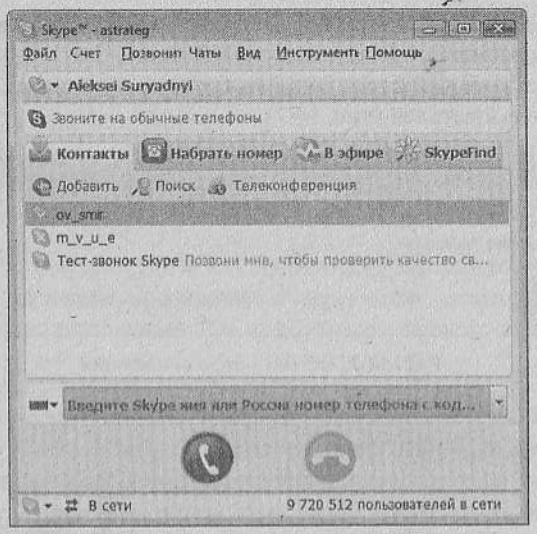


Рис. 14.9. Внешний вид основного окна Skype

В данной программе есть список контактов (аналогично ICQ). Слева от имени пользователя можно увидеть индикатор, который показывает статус контакта: в сети, недоступен, невидимый, не в сети и др. Свой статус можно поменять, нажав кнопку в левом нижнем углу (рис. 14.10).

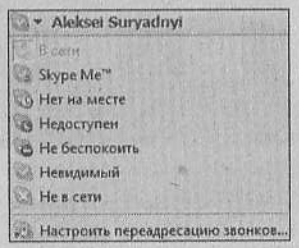


Рис. 14.10. Выбор состояния пользователя

Для того чтобы начать общение, необходимо найти и добавить в список контактов абонентов, использующих Skype. Процедура поиска абонентов предельно проста, понятна и выполнена по аналогии с подобными операциями в ICQ и Windows Live Messenger. Достаточно набрать имя или ник контакта в отведенном поле и нажать *Поиск* (рис. 14.11).

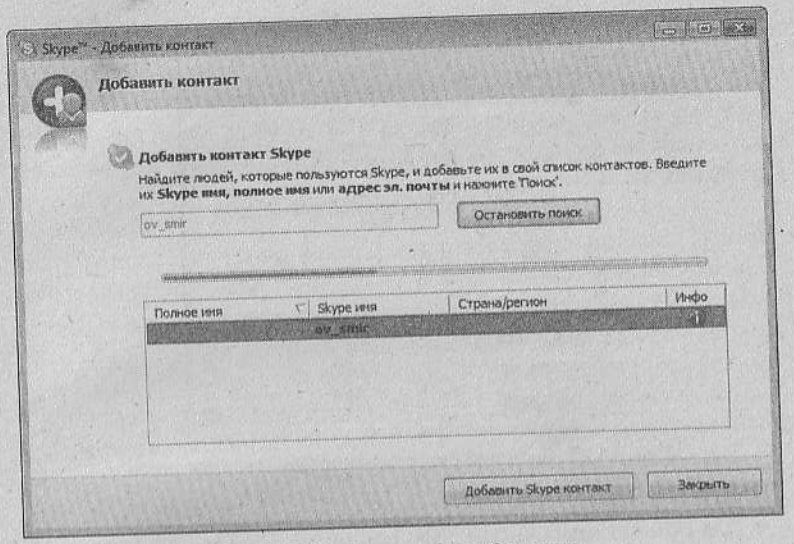


Рис. 14.11. Окно поиска абонентов

Из предлагаемого по результатам поиска списка возможных контактов необходимо выделить нужный и нажать кнопку *Добавить Skype контакт*. При этом появится окно, в котором можно послать сообщение своему другу как запрос для добавления в список контактов.

Чтобы осуществить звонок абоненту Skype, следует найти его в списке контактов, выделить и нажать кнопку вызова в нижней части окна программы. Если же другой абонент хочет поговорить с вами, он выполняет такие же действия, и у вас отображается окно запроса на разговор, показанный на рис. 14.12.

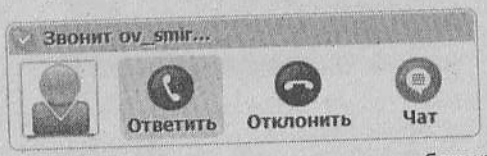


Рис. 14.12. Запрос на разговор от другого абонента

Для начала разговора с пользователем надо нажать кнопку  . Окно разговора, в котором можно увидеть продолжительность вашего диалога, показано на рис. 14.13. Для окончания разговора достаточно нажать кнопку  .

Рис. 14.13. Внешний вид окна телефонного разговора

ЧАТ

Для обмена текстовыми сообщениями с каким-либо пользователем необходимо щелкнуть правой кнопкой по имени пользователя в списке контактов и выбрать команду *Начать чат*. Обмен сообщениями ведется аналогично ICQ – набирается при помощи клавиатуры в нижнюю часть окна (рис. 14.14). Для отправки сообщения следует нажать клавишу **Enter**. Все полученные и отправленные сообщения сохраняются в отдельном файле, если не выключена соответствующая опция.

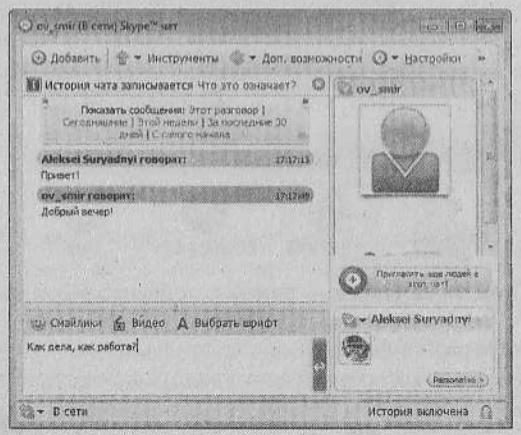


Рис. 14.14. Окно чата в Skype

ВИДЕОЗВОНКИ

Для реализации видеозвонка с помощью программы Skype сначала необходимо подключить и настроить веб-камеру. Программа автоматически обнаружит веб-камеру, и при осуществлении звонка другому абоненту сети Skype будет автоматически установлена видеосвязь (при звонках на обычные телефоны функция видеосвязи не поддерживается).

Процесс выбора абонента для звонка и вызова полностью аналогичны описанным выше для осуществления голосовой связи.

В режиме видеозвонка программа Skype в окне разговора (рис. 14.15) будет выводить миниатюру видеоизображения, которое будет видно вашему собеседнику. Также существует возможность отключить видеотрансляцию и перейти в режим обычного голосового общения. Все остальные настройки полностью аналогичны настройкам программы в режиме голосового общения.

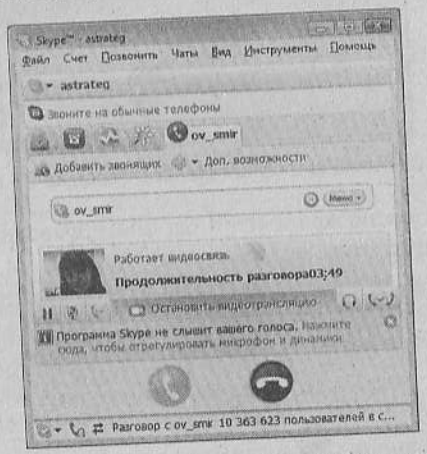


Рис. 14.15. Внешний вид окна видеоразговора

Вызываемый абонент в режиме видеозвонка увидит своего собеседника в окне разговора программы Skype (рис. 14.16).

Во время видеообщения на стороне собеседника доступны следующие параметры вывода видеоизображения:

- вывод видео в отдельное окно (рис. 14.17);
- вывод видео в полноэкранном режиме;
- стандартный режим (видеоизображение выводится в окне программы (рис. 14.16)).

Рис. 14.16. Внешний вид окна видеоразговора на ПК собеседника

В режимах полноэкранного и оконного вывода видео пользователю будут доступны четыре кнопки управления разговором:

- *Видео в окне звонка* – выводит видеоизображение в стандартном режиме (в окне программы);
- *Полноэкранное видео* – позволяет отображать видео на весь экран;
- *Закончить разговор* – служит для окончания видеоразговора (аналогична кнопке в главном окне Skype);
- *Выключить звук* – предназначена для отключения микрофона во время разговора.

Кнопка *Полноэкранное видео* в режиме полноэкранного просмотра видео меняется на кнопку *Видео в окне*, которая выводит видеоизображение в отдельном окне.

Все перечисленные выше кнопки позволяют оперативно управлять видезвонком без необходимости открытия главного окна программы Skype.

Рис. 14.17. Внешний вид окна видеоразговора в режиме *Видео в окне*

Веб-камеры в Интернете

Веб-камера – это цифровая фотокамера, которая фиксирует изображения в реальном времени для последующей передачи по сети Интернет. Веб-камеры обычно выполняют закачку изображений на веб-сервер через определенные промежутки времени (как правило, каждые несколько секунд).

В последнее время наряду с использованием в видеоконференциях веб-камеры получили широкую популярность как средства, позволяющие пользователям сети Интернет увидеть на своем компьютере любой уголок планеты через веб-камеры, подключенные к Интернету другими пользователями.

www.earthcam.com

EarthCam (рис. 14.18) – наиболее популярный сайт этой тематики, который содержит обширную базу данных ссылок на веб-камеры всего мира.

В правой части сайта можно увидеть миниатюрные статичные изображения – ссылки на наиболее популярные веб-камеры мира. При наведении указателя мыши на миниатюру автоматически «всплывает» увеличенное изображение с выбранной веб-камеры, а щелчок по миниатюре позволяет увидеть «живую» трансляцию.

Рис. 14.18. Фрагмент сайта EarthCam

Для того чтобы найти веб-камеру по географическому принципу, нужно щелкнуть по ссылке *World Map (Карта мира)* в верхней части окна (над строкой поиска *Search*). При этом отобразится карта мира. Щелчок мышью по определенному континенту «приближает» карту, позволяя увидеть страны (рис. 14.19). При этом рядом с картой появится алфавитный перечень стран (щелчок по названию страны позволяет вывести список ее веб-камер).

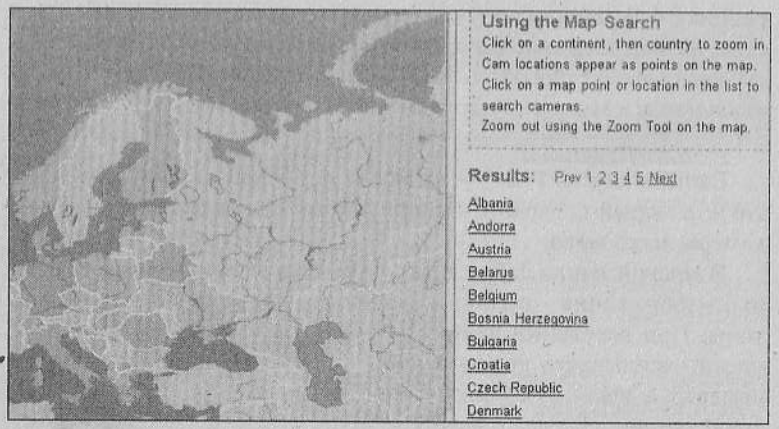


Рис. 14.19. Карта мира, выбор страны в Евразии

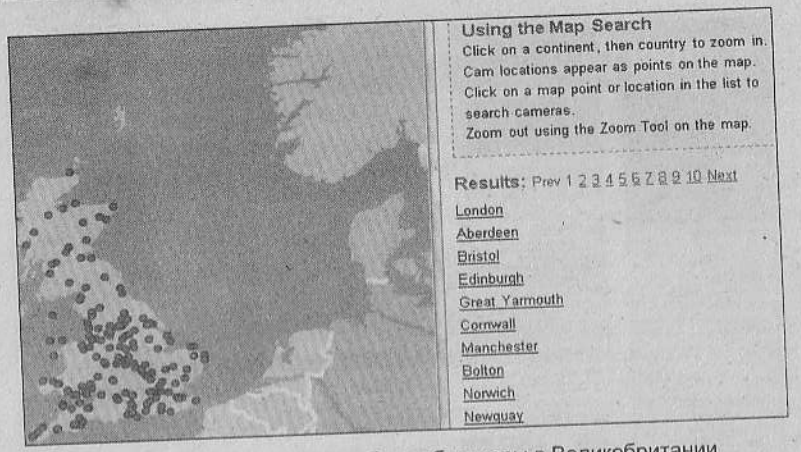


Рис. 14.20. Карта мира, выбор веб-камеры в Великобритании

Последующий щелчок по стране увеличивает ее и отображает в виде кружочков имеющиеся ссылки на веб-камеры этой страны (рис. 14.20). Как и на предыдущем шаге, справа от карты выводится список, но на этот раз – городов выбранной страны, позволяя сузить область поиска. Можно либо щелкнуть по кружочку, соответствующему одной из веб-камер, либо в списке выбрать нужный город, чтобы увидеть перечень имеющихся в нем веб-камер. Например, на рис. 14.21 показаны миниатюры изображений с лондонских веб-камер (Биг Бен, Колесо обозрения, Трафальгарская площадь).

Рис. 14.21. Веб-камеры Лондона

Рис. 14.22. Лондонская веб-камера, показывающая Биг Бен

Щелчок по миниатюре или по названию веб-камеры открывает сайт, транслирующий с нее изображение. Например, на рис. 14.22 показана трансляция с веб-камеры, направленной на Биг Бен.

Множество веб-камер имеется в Нью-Йорке. Среди видов, которые можно лицезреть с их помощью, отметим южную сторону Эмпайр Стейт Билдинг и Статую Свободы (рис. 14.23).

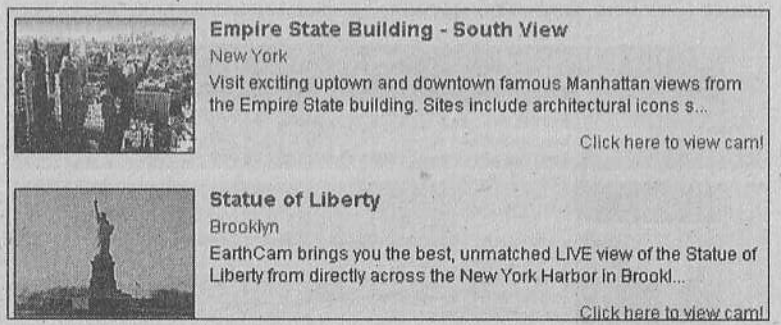


Рис. 14.23. Некоторые веб-камеры Нью-Йорка

На сайте EarthCam также имеется ссылка на московскую веб-камеру на Красной площади, показывающую собор Василия Блаженного (рис. 14.24).

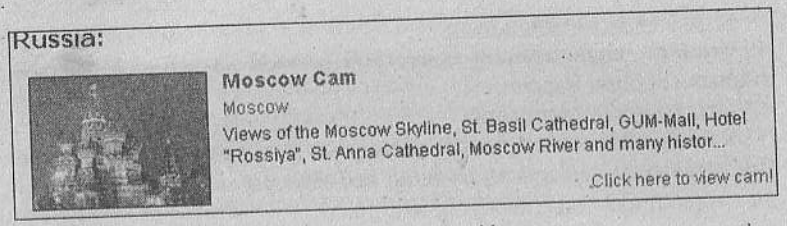


Рис. 14.24. Веб-камера Москвы

http://www.webcams.ru

Популярный российский сайт (рис. 14.25): множество ссылок на веб-камеры во многих странах мира. Поиск можно осуществлять как по категориям (в качестве которых выступают Россия, Европа, Азия, Северная и Южная Америка и т.д.), так и с помощью карты мира – щелчок в том или ином ее месте открывает перечень подкатегорий – стран мира (с указанием для каждой из них количества имеющихся ссылок на веб-камеры).

Рис. 14.25. Фрагмент сайта Webcams

http://www.webkamera.ru

Каталог, включающий более 500 ссылок на веб-камеры различных городов России.

http://www.listcam.com

Каталог веб-камер России, Европы, Америки, Африки и т.д. Представлены ссылки на лучшие веб-камеры по категориям: горы, моря, пирамиды, необычное и др.

Глава 15
Интернет-сервисы Google

Google – общее название американской компании Google Inc, ее сайта и поисковой системы, находящейся на этом сайте.

Google является обладателем множества наград, включая приз «Глас народа» за лучшие технические достижения и награду «Лучшая поисковая система в Интернете» от Yahoo! Internet Life. Google завоевал приз за «Техническое совершенство» журнала PC и «Лучшая поисковая машина» журнала The Net. Многие компании, включая AOL (Netscape) и Washington Post, используют поисковые технологии Google на своих веб-сайтах.

Поисковый сервер Google

http://www.google.ru

Лидер поисковых машин Интернета Google занимает более 70 % мирового рынка. Сейчас служба регистрирует ежедневно около 50 млн поисковых запросов и индексирует более восьми миллиардов веб-страниц. Google может находить информацию на 105 языках.

Интерфейс Google содержит довольно сложный язык запросов, позволяющий ограничить область поиска отдельными доменами, языками, типами файлов и т.д.

Для простого поиска следует набрать нужное слово (или словосочетание) и нажать кнопку *Поиск в Google* (рис. 15.1). В результате появится список ссылок на найденные веб-ресурсы с их кратким описанием и выделением ключевых слов.

В верхней строке данной страницы будет отображено количество найденных веб-ресурсов и время, потраченное на поиск.

Чтобы открыть тот или иной найденный веб-ресурс, который, по мнению пользователя, может быть полезным, следует щелкнуть по соответствующей ссылке в списке.

В нижней части окна расположена область *Страница результатов*, которая позволяет посредством нажатия соответствующей цифры (2, 3, …) перейти на другие страницы со списком ссылок на найденные веб-страницы (рис. 15.2).

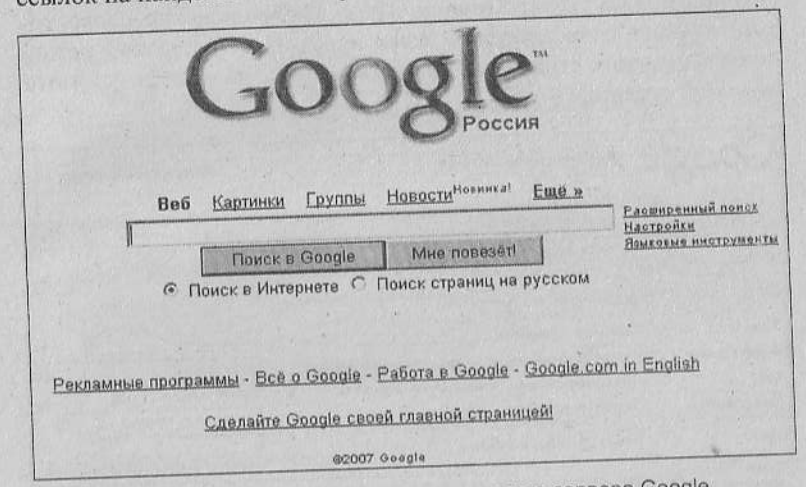


Рис. 15.1. Домашняя страница поискового сервера Google

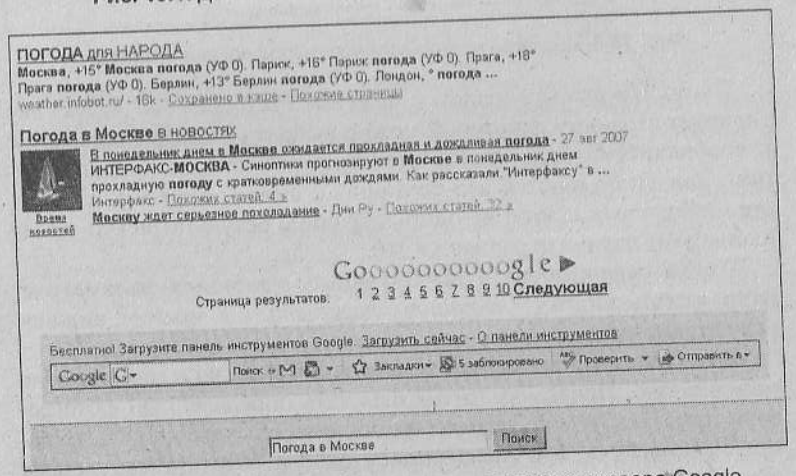


Рис. 15.2. Первая страница результатов поиска на сервере Google

Как правило, наиболее приемлемые результаты поиска содержатся лишь на первых нескольких страницах со списками ссылок на веб-сайты, так как на них размещаются ресурсы, которые включают все запрашиваемые ключевые слова.

Чтобы указать более точные критерии поиска, необходимо щелкнуть по пункту *Расширенный поиск* (находится справа от кнопки *Поиск*). В результате откроется страница (рис. 15.3), на которой можно указать точную фразу, любое искомое слово, отсутствующее слово, нужный язык искомых веб-страниц, режим поиска похожих страниц, количество отображаемых результатов на одной странице и др.

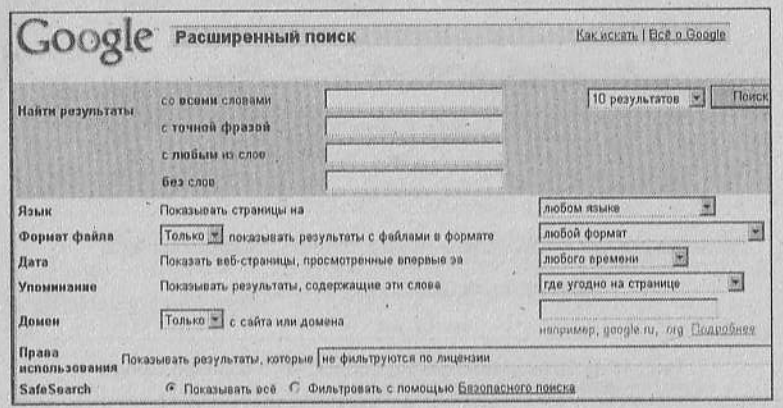


Рис. 15.3. Вид окна настройки параметров поиска в Google

Пункт *Настройки* (рядом с пунктом *Расширенный поиск*) активирует страницу, в которой можно выбрать язык для подсказок и сообщений Google, язык страниц, поиск которых проводится (по умолчанию ищутся веб-страницы с любым языком), количество найденных сайтов на одной странице результатов (по умолчанию этот параметр равняется 10).

Чтобы зафиксировать выполненные изменения параметров, надо нажать кнопку *Сохранить параметры* в правом нижнем углу страницы.

В Google можно искать не только текстовую, но и графическую информацию. Например, чтобы отыскать определенную фотографию ноутбука, нужно вначале выполнить обычный поиск по запросу «ноутбук», а в появившемся окне с результатами поиска щелкнуть в верхней части окна по ссылке *Картинки* (рис. 15.4).

Рис. 15.4. Поиск рисунков в Google

В результате получим множество изображений ноутбуков самых разнообразных моделей.

Почтовый сервис Gmail

http://www.gmail.com

Gmail (от Google Mail) – бесплатная услуга электронной почты от компании Google. Gmail предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколу POP3S.

По сравнению со ставшими уже стандартными почтовыми веб-сервисами Gmail предлагает ряд особенностей и улучшений:

- *просмотр обсуждений* – основная инновация в Gmail – это метод категоризации сообщений, который в Google называют *Conversation View*. В отличие от обычных почтовых сервисов Gmail отслеживает отдельные обсуждения – исходное сообщение с цепочкой ответов на него;
- предоставление более 7 Гбайт дискового пространства для писем (и этот объем постоянно увеличивается). Тем не менее размер одного принимаемого или отсылаемого письма не может превышать 20 Мбайт;

- *автосохранение* – при редактировании сообщений раз в минуту выполняется автоматическое сохранение черновой копии для предотвращения потери данных в случае выключения питания или других сбоев;
- *развитый список контактов* – для каждого собеседника могут задаваться фотография, адреса и телефоны. Адрес электронной почты автоматически подставляется в строку «*Кому*» по имени пользователя, набранного даже частично;
- *«горячие» клавиши* – ускоряют работу с приложением. Использование горячих клавиш в веб-приложениях – редкая практика, и их поддержка стала большим шагом для Google;
- *метки вместо папок* – письма не заносятся в папки, а делятся по категориям, которые пользователь может дополнять и изменять. Эффективность этого механизма такая же, как и более традиционного с папками;
- *поиск по содержимому писем и прикрепленных файлов* – позволяет быстро находить нужное письмо по ключевым словам, что чрезвычайно важно при большом доступном объеме почты;
- *фильтрация от спама* – содержит обучающийся фильтр сообщений, который увеличивает свою эффективность, если пользователь помечает письма как спам;
- *поддержка различных языков* – интерфейс приложения настраивается на большое количество языков, что позволяет сервису быть интернациональным;
- *поддержка RSS* – позволяет читать письма с помощью других RSS-клиентов, например из персонализированных страниц поисковых сайтов, программы Microsoft Deskbar. Это дает возможность проверять почту, не подключаясь к веб-интерфейсу;
- *встроенная проверка орфографии* – автоматически определяет язык сообщения и предлагает варианты написания ошибочных слов;
- *встроенный чат* – сообщения могут доставляться не только с помощью почтовых протоколов, но и через протокол Jabber, благодаря чему пользователи могут обмениваться мгновенными сообщениями, используя программу Google Talk либо любые другие, поддерживающие протокол Jabber.

На стартовой странице службы Gmail.com зарегистрированному пользователю предлагается ввести имя пользователя и пароль для работы со своим ящиком (рис. 15.5).

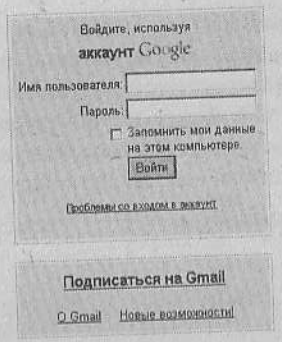


Рис. 15.5. Вход в почтовый ящик Gmail

Если пользователь обращается к почтовой службе с личного компьютера, имеет смысл установить флажок *Запомнить мои данные на этом компьютере*. Эта служба позволяет укорить доступ к почтовому ящику, не вводя каждый раз имя и пароль. Но если доступ к компьютеру имеется у нескольких пользователей, то следует помнить, что служба ускоренного доступа позволит другим пользователям заходить на ваш ящик.

Если пользователь не имеет зарегистрированного почтового ящика, следует щелкнуть по ссылке *Подписаться на Gmail*. Следует внимательно заполнять все поля в предлагаемой форме (рис. 15.6).

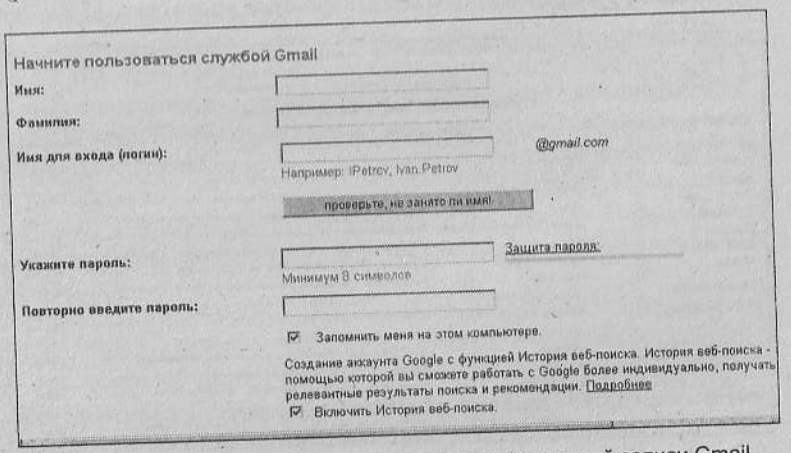


Рис. 15.6. Внешний вид страницы для создания учетной записи Gmail

Чтобы создать письмо, открыв свой почтовый ящик, нужно нажать кнопку *Написать письмо*. В окне отобразятся несколько областей, в которых следует ввести электронный адрес, тему и текст письма (рис. 15.7). Текст можно редактировать, используя кнопки, расположенные над областью текста письма. После ввода всех необходимых данных надо нажать кнопку *Отправить*.

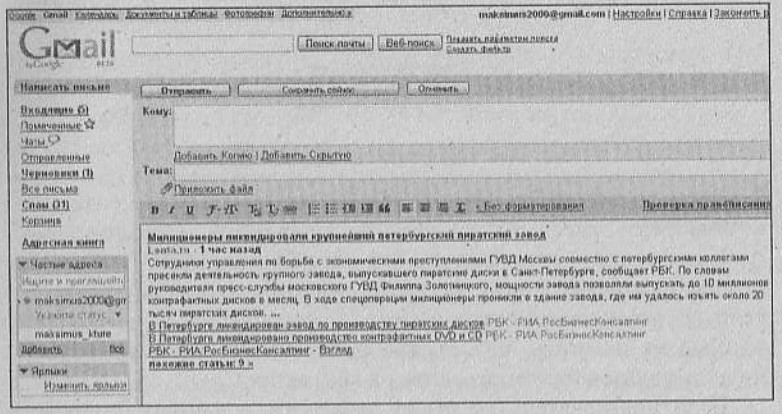


Рис. 15.7. Отправка электронного письма

После нажатия кнопки *Входящие* отобразятся все письма, которые были отправлены на ваш электронный ящик (рис. 15.8).

Рис. 15.8. Просмотр входящих электронных писем

Если нужно быстро найти определенное письмо среди большого количества других, можно воспользоваться поиском, для чего следует в пустое поле справа от надписи «Gmail» ввести тему письма (или характерное слово, употребляющееся в нем), и нажать кнопку *Поиск почты* (рис. 15.9).

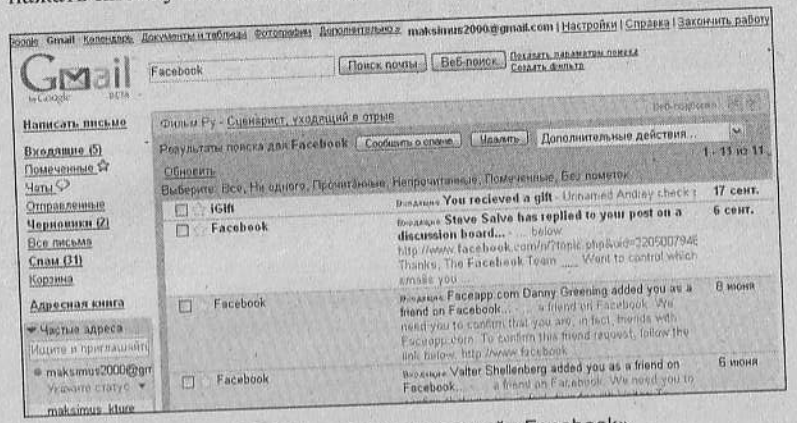


Рис. 15.9. Поиск письма с темой «Facebook»

Календарь Google

Календарь в системе Google многофункционален и в то же время имеет очень простой и интуитивный интерфейс (рис. 15.10). С помощью этого календаря можно отслеживать все важные мероприятия, отправлять приглашения, обмениваться расписаниями с друзьями и родственниками. Этот календарь также позволяет найти интересующие пользователя мероприятия.

Для добавления какой-нибудь записи в календарь нужно выбрать необходимую дату, щелкнуть левой кнопкой мыши по ячейке, соответствующей интересующей дате и времени, и написать название.

Все изменения в календаре автоматически сохраняются в текущем профиле и будут загружены при следующем посещении данной страницы сайта. Так как вся информация сохраняется не на компьютере пользователя, этот календарь можно будет просмотреть и с другого компьютера, зная электронный адрес и соответствующий пароль.

Календарь можно просматривать по дням, неделям, месяцам и др. Переключаться можно при помощи вкладок, расположенных в верхнем правом углу. При этом в основной части окна изменяется графическое отображение календаря, наглядно демонстрируя все занесенные в базу мероприятия. Это дает возможность оперативно просмотреть все предстоящие события. Для быстрого перемещения между более поздней и ранней датой можно использовать кнопки , или клавиши **J** и **K**.

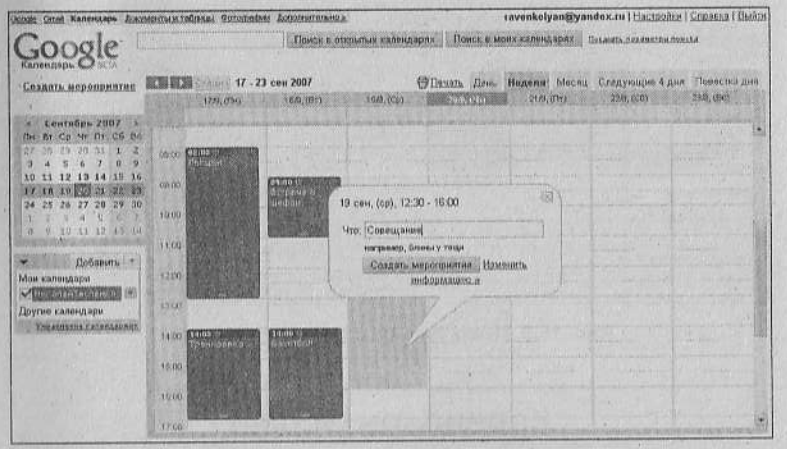


Рис. 15.10. Сервис *Календарь* в Google

Для отправки приглашений на данное мероприятие необходимо просто добавить электронные адреса в разделе *Гости*. Комментарии, написанные для гостей, увидят все, чьи электронные адреса занесены в список.

Календарь в Google предоставляет возможность создать несколько календарей, выбрать для них цвета по своему вкусу, открыть доступ для других пользователей и даже сделать календарь открытым и доступным для поиска.

Карты Google

При помощи Google Maps можно просмотреть карту любой точки Земли, исключая местность севернее 85° северной широты и южнее 85° южной широты, так как на сайте нет снимков данной территории. На ресурс можно попасть, введя в браузере адрес http://maps.google.com.

Детальные карты сделаны при помощи снимков со спутника, а более общие (карты стран и т.п.) – в схематическом варианте. Это позволяет изучить требуемую карту во всех подробностях, подсчитать расстояние между объектами, учитывая шоссе и дороги.

На рис. 15.11 показано основное окно *Карты Google*, в котором изначально отображается схематическая карта США. С помощью кнопок в левом верхнем углу можно прокручивать карту во все стороны. Под кнопками имеется вертикальная полоса с бегунком, перетаскивая который можно изменять масштаб фотографий: вверх – увеличение (детализация), вниз – уменьшение.

В правом нижнем углу всегда доступна миниатюрная карта, на которой просматриваемая область отображается в виде синего прямоугольника. Перемещать область просмотра можно как в основной части программы, так и в миниатюрной карте – путем перетаскивания мышью с нажатой левой кнопкой.

В Google Maps можно искать карту, вводя широту и долготу в произвольном формате. Поиск позволяет быстро найти необходимый фрагмент карты, введя название города или населенного пункта. На рис. 15.12 показана карта центральной части Москвы.

Рис. 15.11. Карты Google: США

Найденные фрагменты карты можно сохранить или распечатать, предварительно выбрав наиболее удобный масштаб отображения. Сохранять можно в форматах BMP и JPEG. Для последнего есть возможность выбирать степень сжатия, что влияет на качество фотографии. Существуют ограничения на размер рисунка в формате BMP – 2 Гбайт.

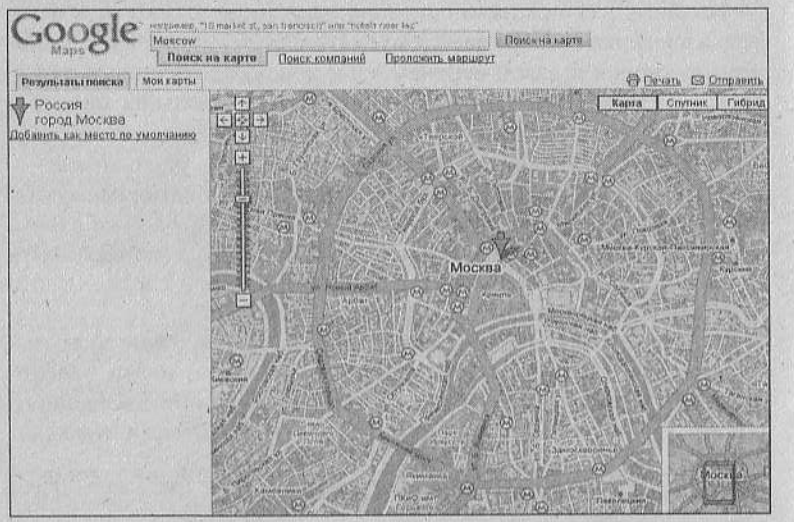


Рис. 15.12. Карты Google: Москва

Совсем недавно в Google Maps появилась новая возможность, позволяющая «прогуляться» по виртуальному городу, осмотреть достопримечательности, витрины магазинов, небоскребы и многое другое. Реализована данная возможность при помощи панорамных снимков улиц. На данный момент на сайте содержатся только снимки улиц американских городов Сан-Франциско, Нью-Йорка, Лас-Вегаса, Денвера и Майами, но в ближайшее время будут добавлены еще несколько городов.

Для включения просмотра улиц нужно лишь нажать кнопку *Просмотр улиц*. После этого отобразятся иконки, показывающие, для каких городов доступна эта функция (рис. 15.13).

Например, щелчок по городу Денверу (штат Колорадо) откроет схематическую карту Денвера с изображением желтого человечка в центре. Чтобы «увидеть мир глазами автолюбителя из Денвера», нужно перетащить человечка на требуемую улицу (или

перекресток). Автоматически отобразится снимок улицы (рис. 15.14), масштаб которого можно изменить при помощи вертикальной полосы в левом верхнем углу.

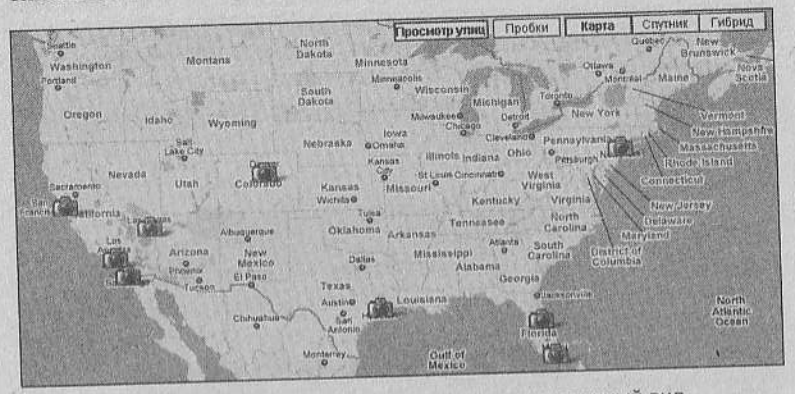


Рис. 15.13. Функция *Просмотр улиц* – схематичный вид

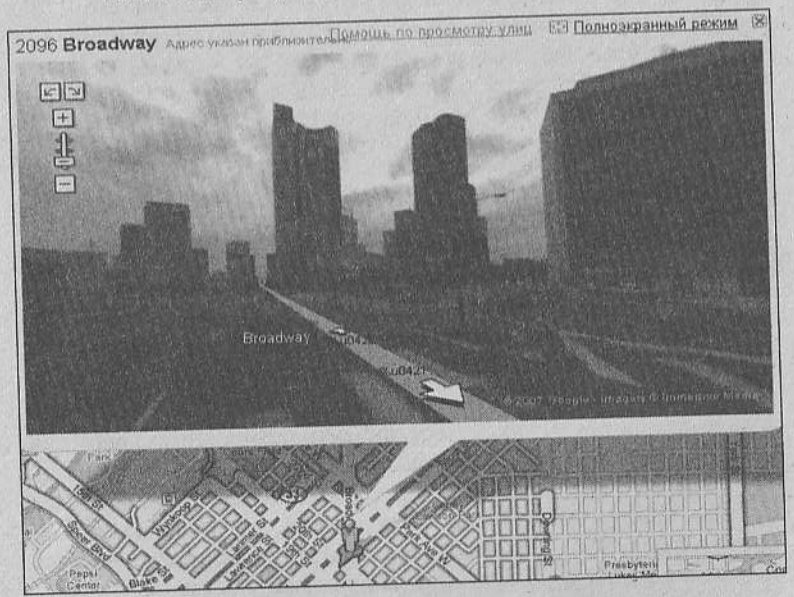


Рис. 15.14. Просмотр улиц: Денвер

Кроме того, можно изменить угол обзора (как бы покрутиться на месте) с помощью кнопок со стрелками: ↶ и ↷. Направление

просмотра улицы со следующей выбранной точки зависит от того, в какую сторону «смотрел» человечек с предыдущей точки.

Чтобы перемещаться по улицам, можно просто перетаскивать фигурку человечка. Если же надо переместиться в определенном направлении по выбранной улице от текущего положения, следует нажать на фотографии соответствующую белую фигурную стрелку (эти стрелки отображаются на желтых полосах, обозначающих улицы).

Google Планета Земля

Этот популярный продукт Google представляет собой трехмерную модель Земного шара в сочетании с огромной базой фотографий со спутника, на каждой из которых изображен какой-то определенный фрагмент земной поверхности (с различной степенью увеличения). Таким образом, можно увидеть любой город, район, улицу и даже отдельный дом. В Google Планета Земля используются лучшие из существующих изображений, большинство из которых были созданы около трех лет назад. База данных изображений регулярно обновляется (в основном это касается фотографий городов США и Западной Европы).

УПРАВЛЕНИЕ МОДЕЛЬЮ ЗЕМЛИ

Начнем знакомство с программой Google Планета Земля (Google Earth) с управления моделью, показанной на рис. 15.15. Ее можно вращать в любой плоскости (расположив над моделью планеты указатель мыши и удерживая нажатой ее левую кнопку).

По аналогии с обычным глобусом модель можно вращать. Для этого достаточно при нажатой левой кнопке мыши резко переместить указатель в любом направлении на несколько сантиметров, после чего отпустить кнопку – «глобус» начнет самостоятельно вращаться. Чтобы его остановить, необходимо просто выполнить по нему щелчок мышью.

Когда пользователь перемещает указатель мыши по поверхности «глобуса», в нижней строке автоматически отображаются координаты текущей точки (широта и долгота). Так, можно выяснить точные координаты родного города или даже собственного дома.

В правом верхнем углу отображается специальная область управления навигацией по «глобусу», показанная на рис. 15.16. Треугольными стрелками в центре навигатора можно пошагово сдвигать область просмотра соответственно влево, вправо, вверх и

вниз. Вращая с помощью мыши «колесо» вокруг этих стрелок, можно вращать карту по часовой стрелке (или против часовой стрелки). На этом колесе имеется символ «N», показывающий направление на север относительно текущего положения «камеры обзора».

Рис. 15.15. Google Планета Земля – общий вид планеты

На навигаторе имеются специальные полоски с ползунками для управления масштабом (справа) и наклоном (вверху). Кнопки по краям полосок позволяют пошагово приближать/удалять изображение, а также наклонять его вверх/вниз. Изменять масштаб можно также путем прокручивания колесика мыши.

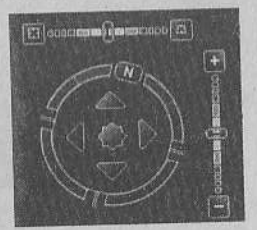


Рис. 15.16. Внешний вид курсора-навигатора

Переместив ползунок правой полоски вверх или вниз, можно соответственно увеличить или уменьшить изображение. Перемещение верхнего ползунка влево или вправо позволит изменить угол обзора.

МАСШТАБИРОВАНИЕ ИЗОБРАЖЕНИЯ

Изначально на «глобусе» видны только границы стран. После двойного щелчка мышью по любому месту «глобуса» оно автоматически «приблизится», позволяя увидеть более детальное изображение. В частности, если щелкнуть по какой-то стране, то после приближения отобразится её название и название столицы, а также названия близлежащих государств и их столиц (рис. 15.17). Столицы для наглядности помечаются звездочками.

Рис. 15.17. Государства и их столицы

Рис. 15.18. Париж с высоты птичьего полета

При изменении масштаба из базы Google в Интернете автоматически скачивается нужная картинка, поэтому нет необходимости загружать все промежуточные фотографии – это позволяет в значительной степени экономить трафик.

Следующий двойной щелчок по любой точке выполнит очередное приближение и т.д. Например, на рис. 15.18 показана часть Парижа после трех приближений.

Рассмотрим более подробно интерфейс программы Google Планета Земля (рис. 15.19).

Рис. 15.19. Внешний вид окна Google Планета Земля. Эйфелева башня

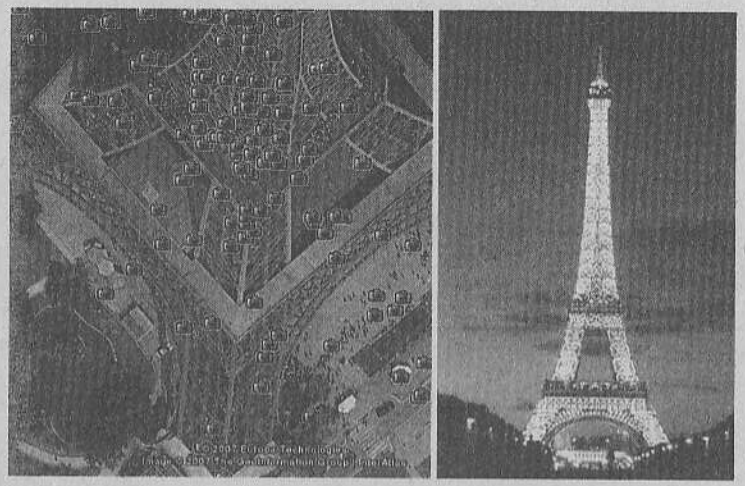
Левую часть приложения занимает так называемая *боковая панель*, а правую – трехмерная карта всего земного шара. И, как в большинстве программ, сверху находится несколько меню и панель инструментов.

В верхней части боковой панели находится область *Поиск*, предоставляющая возможность быстрого «перелета» к определенной точке Земли. Для этого нужно в строке *Перелететь к* (на вкладке *Перелет*) написать требуемое место – название города или какую-то достопримечательность (например, «Эйфелева башня») – и нажать **Enter**.

ФОТОГРАФИИ

Точки, показанные на рис. 15.19, обозначают, что в базе Google имеются фотографии объекта с указанных позиций. Если приблизить камеру, точки превратятся в символы фотоаппаратов (рис. 15.20а). Достаточно щелкнуть мышью по любому из этих

символов – и в отдельном окне появится соответствующая фотография объекта (рис. 15.20б). Сотрудники Google, а также все желающие имеют возможность добавить свои фотографии. Вся поступающая информация обрабатывается разработчиками и выкладывается для общего доступа.



а б

Рис. 15.20. Фотографии объектов в Google Earth:
а – точки, с которых снимались фотографии; б – одна из фотографий

МЕТКИ

Наиболее понравившиеся места можно помечать на карте специальными *метками*. Для добавления метки на карту необходимо выполнить такие действия:

1. Открыть место на карте (с достаточным увеличением), на которое планируется установить метку.
2. Нажать на панели инструментов кнопку  .
3. Щелкнуть по карте – появится специальное обозначение метки и диалоговое окно, в которое нужно ввести название метки и краткое описание. Например, на рис. 15.21 показано создание метки для Петродворца.

Все созданные метки отображаются в области *Метки* боковой панели (рис. 15.22). Для того чтобы камера совершила перелет к той или иной метке, необходимо дважды щелкнуть в списке по

нужной метке. С помощью команд контекстного меню метки можно переименовывать, удалять, группировать по папкам.

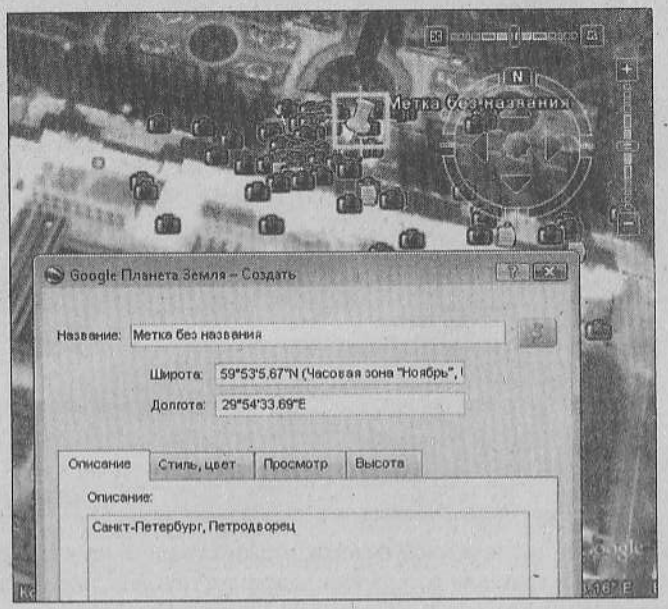


Рис. 15.21. Метка для Петродворца в Санкт-Петербурге

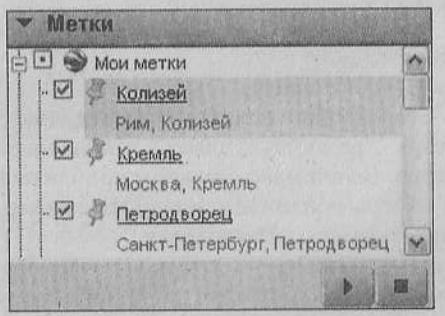


Рис. 15.22. Список созданных меток

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В боковой панели имеется область *Слои*, которая позволяет отобразить на карте специальные обозначения различных объек-

тов (магазины, заправочные станции, гостиницы и т.д.). Фрагмент этой области показан на рис. 15.23.

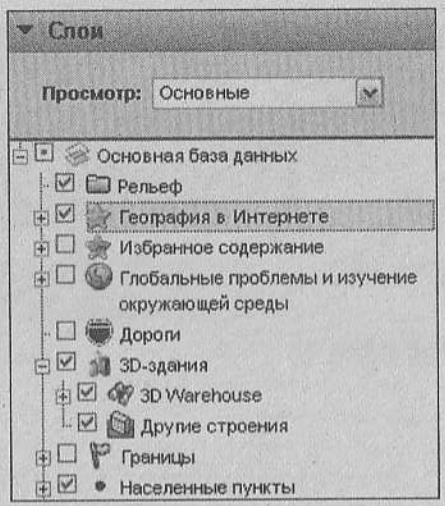


Рис. 15.23. Специальные обозначения на карте

Установив тот или иной флажок, можно увидеть на карте рельеф местности, границы государств, названия городов, дороги, кафе и рестораны, гостиницы, 3D-модели зданий. Некоторые из этих обозначений (например, 3D-модели зданий) появляются на карте только при достижении определенной степени увеличения.

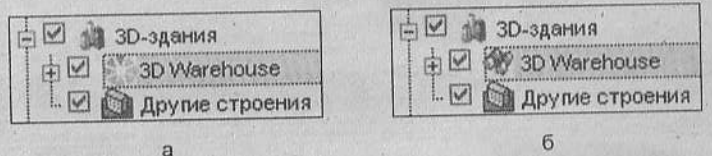
ТРЕХМЕРНЫЕ МОДЕЛИ

В последней версии программы Планета Земля многие участки двумерной территории планеты стали площадкой для трехмерных моделей – различных зданий и ландшафтов. Их лучше всего просматривать при максимальном приближении и наиболее плоском угле обзора (т.е. «вид сбоку»). Например, на рис. 15.24 показан район Манхэттен в Нью-Йорке.

При желании любой пользователь может добавить на карту свою собственную 3D-модель архитектурного сооружения, сделав ее общедоступной для просмотра. Складывается впечатление, что скоро для познания мира не придется даже выходить из дома, – достаточно будет запустить Google Earth и начать трехмерное виртуальное путешествие по самым интересным и загадочным уголкам планеты.

Рис. 15.24. Трехмерная модель Манхэттена в Нью-Йорке

По умолчанию в Google Earth встроена лишь двухмерная (плоская) карта мира с возможностью подключения трехмерных моделей. Для этого нужно в области *Слои* боковой панели установить флажок 3D-здания. При этом рядом с пунктом *3D Warehouse* автоматически отобразится индикатор загрузки 3D-объектов из Интернета (рис. 15.25а). Когда загрузка завершится, индикатор примет другой вид (рис. 15.25б). Теперь на каждом месте карты, где имеется какая-то достопримечательность, будет отображаться ее 3D-модель (если она была создана сообществом Google).



а б

Рис. 15.25. Индикатор 3D-объектов:
а – загрузка; б – отображение загруженных объектов

На самом деле энтузиасты создали достаточно много трехмерных моделей различных достопримечательностей (по несколько экземпляров на каждую). Чтобы получить возможность их просмотра, необходимо скачать из Интернета специальный файл, содержащий информацию обо всех 3D-моделях, доступных на данный момент:

http://services.google.com/earth/kmz/3D_Warehouse.kmz

После того как KMZ-файл загрузится, в программе Google Планета Земля на карте автоматически появится множество трехмерных иконок с изображением домика, означающих, что в этих местах можно просмотреть 3D-модели. Если для какой-то области карты (например, для Парижа или Рима) создано несколько моделей, то при уменьшении масштаба они будут отображаться на карте как один значок группы.

Чтобы увидеть список 3D-объектов какой-либо достопримечательности, достаточно щелкнуть мышью по значку. При этом справа откроется специальное окно с макетами объектов, и щелчок по любому из них отобразит данную модель в отдельном окне.

Например, на рис. 15.26 проиллюстрирован выбор одной из 3D-моделей Колизея.

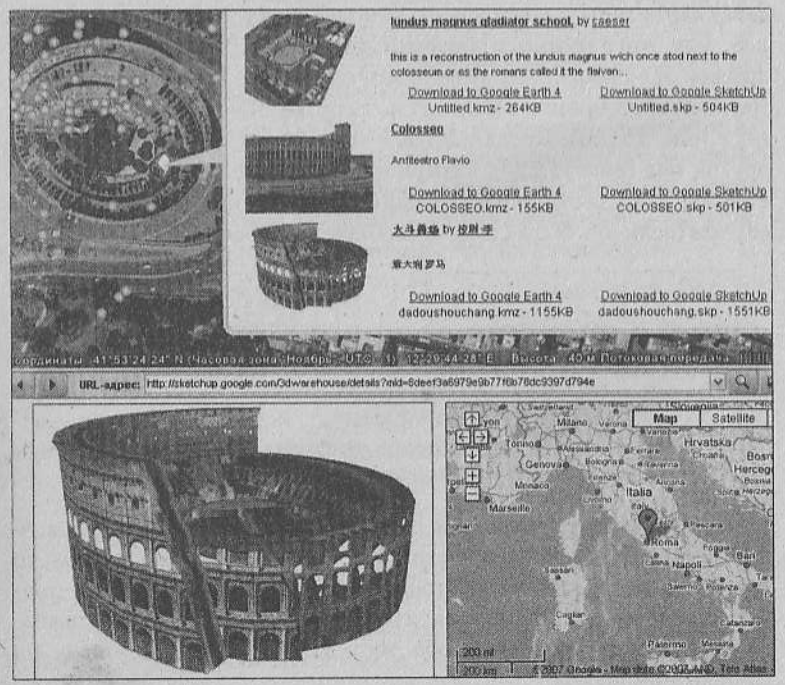


Рис. 15.26. Пример 3D-модели объекта (Рим, Колизей)

Заключение

При подключении компьютера к локальной сети у пользователя появляются такие возможности, о которых несколько лет назад можно было только мечтать, – быстрый обмен документами, фильмами и музыкой, сетевые игры и многое другое.

В книге даны теоретические основы построения сетей, описана методика создания проводной и беспроводной компьютерной сети, предоставление общего доступа к папкам и принтерам, подключение всех компьютеров сети к Интернету с помощью технологий ADSL, Dial-Up и GPRS. Также рассмотрены полезные программы для работы в файлообменных сетях и Интернете.

Авторы выражают надежду, что книга поможет вам самостоятельно построить дома компьютерную сеть и использовать ее многочисленные преимущества для работы и развлечений.