Алексей Чекмарев

Windows 7 в домашней сети

Санкт-Петербург
«БХВ-Петербург»
2011

УДК 681.3.06
ББК 32.973.202
Ч-37

Чекмарев А. Н.

Ч-37 Windows 7 в домашней сети. — СПб.: БХВ-Петербург, 2011. — 240 с.: ил. — (Самое необходимое)

ISBN 978-5-9775-0633-5

Рассматриваются способы организации домашней сети на базе операционной системы Windows 7 и других версий Windows, варианты подключения одного или нескольких компьютеров к Интернету и используемое при этом оборудование (ADSL-модемы, кабельные подключения, телефонные 3G-модемы). Описаны все сетевые параметры и критерии их выбора для той или иной сетевой конфигурации, перечислены возможные типы сетевых подключений и указаны допустимые их значения. Отдельная глава посвящена различным беспроводным сетям (Wi-Fi, Bluetooth, IrDA). Рассказано о способах использования общих папок и принтеров, совместном доступе к библиотекам мультимедиа (включая трансляцию через Интернет), решении возникающих проблем с применением удаленного помощника, принципах установки веб- и FTP-серверов.

Для широкого круга пользователей

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.11.10.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 19,35.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0633-5

© Чекмарев А. Н., 2010
© Оформление, издательство "БХВ-Петербург", 2010

Оглавление

Предисловие

Системы Windows 7 достаточно дружественны по отношению к неопытному пользователю, и в стандартных ситуациях могут автоматически настроить параметры сетевых компонентов. Однако порой даже в не очень сложных случаях у пользователей возникают затруднения: например, при связи нескольких компьютеров через беспроводной маршрутизатор, при "расшаривании" подключения (включении общего доступа) к Интернету или при подключении к общим папкам в сети с разными версиями Windows. Когда требуется ручное конфигурирование или ввод конкретных значений параметров, то оказывается, что сетевых настроек в Windows 7 довольно много, и не всегда очевидно, как поведет себя система при выборе тех или иных установок. Если же пользователь перешел в среду Windows 7 непосредственно из Windows XP, то его вообще может озадачить интерфейс сетевых функций новой системы. Да, хотя принципиально новых вещей в нем не так много, но помимо непривычного внешнего вида имеются и кардинально новые решения, например сетевые профили (сетевое расположение), в решающей степени определяющие работу системы в сети. Всеми этими компонентами нужно уметь правильно управлять, и автор надеется, что данная книга поможет читателю разобраться с настройками системы в любых конфигурациях.

Поначалу некоторые моменты (в тексте книги или в самой системе) могут показаться сложными, но это совсем не так. Если только читать текст и ничего не пробовать делать самому, то, конечно, процесс понимания принципов работы системы осложняется во много раз. Однако если одновременно с чтением выполнять описанные операции или запускать указанные программы и функции, то достаточно быстро окажется, что картина вырисовывается четкая и вполне понятная. От особенностей реализации системных компонентов Windows 7 уже никуда не деться, поэтому следует научиться с ними обращаться!

В системах Windows 7 (особенно в старших редакциях) имеется множество интересных сетевых функций и средств, о которых стоит знать, если есть желание использовать возможности системы полностью и эффективно. Некоторые мелкие детали реализации не лежат на поверхности, и хотелось бы, чтобы они не ускользнули от внимания читателя и пользователя Windows 7. Поэтому в книге немало материала, касающегося новых сетевых возможностей или отличий системных компонентов от их предыдущих версий.

Замечания и вопросы по книге — с указанием ее названия — можно присылать непосредственно автору на адрес: **ATchekmarev@hotmail.com**.

Алексей Чекмарев

ВВЕДЕНИЕ

Обзор сетевых функций Windows 7

Этот обзорный раздел содержит общую информацию о возможностях операционных систем (ОС) семейства Windows 7, причем выбраны те функции, которые имеют отношение к работе в сети. Для полноты картины упомянуты все важные сетевые средства, в том числе и те, которые применяются в больших корпоративных сетях. Получившийся список не особо велик, но следует учесть, что в него намеренно включены только функции и компоненты для работы в *сети*, причем те из них, которые представляют интерес для *конечного пользователя*, а не для программистов и системных администраторов.

В перечне отсутствуют некоторые системные компоненты, которые появились в предыдущих версиях Windows и по-прежнему входят в состав Windows 7:

- общий доступ к интернет-подключению *(глава 2)*;
- поддержка беспроводных сетей *(глава 3)*;
- Защитник Windows (Windows Defender) и встроенный Брандмауэр Windows *(глава 4)*;
- средства управления общими ресурсами *(глава 5)*;
- Удаленный доступ к рабочему столу (Remote Desktop) и Удаленный помощник (Remote Assistance) *(глава 7)* и др.

Некоторые из этих компонентов были заметно модернизированы в Windows 7, и все они подробно описываются в соответствующих главах книги.

Новые возможности для домашних пользователей

Сначала назовем новые возможности Windows 7, представляющие интерес для пользователей домашней сети. Нужно учитывать, что некоторые средства недоступны в младших редакциях — Windows 7 Начальная (Starter Edition) и Windows 7 Домашняя базовая (Home Basic Edition).

Домашняя группа

Компьютеры под управлением Windows 7 можно объединить в так называемую *домашнюю группу* (HomeGroup), пользователи которой могут легко выделять в общее пользование личные ресурсы (документы, фотографии, видео, музыку и принтеры) и получать доступ к файлам других пользователей. При этом настройка максимально упрощена (осуществляется с помощью специальных новых диалоговых окон), и ее может выполнить любой пользователь *(глава 1)*.

Проигрыватель Windows Media Player 12.0

Новая версия проигрывателя файлов мультимедиа позволяет воспроизводить файлы разных форматов (включая AAC, AVCHD, MPEG-2 TS, DVR-MS, WTV и H.264), переписывать аудиодиски на жесткий диск (форматы WMA, WMA lossless, MP3 и WAV) и записывать музыкальные сборники на CD-диски (в формате обычного аудиокомпакт-диска) или переносимые устройства (например, на флэш-плеер). Появилась поддержка новых форматов видео высокой четкости, имеется штатный MPEG-декодер (кроме младших редакций) и декодер форматов DivX/XviD. Файлы любых поддерживаемых форматов можно записывать на внешние устройства, CD- и DVD-диски *(глава 6)*.

Доступ к домашней библиотеке мультимедиа через Интернет

Для редакций Windows 7, начиная с Домашней расширенной (Home Premium), имеется возможность удаленного доступа к файлам, хранящимся на компьютере в библиотеках пользователей. Клиент, запустивший проигрыватель Windows Media на мобильном компьютере, может через Интернет обратиться к домашней библиотеке и воспроизводить хранящиеся в ней файлы стандартным образом, подобно файлам локальной библиотеки *(глава 6)*.

Функция "Воспроизвести на" (Play To)

Пользователь системы Windows 7 может выбрать отдельный файл или целый список и запустить его на воспроизведение на удаленном компьютере с системой Windows 7 и запущенным проигрывателем Windows Media или на бытовом цифровом медиаплеере (мультимедийном обработчике, Digital Media Renderer), поддерживающем стандарт DLNA 1.5 *(глава 6)*.

Браузер Internet Explorer 8.0

Новая версия браузера предлагает эффективные средства просмотра веб-страниц на отдельных вкладках (tabs), средства фильтрации веб-сайтов (InPrivate Filter и SmartScreen), веб-каналы и веб-фрагменты, ускорители (accelerators) для выполнения операций непосредственно с веб-страницы, дополнительные панели, интегрированные средства поиска в Интернете, средства управления устанавливаемыми компонентами (add-ons) и другие функции *(глава 2 — сетевые настройки браузера)*.

Удаленный доступ к рабочему столу (Remote Desktop)

Для удаленной работы в Windows 7 имеются две стандартных функции: *Удаленный рабочий стол* (Remote Desktop) позволяет удаленно подключиться к компьютеру и

использовать все его возможности (для решения задач администрирования или запуска прикладных задач); *Удаленный помощник* (Remote Assistance) по запросу пользователя позволяет удаленному эксперту (из службы поддержки Microsoft, системному администратору или просто знакомому специалисту) наблюдать за тем, что происходит на экране компьютера, вести диалог с пользователем и при необходимости (и при получении соответствующего разрешения) самому выполнять нужные действия. Если для удаленного доступа к рабочему столу необходимо, чтобы целевой компьютер работал под управлением "профессиональных" редакций Windows 7 (Windows 7 Профессиональная (Professional) и старше), то функция Удаленный помощник доступна во всех редакциях, включая "домашние" (Home) *(глава 7)*.

Дополнительные средства для корпоративных сетей

Далее перечислены решения, ориентированные на профессиональных пользователей, работающих в крупных сетях. Почти все эти средства требуют поддержку со стороны соответствующих серверных служб, работающих на базе ОС не ниже Windows Server 2008 или Windows Server 2008 R2[1].

Защита доступа к сети (NAP)

Средство защиты *Network Access Protection* (NAP), работающее вместе с серверной платформой Windows Server 2008 и старше, позволяет предотвратить доступ к внутренней пользовательской сети со стороны небезопасного компьютера, который не отвечает определенным критериям безопасности (эти критерии могут задаваться с помощью групповых политик). Благодаря этому сеть становится менее уязвимой к атакам вирусов и червей, которые могут появиться на мобильных компьютерах, не имеющих последних обновлений безопасности, включенных средств защиты и т. п.

Кэширование файлов BranchCache

Новый компонент BranchCache в системах Windows 7 и Windows Server 2008 R2 позволяет оптимизировать использование файлов, хранящихся в головном офисе. (Данная функция расширяет возможности обычных автономных файлов (offline files).) Для этого организуется кэширование запрошенных файлов в офисе филиала, что позволит в случае повторного запроса этих файлов не обращаться снова к основным серверам, а скачать копии файлов по быстрым каналам внутри филиала. Кэшированные данные могут храниться на сервере филиала, работающего под управлением Windows Server 2008 R2, или же распределяться по компьютерам сотрудников и выдаваться по запросу. При этом можно настраивать дополнительные разрешения на доступ к хранящейся информации.

---

[1] Поэтому в книге они не рассматриваются, за исключением служб IIS 7.5.

Технология удаленного доступа к сети DirectAccess

Новая технология на базе систем Windows 7 и Windows Server 2008 R2 позволяет удаленным клиентам получать защищенный доступ к корпоративной сети через Интернет без установки VPN-канала. Для реализации этой возможности используются протоколы IPv6 и IPsec; для ее развертывания необходимы компьютеры, входящие в домен, компьютер с ОС Windows Server 2008 R2 в качестве сервера DirectAccess, контроллер домена на сервере не ниже Windows Server 2008 и инфраструктура PKI (Public Key Infrastructure), обеспечивающая выдачу сертификатов для проверки подлинности (authentication). Для защиты канала доступа используется шифрование данных с помощью алгоритма IPv6-over-IPsec.

Службы Интернета (IIS 7.5)

В составе Windows 7 поставляются службы *Internet Information Services* (IIS) версии 7.5. Их можно считать платформой для решения серьезных бизнес-задач (так оно и есть!), однако эти службы доступны и в редакции Windows 7 Домашняя расширенная (Home Premium), поэтому и обычный пользователь может установить дома веб- или FTP-сервер, доступный из Интернета (при наличии публичного адреса). Средства управления и настройки служб IIS заметно упрощены, и просмотр домашней страницы веб-узла возможен сразу после установки служб; обращение к файлам по FTP становится возможным после создания сайта с определенными правами доступа. По умолчанию службы IIS не устанавливаются, их нужно активировать через панель управления с помощью стандартной процедуры добавления компонентов Windows *(глава 8)*.

Удаленные компоненты

Некоторые программы и функции, существовавшие в составе предыдущих версий Windows, удалены из Windows 7. Некоторые средства признаны устаревшими, а некоторые функции переданы другим программам. Перечислим компоненты с *сетевыми* функциями (вообще, удаленных программ и функций много больше), которые бесполезно искать в новой системе:

- для совместной работы с приложениями и файлами в Windows Vista предлагаются две программы — *Соседние пользователи* (People Near Me) и *Конференц-зал Windows* (Windows Meeting Space). В Windows 7 они отсутствуют, и им на смену пришли другие продукты Microsoft: Office Communications Server 2007 R2, Live Meeting и Microsoft SharedView;
- программа "Календарь Window"s (Windows Calendar);
- почтовый клиент "Почта Windows" (Windows Mail);
- команда `Net print` удалена, поскольку ее функции могут выполнять другие команды;
- вместо команды `Net send`, используемой для передачи пользователям сети коротких сообщений, предлагается утилита `Msg.exe` с дополнительными возможностями.

Программа обмена мгновенными сообщениями Windows Messenger была удалена еще раньше (из Windows Vista).

На замену некоторым из удаленных приложений пришли компоненты с аналогичными функциями[1], объединенные названием Windows Live™ и свободно загружаемые с веб-сайта Microsoft.

Поддержка некоторых протоколов и служб была прекращена уже в Windows Vista; среди них отметим следующие:

- Клиент для сетей Netware (Client Service for Netware);
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol;
- Serial Line Interface Protocol (SLIP).

В составе служб IIS 7.5, имеющихся в системах Windows 7, отсутствуют какие-либо средства, обеспечивающие хранение сообщений и передачу их клиентам по протоколу POP3.

Установка дополнительных сетевых компонентов

В составе систем Windows 7 (но не во всех редакциях!) имеются следующие стандартные программные компоненты и сервисы, которые по умолчанию ***не*** установлены:

- SNMP-протокол (Simple Network Management Protocol (SNMP));
- Клиент Telnet (Telnet Client);
- Telnet-сервер (Telnet Server);
- Клиент TFTP (TFTP Client);
- Прослушиватель RIP (RIP Listener);
- Простые службы TCPIP (echo, daytime и т. д. — Simple TCPIP services);
- Службы для NFS (Services for NFS).

Для их установки используется ссылка **Включение или отключение компонентов Windows** (Turn Windows features on or off) в окне задачи **Программы и компоненты** (Programs and Features), имеющаяся на панели управления.

[1] Какие-то новые компоненты соответствуют старым по функциональности и даже превосходят их (например, "Почта Windows Live" (Windows Live Mail) или "Фотоальбом Windows Live" (Windows Live Photo Gallery)), а некоторые в чем-то уступают — это относится к программе "Киностудия Windows Live" (Windows Live Movie Maker), которая не имеет таких возможностей монтажа, как Windows Movie Maker, хотя и предоставляет больше опций публикации проектов.

ГЛАВА 1

Работа в сетевой среде

В этой главе рассматриваются общие принципы использования Windows 7 в сети: базовые понятия и концепции, необходимые для понимания реализованных функций и возможностей сетевых компонентов, пользовательский интерфейс, используемый для выполнения основных операций — одним словом, все, что *не связано* с конкретными типами сетевых подключений и задействованных устройств. Описываемые процедуры будут одинаковыми и при работе с ноутбуком и беспроводным Wi-Fi-подключением, и для настольного компьютера с подключением по локальной сети.

Различные типы сетевых подключений и настройка их параметров описываются в *главе 2*, а беспроводным подключениям целиком посвящена *глава 3*. Это единственные две главы, "привязанные" к аппаратным средствам и свойствам протоколов, а последующие главы также не зависят от сетевых настроек и рассмотренные там принципы и функции применимы к любой конфигурации сети.

Категории сетей (сетевое размещение)

С самого начала необходимо остановиться на понятии *категория сети*[1] (network category), или *сетевое размещение* (network location), которое появилось впервые еще в Windows Vista; оно связано с множеством параметров, которые определяют уровень безопасности, предъявляемый к определенной сети, к которой подключается компьютер. Это очень важный момент, поскольку выбранное для компьютера размещение в значительной степени определяет набор сетевых функций и возможностей, особенно в локальной сети при взаимодействии между разными системами.

В первую очередь сетевое размещение актуально для пользователей мобильных компьютеров, которые часто перемещаются между разными сетями — домашними, корпоративными и общедоступными. (Такие перемещения требуют постоянно-

[1] В пользовательском интерфейсе систем Windows 7 в основном используется термин *сетевое размещение* (network location).

го изменения сетевых параметров!) Для этих пользователей важно, чтобы компьютер (в первую очередь встроенный брандмауэр Windows) "помнил" параметры блокировки трафика для различных сетевых сервисов (например, для Службы доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks)) и мог быстро переключаться на работу с измененными параметрами.

Как и в Windows Vista, в системах Windows 7 предусмотрены три категории (типа) сетей:

- *Домашняя сеть* (Home network) — домашняя сеть или сеть малого офиса, используемая ограниченным и известным кругом людей. По умолчанию в таких сетях разрешено распознавание компьютера и его ресурсов, что позволяет другим пользователям сети обращаться к сервисам компьютера (в том числе — к дискам и принтерам). Для упрощения конфигурирования общих ресурсов и сетевых параметров в домашней сети разработана новая концепция *домашней группы* (HomeGroup) *(см. далее)*;
- *Общественная сеть* (Public network) — сеть с точками доступа, располагающимися в публичных местах (интернет-кафе и т. п.). Для такой сети устанавливаются наиболее жесткие ограничения, позволяющие максимально обезопасить компьютер, например отключено распознавание компьютера;
- *Рабочая сеть* (Work network), или *Сеть предприятия* — корпоративная сеть с известными пользователями. Эта категория выбирается автоматически при подключении компьютера к домену, и ее вручную изменить нельзя.

В зависимости от выбранной категории сети брандмауэр Windows (Windows Firewall) автоматически выбирает стандартные для этой категории исключения (exceptions) *(см. главу 4)*, блокируя или, наоборот, открывая те или иные порты TCP/UDP, используемые системными сервисами и приложениями. При этом могут меняться некоторые параметры безопасности (это касается учетной записи Гость (Guest) и общего доступа к папкам).

Итак, можно сказать, что сетевое размещение — это совокупность настроек сетевых компонентов, определяющих возможности доступа извне к его общим ресурсам (определенных автоматически или самим пользователем — *см. главу 5*). Благодаря этому механизму система всегда остается максимально функциональной и, в то же время, защищенной в каждой конкретной сетевой среде. Из сказанного ясно, что вопрос выбора правильного размещения (типа сети) для имеющихся сетевых подключений и конкретных параметров каждого размещения (профиля) является ключевым при работе компьютера в сети или при подключении компьютеров друг к другу.

> ***Примечание***
>
> Первоначальный выбор категории сети осуществляется еще при установке операционной системы: по окончанию этой операции после перезагрузки задаются имена пользователя и компьютера, после чего определяются параметры обновления Windows и указывается текущее сетевое местоположение компьютера. В дальнейшем сетевое размещение можно менять в соответствии с рабочей средой *(см. далее)*.

Подключение к сетям и удаленным компьютерам

По умолчанию значок сети всегда отображается на панели задач в области уведомлений[1] (рис. 1.1, *слева*). Вид этого значка может меняться в зависимости от сетевых возможностей системы (это мы рассмотрим чуть позже). Поскольку сейчас редко встретишь настольные компьютеры или ноутбуки без сетевого Ethernet-адаптера[2], то в процессе установки Windows 7 при наличии соответствующих драйверов автоматически создается сетевое подключение — обычно это *подключение по локальной сети* (Local Area Connection). На мобильных компьютерах к этому как правило добавляется *беспроводное соединение* (Wireless Connection).

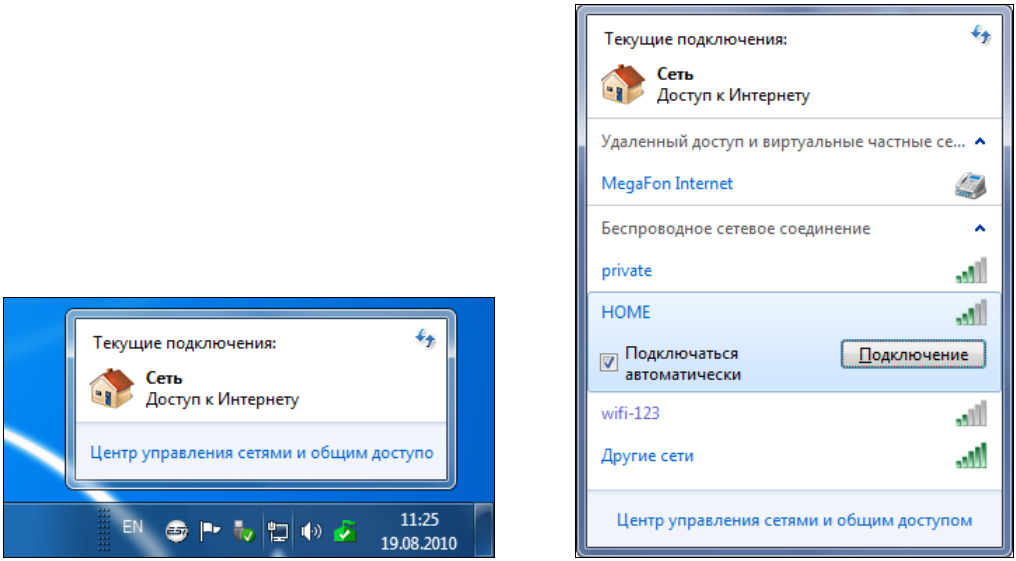

Рис. 1.1. Окно сетевых подключений компьютера и доступных сетей

Если щелкнуть по значку сети, то появится окно, в котором указаны имена подключений и сетей, которые может задействовать компьютер[3] по запросу пользователя (в верхней части всегда показаны все *активные* подключения). В простейшем случае (рис. 1.1, *слева*) мы увидим единственное сетевое подключение; при наличии нескольких сетевых адаптеров и устройств связи в данном окне может образоваться целый список доступных подключений и сетей. В примере, приведенном на

---

[1] Анимация значка сетевых подключений в Windows 7 отсутствует.

[2] Ethernet — самый распространенный стандарт проводных локальных сетей. В спецификациях производителей интерфейс для этих сетей обычно называют просто LAN-адаптером (LAN — Local Area Network, локальная сеть).

[3] Если нужно часто обращаться к этому окну, то включите в меню **Пуск** (Start) опцию **Подключение к** (Connect To) — для этого установите соответствующий флажок в окне свойств панели задач и кнопки "Пуск".

рис. 1.1, *справа*, помимо текущего сетевого подключения по локальной сети, можно также видеть имеющееся коммутируемое подключение, обеспечивающее доступ по беспроводному USB-модему (значок с изображением телефона), и список Wi-Fi-сетей, видимых через беспроводной адаптер.

Чтобы соединиться с другой сетью или активизировать подключение, достаточно щелкнуть по названию и нажать кнопку **Подключение** (Connect). Так же легко отключиться от любой сети или разорвать соединение.

Доступ к Интернету

Сообщение о наличии доступа к Интернету появляется в окне сетевых подключений (см. рис. 1.1) в том случае, если успешно выполняются служебные проверки: система проверяет правильность разрешения DNS-имени специального сайта компании Microsoft и выполняет HTTP-запрос к имеющемуся там тестовому текстовому файлу. Иногда при использовании прокси-серверов поставщиков Интернета или корпоративных брандмауэров, ограничивающих трафик, выполнение этих запросов может быть затруднено, и сообщение будет отсутствовать при фактическом наличии доступа к Сети. Если указанные выше служебные проверки для всех соединений заканчиваются неудачей, то в окне подключений отображается фраза "Без доступа к Интернету" и на значке сети появляется желтый треугольник с восклицательным знаком  .

В случае полной недоступности сетевых ресурсов из-за отсутствия сетевых адаптеров, при отключении сетевого кабеля или при неправильной работе драйверов на значке сети появляется красный крест  . Тогда в окне подключений (рис. 1.2) отображается соответствующее сообщение, и можно запустить диагностику или начать самостоятельную проверку устройств и драйверов[1]. Если аппаратная или программная ошибка будет устранена, система автоматически обновит состояние сетевого адаптера и значок поменяется.

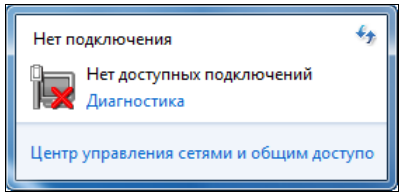

Рис. 1.2. Вид окна сети в случае отсутствия сетевых подключений

Беспроводные сети

Если в системе имеется только беспроводное соединение или такое соединение является *приоритетным*, то значок сети будет выглядеть иначе: при наличии подключения к внешней сети (или к другому компьютеру) с выходом в Интернет мы видим "белые" столбики  (сравните со значком на рис. 1.1). Если при этом *отсутствует* доступ к Интернету, то на значке появляется желтый треугольник с восклицательным знаком  . В случае, когда подключение к внешней сети не установлено, но имеются доступные беспроводные сети, столбики на значке будут темно-серыми, а на самом значке появится желтая "звездочка"  .

[1] Обычно для этих целей используется Диспетчер устройств (Device Manager).

ВНИМАНИЕ!

Поведение значка сети не всегда корректно (например, при включении входящих подключений на значке ***всегда*** будет присутствовать красный крест — это признанная ошибка). В некоторых случаях значок желтого треугольника с восклицательным знаком появляется, даже если все подключения работают нормально (такое бывает при наличии нескольких подключений разного типа или в сложных, нестандартных сетевых конфигурациях). Поэтому полагаться на вид значка можно только в известных сетях с хорошо проверенными режимами работы. Иногда просто не следует обращать на него внимания[1].

Ссылка **Центр управления сетями и общим доступом** (Open Network and Sharing Center) в окне текущих подключений (см. рис. 1.1) позволяет перейти в главное окно всех сетевых настроек Windows 7 *(см. далее)*. (Из Центра управления сетями обратно в окно текущих подключений легко попасть по ссылке **Подключиться к сети** (Connect to a network) (см. рис. 1.7).)

Если по значку сети щелкнуть правой кнопкой мыши, то в контекстном меню можно увидеть команду **Диагностика неполадок** (Troubleshoot problems), которая запускает программу-мастер, позволяющую устранить неисправности при ошибках подключения. При этом проверяются и могут сбрасываться сетевые параметры, может обновляться IP-адрес, если он получается автоматически, и т. п. Данную команду можно выполнять при отсутствии подключения к веб-сайтам — она позволит диагностировать или устранить причину. Также ее полезно выполнить, если на компьютере были сетевые ошибки и менялась конфигурация сети (адреса, параметры, параметры общего доступа к Интернету и т. д.). В этом случае компьютер автоматически получит новые установки, и проблемы могут быть устранены.

Просмотр ресурсов локальной сети

Для просмотра разнообразных общих сетевых ресурсов[2] в локальной сети или на других компьютерах (при непосредственном подключении) в системах Windows традиционно используется папка **Сеть**[3] (Network), отображаемая в окне Проводника (Windows Explorer) (см. рис. 1.4). Кроме того, компьютеры, работающие под управлением Windows 7, могут объединяться в так называемую *домашнюю группу* (HomeGroup) и для настройки ресурсов для работы в такой конфигурации в Windows 7 имеются специальные, новые возможности, которые будут рассмотрены *далее*.

ПРИМЕЧАНИЕ

Все операции настройки, просмотра и подключения общих папок и принтеров подробно рассматриваются в *главе 5*.

---

[1] Значок сети можно *вообще* убрать, выполнив соответствующие настройки области уведомлений.

[2] Настройка общих папок и принтеров подробно рассматривается в *главе 5*.

[3] Для быстрого доступа к папкам **Сеть** (Network) и **Домашняя группа** (Homegroup) можно использовать одноименные опции в меню **Пуск** (Start). По умолчанию они не отображаются, и их следует включать вручную в окне свойств панели задач и кнопки "Пуск".

Компьютеры с обычными общими папками и принтерами

При первом обращении к содержимому папки **Сеть** (Network) в окне Проводника может появиться сообщение *"Сетевое окружение и общий доступ к файлам отключен. Сетевые компьютеры и устройства не видны. Щелкните для изменения"*. Это объясняется тем, что для общественной сети во вновь установленной системе сетевое обнаружение и общий доступ к папкам отключены. Для домашней сети сетевое обнаружение по умолчанию разрешено, но доступ к общим папкам также закрыт (рис. 1.3). Чтобы включить видимость компьютеров в сети или разрешить общий доступ, достаточно щелкнуть по появляющемуся в Проводнике сообщению и выбрать в контекстном меню соответствующую команду; для обеспечения доступа к общим ресурсам компьютера следует также выполнить ручную настройку общих папок и принтеров *(см. главу 5)*.

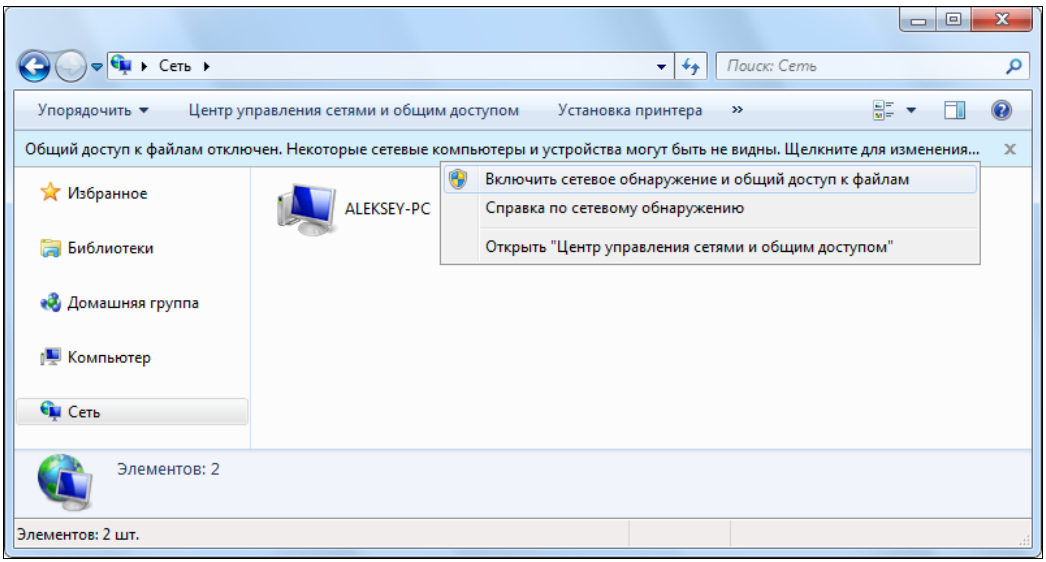

Рис. 1.3. Включение сетевого обнаружения и разрешение доступа к общим ресурсам

Чтобы компьютеры были видны в сетевом окружении, необходимо чтобы они все принадлежали к одной рабочей группе (workgroup) (как назначить имя группы или самого компьютера — рассказано *далее* в этой главе). Помимо значков компьютеров (рис. 1.4), можно видеть имеющиеся в сети устройства и библиотеки мультимедиа, к которым разрешен общий доступ или которые обеспечивают потоковое воспроизведение мультимедиа (подробнее об этом рассказывается в *главе 6*). Как видно из примера, такие библиотеки могут работать как под управлением Windows 7, так и в системах более ранних версий (см. компьютер XPRUS) при установке Проигрывателя Windows Media (Windows Media Player) версии 11.0.

Щелкнув по значку компьютера, можно увидеть общие папки и принтеры, имеющиеся на данном компьютере. Можно просматривать их содержимое или подклю-

чать в качестве дисков или удаленных устройств печати (подробнее эти операции рассматриваются в *главе 5*). Также, с помощью команды из контекстного меню (см. рис. 1.4), легко подключиться к удаленному рабочему столу *(см. главу 7)*.

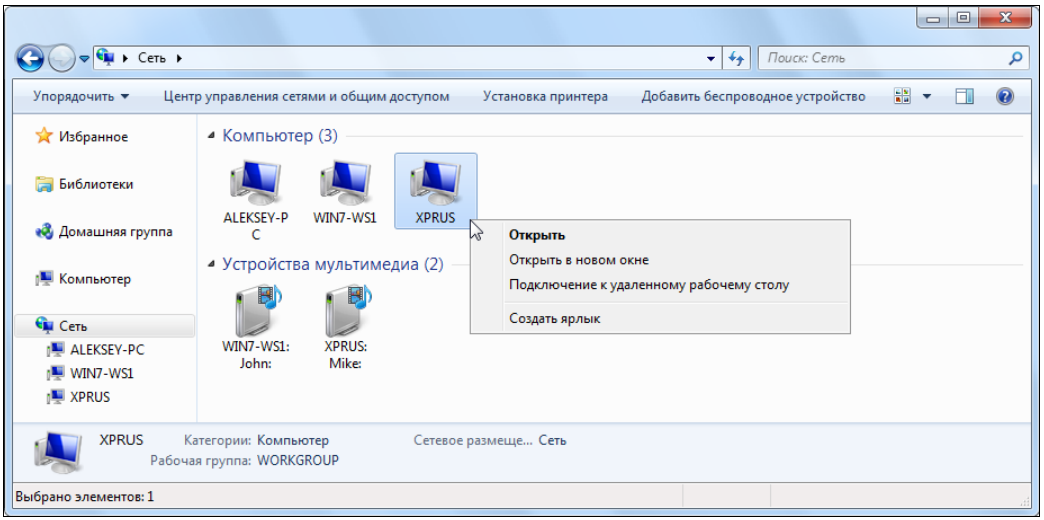

Рис. 1.4. Просмотр списка компьютеров, входящих в рабочую группу

Если для папки **Сеть** (Network) выбрать представление "Таблица" (Details), то затем можно включить отображение дополнительных столбцов (щелкнув правой кнопкой мыши по заголовку таблицы и установив нужные флажки в контекстном меню) (рис. 1.5). Здесь можно увидеть имя рабочей группы, название сети (сетевого подключения), а также MAC-адрес сетевых адаптеров и IP-адрес компьютеров и устройств (для своей системы указывается адрес 127.0.0.1).

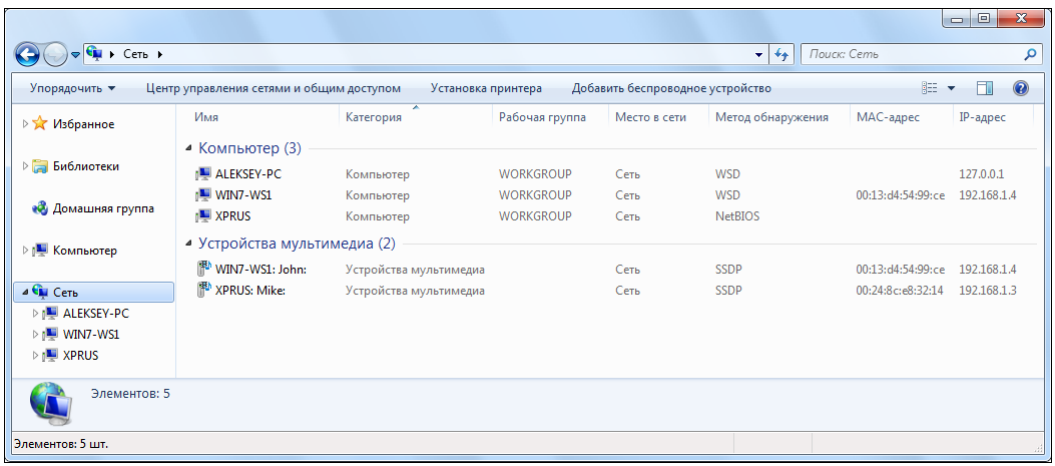

Рис. 1.5. Дополнительные свойства компьютеров рабочей группы

Метод обнаружения (см. рис. 1.5) указывает на протокол, используемый для разрешения имен в сети и поиска устройств. Спецификация *Web Services on Devices* (WSD) представляет собой стандарт Microsoft для связи систем Windows и устройств, ориентированных на работу с веб-службами (это могут быть карманные компьютеры (PDA), периферийные устройства, бытовая аппаратура и т. п.). Данный метод обнаружения является основным для систем Windows Vista и Windows 7. Более старые версии (например, Windows XP — см. рис. 1.5) используют традиционный протокол NetBIOS.

Протокол *Simple Search and Discovery Protocol* (SSDP) служит для обнаружения UPnP[1]-устройств, совместимых со спецификацией Microsoft SSDP media stack, и получения описаний таких устройств.

Все описанные выше параметры иногда полезно знать для тонкой настройки сетевых устройств или при анализе неисправностей.

Компьютеры в составе домашней группы

В домашней группе (HomeGroup) конфигурирование общих ресурсов упрощается до максимума *(см. далее разд. "Настройка компьютеров домашней группы")*, и все доступные ресурсы сразу видны в окне Проводника (Windows Explorer) внутри папки **Домашняя группа** (HomeGroup) (рис. 1.6). Здесь отображаются личные библиотеки, к которым разрешен общий доступ. В нашем примере зарегистрированному в системе пользователю доступна папка **Изображения** (Pictures), принадлежащая пользователю User, работающему на *этом* же компьютере (ALEKSEY-PC), а также некоторые папки, хранящиеся на *удаленном* компьютере (WIN7-WS2) и принадлежащие двум пользователям — Aleksey и Mike — того компьютера (регистрация этих пользователей в системе не требуется, достаточно лишь загруженной системы).

На рис. 1.6 можно видеть, что набор личных папок, выделенных пользователями в общий доступ, индивидуален и определяется исключительно самим пользователем. При этом механизм домашней группы позволяет организовать общий доступ к файлам и для разных пользователей *одного и того же* компьютера (помимо организации общих папок, описываемых в *главе 5*). Работа с любыми типами файлов, хранящихся в библиотеках участников домашней группы, происходит так же, как и с обычными локальными файлами. Использование библиотек мультимедиа подробно описывается в *главе 6*.

> ***Внимание!***
>
> Участники рабочей группы имеют только право *чтения* чужих личных библиотек. Любые операции создания файлов переназначаются в соответствующие общие папки *(см. разд. "Личные папки и папка Общие (Public)" главы 5)*.
>
> Для доступа к библиотекам, хранящимся на других компьютерах домашней группы, необходимо, чтобы учетная запись пользователя ***имела пароль*** — это стандартное требование Windows 7 при обращении к удаленным общим сетевым папкам, распространяемое и на домашнюю группу.

[1] Universal Plug and Play.

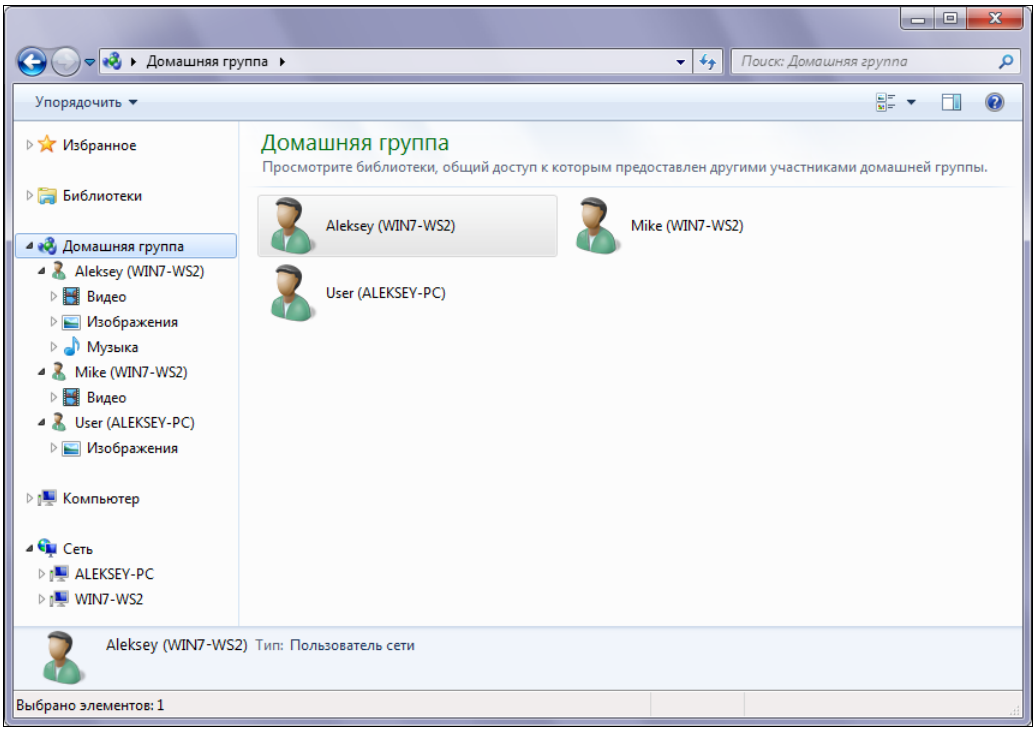

Рис. 1.6. Просмотр ресурсов, предоставленных в общее пользование членами домашней группы

Если папка **Домашняя группа** (HomeGroup) пустая, это означает, что компьютер не входит в домашнюю группу или имеются проблемы в ее работе. В этом случае в окне отображаются кнопка подключения к группе, ссылка на дополнительные сведения или опция запуска средства устранения неполадок, позволяющего автоматически диагностировать и/или устранить возникшие ошибки.

Просмотр свойств сети и конфигурирование компонентов

Как и в системах Windows Vista, все операции по мониторингу и конфигурированию сетевых средств в Windows 7 осуществляются в окне *Центра управления сетями и общим доступом*[1] (Network and Sharing Center) (рис. 1.7) — здесь можно видеть все активные подключения, менять параметры созданных подключений, управлять общим доступом к файлам и принтерам, а также инициировать операции подключения к сетям и создания новых подключений[2].

[1] Дизайн и возможности этого окна в Windows 7 заметно изменились.

[2] Ссылка **Управление беспроводными сетями** (Manage wireless networks) появляется в левой части окна, если только на компьютере имеется беспроводной адаптер и разрешены беспроводные соединения.

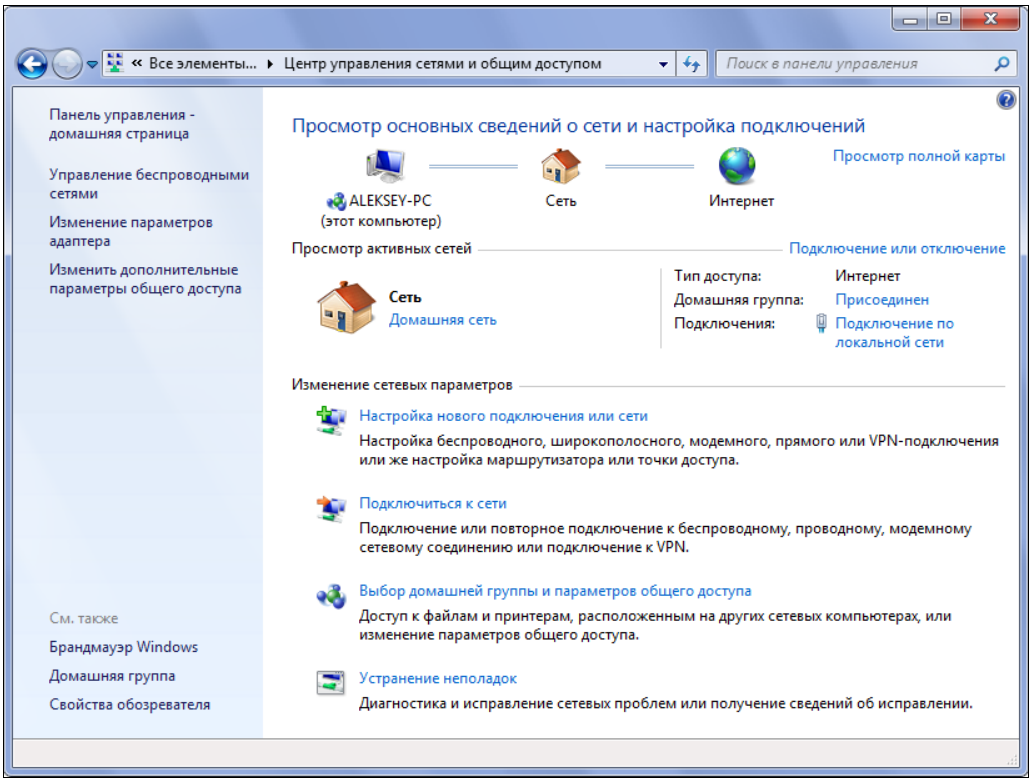

Рис. 1.7. Окно Центра управления сетями и общим доступом

Окно Центра управления сетями можно открыть с панели управления или из окна сетевых подключений (см. рис. 1.1). Хотя в системах Windows 7 способ организации сетевых функций и интерфейс этого окна изменились по сравнению с Windows Vista, однако суть и количество операций по настройке сети практически остались прежними[1] (если не считать настройку параметров домашней группы).

В окне сетевого центра показаны режимы использования всех активных в данный момент подключений или сетей (рис. 1.8). Для каждого подключения указано выбранное для него сетевое размещение (Network Location): в нашем примере подключение **Сеть** относится к *Домашней сети* (Home network), а подключение **MegaFon Internet** — к *Общественной сети* (Public network).

Если компьютер входит в домашнюю группу, то это отмечено в окне сетевого центра — см. ссылку **Присоединен** (Joined) на рис. 1.8. Щелкнув по этой ссылке, можно сразу попасть в окно настройки параметров общих библиотек — окно **Домашняя группа** (Homegroup) (см. рис. 1.22), где в любой момент можно изменить членство в домашней группе, а также выбрать библиотеки, доступные для воспроизведения другим участникам домашней группы (к этим библиотекам можно будет

[1] Даже если сравнивать с предыдущими версиями Windows; существенно изменился лишь пользовательский интерфейс операций настройки.

обращаться из Проигрывателя Windows Media (Windows Media Player) версии 12.0 — см. список библиотек в левой части окна программы на рис. 6.2).

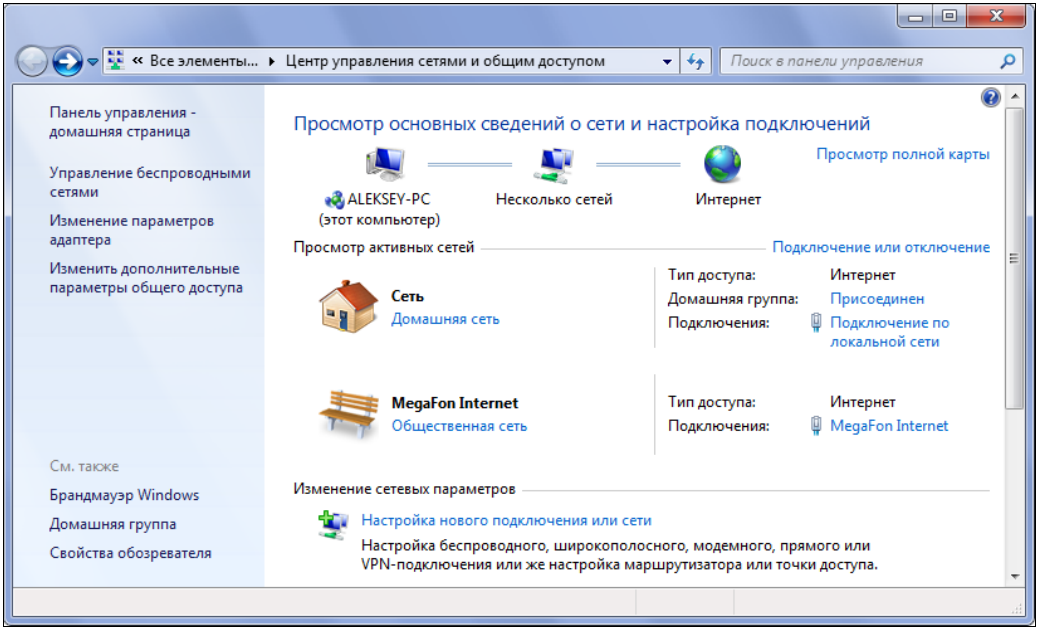

Рис. 1.8. Просмотр общих характеристик двух активных подключений

Многочисленные параметры общего доступа, определяющие настройки брандмауэра для сервисов обнаружения сети (Network Detection) и службы доступа к папкам и принтерам (File and Printer Sharing), а также связанные с некоторыми параметрами системы безопасности (например, с состоянием учетной записи Гость (Guest)), настраиваются в специальном окне, которое открывается по ссылке **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) в левой части окна Центра управления сетями (см. рис. 1.8). Эти параметры подробно рассматриваются *далее в разд. "Настройка сетевого доступа к общим папкам и принтерам"*.

Выбор сетевого размещения и названия сети

Щелкнув по ссылке с указанием сетевого размещения (см. рис. 1.8), можно в специальном окне (рис. 1.9) изменить тип (категорию) сети — в этом окне подробно перечислены особенности каждого варианта. (Обратите внимание на то, что для этого требуются административные права — соответствующие опции отмечены значком щита, указывающего на необходимость дополнительных полномочий.) Это можно делать свободно только для компьютеров, не входящих в домен Active Directory, поскольку для членов домена размещение в *Рабочей сети* и соответствующий профиль встроенного брандмауэра Windows (доменный профиль) устанавливаются автоматически, и вручную их поменять нельзя.

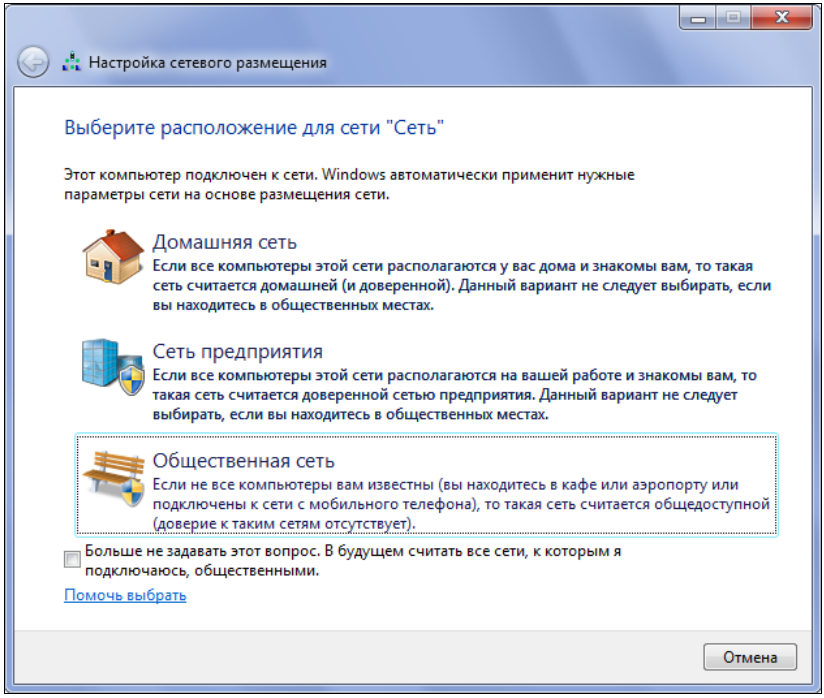

Рис. 1.9. Выбор сетевого размещения для данного подключения

При переключении от общественной сети к домашней система также предлагает создать домашнюю группу или подключиться к существующей. Если это не требуется, достаточно просто отказаться от операции.

Неопознанная сеть

Иногда, в силу особенностей сетевой конфигурации, сеть, связанная с некоторым подключением, получает имя "Неопознанная сеть" (Unknown network) и имеет размещение *Общественная сеть* (Public network), которое напрямую поменять нельзя[1]. Это не всегда принципиально влияет на работоспособность компьютера в сети, однако нужно проанализировать ситуацию, разобраться в причинах *(см. разд. "Выбор параметров" и "Особенности работы с несколькими сетевыми подключениями" главы 2)* и проследить за тем, какие при этом используются параметры сетевого обнаружения и общего доступа *(см. далее разд. "Настройка сетевого доступа к общим папкам и принтерам")*. Возможно, потребуется индивидуально настроить некоторые правила фильтрации протоколов *(см. главу 4)*.

Чтобы изменить *название* сети и соответствующий ей *значок* (см. список активных сетей на рис. 1.8), нужно щелкнуть по значку сети и в специальном окне ввести произвольное имя и/или выбрать значок (в этом качестве можно также использовать любой графический файл). Эта операция доступна любому пользователю, не только администраторам.

[1] В этом случае возможности изменения имени сети и размещения просто блокируются.

Карта сети

Ссылка **Просмотр полной карты** (See full map) (см. рис. 1.7) позволяет увидеть так называемую *карту сети* (network map) для выбранного подключения (рис. 1.10). На этой карте видны компьютеры, с которыми имеется связь, а также показано, имеется ли выход в Интернет[1] (связь с изображением глобуса) и через какое оборудование. Наведя курсор мыши на объект, можно сразу увидеть основные сетевые параметры для взаимодействующих узлов (в частности, легко определить адрес шлюза, через который осуществляется подключение к Интернету[2]).

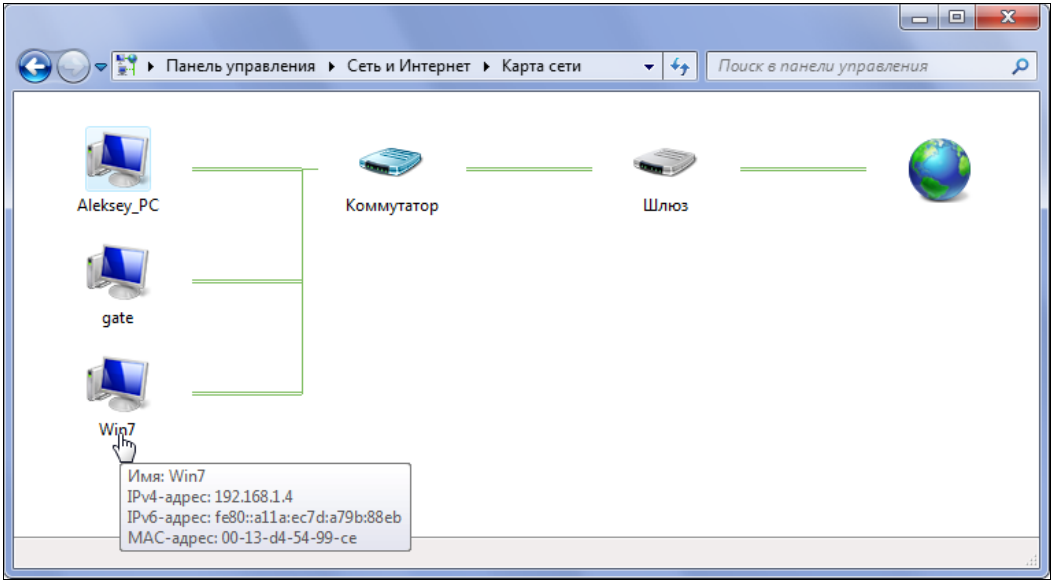

Рис. 1.10. Пример карты кабельной локальной сети с несколькими компьютерами

> ***Внимание!***
>
> Просмотр карты сети по умолчанию запрещен для компьютеров, входящих в домен. Однако с помощью групповых политик администратор может включить функцию построения карты сети. Для общественных сетей (Public network) создание карты сети невозможно.

Если в системе имеется несколько сетевых подключений, то карта сети создается *индивидуально* для каждого подключения и его сначала нужно выбрать из списка. На рис. 1.11 показан пример карты сети для смешанной сети (при этом видно имя сети, к которой выполнено данное подключение — это может быть точка доступа или другой компьютер в случае соединения "точка-точка"). Здесь два компьютера и

---

[1] Если доступ к Интернету отсутствует, то соответствующая связь будет перечеркнута красным крестом.

[2] Если шлюз не настроен (отсутствует), то и соответствующий значок шлюза и изображение глобуса будут также отсутствовать.

медиасервер WDTVLIVE подключены через Wi-Fi-адаптеры к точке доступа (эти соединения показаны пунктиром), которая в свою очередь по локальной сети связана с коммутатором, обеспечивающим третьему компьютеру доступ по кабелю.

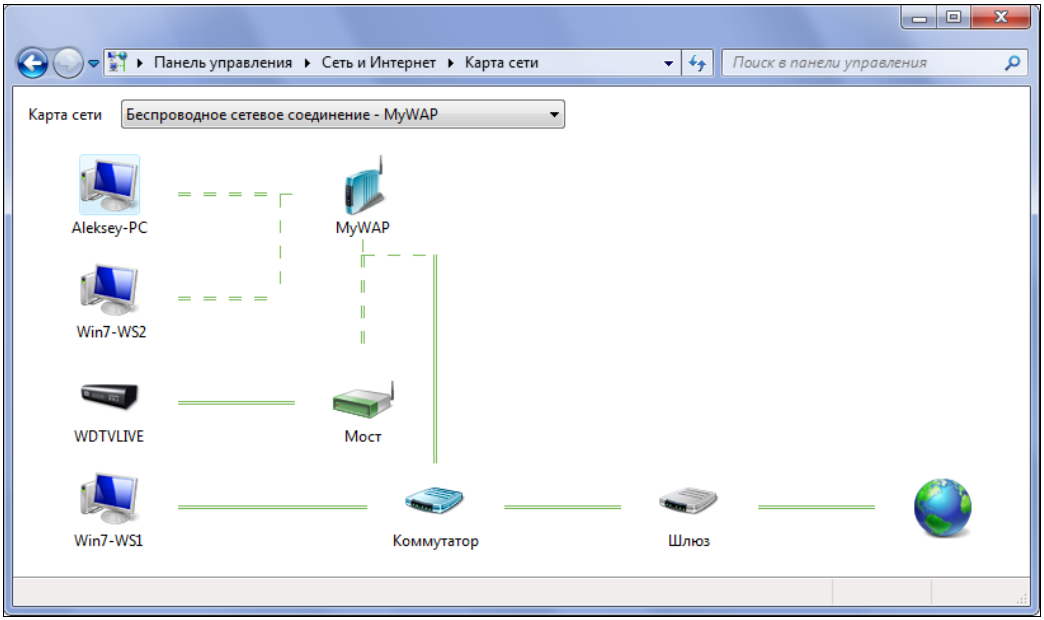

Рис. 1.11. Карта сети, в которой имеются проводные и беспроводные подключения

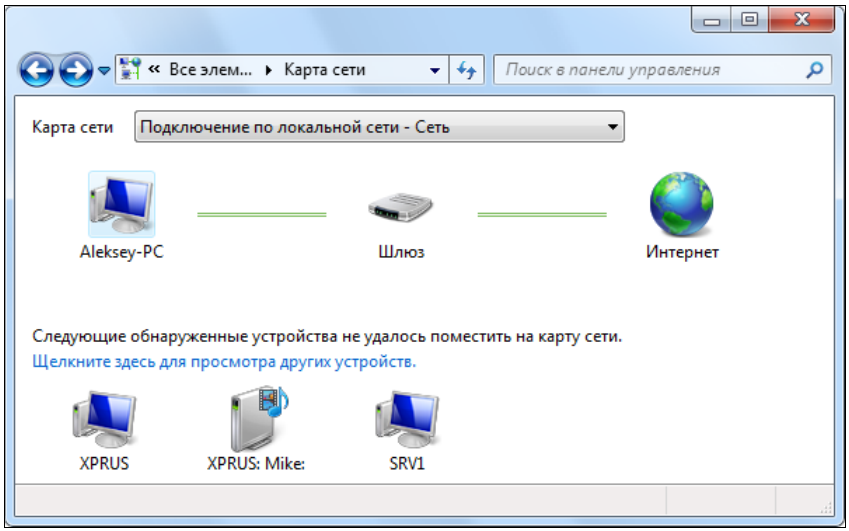

Рис. 1.12. Карта сети с нераспознанными компьютерами и устройствами

Если в сети имеются компьютеры и устройства, работающие под управлением Windows версий более ранних, чем Windows Vista, то при построении карты сети система Windows 7 не сможет отобразить на ней такие устройства (рис. 1.12) из-за

отсутствия специального сетевого компонента, который называется *"Ответчик обнаружения топологии канального уровня"* (Link Layer Topology Discovery (LLTD) responder) (его можно видеть в списке компонентов на рис. 1.17, *слева*).

При необходимости недостающий компонент для систем Windows XP Service Pack 2 можно загрузить с веб-сайта Microsoft; для других систем может потребоваться индивидуальный запрос к службе поддержки Microsoft. Чтобы найти ссылку на файл, на веб-сайте Microsoft выполните поиск статьи базы знаний с номером KB922120[1], где описана данная проблема. Полученный файл следует установить в системе, а затем включить указанный компонент.

Управление подключениями

Ссылка **Изменение параметров адаптера** (Change adapter settings) в левой части окна Центра управления сетями (см. рис. 1.7) позволяет открыть окно, обеспечивающее доступ ко *всем* подключениям, имеющимся в системе. (В это окно также можно попасть с помощью команды `ncpa.cpl`. Для упрощения доступа к окну можно создать ярлык с данной командой и поместить его, к примеру, на рабочий стол.) В окне сетевых подключений (рис. 1.13) видны их состояние и свойства[2]; здесь

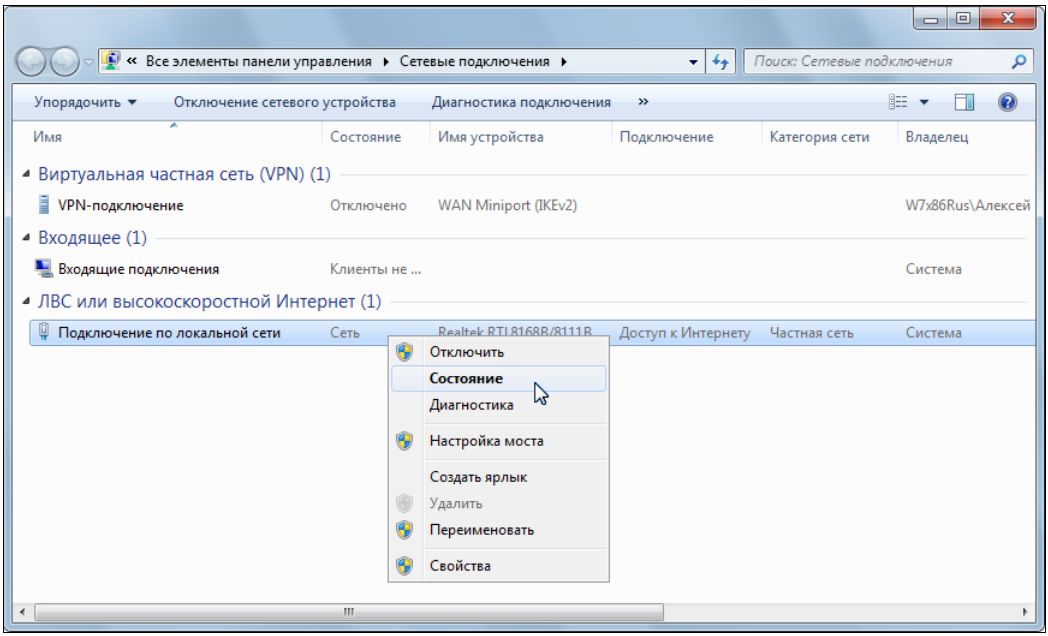

Рис. 1.13. Окно сетевых подключений в режиме просмотра "Таблица"

[1] При поиске достаточно просто ввести этот номер.

[2] Некоторые настройки доступны в специальном окне, которое открывается по команде **Дополнительно** | **Дополнительные параметры** (Advanced | Advanced Settings). Чтобы открыть меню в окне подключений, достаточно нажать клавишу <Alt>.

можно изменять имена подключений и выбирать наиболее удобный способ просмотра их параметров (с помощью команд **Вид** (View), **Сортировка** (Sort by) и **Группировка** (Group by) в контекстном меню). Также подключения можно активизировать (команда **Подключить** (Connect)) или разрывать (при наличии полномочий — обратите внимание на значки безопасности в виде щита!). По умолчанию подключения группируются по типу, поэтому легко ориентироваться в их назначении. Обычно для окна выбирается вид "Плитка" (Tiles), удобно также табличное представление, как показано на рисунке.

Просмотр состояния и параметров сетевых подключений

По ссылке, расположенной рядом с названием подключения (на рис. 1.7 это — **Подключение по локальной сети** (Local Area Connection)), можно попасть в типичное для всех версий Windows окно состояния сетевого подключения[1] (рис. 1.14). Здесь можно видеть следующие параметры: продолжительность и скорость подключения; число байтов, отправленных (Sent) и принятых (Received) во время активности подключения. Обратите внимание на то, что раздельно отображается состояние активности для протоколов IPv4 и IPv6. Для коммутируемых и VPN-подключений

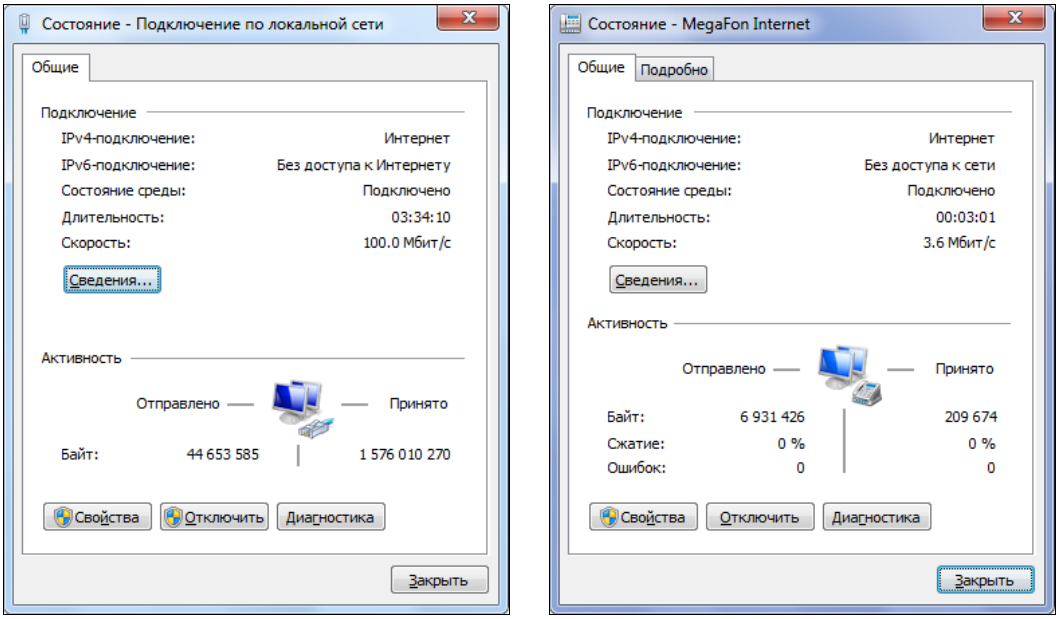

Рис. 1.14. Примеры окна состояния сетевого подключения (*справа* — для различных подключений по запросу)

[1] Также для этого можно просто дважды щелкнуть по названию *активного* соединения в окне сетевых подключений (см. рис. 1.13). Для неактивных подключений такой щелчок будет означать попытку установки соединения.

(рис. 1.14, *справа*) дополнительно указываются коэффициент сжатия (Compression) и количество ошибок (Errors), а на вкладке **Подробно** (Details) — имя порта, протоколы проверки подлинности, шифрования и сжатия.

Для беспроводного адаптера в окне состояния (рис. 1.15) также можно видеть идентификатор сети (SSID) и уровень качества сигнала. Кнопка **Свойства беспроводной сети** (Wireless Properties) позволяет открыть окно, где определяются параметры подключения и безопасности (см. рис. 3.14).

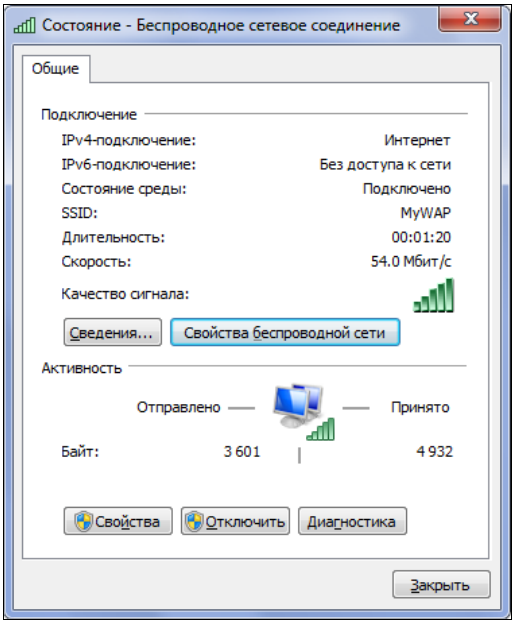

Рис. 1.15. Окно состояния беспроводного подключения

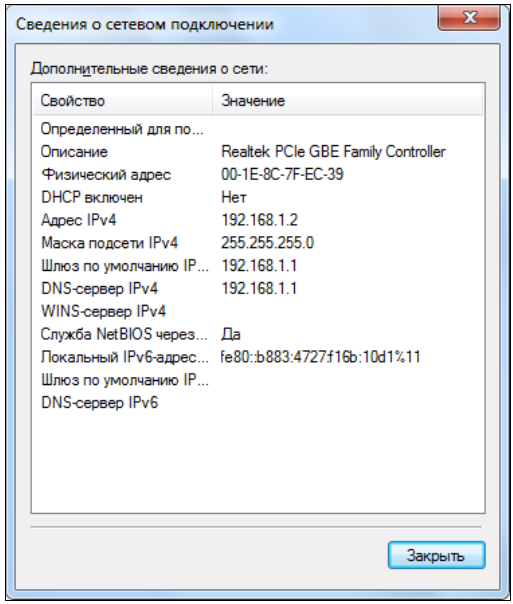

Рис. 1.16. Окно дополнительных сведений о сетевом подключении

Нажав кнопку **Сведения** (Details), можно увидеть дополнительные свойства сеанса связи (рис. 1.16): заданные адреса стека протоколов TCP/IP (IPv4 и IPv6); способ получения адресов (динамически, от DHCP, или статически[1]); наличие и тип шифрования; протокол аутентификации, а также другие параметры (они индивидуальны для каждого типа подключения). Все эти параметры особенно важны для анализа ситуации в случае ошибок подключения.

Нажав в окне состояния (см. рис. 1.14) кнопку **Диагностика** (Diagnose), подключение можно проверить и сделать попытку восстановления в случае неисправности (при этом запускается соответствующая программа-мастер), а кнопка **Свойства** (Properties) позволяет — при наличии административных полномочий — попасть в окно свойств подключения (рис. 1.17), в котором перечислены все параметры подключения — в частности, установленные протоколы и компоненты. (Обратите внимание на то, что по умолчанию установлен протокол TCP/IPv6.)

[1] Способы задания адресов и используемые значения подробно описаны в *главе 2*.

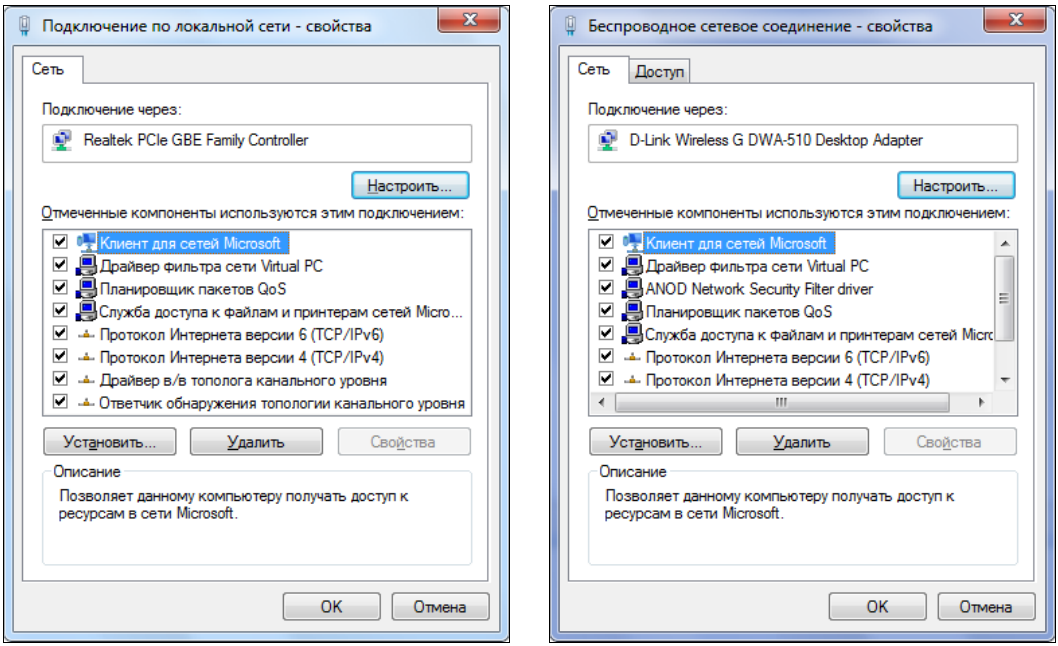

Рис. 1.17. Окно свойств подключения — подключение по локальной сети *(слева)* и беспроводное соединение *(справа)*

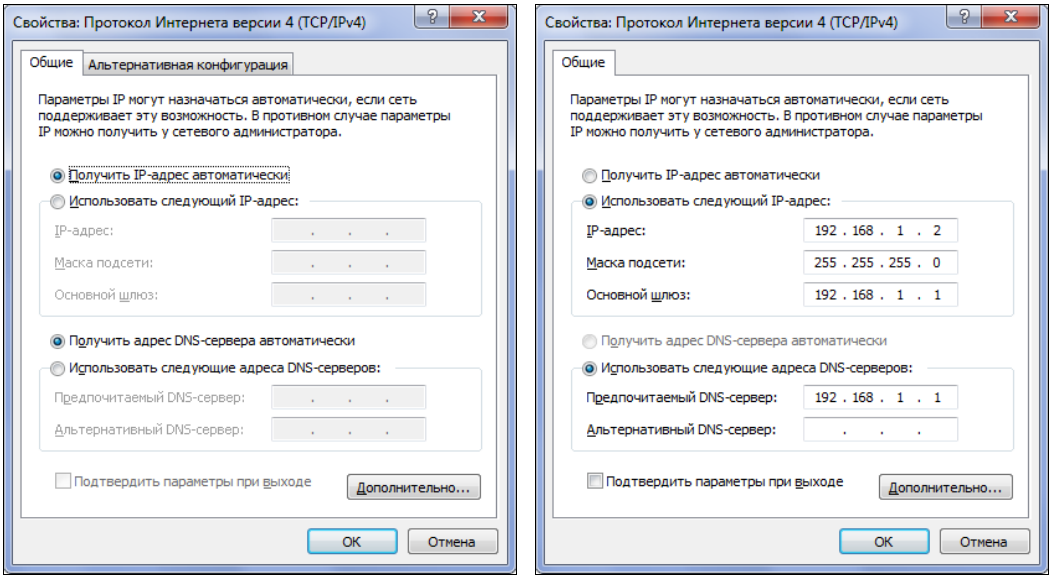

Рис. 1.18. Окно параметров протоколов TCP/IP — при автоматической настройке *(слева)* и в случае ручного определения параметров *(справа)*

В окне свойств подключения важнейшими являются параметры протоколов TCP/IP, которые по умолчанию получаются автоматически (от DHCP-сервера) (рис. 1.18, *слева*), но можно их задать и явно (рис. 1.18, *справа*). При работе в сети важно про-

верять основные параметры: IP-адрес компьютера и маску подсети, а также адреса предпочитаемого DNS-сервера и шлюза, если компьютер имеет выход во внешнюю сеть. Подробно выбор параметров для сетевых подключений рассматривается в *главе 2*.

В окне свойств коммутируемых и VPN-подключений имеются дополнительные вкладки[1] (рис. 1.19), поскольку для работы этих подключений требуется контролировать гораздо больше параметров, чем для подключения по локальной сети, имеющего единственную вкладку в окне свойств. Например, важнейшие параметры находятся на вкладке **Безопасность** (Security) — все настройки должны быть согласованы с VPN-сервером или сервером удаленного доступа (для коммутируемого подключения), иначе соединение установить не удастся.

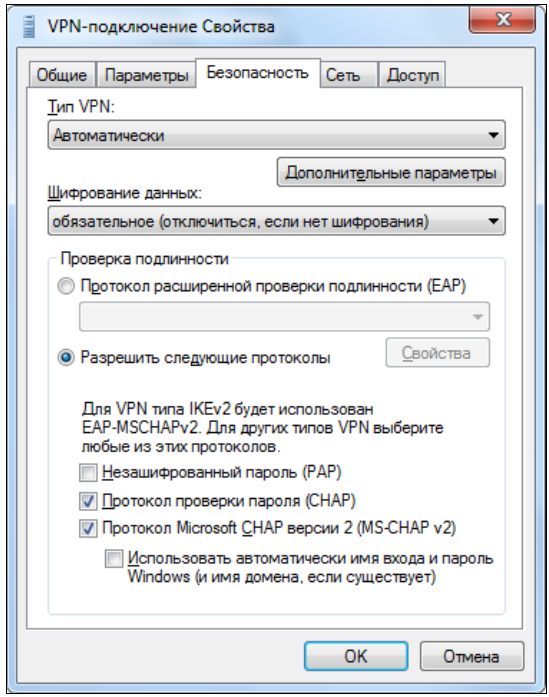

Рис. 1.19. Окно свойств подключения по локальной сети

Изменение имени компьютера и рабочей группы

Чтобы получить возможность изменить описание или имя компьютера, необходимо открыть окно свойств системы (см. рис. 1.20). Для этого проще всего ввести строку `sysdm.cpl` в меню **Пуск** (Start), в окне консоли или в окне **Выполнить** (Run). Или

[1] Подробно они описаны в *главе 2*.

же откройте окно системы Windows 7, нажав клавиши <Win>+<Pause/Break>, и щелкните по ссылке **Дополнительные параметры системы** (Advanced System Settings).

На вкладке **Имя компьютера** (Computer Name) (рис. 1.20) указывается описание компьютера, которое могут видеть клиенты сети, работающие в системах ***ниже*** Windows Vista (начиная с Windows Vista, описание компьютера в папке **Сеть** (Network) ***не отображается***[1]!). Кнопка **Изменить** (Change) на вкладке описания компьютера позволяет открыть окно (рис. 1.20), где задано имя компьютера. Это имя можно изменить; после этого потребуется перезагрузка системы.

Все компьютеры по умолчанию принадлежат к рабочей группе WORKGROUP, которая задается при установке системы. Для систем Windows 7 имя группы и принадлежность к домену можно задавать только после инсталляции (если не использовать автоматическую установку). В указанном окне имя группы можно изменить, после чего требуется перезагрузить компьютер.

Совет

Не рекомендуется *одновременно* менять имя компьютера и подключать его к рабочей группе или домену (или отключать). Это может привести к путанице с именами.

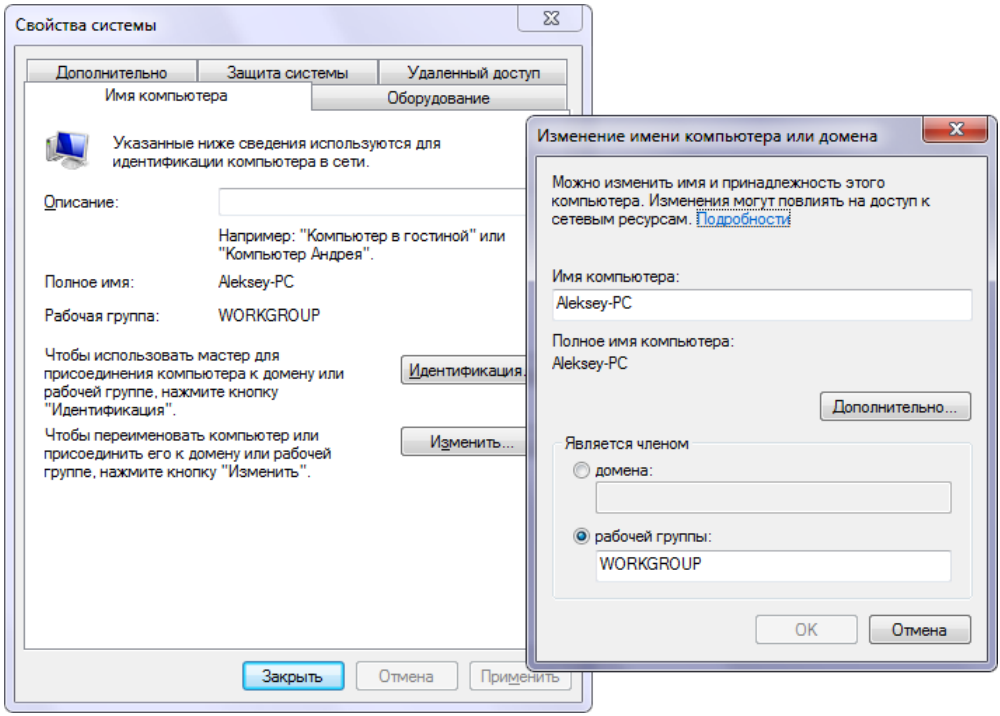

Рис. 1.20. Окно выбора имени компьютера и домена или локальной группы

[1] Эта функция признана устаревшей, и путей исправления ситуации не существует. При необходимости следует создавать пользователям ярлыки для доступа к конкретным ресурсам, а просмотр (browsing) сетевого окружения не приветствуется.

Настройка компьютеров домашней группы

Удобная функция, появившаяся в системах Windows 7, позволяет с минимальными административными затратами обеспечить совместный доступ к файлам, принадлежащим пользователям сети. Компьютеры, расположенные в небольшой локальной сети, можно объединить в *домашнюю группу* (HomeGroup). Для этого должны обязательно соблюдаться два требования:

- на компьютерах ***должен быть включен протокол IPv6***;
- для используемого сетевого подключения должно быть ***установлено размещение "Домашняя сеть"*** (Home network) (см. рис. 1.7).

Если в сети имеется маршрутизатор(ы) (особенно это относится к беспроводным сетям!), то появляется третье требование:

- убедитесь в том, что ***маршрутизатор обеспечивает передачу протокола IPv6***.

> ***Внимание!***
>
> Не следует путать не имеющую имени *домашнюю* группу (HomeGroup), в которую можно объединить только системы Windows 7 (любых редакций) и которая может быть только одна в сети, и обычные *рабочие* группы (workgroup), имена которых задаются достаточно произвольно и которые могут объединять в сети компьютеры с разными версиями Windows.
>
> Перед тем как планировать развертывание домашней группы, познакомьтесь со всеми особенностями использования нескольких сетевых подключений, подробно рассмотренными в *разд. "Подключение и настройка ADSL-модема" главы 2* (эти соображения справедливы и при работе с другими устройствами!). Оптимальным (а иногда и единственным) вариантом подключения компьютеров домашней группы к Интернету является использование аппаратного маршрутизатора (см. пример на рис. 3.2), общее подключение к Интернету нельзя будет использовать.

При использовании домашней группы упрощается настройка доступа к общим ресурсам (при этом общие папки для отдельных личных библиотек пользователя не создаются[1] — это можно проверить с помощью команды `net share`) — достаточно лишь, чтобы на компьютерах были созданы учетные записи с одинаковыми именами и паролями.

> ***Примечание***
>
> Создавать домашнюю группу и подключать к ней компьютеры (а также отключать) может любой локальный пользователь, даже без административных прав[2].

---

[1] Только при разрешении использования *локального принтера* автоматически включается общий доступ к устройству печати (это подтверждает команда `net share`), и он становится видным в сетевом окружении.

[2] Нам это кажется довольно странным: получается, что рядовой пользователь может не только менять права доступа к своим папкам, но и влиять на глобальные параметры — отключать доступ к папкам других пользователей (в случае выхода компьютера из домашней группы).

Внимание!

Домашнюю группу нельзя *создать* на компьютерах, работающих под управлением редакции Windows 7 Домашняя Базовая (Home Basic), эти компьютеры можно только *подключать* к существующей домашней группе. Для ее создания необходимы более старшие редакции Windows 7.

Создание группы

По умолчанию при установке Windows 7 первый компьютер в сети автоматически *включается* в создаваемую домашнюю группу.

Если система в процессе установки обнаруживает в сети уже существующую домашнюю группу[1], то она предлагает *включить компьютер в эту группу* и разрешить совместное использование некоторых личных папок и принтеров (рис. 1.21). Для этого следует отметить нужные папки и ввести пароль домашней группы, по-

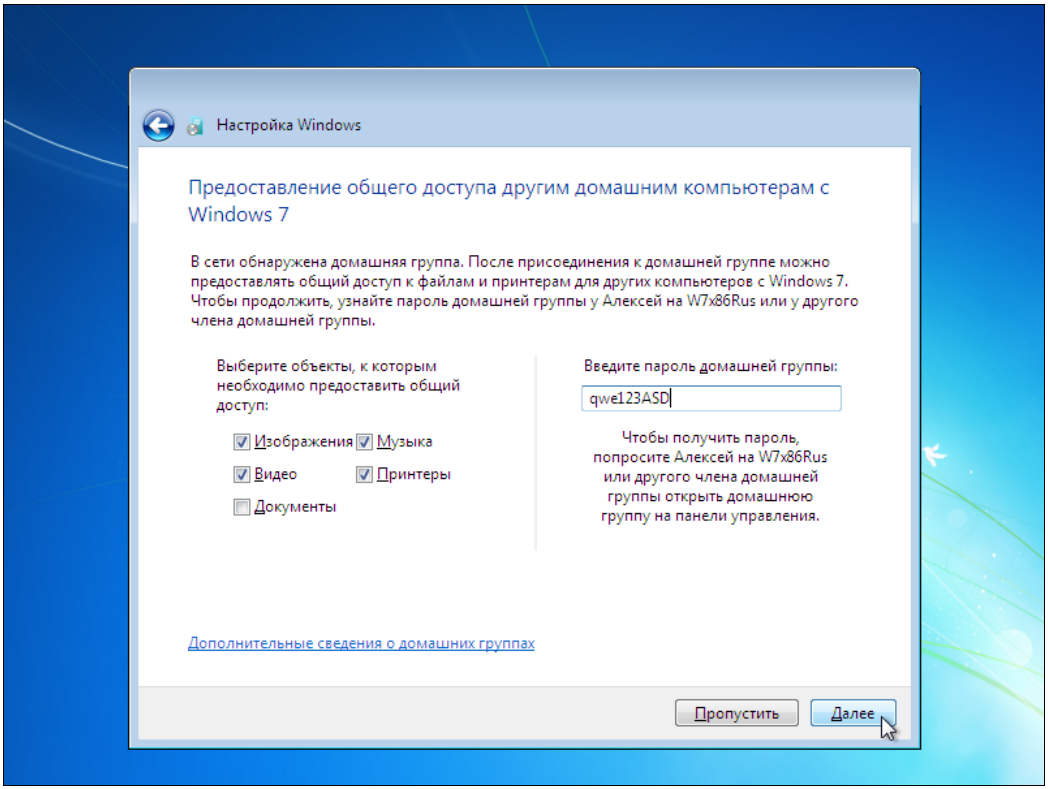

Рис. 1.21. Подключение к домашней группе и выбор личных папок, к которым будет разрешен общий доступ, при установке операционной системы

[1] Следует иметь в виду, что сетевые компоненты изначально устанавливаются на автоматическое получение параметров, поэтому IP-адреса для компьютера могут быть уже определены — например получены от маршрутизатора

лученный от участников этой группы (для имеющейся группы пароль легко получить в окне **Домашняя группа** (Homegroup) — см. ссылку **Показать или распечатать пароль домашней группы** (View or print the homegroup password) на рис. 1.22). Можно отказаться от операции, нажав кнопку **Пропустить** (Skip), и при необходимости подключиться к домашней группе позднее *(см. далее)*.

Если домашняя группа вообще отсутствует в сети, то ее можно *создать* на любом компьютере, работающем под управлением Windows 7. Для этого в окне сетевого центра (см. рис. 1.7) выберите ссылку **Выбор домашней сети и параметров общего доступа** (Choose homegroup and sharing options) или же ссылку **Готовность к созданию** (Ready to create) и в окне **Домашняя группа** (HomeGroup) нажмите кнопку **Создать домашнюю группу** (Create a homegroup). При этом нужно выделить ресурсы для общего пользования (см. рис. 1.21) и сохранить (записать или распечатать) пароль домашней группы, который затем потребуется раздать всем новым участникам этой группы. В этом случае на других компьютерах можно будет только *подключаться* к имеющейся сети.

> ***Внимание!***
>
> При подключении компьютера к домену Active Directory или при выборе сетевого размещения *Общественная сеть* (Public network) функция домашней группы отключается, а при отключении от домена или при включении в *Домашнюю сеть* (Home network) все возможности автоматически восстанавливаются, и компьютер снова может работать в домашней группе.

Подключение к существующей группе

Подключиться к домашней группе можно в любой момент, выбрав для этого в окне Центра управления сетями (Network and Sharing Center) (см. рис. 1.7) ссылку **Выбор домашней сети и параметров общего доступа** (Choose homegroup and sharing options) или ссылку **Может присоединиться** (Available to join) и нажав кнопку **Присоединиться** (Join now) в открывшемся окне. Затем следует указать, какие именно локальные библиотеки текущего пользователя будут доступны для других участников домашней группы (см. рис. 1.21), после чего потребуется ввести пароль домашней группы.

В результате выполненных операций пользователь сможет в окне программы Проводник (Windows Explorer) увидеть предоставленные в общее пользование библиотеки — все ресурсы отображаются внутри папки **Домашняя группа** (Homegroup) (рис. 1.6).

Изменение параметров домашней группы

Участник домашней группы может видеть текущие параметры и опции, связанные с управлением группы, в специальном окне **Домашняя группа** (HomeGroup) (рис. 1.22). В первую очередь, здесь указываются личные библиотеки и принтеры, к которым сам пользователь может разрешить общий доступ. (Возможности использования библиотек мультимедиа рассматриваются в *главе 6*.) Соответствующие команды позволяют увидеть или изменить пароль домашней группы, выйти из

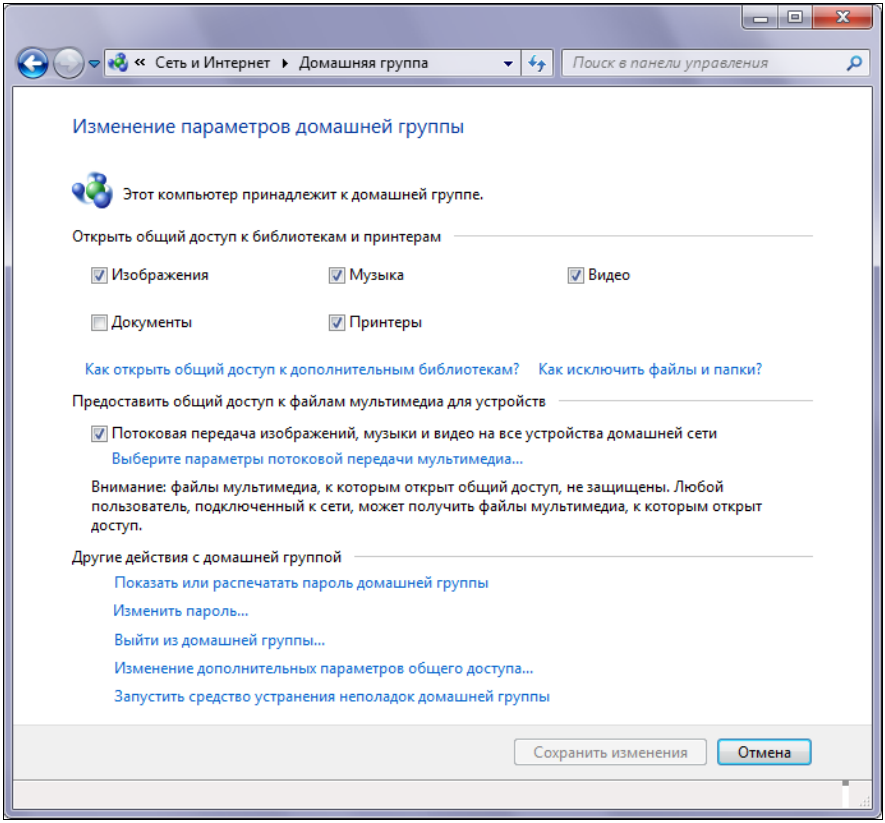

Рис. 1.22. Окно параметров домашней группы

группы[1], изменить параметры доступа (перейти в окно, показанное на рис. 1.23) и запустить мастер устранения неполадок.

Устранение неисправностей

В случае появления ошибок в работе домашней группы (например, при отсутствии доступа к локальным или удаленным папкам, невидимости других компьютеров домашней группы и т. п.) может помочь мастер устранения неполадок, запускаемый непосредственно из папки **Домашняя группа** (HomeGroup) (см. рис. 1.6) в окне Проводника или из окна **Домашняя группа** (HomeGroup) *(см. выше)*. Этот мастер позволяет диагностировать проблемы конфигурации (включая сетевые параметры) и устранить простые ошибки.

Если мастер устранения неполадок не может справиться с проблемой, то рекомендуются следующие процедуры:

1. Выведите компьютер из домашней группы и подключите снова. Эту операцию можно поочередно выполнить с каждым компьютером, входящим в группу. Па-

[1] В этом случае в данном окне появятся кнопки создания домашней группы или подключения к существующей.

роль группы при этом не меняется (он сохраняется на компьютере, остающемся в группе).

2. Если ошибки не устранены, то выведите из домашней группы *все* компьютеры и создайте группу заново на любом компьютере. Затем подключите остальные компьютеры. Как правило, этот вариант помогает даже в самых тяжелых случаях (если домашняя группа хотя бы раз была создана и сетевые параметры существенно не менялись).

> ***Внимание!***
> Как показывает практика, функция домашней группы "не любит" изменений имен компьютеров, да и вообще — любых изменений в сетевой конфигурации. Поэтому лучше включать эту функцию тогда, когда все настройки уже будут выбраны. В крайнем случае, для восстановления работоспособности группы всегда помогает операция ее создания "с нуля".

Настройка сетевого доступа к общим папкам и принтерам

Для того чтобы пользователи других компьютеров могли обращаться к общим ресурсам (папкам и принтерам) данного компьютера, необходимо не только предоставить им права доступа, но и разрешить в брандмауэре Windows соответствующие порты стека протоколов TCP/IP.

Необходимые для работы сетевые параметры и настройки безопасности проще всего выбрать, используя возможности Центра управления сетями и общим доступом (Network and Sharing Center) (см. рис. 1.7). Ссылка **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) в левой части его главного окна позволяет перейти в окно многочисленных настроек элементов, определяющих возможности удаленных пользователей при обращении к ресурсам компьютера (рис. 1.23) (все переключатели даже невозможно показать на одном рисунке!). Если активно только одно сетевое подключение, то по умолчанию в окне раскрывается профиль, используемый в данный момент (текущий профиль). Далее объясняется назначение имеющихся параметров.

В группе **Сетевое обнаружение** (Network discovery) находятся переключатели, фактически разрешающие или запрещающие просмотр папки **Сеть** (Network) в окне Проводника. Если обнаружение отключено, то в этой папке ничего не отображается (см. рис. 1.3), а сам компьютер не виден никому в сети (команды ping с адресом этого компьютера тоже не проходят). Это распространяется и на компьютеры, входящие в домашнюю группу.

Переключатели в группе **Общий доступ к файлам и принтерам** (File and printer sharing) позволяют разрешить или запретить доступ на "глобальном" уровне. Если доступ запрещен, то остальные параметры уже не действуют (на домашнюю группу этот запрет тоже распространяется). В *Общественной сети* (Public network) по умолчанию запрещено и сетевое обнаружение, и общий доступ. В *Домашней сети*

(Home network) разрешено сетевое обнаружение и общий доступ с парольной защитой *(см. ниже)*.

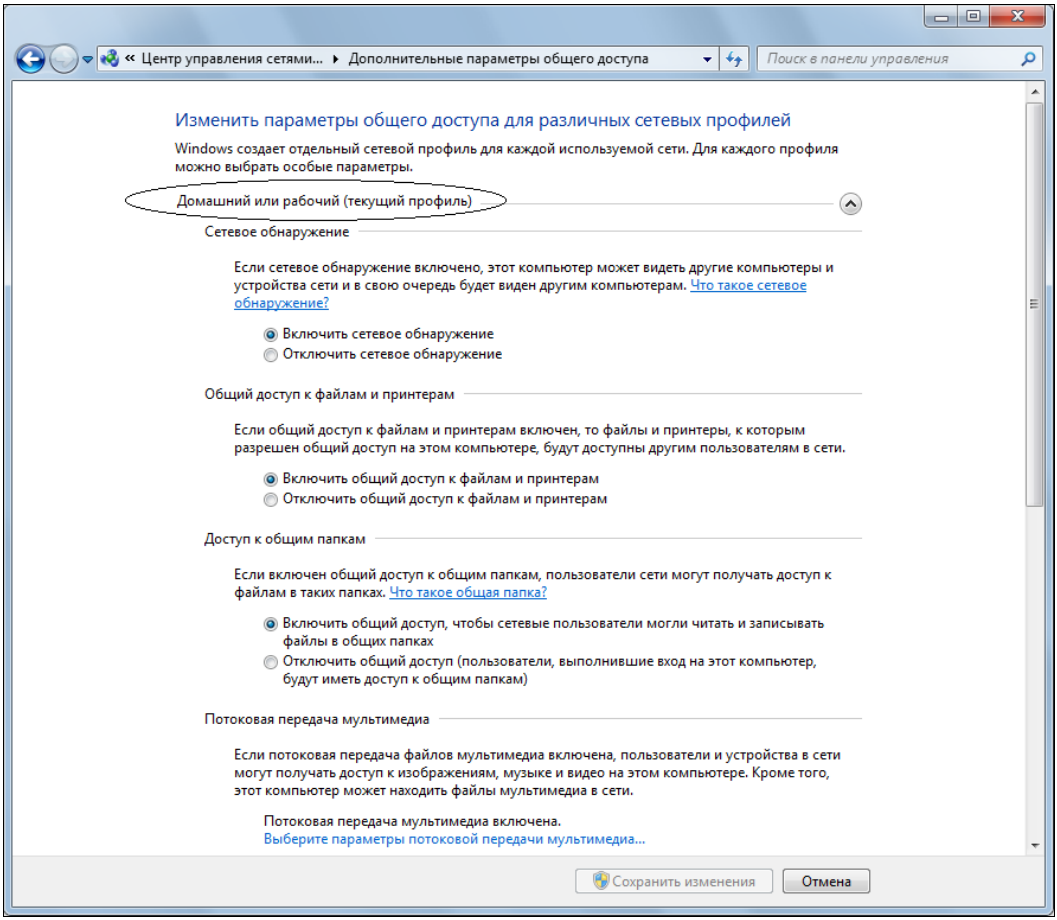

Рис. 1.23. Параметры доступа к общим ресурсам

Если для *Общественной сети* (Public network) включается обнаружение сети и общий доступ, то система предлагает подтвердить эту операцию или поменять сетевое размещение и сделать сеть частной (рабочей[1], размещение *Рабочая сеть* (Work network)) (это опция по умолчанию) (рис. 1.24). В таких случаях рекомендуется менять именно тип сети, но не понижать уровень безопасности для всех общественных сетей.

Переключатели в группе **Доступ к общим папкам** (Public folder sharing) разрешают доступ к папке **Общие** (Public) (см. рис. 5.5). Их состояние никак не влияет на папки, доступ к которым разрешен вручную *(см. главу 5)*.

[1] К большому сожалению, здесь отсутствует опция *Домашняя сеть* (Home network).

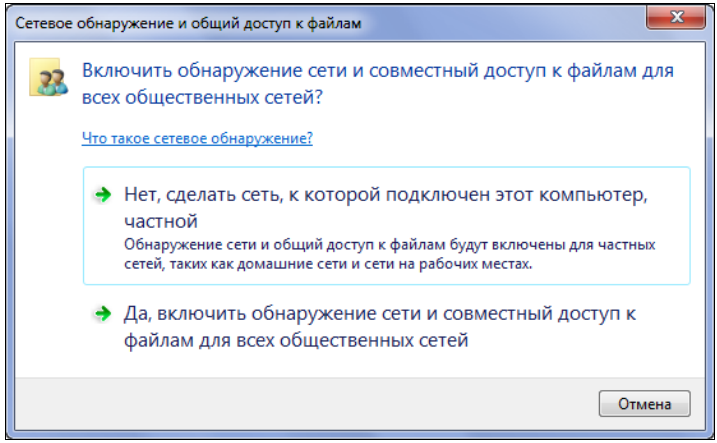

Рис. 1.24. Запрос на изменение параметров сетевого профиля или изменение сетевого размещения

Параметры потоковой передачи мультимедиа рассматриваются подробно в *главе 6*. Вопросы выбора уровня шифрования для защиты подключений общего доступа и связанные с этим групповые политики рассмотрены в конце *главы 4*.

Переключатели в группе **Общий доступ с парольной защитой** (Password protected sharing) определяют необходимость использования паролей: при отключении парольной защиты доступ получают *любые* пользователи (поскольку разблокируется учетная запись Гость (Guest) — это легко проверить с помощью оснастки **Управление компьютером** (Computer Management), узел **Локальные пользователи и группы** (Local Users and Groups)).

По умолчанию операционная система сама управляет параметрами доступа для участников домашней группы (это последняя опция в окне дополнительных параметров), используя для этого встроенную учетную запись пользователя *HomeGroupUser$* и учетную запись группы *HomeUsers*. При использовании другой опции для доступа к другим компьютерам домашней группы нужно будет явно указывать имя пользователя и пароль.

> ***Внимание!***
>
> Параметры общего доступа устанавливаются индивидуально для каждого сетевого профиля: домашнего, доменного и общего. Поэтому нужно следить за текущим сетевым размещением и выбирать настройки, соответствующие ситуации (при работе в домашней сети или в общедоступном месте).

Мониторинг сетевых подключений

В процессе работы может возникнуть необходимость в анализе сетевой активности компьютера: например, для определения объема сетевого трафика или загруженности подключений, для обнаружения программ или процессов, вообще обращающихся к сети или создающих большую нагрузку на сеть, и т. п. Далее рассматрива-

ются два основных стандартных инструмента Windows 7, всегда находящихся под рукой и позволяющих легко решить перечисленные задачи[1].

Диспетчер задач

В системах Windows главным "подручным" средством мониторинга ключевых показателей производительности компьютера является *Диспетчер задач* (Task Manager; taskmgr.exe). Для его запуска имеются различные способы.

- Щелкните правой кнопкой мыши по панели задач и выберите в контекстном меню пункт **Диспетчер задач** (Task Manager).
- Нажмите клавиши <Ctrl>+<Shift>+<Esc>.
- Нажмите клавиши <Ctrl>+<Alt>+<Del> и в окне безопасности нажмите кнопку **Запустить диспетчер задач** (Start Task Manager).
- Откройте окно **Выполнить** (Run) и введите команду `taskmgr`; эту команду можно задать и непосредственно в поле поиска меню **Пуск** (Start).

Если диспетчер задач запущен, то в правом нижнем углу экрана на панели задач в области уведомлений появляется индикатор загрузки процессора  . Если подвести указатель мыши к этому индикатору, то показывается степень загруженности процессора в процентах от максимума. Теперь свернутое окно диспетчера задач можно открывать, дважды щелкая мышью по данному значку.

В окне диспетчера задач на вкладке **Сеть** (Networking) (см. рис. 1.25) можно в виде графика увидеть степень загрузки активных сетевых подключений в данный момент и на протяжении некоторого уже прошедшего времени, а также оценить объем информации, переданной по каждому подключению. Если на компьютере установлены несколько сетевых адаптеров, то для каждого адаптера отображается отдельная панель, где цветными линиями представлена загрузка этого адаптера. По умолчанию желтый график соответствует принятой информации, а красный — переданной.

С помощью команды **Вид | Выбрать столбцы** (View | Select Columns) можно перейти в окно отображаемых столбцов и добавить к таблице, к примеру, вывод числа *полученных* (Bytes Received) и/или *отправленных байтов* (Bytes Sent) для всех сетевых адаптеров (см. рис. 1.25).

В нашем примере (рис. 1.25) представлены три типа подключений. *Беспроводные* и *Bluetooth* соединения всегда представлены в окне, даже если и нет подключения к удаленной сети, устройству или компьютеру. Панель подключения *по локальной сети* также присутствует всегда, поскольку это соединение фактически постоянно и обычно не отключается[2]. Для *коммутируемого* подключения (в нашем случае ис-

---

[1] Для еще более подробного и точного анализа можно использовать счетчики производительности системы и оснастку **Системный монитор** (Performance Monitor, perfmon.msc).

[2] Если беспроводное, Bluetooth или локальное подключение включено, но не активно (соответственно — нет подключения к беспроводной сети или устройству или же отсоединен сетевой кабель), то панель для такого подключения все равно отображается в окне диспетчера заданий (или монитора ресурсов — *см. далее*), однако состояние таких подключений — "Соединение прервано" (Disconnected) (см. рис. 1.11).

пользуется USB-модем стандарта 3G) можно видеть максимальную скорость канала и его загруженность (нижняя панель).

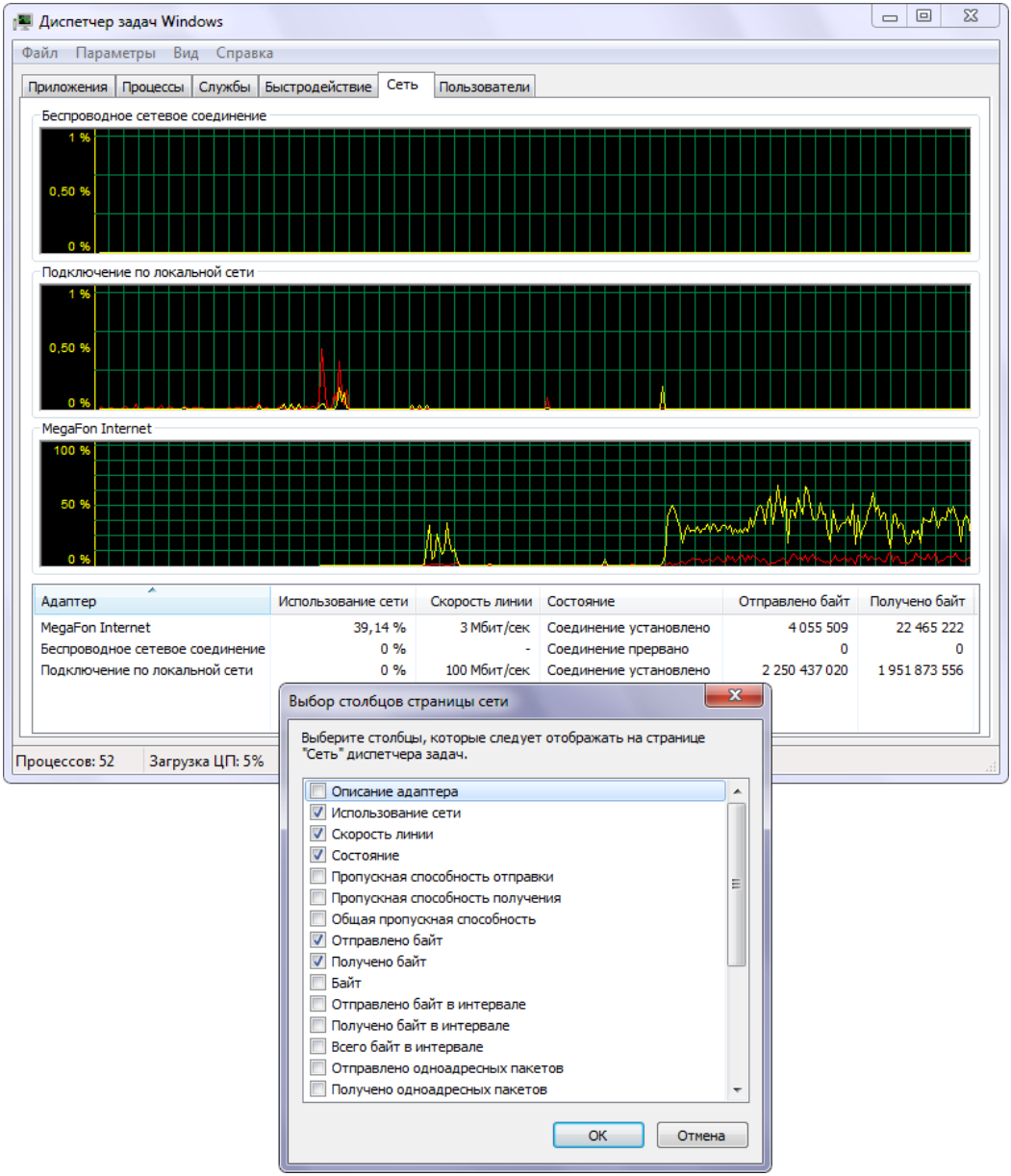

Рис. 1.25. Отображение загруженности сетевого адаптера

Команда **Вид | Журнал сетевого адаптера** (View | Network Adapter History) позволяет отдельно отображать на графике число полученных (**Получено байт** (Bytes Received)) и/или отправленных байтов (**Отправлено байт** (Bytes Sent)). Также можно включить график (зеленого цвета), соответствующий общему числу пере-

данных байтов. При необходимости можно добавить столбцы, в которых будет отображаться общее количество переданных байт за некоторый временной интервал, причем если установить флажок **Параметры | Отображать накапливаемые данные** (Options | Show Cumulative Data), то будут учитываться не только те данные, которые были получены после запуска диспетчера задач, но и суммарные — с момента загрузки системы. Например, для адаптера, через который осуществляется подключение к Интернету или внешней сети, на вкладке **Сеть** (Networking) можно весьма точно оценить сетевой трафик.

Если флажок **Параметры | Отображать накапливаемые данные** (Options | Show Cumulative Data) не установлен, то по команде **Параметры | Сброс** (Options | Reset) можно сбросить в 0 все отображаемые показания и начать сбор данных заново, с определенного момента времени.

По умолчанию графики загрузки подключений появляются на вкладке **Сеть** (Networking) *с момента выбора этой вкладки*, и предыдущие показания видеть нельзя. Если в меню **Параметры** (Options) установить флажок **Вкладка всегда активна** (Tab Always Active), то информация об использовании сети начинает собираться сразу же *после запуска диспетчера задач*, даже если вкладка **Сеть** (Networking) и не открывалась. В этом случае после выбора вкладки можно в виде графика видеть уже накопленные данные.

Монитор ресурсов

Новый компонент систем Windows 7 — *Монитор ресурсов*[1] (Resource Monitor, `resmon.exe`) позволяет в реальном времени видеть, как используются процессор, диск, сеть и оперативная память. Монитор ресурсов можно запустить, нажав одноименную кнопку в окне диспетчера задач на вкладке **Быстродействие** (Performance) или выбрав соответствующую команду в подменю **Пуск | Все программы | Стандартные | Служебные** (Start | All programs | Accessories | System Tools). (Также для запуска из меню **Пуск** (Start) или командной строки можно использовать команду `perfmon /res` или просто имя файла программы.)

> ***Внимание!***
> Для запуска монитора ресурсов требуются права администратора.

На рис. 1.26 показана вкладка **Сеть** (Network), где перечисляются все процессы, обращающиеся в данный момент к сети по всем сетевым подключениям (в данном примере активно только подключение по локальной сети, но на этой панели могут быть диаграммы и для других соединений). Это уже весьма информативно само по себе, поскольку сразу можно увидеть "подозрительные" процессы или процессы, создающие значительный трафик. Включив фильтрацию (установив на верхней панели флажки для представляющих интерес процессов), легко получить более подробную информацию: например, сведения о том, куда именно обращается про-

[1] Одноименный компонент имеется и в Windows Vista, но там он имеет на порядок меньше возможностей.

грамма, какие порты использует и как быстро она получает ответы. Таким образом, можно, что называется "до последнего байта", контролировать сетевую активность компьютера.

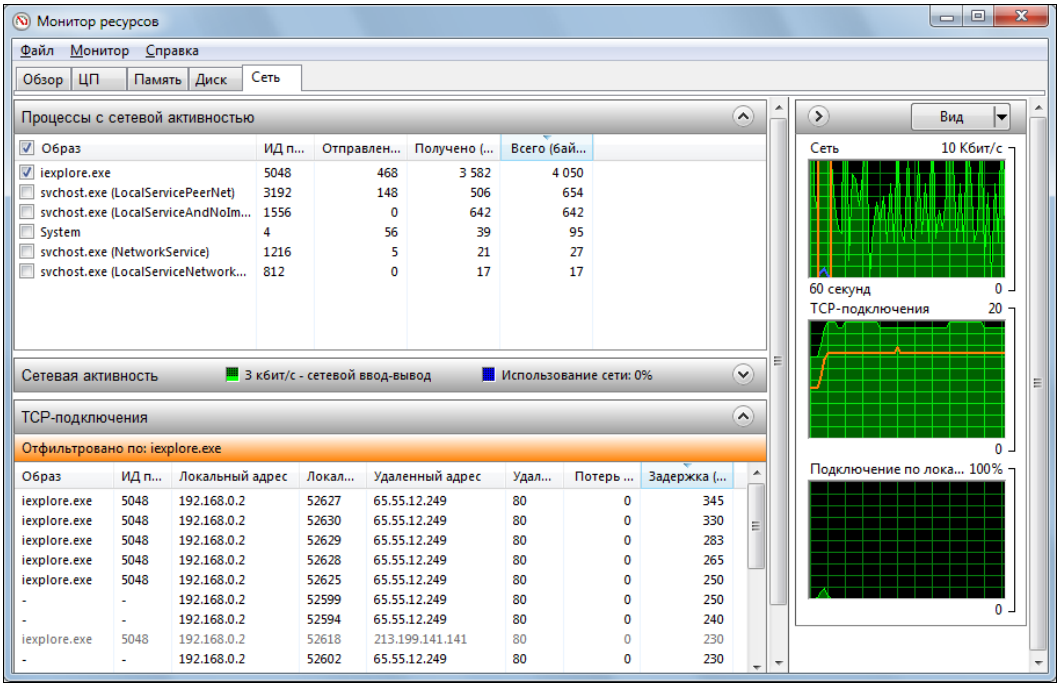

Рис. 1.26. Список сервисов и приложений с сетевой активностью и подробная информация по выбранной программе (Internet Explorer, iexplorer.exe)

Для панели **TCP-подключения** (TCP Connections) помимо стандартных столбцов (показанных на рис. 1.26), можно выбирать и дополнительные (как в диспетчере задач). Например, можно включить индивидуальное отображение количества переданной информации за секунду для *каждого* TCP-подключения.

ГЛАВА 2

Создание и конфигурирование сетевых подключений

Для того чтобы использовать компьютер в сетевой среде, необходимо создать и настроить сетевое подключение (одно или несколько), соответствующее поставленным задачам, типу сети или используемым сетевым устройствам. Все эти вопросы подробно рассматриваются в данной главе, и, кроме того, рассказывается о совместном использовании подключения к Интернету всеми клиентами локальной сети.

Различные типы *беспроводных* соединений рассматриваются отдельно, в *главе 3*. Однако все принципы настройки нескольких подключений и разрешение общего доступа к интернет-подключению, которые описаны в последней трети данной главы, распространяются полностью и на беспроводные подключения. Поэтому с соответствующими разделами главы следует обязательно ознакомиться, даже если вы и не используете кабельную сеть, ADSL-модем или другие подобные устройства.

Типы подключений

Для создания нового подключения в окне Центра управления сетями и общим доступом (Network and Sharing Center) (см. рис. 1.7) используется ссылка **Настройка нового подключения или сети** (Set up a connection or network). С ее помощью запускается мастер создания подключений, позволяющий в интерактивном режиме легко сконфигурировать подключение любого типа — нужно лишь выбрать соответствующую опцию в первом окне мастера[1] (рис. 2.1) и ответить на последующие запросы (каждый вариант будет рассматриваться подробнее далее, а беспроводным подключениям любых типов полностью посвящена *глава 3*). Определенную специфику имеют только операция разрешения входящих подключений *(см. далее)*, а также работа с Bluetooth-устройствами и ИК-портами (IrDA).

В системах Windows 7 поддерживаются сетевые подключения практически любых типов — все они перечислены в табл. 2.1. (Bluetooth-подключения и связь через

[1] Для наглядности это окно как бы "растянуто" по вертикали, чтобы в нем поместились *все* имеющиеся опции без прокрутки окна. Варианты для беспроводных сетей или Bluetooth-устройств появляются в нем только при наличии соответствующих включенных адаптеров.

ИК-порты выделены в отдельную группу потому, что для взаимодействия с подобными устройствами имеется специальный пользовательский интерфейс, причем для каждого типа свой — *см. главу 3*.)

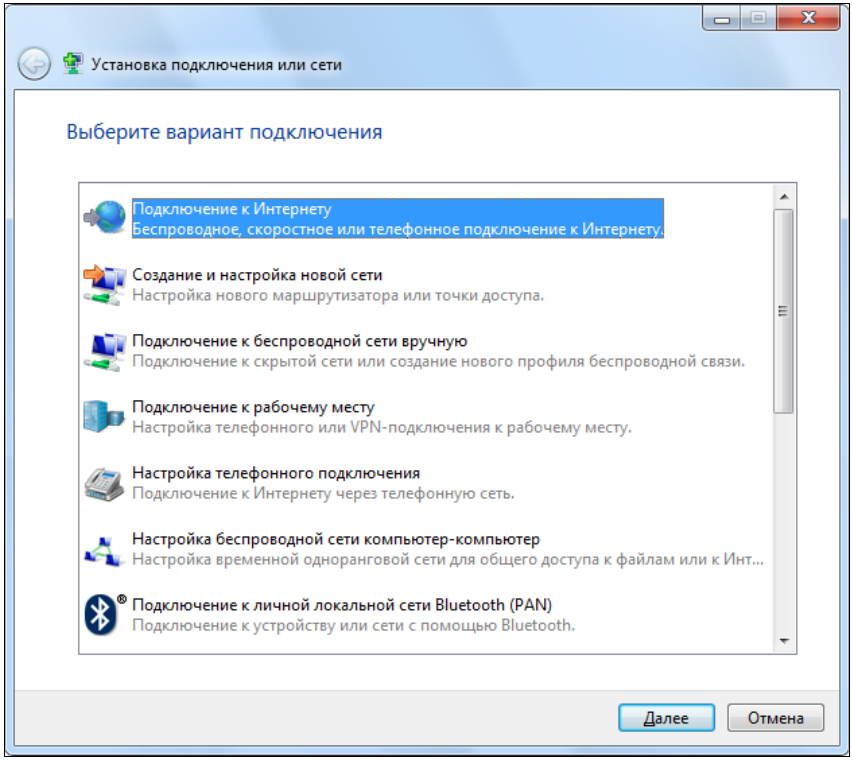

Рис. 2.1. Выбор типа создаваемого сетевого подключения

Таблица 2.1. *Типы сетевых подключений в Windows 7*

Тип подключения	**Технология связи и устройства**	**Пример**
Подключение по локальной сети (Local Area Connection)	Сети Ethernet, кабельные и ADSL-модемы, оптоволокно, каналы E1/T1 и т. п.	Обычное подключение к высокоскоростной сети (локальной сети или выделенному каналу)
Телефонное (коммутируемое) подключение (Dial-up connection)	Телефонные модемы, ISDN-и ADSL-модемы, USB-модемы стандартов GSM/GPRS/EDGE, CDMA, WiMAX и др.[1]	Соединение с корпоративной сетью или Интернетом с использованием коммутируемого телефонного подключения и обычного модема; ADSL-модемы также могут работать с данным типом подключений (по протоколу PPPoE)

[1] Нередко поставщики и операторы связи указывают тип модема обобщенно, например, "3G-модем" (добавляя при этом конкретные протоколы, используемые для связи).

Таблица 2.1 *(окончание)*

Тип подключения	Технология связи и устройства	Пример
VPN-подключение (Virtual Private Network)	Виртуальные частные сети (VPN) с использованием протоколов PPTP, L2TP/IPSec, SSTP и IKEv2	Безопасное соединение компьютера с корпоративной сетью через Интернет или другую сеть общего пользования (public network)
Беспроводное подключение (Wireless Connection)	Wi-Fi сети (стандарт IEEE 802.11, модификации a, b, g, n)	Подключение мобильного компьютера к локальной сети или общедоступной точке доступа (хот-споту). Временное соединение двух компьютеров или компьютера и электронного устройства (медиаплеера, принтера и т. д.)
Bluetooth-подключения, связь по инфракрасному каналу (IrDA)	Устройства, отвечающие спецификации Bluetooth; ИК-порты[1]	Временное соединение между компьютером и мобильным телефоном, КПК, принтером, фотоаппаратом и другими бытовыми электронными устройствами
Входящие подключения (Incoming connection)*	Коммутируемый модем, VPN- или прямое подключение	Подключение к компьютеру с использованием коммутируемой линии (модема) или VPN-канала от удаленных клиентов

* При разрешении входящих подключений в окне подключений (см. рис. 1.13) всегда имеется только один значок (одна строка таблицы): тип разрешенных входящих подключений — с использованием модема и/или VPN-канала — указывается в свойствах этого значка.

Прямые подключения

Прямые подключения (Direct Connection) выполняются путем физического соединения одного компьютера с другим через последовательный кабель, специальный USB-кабель[2], кабель прямого параллельного подключения (DirectParallel) и т. д. Мы не будем отдельно рассматривать такие подключения, поскольку они уже практически не используются и им на смену пришли другие технологии соединения "точка-точка", такие как Bluetooth или связь через ИК-порт (IrDA) *(см. главу 3)*.

Кроме того, два компьютера очень легко можно соединить друг с другом через LAN-порты (Ethernet) с помощью специального кросс-кабеля (кабель, у которого входные линии одного разъема "перекрещены" и замкнуты на выходные другого разъема) или, даже, *обычного* кабеля (патч-корда), используемого для подключения компьютеров

[1] Инфракрасный порт (стандарт Infrared Data Association, IrDA).

[2] Это особый кабель для прямого соединения компьютеров; обычные кабели-удлинители USB применять нельзя! Такой кабель, к примеру, может использоваться стандартной утилитой "Средство переноса данных Windows" (Windows Easy Transfer) при переносе настроек и файлов с одного компьютера на другой при переустановке операционной системы.

к коммутаторам и маршрутизаторам[1]. В этом случае адаптеры нужно настроить на автоматическую настройку или дать им статические адреса и маску из одной подсети; потом стандартным образом следует включить сетевое обнаружение для "неопознанной сети" (см. рис. 1.3).

Подключение по локальной сети

При инсталляции операционная система автоматически обнаруживает сетевой адаптер Ethernet, устанавливает соответствующий драйвер и создает *подключение по локальной сети* (Local Area Connection) для данного адаптера (одна плата — одно подключение). Это подключение сразу отображается (как и любые другие, созданные уже пользователем) в окне сетевых подключений (см. рис. 1.13).

По умолчанию локальное подключение всегда включено и активно, если сетевой кабель подключен к концентратору/коммутатору (хабу) или маршрутизатору; это единственный тип подключений, который автоматически становится активным после запуска компьютера. (Также сразу же могут становиться активными и беспроводные соединения, но только при наличии предпочитаемой сети и при условии автоматического подключения к ней.) Если локальное подключение отключить, то после перезагрузки системы оно активизироваться не будет и для его работы потребуется принудительное включение.

Соединения с удаленной сетью (интернет-провайдером), осуществляемые с помощью кабельных или ADSL-модемов и т. п. (все постоянные, автоматически устанавливаемые соединения, для которых ***не*** требуется аутентификация на противоположной стороне), также могут конфигурироваться в системе как "подключения по локальной сети" *(см. далее разд. "Подключение и настройка ADSL-модема")*. Если при установке ADSL-модема используется соединение с авторизацией, то для модема автоматически или вручную создается коммутируемое подключение (см. рис. 2.4).

Выбор параметров[2]

Правильно выбранные параметры позволяют компьютерам свободно взаимодействовать в локальной сети. Чтобы компьютеры могли "видеть" друг друга[3] и иметь доступ к Интернету, необходимо выполнение следующих условий:

1. Компьютеры должны иметь уникальные *имена* (имя компьютера задается при установке операционной системы).

---

[1] Возможность *такого* использования стандартного кабеля зависит от типа сетевого адаптера и не для всех моделей возможна — с каждым случаем нужно разбираться отдельно.

[2] Читатели, знакомые с основами сетей, захотят, возможно, пропустить данный раздел. Да, ничего нового в нем почти не говорится, но обратите внимание на связь сетевых параметров, имя сети и сетевое размещение — это важный и неочевидный момент!

[3] Мы не будем углубляться в теорию, а для краткости подойдем к вопросу чисто практически! Ограничения, накладываемые брандмауэром и параметрами безопасности, здесь мы не учитываем.

2. Компьютеры должны принадлежать к одной *рабочей группе* (workgroup) или входить в *домашнюю группу* (HomeGroup). Рабочая группа WORKGROUP по умолчанию используется для всех устанавливаемых систем.
3. Для подключений по локальной сети должны быть заданы *согласованные параметры стека протоколов TCP/IP*[1]. Именно эти настройки и рассматриваются ниже.

   Компьютеры смогут обмениваться информацией, если каждый из них имеет уникальный для данной сети *IP-адрес* и *маску подсети*. Этого уже достаточно для совместной работы компьютеров в сети.

   Примечание

   При установке операционной системы для сетевых подключений задается автоматическое получение параметров TCP/IP. Даже если в сети нет службы, выдающей IP-адреса, сетевые подключения настраиваются на использование так называемых APIPA-адресов *(см. далее)*, и компьютеры, подключенные к обычному коммутатору, смогут работать друг с другом. Однако даже в этом случае адреса компьютеров лучше ***задавать статически*** (в первую очередь это связано с механизмом определения сетевого размещения). При подключении к внешним сетям (когда используется перенаправление сетевых пакетов — маршрутизация) это требование становится обязательным (при отсутствии в сети DHCP-сервера).

4. Чтобы компьютеры могли "выходить" во внешнюю сеть (в Интернет), на каждом должен быть указать IP-адрес *шлюза* (gateway). При этом чтобы компьютеры могли разрешать DNS-адреса Интернета (преобразовывать имя в IP-адрес), должен быть указан IP-адрес *предпочитаемого DNS-сервера* (preferred DNS server). (Если подключение осуществляется через прокси-сервер провайдера, то это требование необязательно, но тогда в браузере этот прокси должен быть обязательно указан — см. рис. 2.11.)

Вот, собственно, и все параметры, которые нужно указать для нормальной работы в сети. Это касается как подключений по локальной сети, так и любых других соединений. Рассмотрим теперь все сказанное на примерах, с конкретными значениями.

Внимание!

Все вышесказанное касается как подключений по локальной сети, так и любых других соединений. Хотя для коммутируемых и беспроводных подключений обычно используется автоматическое получение параметров, важно понимать — а какие *именно* адреса получает компьютер и почему? Это важно для определения сетевого размещения и совместной работы компьютеров.

IP-адрес состоит из четырех десятичных цифр в диапазоне от 0 до 255, разделенных точкой. Это позволяет каждое число хранить в одном восьмиразрядном байте, а весь IP-адрес, таким образом, будет состоять из четырех байт.

[1] Мы ограничимся только протоколом IPv4, поскольку нет смысла использовать в домашней сети протокол IPv6 и обсуждать его особенности. Поэтому везде будет подразумеваться только IPv4, без указания версии протокола.

Диапазоны используемых IP-адресов определяются так называемыми *классами сетей*, а все адреса делятся на *публичные* (public) и *частные* (private). Публичные (или *выделенные*) адреса используются для связи узлов в Интернете, и их может выдавать интернет-провайдер из диапазона имеющихся в его распоряжении адресов. Частные адреса можно использовать в любой локальной сети без ограничений, поскольку они не входят в пространство адресов Интернета.

Все IP-адреса делятся на три следующие класса сетей:

Класс подсети	Маска	Максимальное число узлов
Класс A	255.0.0.0	16 777 214
Класс B	255.255.0.0	65 534
Класс C	255.255.255.0	254

Адрес 255.255.255.0 в двоичном виде записывается как 11111111.11111111.11111111.00000000. Узлам (хостам) сети могут выдаваться только те разряды, которые заняты нулями; старшие разряды (три байта) относятся к идентификатору (ID) сети. Таким образом, в сети класса C может быть 256 – 2 = 254 узла (два адреса являются зарезервированными: 0 относится к адресу самой сети, а 255 является широковещательным адресом[1]).

Для частных адресов выделены три следующих подсети (причем для небольших сетей, как правило, используются адреса сети класса C):

Идентификатор сети (ID)	Маска подсети	Диапазон IP-адресов узлов	Широковещательный адрес
10.0.0.0	255.0.0.0	10.0.0.1—10.255.255.254	10.255.255.255
172.16.0.0	255.255.0.0	172.16.0.1—172.31.255.254	172.16.255.255
192.168.1.0	255.255.255.0	192.168.1.1—192.168.255.254	192.168.255.255

Особая подсеть класса B выделена для адресов, назначаемых узлам при автоматическом конфигурировании параметров — *Automatic Private IP Address* (APIPA):

Идентификатор сети (ID)	Маска подсети	Диапазон IP-адресов узлов	Широковещательный адрес
169.254.0.0	255.255.0.0	169.254.0.1—169.254.255.254	169.254.255.255

Адрес из этого диапазона и маска назначаются адаптеру в том случае, если он настроен на получение параметров от DHCP-сервера[2], но не смог получить от сервера

[1] Особый адрес, не используемый для связи между *двумя* компьютерами.

[2] Dynamic Host Configuration Protocol (DHCP) — протокол динамической конфигурации хоста. Это сетевой стандарт, определяющий процесс централизованного присваивания IP-адресов и других параметров стека TCP/IP машинам-клиентам (компьютерам, сетевым устройствам и т. п.).

ответ по каким-то причинам (например, из-за недоступности или отсутствия сервера). Таким образом, если в сети отказала служба выдачи IP-адресов, то компьютеры, получившие APIPA-адреса (которые формируются случайным образом в пределах заданной маски), смогут взаимодействовать между собой, однако взаимодействие с другими (внешними) сетями при этом нарушается. Сеть, связанная с подключением, получившим такой адрес, обозначается как *неопознанная общественная сеть*, что очень важно для видимости компьютера и использования общих ресурсов (подробно это описано далее в *разд. "Особенности работы с несколькими сетевыми подключениями"*[1]).

Из всего вышесказанного можно сделать следующие практические выводы. В домашних локальных сетях обычно используются адреса подсетей 192.168.0.0 и 192.168.1.0 (маска 255.255.255.0):

192.168.0.0 — адреса от 192.168.0.2 до 192.168.0.254

192.168.1.0 — адреса от 192.168.1.2 до 192.168.1.254

Адреса 192.168.0.1 и 192.168.1.1 (192.168.0.254 или 192.168.1.254) обычно назначаются шлюзу — компьютеру, обеспечивающему выход во внешнюю сеть (Интернет), или аппаратному маршрутизатору (точке доступа).

Если в сети используется DHCP-сервер (например, встроенный в маршрутизатор или реализованный на отдельном сервере), то адреса из указанных диапазонов, маска и адрес шлюза настраиваются для раздачи всем клиентам сети. К этому еще добавляется адрес (адреса) предпочитаемого DNS-сервера, роль которого обычно также выполняет маршрутизатор.

Примеры настройки параметров TCP/IP приведены на рис. 1.18. По умолчанию задается автоматическая настройка (рис. 1.18, *слева*), и все значения компьютер получает от DHCP-сервера. В случае ручного определения параметров (рис. 1.18, *справа*) все адреса указываются явно.

> ***Совет***
>
> Все сетевые настройки проще всего увидеть с помощью команды `ipconfig /all`, выполняемой в окне командной строки. Она позволяет увидеть IP-адреса для всех подключений и способ получения параметров (с помощью DHCP или без него, статически). В случае ошибок полезно запустить диагностику сети, щелкнув правой кнопкой мыши по значку сети в области уведомлений (см. рис. 1.1).

Параметры TCP/IP, название сети и сетевое размещение

Для связи нескольких компьютеров в локальной проводной сети достаточно, чтобы каждый из них имел *IP-адрес* и *маску* (в пределах одной подсети). Однако в этом случае сеть, связанная с подключением по локальной сети, получает имя "Неопознанная сеть" (Unknown network) и имеет размещение *Общественная сеть* (Public

[1] Не обращайте здесь внимания на название раздела — даже если *одно* сетевое подключение относится к неопознанной сети, все проблемы использования общих папок будут такими же, как и при работе с несколькими подключениями.

network), причем имя сети и ее категорию непосредственно поменять невозможно. В результате на компьютеры локальной группы действуют более жесткие ограничения, уместные для общедоступной сети, и самое главное — становится невозможным доступ к другим компьютерам (поскольку запрещено сетевое обнаружение) и общим ресурсам.

Чтобы обойти этот нюанс реализации сетевых функций Windows 7, предлагаем следующее решение: укажите также на каждом компьютере адрес *шлюза*, соответствующий выбранной подсети (см. примеры выше). Тогда сеть будет распознаваться как *Домашняя сеть* (Home network), и можно будет выбрать правильные опции сетевого размещения и общего доступа. В простых конфигурациях это очень часто помогает; при одновременной работе с несколькими подключениями не обойтись без использования политик безопасности *(см. окончание главы)*: необходимо поменять тип сети для неопознанных сетей. Если и это не помогает, то нужно менять параметры сетевого обнаружения и совместного доступа для общего (public) профиля (см. рис. 1.23). Такое решение возможно только в "статических" сетевых конфигурациях (в небольшой локальной сети с постоянно заданными подключениями), поскольку ослабление параметров для общедоступных сетей (в общем профиле) может отрицательно сказаться на безопасности компьютера.

Более подробная информация, касающаяся настройки сетевых подключений и выбора профилей, содержится *далее в разд. "Подключение и настройка ADSL-модема"*.

Диагностика ошибок

При возникновении проблем в работе сети рекомендуется в первую очередь открыть окно командной строки, ввести команду `ipconfig /all` и проверить правильность назначения основных параметров используемому адаптеру. Появление APIPA-адреса вида 169.254.x.x указывает на то, что настройки должны были выполняться автоматически, но связь с DHCP-сервером была потеряна (или же он неработоспособен). Следует проверить работу сервера или задать адреса статически (явно); в любом случае нужно проверить соответствие адресов общей конфигурации сети.

- Связь между компьютерами (или связь со шлюзом) проверяется с помощью команды `ping` (если эхо-запросы не заблокированы брандмауэром — *см. главу 4*):

```
C:\>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=5мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=5мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=4мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=5мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

```
Приблизительное время приема-передачи в мс:
    Минимальное = 4мсек, Максимальное = 5 мсек, Среднее = 4 мсек
```

- Помимо запросов по адресу, нужно выполнять запросы и по имени компьютера — например, **ping** Win7-WS1 — это позволит проверить разрешение имен.
- Утилита nslookup позволяет проверить правильность разрешения DNS-имен Интернета, например:

```
C:\>nslookup microsoft.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    microsoft.com
Addresses:  207.46.197.32
          207.46.232.182
```

  Если IP-адреса для указанного имени получить не удается, то следует проверять адрес предпочитаемого DNS-сервера и настройки маршрутизатора, если он кэширует (хранит локально) ответы внешних DNS-серверов (указываемых интернет-провайдером). На ошибки разрешения имен указывает и факт отсутствия подключения к Интернету в окне сети (см. рис. 1.1), поскольку эта проверка входит в число служебных тестов.

Если базовые тесты проверки связи между компьютерами проходят успешно, то можно разбираться с вопросами сетевого обнаружения и общего доступа — *см. разд. "Настройка сетевого доступа к общим папкам и принтерам" главы 1*. Особенности настройки компьютеров, входящих в домашнюю группу, рассмотрены в соответствующем разделе *главы 1*.

Телефонные (коммутируемые) подключения

Телефонное, или *коммутируемое*, *подключение* (dial-up connection) соединяет компьютер с интернет-провайдером, корпоративной сетью или другим компьютером при помощи устройств, подключаемых к обычной коммутируемой телефонной сети.

Такими устройствами чаще всего являются телефонные (телефонные) модемы, но для подключения к Интернету сейчас все шире используются USB-модемы стандартов мобильной связи (GSM, CDMA, WiMAX и др.). Сетевые подключения для работы с этими модемами обычно создаются с помощью собственных программ установки *(см. главу 3)*, поэтому в следующих двух разделах мы будем подразумевать использование только традиционных телефонных модемов или модемов, эмулируемых устройствами с Bluetooth-адаптерами[1] (мобильными телефонами, КПК и т. п.). Однако операции просмотра и изменения параметров коммутируемых под-

[1] Пример подключения такого устройства рассматривается в *главе 3*.

ключений будут одинаковыми для модемов любых типов — от аналоговых до ADSL-модемов с авторизацией и 3G-модемов *(см. далее разд. "Просмотр и изменение параметров подключения")*.

Установка и настройка модема

Прежде чем создавать коммутируемое подключение, установите модем в соответствии с рекомендациями производителя. Для конфигурирования модемов на панели управления имеется задача **Телефон и модем** (Phone and Modem). В одноименном окне на вкладке **Модемы**[1] (Modems) (рис. 2.2) перечислены установленные модемы, здесь же их можно добавлять и удалять, а также настраивать и тестировать. Как можно видеть, в этом списке появляются и модемы, эмулируемые устройствами с Bluetooth-адаптером (например, мобильными телефонами, имеющими выход в Интернет — *см. главу 3*). Обычно настройки в данном окне требуются только для аналоговых телефонных модемов (для других типов модемов может потребоваться разве что опрос модема для его проверки).

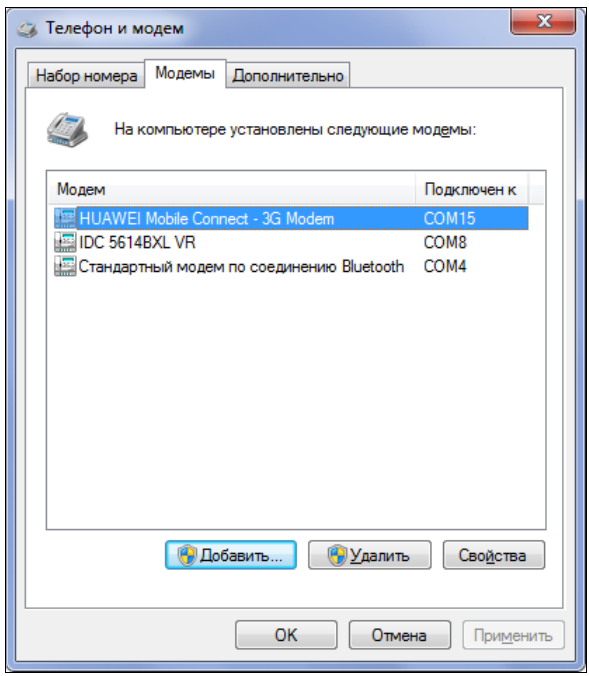

Рис. 2.2. Окно с перечнем модемов, установленных в системе

В окне свойств модема на нескольких вкладках отображаются параметры, определяющие работу модема данного типа. Например, на вкладке **Модем** (Modem)

[1] Обратите внимание на то, что в примере перечислены модемы разных типов — 3G-модем, телефонный модем и модем, представляющий мобильный телефон, подключенный по каналу Bluetooth. Коммутируемые подключения с использованием любых подобных модемов настраиваются и устанавливаются одинаково.

(рис. 2.3, *слева*) можно задавать максимальную скорость порта[1], а на вкладке **Диагностика** (Diagnostics) (рис. 2.3, *справа*) имеется кнопка **Опросить модем** (Query Modem), которую стоит нажать после подключения модема (особенно, если это делается в первый раз) — это позволит убедиться в его работоспособности. Если в окне появится длинный список команд и соответствующих ответов модема, то модем правильно реагирует на команды и можно продолжать работу; если же ответа не будет, то нужно проверять правильность физического подключения устройства и установки (выбора) драйверов.

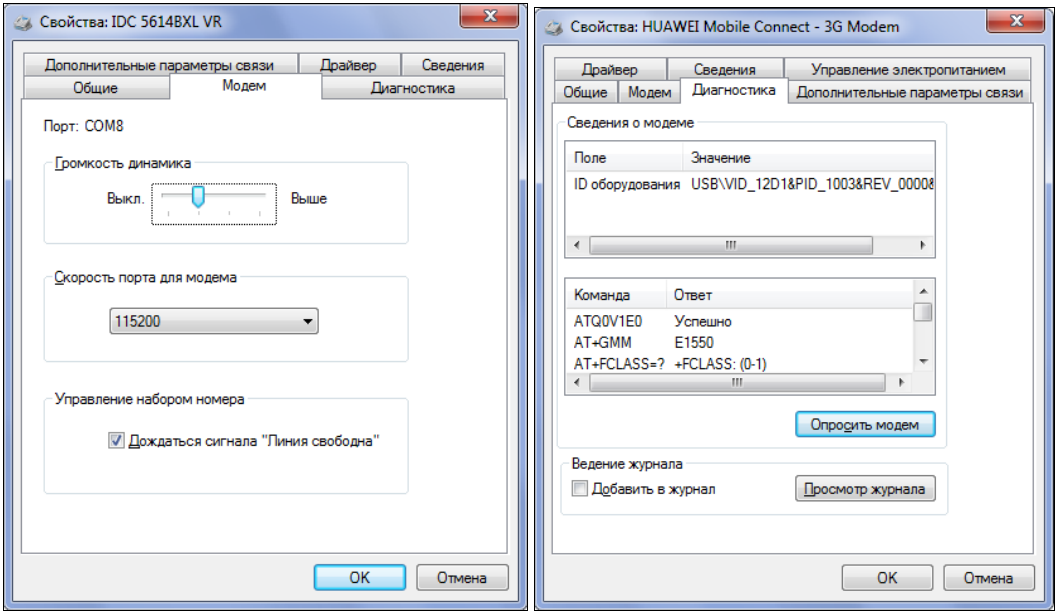

Рис. 2.3. Различные параметры модемов (аналоговый модем *слева* и 3G-модем *справа*)

На вкладке **Дополнительные параметры связи** (Advanced) может задаваться специальная строка инициализации модема, если это требует производитель или необходимо для установки особого режима связи (скорости, сжатия и т. п.). Другие параметры, определяющие работу модема, задаются уже в свойствах конкретного коммутируемого подключения *(см. далее)*.

Создание подключения

Если модем работоспособен (его тип далее уже не имеет значения), то в окне мастера сетевых подключений (см. рис. 2.1) выберите одну из трех опций, которые позволят создать телефонное подключение — дальнейшие шаги будут по сути одина-

[1] Не следует путать скорость порта с реальной скоростью работы модема (скоростью соединения) — обычно скорость порта устанавливается в несколько раз выше, поскольку протоколы аппаратного сжатия позволяют передавать больший объем информации, нежели тот, что соответствует чистой скорости соединения ("коннекта").

ковыми, а отличия для каждой опции проявятся лишь в назначении подключения (от этого зависят используемые сетевые настройки и свойства браузера Internet Explorer: в одних случаях его параметры будут меняться, в других — нет). Для подключения к интернет-провайдеру можно использовать самую простую опцию — **Настройка телефонного подключения** (Set up a dial-up connection). Если нужно подключиться к корпоративному серверу удаленного доступа (RAS), выбирайте опцию **Подключение к рабочему месту** (Connect to a workplace) (в этом случае указывается только номер телефона, а имя пользователя и его пароль определяются учетной записью безопасности, которая будет использоваться при выполнении подключения). Опция **Подключение к Интернету** (Connect to the Internet) позволяет создавать или использовать соединения *различных* типов, в том числе и телефонные.

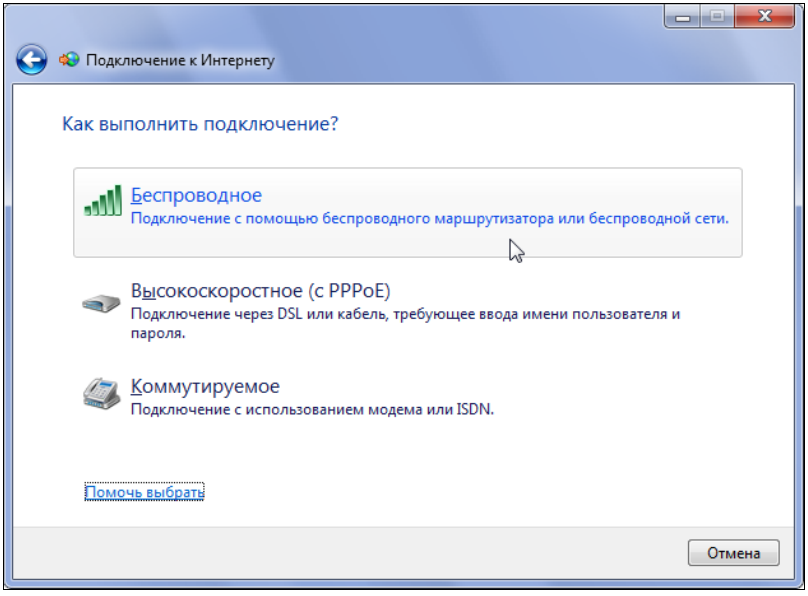

Рис. 2.4. Выбор типа устройства для подключения к интернет-провайдеру

Если создается подключение к Интернету, то можно указать, через какое устройство это подключение будет осуществляться (рис. 2.4). При выборе беспроводного соединения просто открывается окно подключения к доступным сетям (см. рис. 1.1, *справа*). Если используется ADSL- или другой скоростной модем, настроенный на подключение с авторизацией, то тип подключения — высокоскоростное с PPPoE или коммутируемое — определяется изготовителем и, в первую очередь, интернет-провайдером[1] (обычно такие подключения создаются автоматически, с помощью программы установки модема, но иногда их можно создавать и вручную). Коммутируемые подключения используются при работе с аналоговыми телефонными мо-

[1] Тип подключения даже для одного провайдера и для одной модели модема может отличаться для разных телефонных станций (в зависимости от используемого оборудования).

демами и модемами, эмулируемыми Bluetooth-устройствами и устройствами, подключаемыми к ИК-порту *(см. главу 3)*.

При выборе коммутируемого подключения (см. рис. 2.4) нужно будет указать используемый модем *(см. ниже)*. Аналогичным образом, если изначально была выбрана опция **Настройка телефонного подключения** (Set up a dial-up connection), то в специальном окне (рис. 2.5) перечисляются все установленные модемы, и нужно выбрать устройство, через которое будет осуществляться выход в Интернет. Если модем единственный, то этот шаг вообще отсутствует.

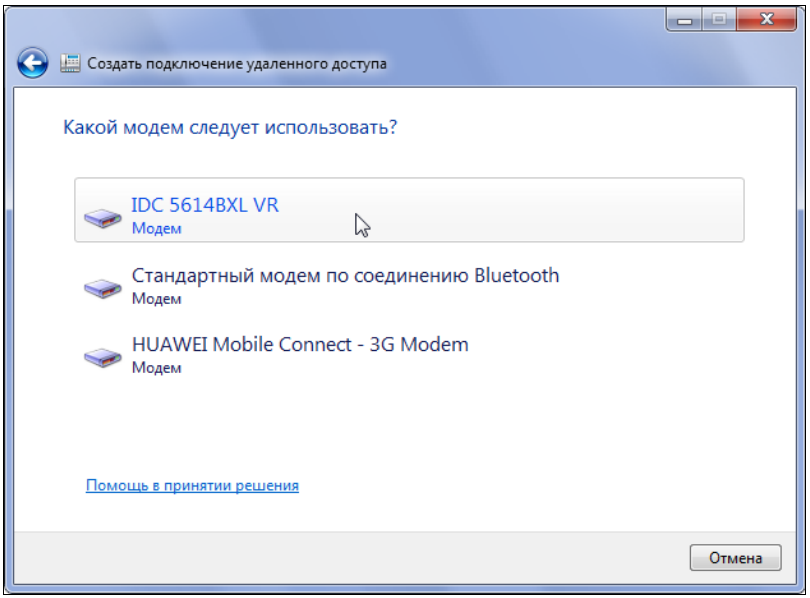

Рис. 2.5. Выбор модема для создаваемого подключения

На следующем этапе (рис. 2.6) введите данные, полученные от интернет-провайдера или оператора связи: номер телефона, имя и пароль. Имя подключения можно устанавливать произвольным, но лучше, чтобы оно было смысловым (например, соответствовать имени провайдера). Если подключение создается для всех пользователей компьютера, то установите соответствующий флажок. Сразу после нажатия кнопки **Подключить** (Connect) система попытается установить созданное подключение.

В случае неудачи пользователь может повторить попытку, запросить диагностику или разрешить создание подключения, несмотря на ошибку (в этом случае при установлении соединения пароль нужно будет вводить снова; в случае успеха он запоминается сразу). По завершении операции новый значок появится в окне сетевых подключений (см. рис. 1.13) и будет отображаться в списке подключений в окне активных сетей (см. рис. 1.1). Устанавливать и разрывать подключение можно из любого названного окна, а вызвав контекстное меню для подключения и выбрав команду **Свойств** (Properties), можно открыть окно, в котором перечислены многочисленные параметры подключения.

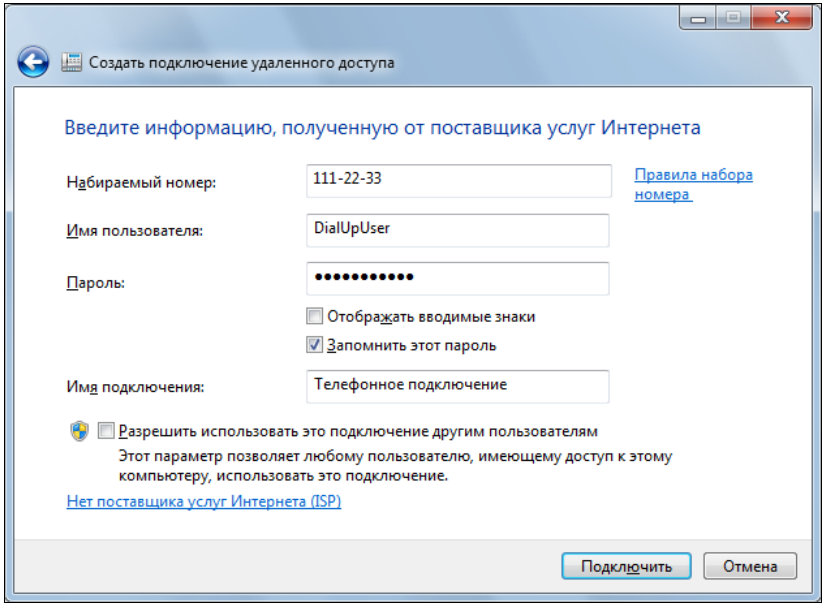

Рис. 2.6. Ввод параметров для подключения к провайдеру

Просмотр и изменение параметров подключения

В окне свойств телефонного подключения[1] на вкладке **Общие** (General) (рис. 2.7, *слева*) указан используемый модем и основной набираемый номер телефона (кнопка **Другие** (Alternates) служит для указания дополнительных номеров и выбора режимов набора номеров). Кнопка **Настроить** (Configure) позволяет открыть очень важное для аналоговых модемов окно, где задаются скорость порта и параметры управления потоком данных (аппаратный контроль, обработка ошибок и сжатие) (рис. 2.7, *справа*).

> ***Совет***
>
> Если для набора номера вместо тонового (tone) нужно использовать импульсный (pulse) режим, то добавьте перед первой цифрой номера латинскую букву "p", как показано на рис. 2.7.

На вкладке **Параметры** (Options) (рис. 2.8, *слева*) перечислены настройки, управляющие ходом подключения и действиями при повторном наборе номера. Флажок **Перезвонить при разрыве связи** (Redial if line is dropped) рекомендуется устанавливать, чтобы автоматически восстанавливать подключение при разрыве. На вкладке **Безопасность** (Security) (рис. 2.8, *справа*) показаны стандартные парамет-

[1] Мы рассмотрим параметры аналогового телефонного подключения подробно по той причине, что аналогичные настройки используются и для коммутируемых соединений с использованием более современных устройств, таких как 3G-модемы или Bluetooth-устройства, а также для VPN-подключений.

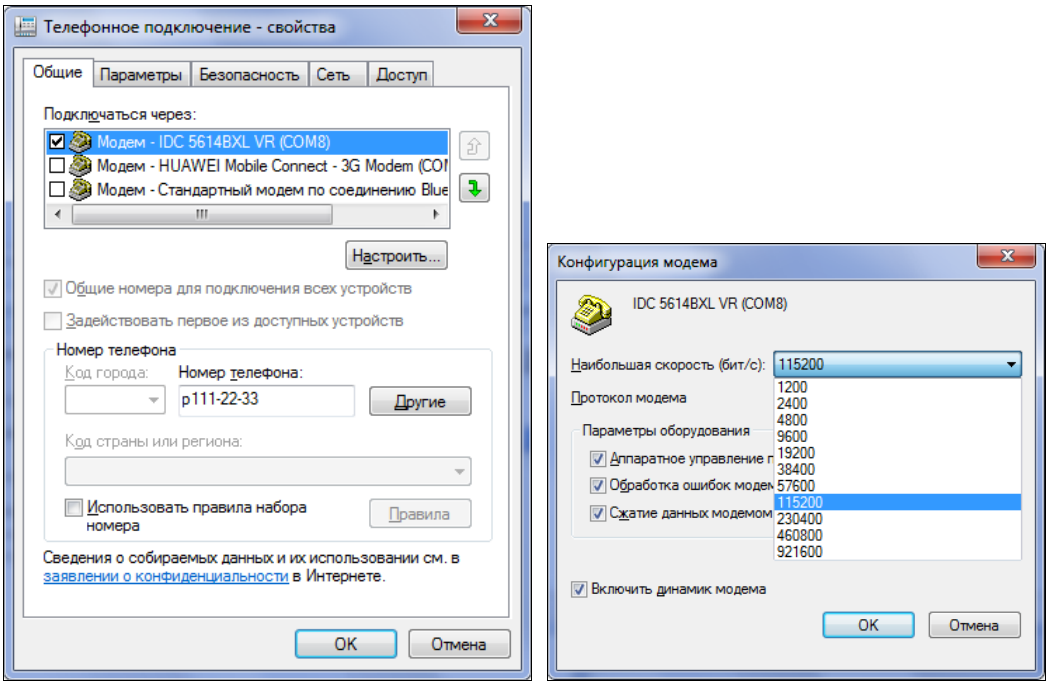

Рис. 2.7. Основные параметры телефонного подключения и используемого модема

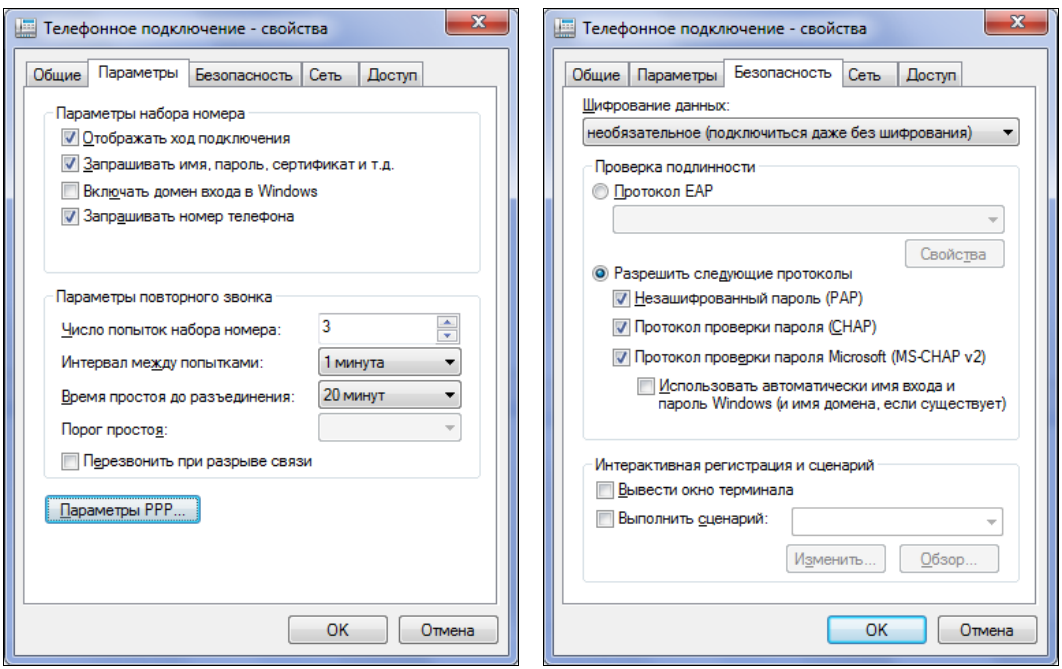

Рис. 2.8. Параметры активизации подключения *(слева)*
и настройки безопасности канала связи *(справа)*

ры безопасности, определяющие протоколы защиты подключения. Их следует задавать в соответствии с требованиями интернет-провайдера или удаленного сервера доступа (RAS).

Протоколы и сетевые компоненты, используемые для связи с провайдером, перечислены на вкладке **Сеть** (Networking) (рис. 2.9). Для обычных телефонных подключений здесь нужно оставить только протокол IPv4, настроенный на автоматическое получение параметров (см. пример на рис. 1.18, *слева*). Если провайдер требует указывать параметры явно, то нужно выбрать протокол, нажать кнопку **Свойства** (Properties) и ввести заданные настройки.

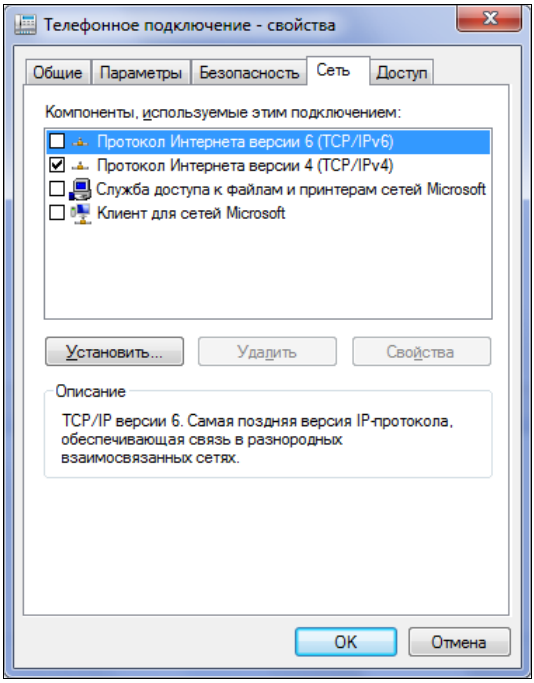

Рис. 2.9. Сетевые компоненты и протоколы, используемые данным подключением

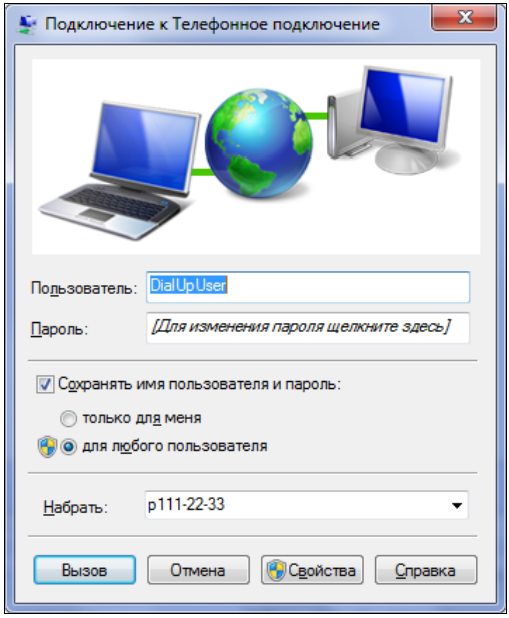

Рис. 2.10. Параметры учетной записи и номер, используемые для подключения к провайдеру или удаленному серверу

Параметры на вкладке **Доступ** (Sharing) позволяют разрешать совместное использование данного подключения всем клиентам сети (т. е. включать ICS — эта процедура подробно описана *далее в разд. "Разрешение общего доступа к Интернету"*).

При запуске подключения появляется окно, где можно проверить имя пользователя, пароль и набираемый номер (рис. 2.10), а также определить круг пользователей, которые смогут пользоваться данным подключением. При успешном установлении соединения пароль запоминается и при повторных подключениях данное окно уже появляться не будет.

Сетевые настройки браузера Internet Explorer для соединений по запросу

Для нормальной работы браузер должен "знать", какое коммутируемое подключение ему использовать и в каких случаях. Настройки для браузера Internet Explorer задаются на вкладке **Подключения** (Connections) (рис. 2.11) в окне свойств (оно открывается по команде **Сервис** | **Свойства обозревателя** (Tools | Internet Options)). Кнопка **Установить** (Setup) запускает мастер создания подключений (см. опцию **Подключение к Интернету** (Connect to the Internet) на рис. 2.1), и при необходимости можно создать новое подключение. Аналогичные функции — для разных типов подключений — выполняют кнопки **Добавить** (Add) и **Добавить VPN** (Add VPN).

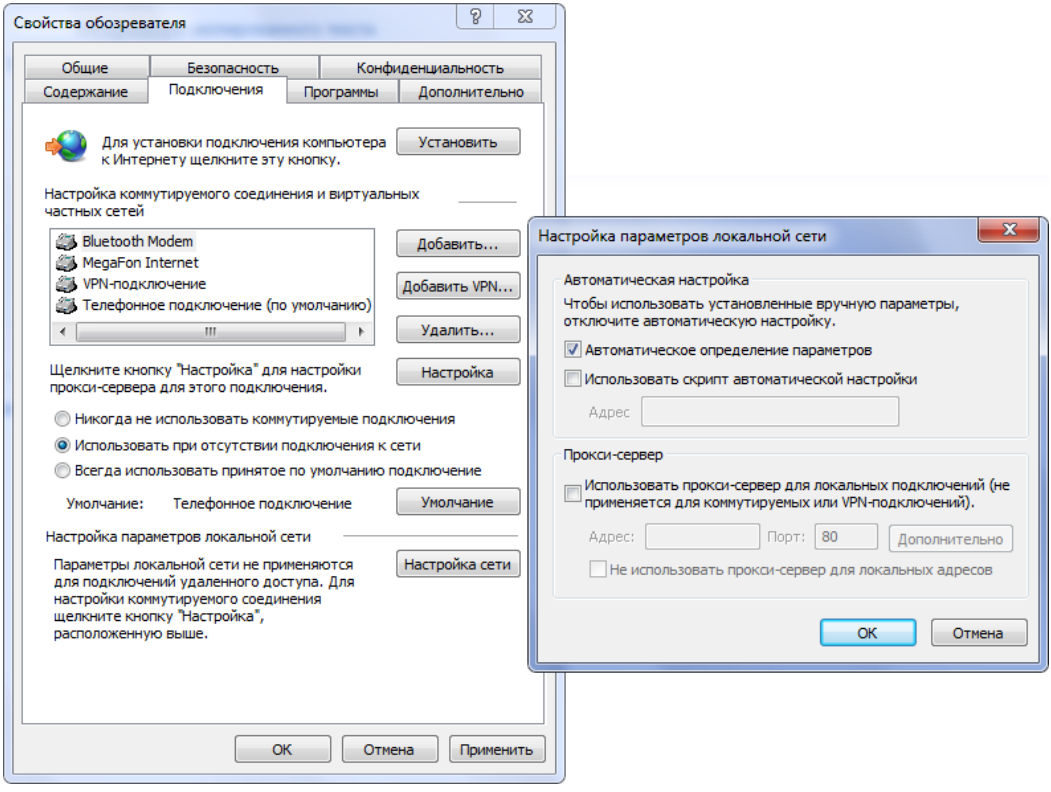

Рис. 2.11. Выбор сетевого подключения для работы с браузером и дополнительная настройка параметров

Кнопка **Настройка** (Settings) позволяет указать режим выбора параметров для выбранного подключения (для каждого соединения параметры свои, а для подключения по локальной сети используется и индивидуальная кнопка **Настройка сети** (LAN settings)) — пример для локальной сети показан на рис. 2.11. Важным параметром здесь является прокси-сервер, который в некоторых случаях нужно использовать обязательно (например, такое требование может предъявлять интернет-

провайдер). В локальных сетях прокси обычно не используется, но следует проследить за тем, чтобы флажок **Автоматическое определение параметров** (Automatically detect settings) был установлен.

Также очень важно выбрать режим использования коммутируемых подключений. Для этого имеются три переключателя. Если нежелательно, чтобы запуск браузера вызывал запуск подключений, то следует выбрать опцию **Никогда не использовать коммутируемые подключения** (Never dial a connection). Переключатель **Использовать при отсутствии подключения к сети** (Dial whenever a network connection is not present) разрешит системе устанавливать выбранное по умолчанию соединение, только если связь с внешней сетью отсутствует. Выбор опции **Всегда использовать принятое по умолчанию подключение** (Always dial my default connection) указывает на то, что при необходимости *всегда* будет задействовано то подключение, которое указал пользователь (выбрав его в списке и нажав кнопку **Умолчание** (Set default)).

> ***Внимание!***
>
> На рис. 2.11 обратите внимание на то, что выбранные настройки распространяются на все типы подключений, устанавливаемых по запросу, — от телефонных до VPN. Такой механизм позволяет использовать для работы в Интернете только то подключение, которое требуется, или же не запускать их вообще.

Автоматическая установка подключения по запросу

Любое коммутируемое подключение[1] легко запустить или разорвать вручную в окне активных подключений (см. рис. 1.1) или в окне сетевых подключений (см. рис. 1.13). Однако что делать, если хочется видеть подключение активным сразу, с момента входа в систему? Или необходимо, чтобы подключение активизировалось даже без регистрации пользователя, просто после загрузки системы? — Для этого нужно задействовать стандартную утилиту `rasdial`, которая служит для запуска коммутируемых подключений (с модемами разных типов — аналоговых, 3G и др.) и VPN-подключений.

Для установки подключения из окна командной строки достаточно указать его имя (отображаемое в окне сетевых подключений — см. рис. 1.13), например:

```
C:\>rasdial "MegaFon Internet"
Установка связи с MegaFon Internet...
Проверка имени и пароля пользователя...
Регистрация компьютера в сети...
Установлена связь с MegaFon Internet.
Команда успешно выполнена.
```

Для разрыва подключения к команде нужно добавить соответствующий ключ:

```
C:\>rasdial "MegaFon Internet" /DISCONNECT
Команда успешно выполнена.
```

[1] Управление беспроводными подключениями (Wi-Fi) рассматривается в *главе 3*.

Команда `rasdial` без параметров перечисляет активные в данный момент коммутируемые подключения.

При установке VPN-подключения необходимо также указать имя пользователя и пароль, например:

```
rasdial "VPN connection" userName PassWord
```

Чтобы команда установки подключения выполнялась автоматически, без участия пользователя, нужно сначала показанную выше команду запуска соединения записать в текстовый файл с расширением .cmd и дать ему произвольное имя. Затем можно пойти двумя путями.

- Введите в поле поиска меню **Пуск** (Start) строку `gpedit.msc`, которая запустит редактор групповых политик.

  Если подключение нужно устанавливать при запуске системы, найдите узел **Конфигурация компьютера | Конфигурация Windows | Сценарии (запуск/завершение)** (Computer Configuration | Windows Settings | Scripts (Startup/Shutdown)). Дважды щелкните в правой половине окна оснастки по опции **Автозагрузка** (Startup) и в открывшемся окне, нажав кнопку **Добавить** (Add), выберите созданный ранее CMD-файл.

  Если подключение требуется после регистрации пользователя, то аналогичные действия нужно проделать с опцией **Вход в систему** (Logon) в папке **Конфигурация пользователя | Конфигурация Windows | Сценарии (вход/выход из системы)** (User Configuration | Windows Settings | Scripts (Logon/Logoff)).

- Аналогичные результаты можно получить с помощью папки **Автозагрузка** (Startup). Сначала для получившегося CMD-файла создайте ярлык.

  Если действия необходимы при запуске системы, то нужно открыть папку **Пуск | Все программы | Автозагрузка** (Start | All Programs | Startup), щелкнуть правой кнопкой мыши и в контекстном меню выполнить команду **Открыть общее для всех меню** (Open all users). Полный путь к нужной папке выглядит так: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup. Теперь в данную папку следует переместить созданный ярлык для запуска командного файла.

  Чтобы действия выполнялись при входе пользователя в систему, можно просто перетащить ярлык в папку **Пуск | Все программы |Автозагрузка** (Start | All Programs | Startup). Ее физическое расположение на диске — C:\Users*%UserName%*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup.

> ***Внимание!***
>
> Чтобы подключения можно было запускать из командных файлов, давайте им названия с использованием только латинских букв. Каждый созданный командный файл нужно сначала проверить вручную и убедиться в правильности выполнения операций. Только потом его можно включать в автозагрузку или выбирать в редакторе групповых политик.
>
> Если перед установкой VPN-подключения требуется активизировать подключение по вызову, то в командный файл следует включить утилиту `rasdial` с параметрами для *обоих* подключений.

Виртуальные частные сети (VPN)

Если для создания канала связи с удаленной частной (private) сетью используется общедоступная (public) сеть, то совокупность всех соединений между конечными узлами называется *виртуальной частной сетью* (Virtual Private Network, VPN). Поддерживаемые системами Windows 7 туннельные протоколы PPTP, L2TP/IPSec, SSTP и IKEv2 обеспечивают надежный и защищенный доступ к сетевым ресурсам при соединении с сервером удаленного доступа (Remote Access Server, RAS) через Интернет или другую сеть. В качестве RAS-сервера может выступать не только специальный выделенный сервер, но и обычный клиентский компьютер, работающий под управлением Windows XP/Vista/7.

> ***Внимание!***
>
> Для использования *входящих* VPN-подключений необходимо, чтобы в брандмауэре, на общем подключении к Интернету (см. рис. 2.32) и в маршрутизаторе (если таковой используется) был открыт TCP-порт 1723. Для проверки портов, открытых для доступа из Интернета, можно воспользоваться специальными сайтами, например **http://2ip.ru** и **http://canyouseeme.org**.

Для создания VPN-канала между двумя системами необходим минимум действий: на одном компьютере настраивается входящее подключение *(см. далее)* и разрешается VPN (этот компьютер будет выполнять функции *VPN-сервера*), а на другом — в окне мастера подключений (см. рис. 2.1) нужно выбрать опцию **Подключение к рабочему месту** (Connect to a workplace), а затем в окне выбора типа соединения (рис. 2.12) указать на использование VPN-подключения (Use my Internet connection (VPN)).

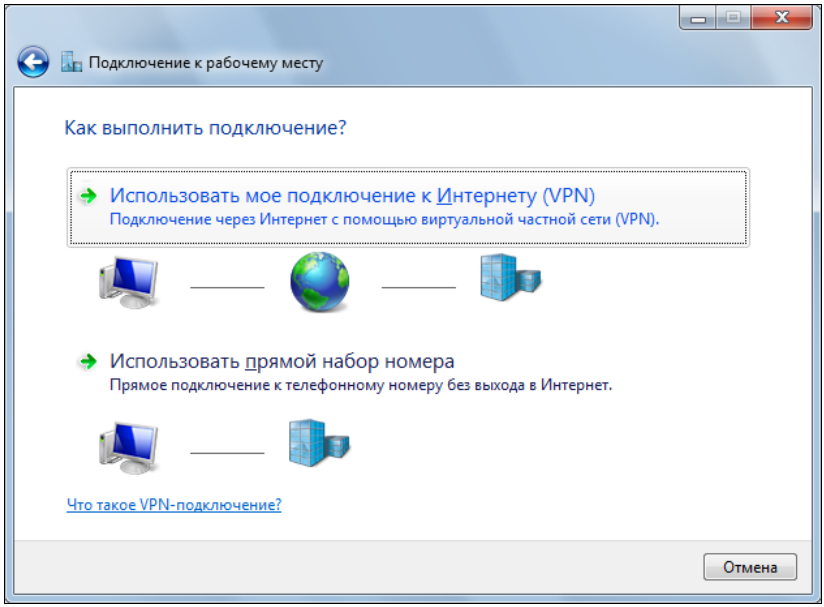

Рис. 2.12. Выбор способа подключения к удаленному рабочему месту

Далее следует ввести DNS-имя или IP-адрес VPN-сервера и дать VPN-подключению значащее имя (рис. 2.13). (Подключение может устанавливаться сразу же или в будущем — см. соответствующий флажок на рисунке.) Затем для регистрации на сервере нужно указать имя учетной записи и пароль, а также имя домена (сервера). Когда подключение создано (и установлено), можно закрыть окно мастера.

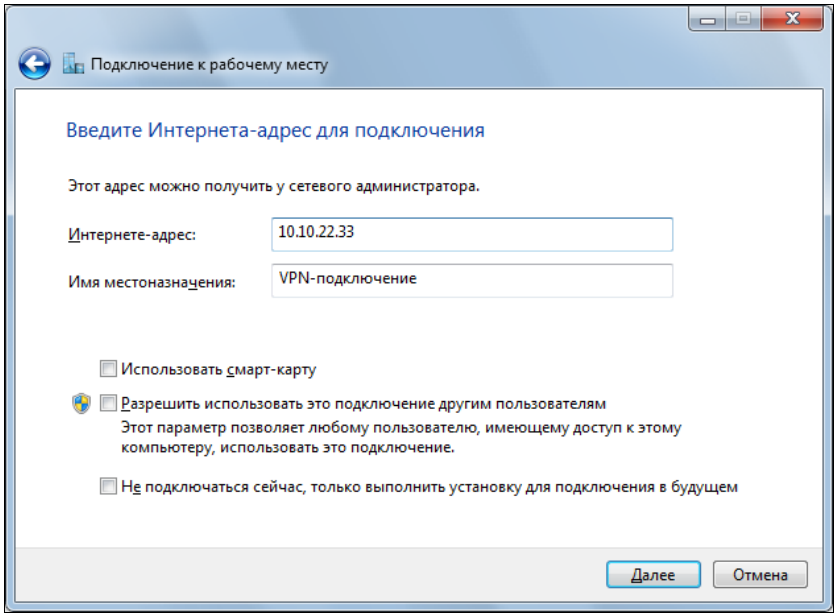

Рис. 2.13. Параметры создаваемого VPN-подключения

Передача информации по VPN-подключению по умолчанию шифруется. (Убедиться в этом можно, открыв окно состояния подключения.) VPN-подключение, как и любое другое, можно сделать общим для всех компьютеров сети (т. е. разрешить "Общий доступ к подключению к Интернету" (Internet Connection Sharing, ICS)).

Основные параметры VPN-подключений такие же, как и для рассмотренных ранее коммутируемых подключений. Обратить внимание следует только на вкладку **Общие** (General), где указано введенное при создании подключения имя или адрес VPN-сервера, а также есть возможность выбора подключения по запросу, если оно требуется для связи с внешней сетью (Интернетом) (рис. 2.14). В этом случае нужно установить флажок **Сначала набрать номер для этого подключения** (Dial another connection first) и выбрать подключение из списка.

Если задана очередность подключений, то при первом запуске VPN-подключения появится окно запроса на установку коммутируемого подключения. Перед тем как согласиться, можно установить специальный флажок, и окно с напоминанием больше выводиться не будет.

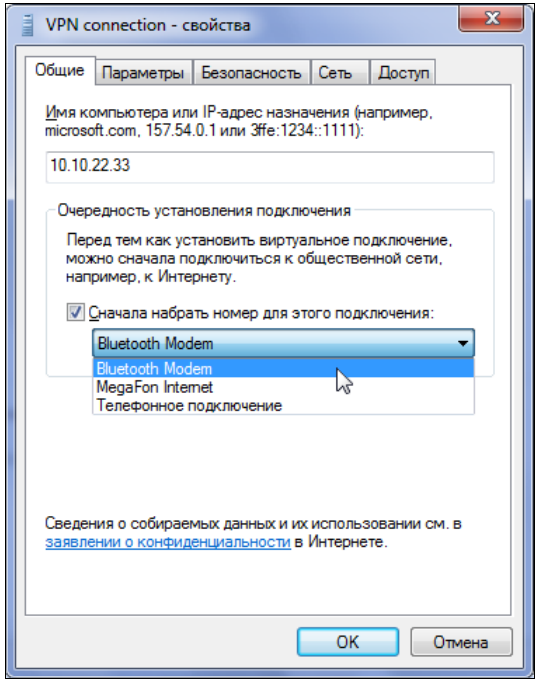

Рис. 2.14. Общие параметры VPN-подключения

Входящие подключения

При наличии *входящего подключения* компьютер может служить сервером удаленного доступа — т. е. предоставлять удаленным клиентам возможности использования локальных ресурсов и приложений. Входящие подключения обеспечивают прием вызовов посредством телефонного подключения (модем, ISDN), виртуальной частной сети (VPN) или прямого подключения (последовательный и параллельный кабель, беспроводная связь). В любом случае используется одна и та же процедура создания входящего подключения (иначе говоря — входящие подключения включаются только один раз).

Процедура разрешения входящих подключений в системах Windows Vista/Windows 7 инициируется особенным образом (без помощи программы-мастера, показанного на рис. 2.1). В окне сетевых подключений (см. рис. 1.13) нажмите кнопку <Alt> — появится классическое меню, где следует выполнить команду **Файл | Новое входящее подключение** (File | New Incoming Connection).

При разрешении входящих подключений определяются пользователи, которые смогут подключаться к данному компьютеру из удаленных точек (рис. 2.15). Для каждого такого пользователя должна существовать локальная учетная запись (ее можно создать непосредственно при настройке входящих подключений).

На следующем шаге нужно указать тип входящих подключений, которые будут использоваться: доступ может осуществляться через *Интернет* и/или с помощью

модема, подключенного к компьютеру (рис. 2.16). В первом случае компьютер будет выполнять функции *VPN-сервера*, во втором — *RAS-сервера* (Remote Access Server; сервер удаленного доступа).

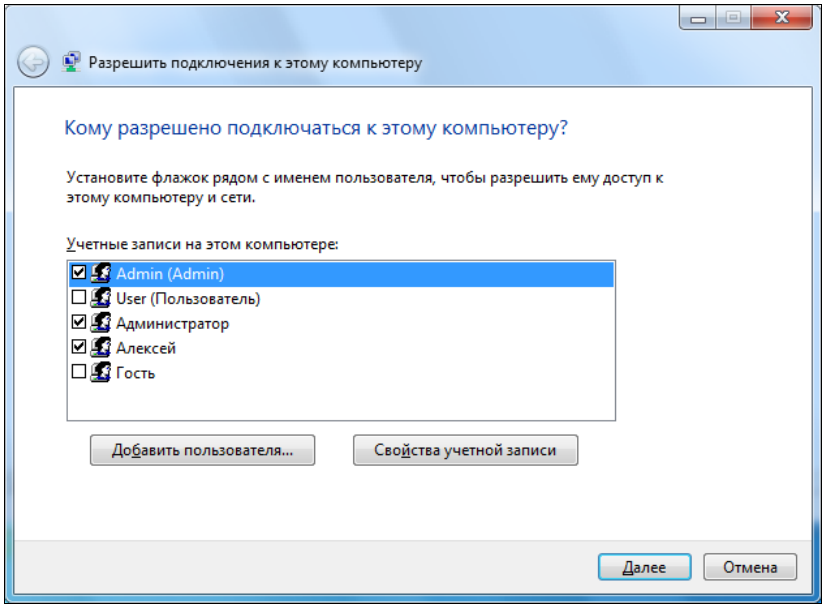

Рис. 2.15. Выбор учетных записей, которые можно будет использовать для удаленного доступа к данному компьютеру

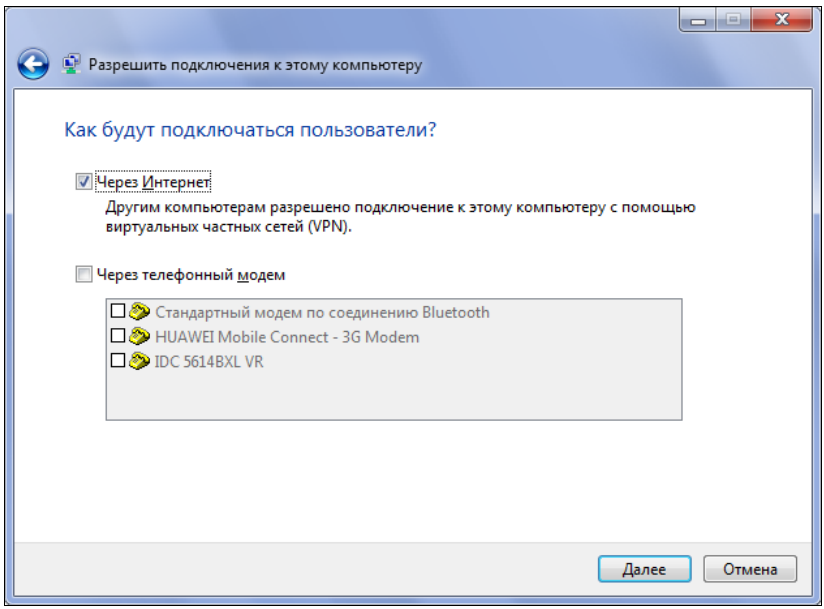

Рис. 2.16. Выбор типа разрешенных входных подключений

Далее следует выбрать службы и протоколы для входящих подключений (рис. 2.17) и, что очень важно, определить *свойства* протоколов (поскольку они указывают на возможность доступа к локальной сети и способ назначения IP-адресов). Когда все параметры выбраны, нужно нажать кнопку **Разрешить доступ** (Allow access). После этого удаленные клиенты смогут подключаться к локальному компьютеру.

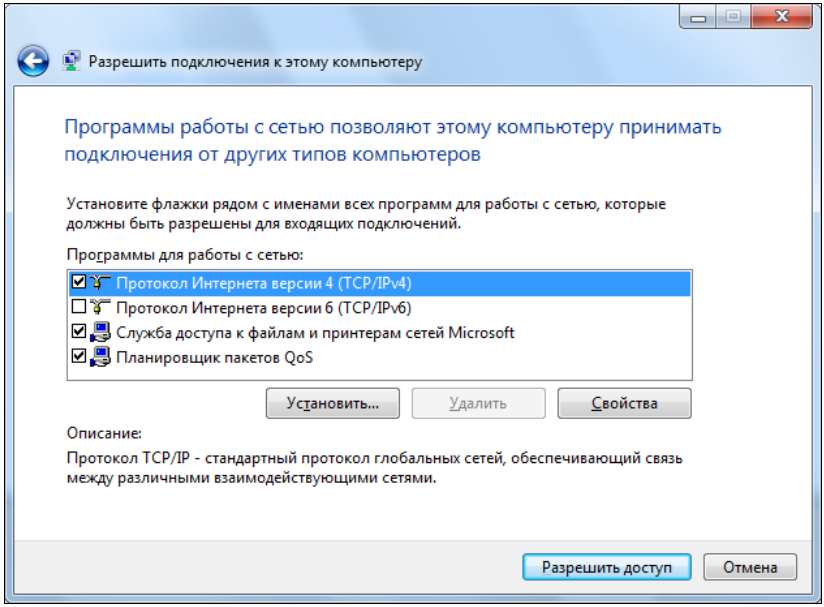

Рис. 2.17. Выбор протоколов и служб, используемых входящими подключениями

После выполнения описанной процедуры в окне сетевых подключений (см. рис. 1.13) появляется значок **Входящие подключения** (Incoming Connections). Открыв для него окно свойств, можно просмотреть и изменить любые перечисленные выше настройки, выбранные при разрешении подключений. Если окно сетевых подключений представлено в режиме "Таблица" (Details), то легко видеть, какие клиенты подключаются к компьютеру.

Совместное использование интернет-подключения (ICS)

Функция *Общий доступ к подключению к Интернету* (Internet Connection Sharing, ICS) позволяет через единственное сетевое соединение[1], созданное на компьютере, подключить к Интернету (или внешней сети) всю домашнюю локальную сеть. В этом случае данный компьютер предоставит всем другим компьютерам домашней сети возможность использования служб *преобразования сетевых адресов*

[1] Постоянное или устанавливаемое по запросу.

(Network Address Translation, NAT), *выдачи адресов* (DHCP) и *разрешения имен* (DNS).

Компьютеру (будем его называть *центральным*), обеспечивающему общий доступ к Интернету (ICS), требуется два сетевых подключения:

- *внутреннее* — подключение, используемое для связи между компьютерами и устройствами в локальной сети;
- *внешнее* — коммутируемое или постоянное подключение для связи компьютера с Интернетом (внешней сетью) или VPN-подключение к удаленному серверу.

Общий доступ к подключению к Интернету (Internet Connection Sharing, ICS) ***всегда*** включается на внешнем подключении. Это аксиома, и исключений нет. Вторая аксиома — набор служб *(см. выше)*, предоставляемых центральным компьютером.

> ***Внимание!***
>
> Поскольку при включении ICS на компьютере запускается DHCP-сервер, выполняющий выдачу параметров TCP/IP, для нормальной работы требуется, чтобы в сети ***отсутствовали другие службы DHCP*** (например, на других компьютерах или встроенные в аппаратные маршрутизаторы). Поэтому в конфигурации сети нужно заранее учесть расположение всех служб и скоординировать их работу.
>
> На компьютере ICS можно включить только один раз, только на одном подключении.

Рассмотрим эти требования на примере *кабельной* локальной сети, показанной на рис. 2.18. Для подключения к Интернету используется ADSL-модем, подключенный к компьютеру через USB-порт. Несколько компьютеров сети связаны между собой через коммутатор Ethernet. В данной конфигурации каждый компьютер имеет выход в Интернет через ADSL-модем, используемый совместно, поскольку компьютер с ICS обеспечивает маршрутизацию сетевых пакетов и трансляцию имен (при этом, как можно видеть, все сетевые адреса строго согласованы).

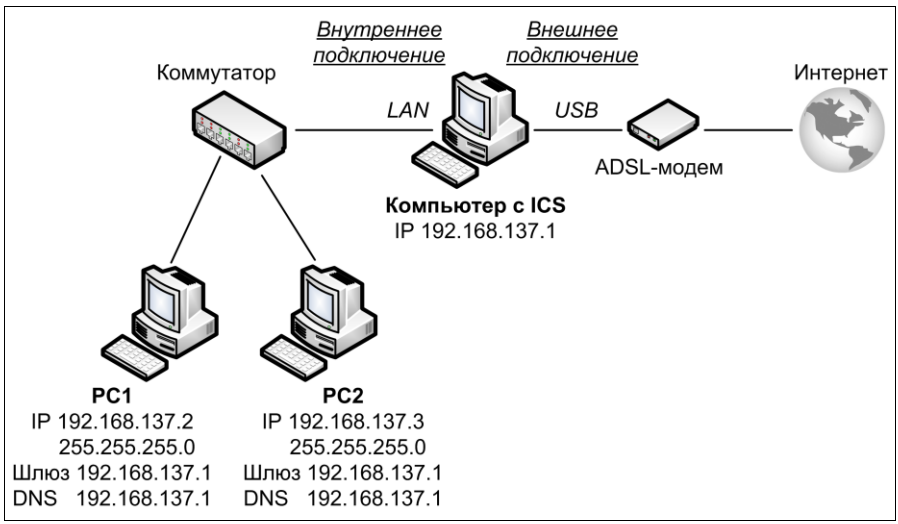

Рис. 2.18. Кабельная сеть с общим доступом к интернет-подключению

Конфигураций сетей с общим интернет-подключением можно придумать множество (просто невозможно описать все используемые устройства и технологии связи!), но главный принцип меняться не будет: *одно* внешнее подключение будет обеспечивать доступ к Интернету, а по всем остальным подключениям компьютеры и устройства могут общаться между собой и выходить во внешнюю сеть через компьютер, который это внешнее подключение поддерживает.

> ***Примечание***
>
> Следует отметить, что в большинстве случаев идеалом, все же, является использование аппаратных маршрутизаторов различных типов — кабельных или беспроводных, с встроенным ADSL-модемом или Ethernet-портом WAN[1]. Это позволяет значительно упростить конфигурирование сети и обеспечить гибкость в подключении устройств. Стоимость маршрутизатора конечно выше, чем цена коммутатора, но вполне компенсируется удобством в работе. Пример использования маршрутизатора показан на рис. 3.2.

Можно также рассмотреть пример с использованием *беспроводных* технологий (рис. 2.19). Здесь центральный компьютер соединяется с Интернетом через 3G-модем (связь с оператором мобильной связи) — это внешнее подключение. Соединение может выполняться и по Wi-Fi, и даже через мобильный телефон, подключенный к Bluetooth-адаптеру. Центральный компьютер также имеет внутреннее подключение через адаптер Wi-Fi, обслуживающий все устройства локальной сети (посредством ad-hoc подключений, которые подробно описаны в *главе 3*). Вместо этого адаптера можно было бы использовать и точку доступа (WAP), подключенную к центральному компьютеру по кросс-кабелю или через Ethernet-коммутатор. Принцип конфигурирования подключений центрального компьютера от этого не изменился бы (хотя такая конфигурация будет и несколько сложнее в настройке за счет дополнительного конфигурирования точки доступа).

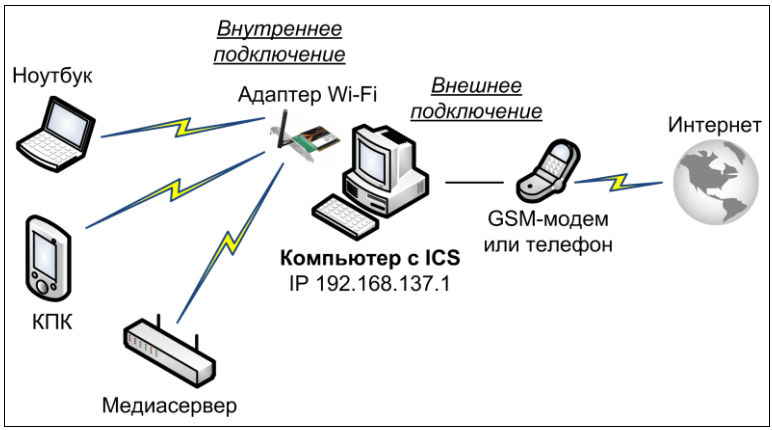

Рис. 2.19. Пример беспроводной сети, использующей общее подключение к Интернету

[1] Wide-Area Network — глобальная сеть; так часто маркируют на устройствах подключение к Интернету или внешней сети.

При разрешении совместного использования внешнего подключения компьютер с ICS становится DHCP-сервером для всей локальной сети, динамически выделяя компьютерам IP-адреса при запуске систем — для этого все клиенты сети должны быть настроены на автоматическое получение параметров IP (этот режим обычно задается сразу при установке систем). Помимо этого, центральный компьютер выполняет функции кэширующего DNS-сервера, осуществляя разрешение имен для клиентов "своей" сети (при этом используются параметры внешнего подключения и DNS-серверы интернет-провайдера). Поэтому при анализе параметров TCP/IP на клиентских компьютерах видно, что IP-адрес компьютера с ICS указывается в качестве основного шлюза, DHCP-сервера и DNS-сервера (см. рис. 2.18).

ВНИМАНИЕ!

Операция разрешения общего доступа к подключению к Интернету довольно ответственна, поскольку влияет на существующие сетевые параметры компьютера и требует изменения настроек протокола IP у клиентов локальной сети. Когда разрешается совместное использование подключения, сетевой адаптер, связанный с локальной сетью, получает новый статический IP-адрес — ***192.168.137.1***[1]. Соответственно должны быть изменены сетевые настройки всех клиентов (при этом может потребоваться их перезагрузка или разрыв и восстановление подключений). Поэтому данную операцию следует выполнять в самом начале работы, при развертывании сети. При этом требуются полномочия администратора.

Подключение и настройка ADSL-модема

ADSL-модемы являются распространенным средством для подключения к Интернету по обычной телефонной линии. Рассмотрим подробно подключение к компьютеру такого устройства и разрешение общего доступа через это соединение. Многие операции и принципы настройки применимы и при подключении других устройств[2].

Для установки драйверов и дополнительных сервисных программ обычно используется установочный диск, предоставляемый интернет-провайдером вместе с устройством. Здесь важно то, что при подключении провайдеры используют различные протоколы и способы авторизации клиента (иногда она не требуется, а иногда нужна — в таких случаях связь осуществляется посредством автоматически создаваемого коммутируемого подключения с указанием имени пользователя и пароля). Поэтому все требуемые параметры лучше вводить не вручную, а воспользоваться программой-мастером (рис. 2.20). В данном примере важно, что модем устанавливается как сетевое устройство без авторизации (подключение по локальной сети);

---

[1] В предыдущих версиях Windows использовался адрес 192.168.0.1. Маска подсети та же самая — 255.255.255.0.

[2] Некоторые из последующих разделов могут показаться сложными на первый взгляд, но если самостоятельно проверить все описываемые действия, то смысл будет вполне понятен. Тут ничего не поделаешь — без понимания затронутых вопросов сеть с несколькими компьютерами и доступом к Интернету сложно будет настроить правильно или в соответствии с нужными требованиями.

при этом задаются важные для связи параметры, например, тип инкапсуляции пакетов.

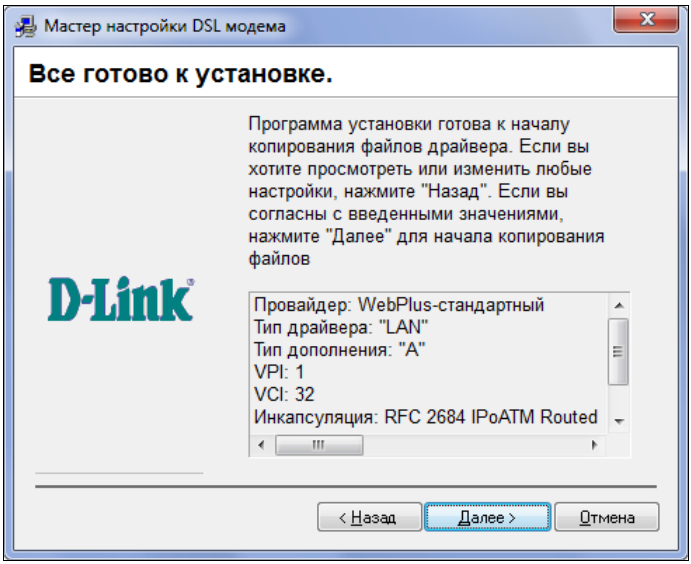

Рис. 2.20. Просмотр параметров модема, используемых для подключения к провайдеру

После установки драйверов необходимо физически подключить модем к компьютеру (к USB порту). При этом в области уведомлений появится стандартное сообщение Windows об установке устройства и мигающий значок  , указывающий статус модема при наведении на него курсора мыши (при отсутствии модема или сигнала значок красный, при установке связи он желтый, а в процессе работы зеленый и мигает при передаче данных). Затем требуется перезагрузка компьютера, и нужно дождаться сообщения программы установки об успешном завершении операции. Если все нормально, то можно переходить к настройке модема.

В окне сетевых подключений (см. рис. 1.13) для модема появится значок подключения — для большей наглядности переименуем стандартное название "Подключение по локальной сети 2" в более понятное "ADSL" (рис. 2.21, *слева*). Изначально сеть, использующая подключение по модему, обозначается как *неопознанная обще-*

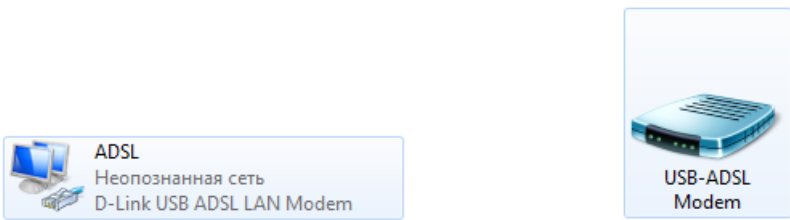

Рис. 2.21. Значки сетевого подключения ADSL-модема *(слева)*
и его изображение в окне устройств, подключенных к компьютеру *(справа)*

ственная сеть. В окне **Устройства и принтеры** (Devices and Printers) (см. рис. 3.24), которое можно открыть прямо из меню **Пуск** (Start), для модема также появится свой значок (рис. 2.21, *справа*), в контекстном меню которого имеются команды, позволяющие обращаться к настройкам устройства.

Подключенный модем пытается установить ADSL-соединение (при этом значок мигает и в статусе видно слово *Training*[1]) и подключиться к сети провайдера. Если все нормально, то соединение должно установиться, но подключиться к провайдеру модем не может, потому что ему не заданы параметры TCP/IP. В окне сетевых подключений нужно найти значок модемного подключения (см. рис. 2.21, *слева*) и открыть окно свойств (рис. 2.22, *слева*). Для подключения к провайдеру требуется только протокол IPv4, флажки остальных компонентов можно сбросить.

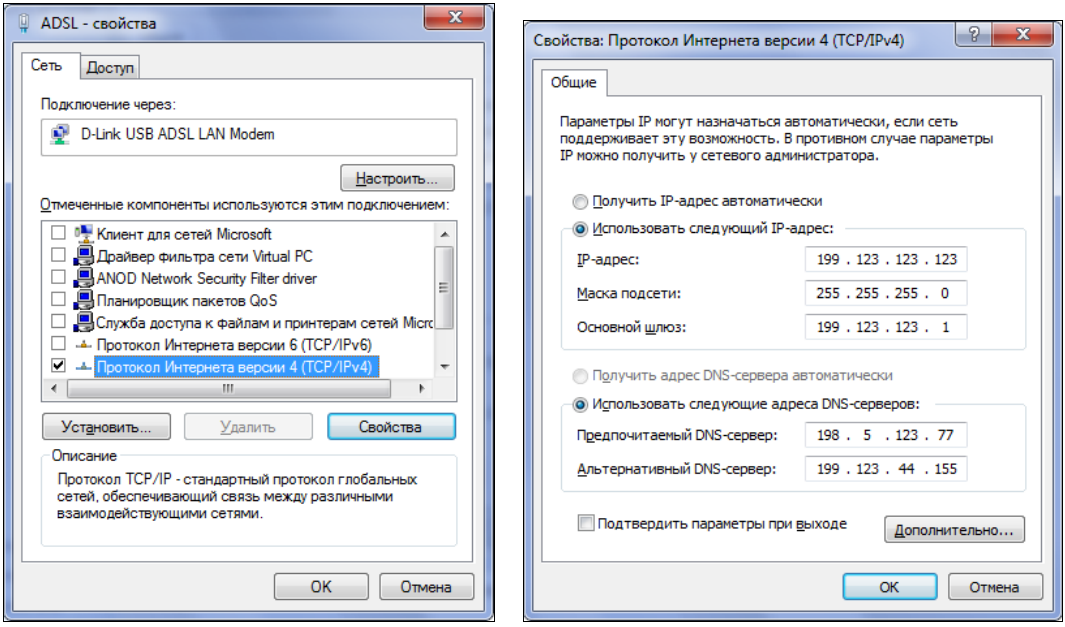

Рис. 2.22. Используемые сетевые компоненты и параметры протокола IP для ADSL-подключения[2]

В окне свойств протокола (см. рис. 2.22, *справа*) нужно ввести параметры, полученные от провайдера. Частный IP-адрес выделяется из пространства адресов внутренней локальной сети провайдера (например, из подсети класса C 192.168.x.x) или же адрес может быть публичным (видимым в Интернете), если эта услуга оплачена дополнительно или входит в выбранный клиентом тарифный план. Провайдер предоставляет IP-адрес, маску, адрес основного шлюза и адреса DNS-серверов (обычно

[1] Этот термин означает согласование режимов работы устройств (обычно — модемов различных типов) и параметров связи при установке соединения между ними.

[2] Адреса фиктивные, но вполне "правдоподобные" и согласованные (внешний IP-адрес и адрес шлюза располагаются в одной подсети!).

их два, для отказоустойчивости). Если используется частный адрес, то также задаются параметры прокси-сервера, которые нужно указать в настройках веб-браузера для локальной сети.

После ввода параметров TCP/IP связь с провайдером должна быть установлена, и это легко проверить, запустив браузер и обратившись к какому-нибудь веб-сайту.

Теперь в окне центра управления сетями (см. рис. 1.7) можно изменить название и значок сети, подключенной через ADSL-модем[1]. Если домашней компьютер не подключен к локальной сети, то подключение по локальной сети (связанное с LAN-адаптером) можно вообще отключить в окне сетевых соединений (см. рис. 1.13). В случае отсутствия локальной сети[2] сетевая конфигурация может выглядеть следующим образом (рис. 2.23). Аналогичная картина получится и в том случае, если доступ к Интернету будет осуществляться по сети Wi-Fi или с помощью 3G-модема — меняться будут только тип подключения и название сети.

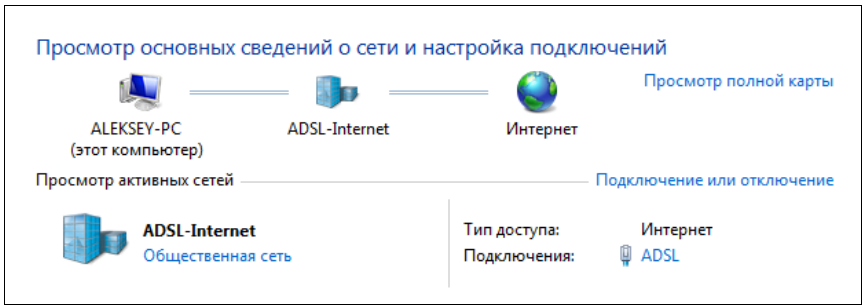

Рис. 2.23. Сетевая конфигурация в окне центра управления сетями при использовании единственного подключения

Таким образом, с одним адаптером сеть на одном компьютере настраивается достаточно легко, сложности начинаются при подключении к Интернету сети из нескольких компьютеров. Здесь немалую роль играют особенности реализации сетевых функций в Windows 7, поэтому с двумя следующими разделами нужно хорошо разобраться.

Особенности работы с несколькими сетевыми подключениями

Если LAN-адаптер разрешен, но сетевой кабель не подключен к коммутатору, то команда `ipconfig` сообщает, что "Среда передачи недоступна" и параметры подключению по локальной сети не назначаются (оно не видно в окне центра управления сетями). По умолчанию настройки TCP/IP назначаются автоматически от DHCP-сервера, поэтому при подключении сетевого кабеля адаптер пытается найти такой сервер и получить от него параметры. Если это не удается, то подключение

[1] Это делать вовсе необязательно, просто полезно для большей наглядности и удобства в работе.

[2] Если LAN-адаптер отключен или если просто сетевой кабель не подключен к нему.

по локальной сети получает так называемый APIPA-адрес *(см. ранее разд. "Выбор параметров")* из подсети 169.254.0.0 с маской 255.255.0.0. Связанная с этим адаптером активная сеть идентифицируется как *неопознанная общественная сеть* (public network) (рис. 2.24). Компьютер сможет выходить в Интернет через ADSL-модем.

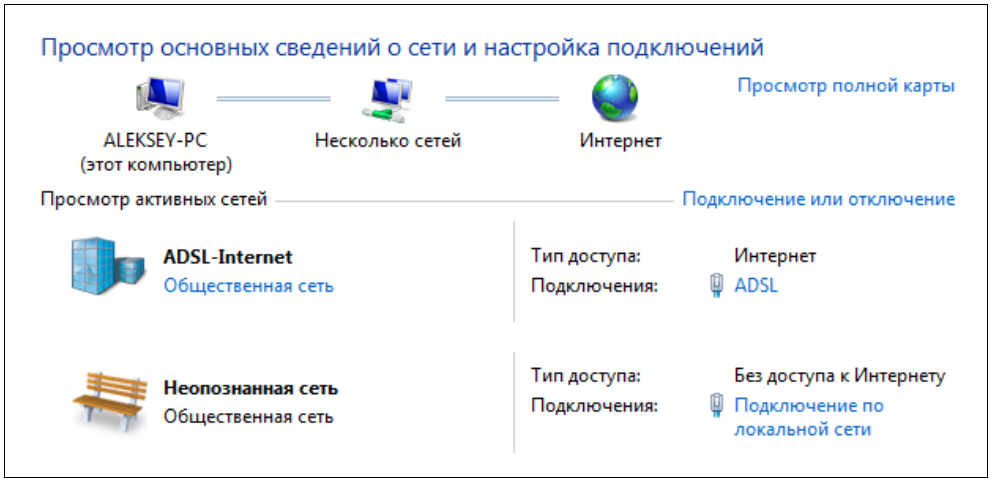

Рис. 2.24. Сетевая конфигурация при использовании ADSL-модема и LAN-адаптера

Примечание

Не нужно обращать внимание на то, что для подключения по локальной сети указано "Без доступа к Интернету": это объясняется тем, что у этого подключения не указан (и не может быть указан!) адрес шлюза и, как следствие, система не может выполнить нужные проверки через это подключение[1]. Сам компьютер обращается к Интернету через ADSL-подключение, все клиенты сети тоже будут работать через это же подключение — так что проблем никаких!

Если даже назначить подключению по локальной сети статический IP-адрес, то сеть останется неопознанной, поскольку подключению нельзя назначить адрес шлюза (обязательное требование для идентификации сети!) — шлюз уже указан в свойствах ADSL-подключения, а два шлюза в Windows 7 задавать нельзя. На компьютере с одним LAN-адаптером все проще: можно указать адрес шлюза, соответствующий выбранной подсети (192.168.0.1 и 192.168.1.1), и размещение сети можно изменить на *рабочую сеть* (work network).

Если нескольким компьютерам в проводной локальной сети назначить статические адреса с указанием шлюза (шлюз будет отсутствовать на компьютере с ADSL-модемом), то компьютеры смогут "видеть" друг друга и общие ресурсы (однако доступ к Интернету будет иметь только компьютер с ADSL-подключением!). Только перед этим нужно переключить тип сети для LAN-адаптера компьютера с под-

[1] Такова специфика работы механизма обнаружения сетей *Network Location Awareness* (Осведомленность о местоположении сети).

ключенным ADSL-модемом (иначе сетевое обнаружение[1] будет невозможно, а включать его для общественной сети нежелательно по соображениям безопасности). Напрямую это сделать нельзя, и нужно применить следующее обходное решение.

Для изменения размещения общественной сети откройте окно Проводника и обратитесь к папке **Сеть** (Network). При появлении информационного сообщения (см. рис. 1.3) разрешите сетевое обнаружение и общий доступ. При появлении запроса на подтверждение операции (см. рис. 1.24) укажите, что хотите сделать сеть частной. Тип локальной сети изменится на *Рабочая сеть* (Work network) (рис. 2.25), и станет возможной совместная работа компьютеров: общие ресурсы данного компьютера будут видны в сети.

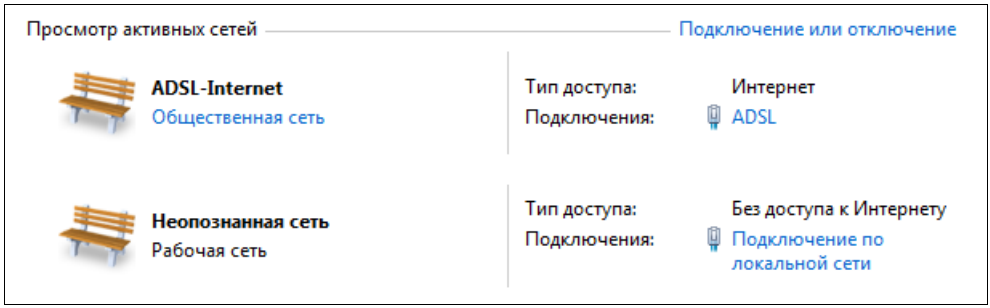

Рис. 2.25. Модифицированная конфигурация, обеспечивающая клиентам доступ к Интернету и позволяющая им видеть компьютер с ICS и его общие ресурсы

Это решение дает два негативных побочных эффекта:

- меняется сетевое размещение и для ADSL-подключения (при этом "теряется" и значок сети, если он задавался индивидуально), и его снова нужно переключить на *общественную сеть*;
- после перезагрузки компьютера все вернется к исходному состоянию, показанному на рис. 2.24 (при этом значок ADSL-подключения снова будет стандартным — изображение скамейки), и настройки сети потребуется опять менять вручную.

> ***Внимание!***
>
> Устранить описанные выше побочные эффекты можно с помощью политик диспетчера списка сетей, описанных *в следующем разделе*.

Из всего сказанного выше можно сделать вывод, что использование домашней группы (HomeGroup) в такой конфигурации невозможно, поскольку нельзя выбрать размещение *Домашняя сеть* (Home network). Правда, домашнюю группу можно организовать на *других* компьютерах, входящих в локальную сеть.

[1] См. также *разд. "Настройка сетевого доступа к общим папкам и принтерам" главы 1*.

Управление сетевым размещением с помощью политик

Как было рассказано в предыдущем разделе, в некоторых ситуациях автоматический выбор сетевого размещения для сетей, связанных с различными подключениями, может создавать проблемы и неудобства. Частично эти вопросы можно разрешить с помощью *Политик диспетчера списка сетей* (Network List Manager Policies). Расскажем на примере двух сетевых подключений, описанных выше, как избавиться о необходимости ручного восстановления нужных размещений (категорий сети).

Для запуска редактора политик безопасности введите `secpol.msc` в поле поиска меню **Пуск** (Start). Нам нужна папка **Политики диспетчера списка сетей** (Network List Manager Policies), показанная на рис. 2.26. Помимо трех стандартных политик, перечисленных внизу списка, здесь отображаются имена всех ***активных*** и ***распознанных***[1] в данный момент сетей (включая сети по локальному подключению), для которых также можно задать индивидуальные настройки.

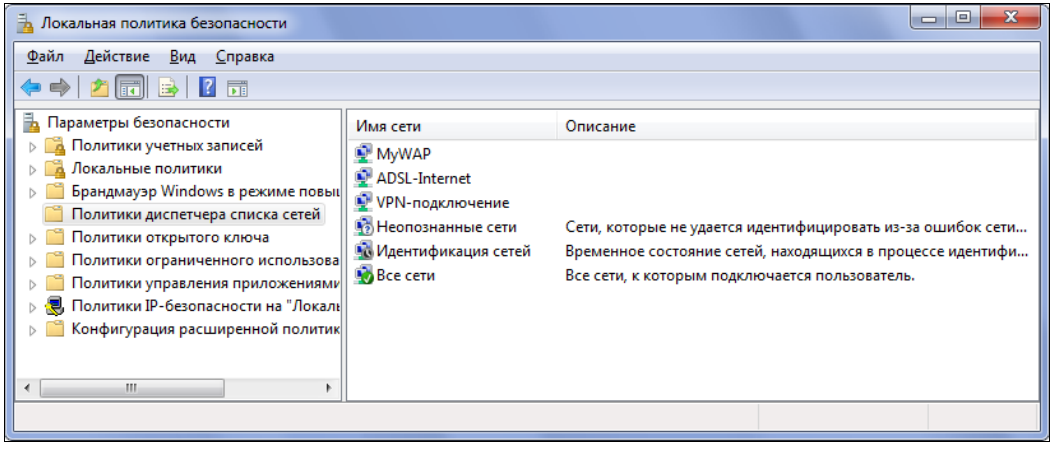

Рис. 2.26. Политики диспетчера списка сетей

Разобраться с использованием указанных политик не так сложно, если понятны проблемы, возникающие при использовании нескольких сетевых подключений. Для этого достаточно лишь внимательно прочитать предыдущий раздел. Для краткости мы не будем рассматривать *все* имеющиеся возможности (они и так понятны, если открыть окна свойств политик), перечислим лишь настройки, позволяющие избавиться от ручного восстановления параметров при использовании ADSL-модема и подключения по локальной сети.

Все политики для ADSL-подключения показаны на рис. 2.27. Выбраны самые "жесткие" ограничения: пользователь не сможет менять заданное имя сети, вы-

[1] То есть таких, для которых не указано "Неопознанная сеть".

бранный значок и заданное (общее) расположение сети (т. е. это всегда будет *Общественная сеть* (Public network)).

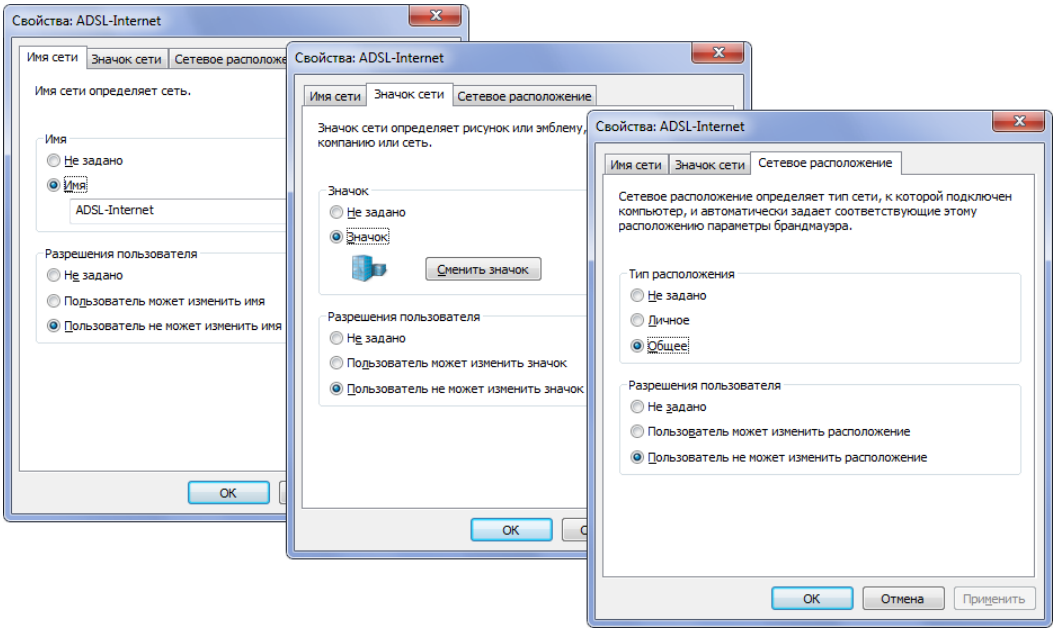

Рис. 2.27. Политики для ADSL-подключения

Самыми важными для нас являются политики для *неопознанных сетей* (Unidentified Networks). В окне свойств политики (аналогичное окно показано на рис. 2.27, *справа*) выберем *личное* (Private) расположение (соответствует *Рабочей сети* (Work network)) и запретим пользователю *изменять расположение* (User cannot change location) (он все равно не сможет это делать, поскольку тип расположения задан явно). Значок для сети задается стандартный, и его менять нельзя.

Теперь после перезагрузки мы будем сразу получать требуемую рабочую конфигурацию подключений, изображенную на рис. 2.25 (только значки будут другими — как было задано в политике на рис. 2.27 и стандартный значок ). Таким образом, необходимость в ручной настройке размещений полностью устранена.

> ***Внимание!***
> Проблема с невозможностью использования домашней группы (HomeGroup), к сожалению, остается, поскольку для нее в обязательном порядке требуется размещение *Домашняя сеть* (Home network), которое с помощью данных политик установить невозможно.

Разрешение общего доступа к Интернету

Заключительным этапом настройки компьютера, имеющего ADSL-модем и подключенного к локальной сети, является обеспечение доступа к Интернету остальным членам сети — этому вопросу и посвящен данный раздел.

Чтобы разрешить совместное использование некоторого подключения[1] (Internet Connection Sharing, ICS), необходимо выбрать его в окне сетевых подключений (см. рис. 1.13), открыть окно свойств и на вкладке **Доступ** (Sharing) (рис. 2.28) установить флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера** (Allow other network users to connect through this computer's Internet connection). Если на компьютере кроме ADSL-модема и подключения по локальной сети имеются и другие сетевые подключения, то в данном окне появляется список **Подключение домашней сети** (Home networking connection), и в нем нужно выбрать подключение, которое станет внутренним для создаваемой конфигурации (см. примеры на рис. 2.18 и 2.19) — это может быть и беспроводное подключение. По умолчанию другие пользователи сети могут управлять общим подключением.

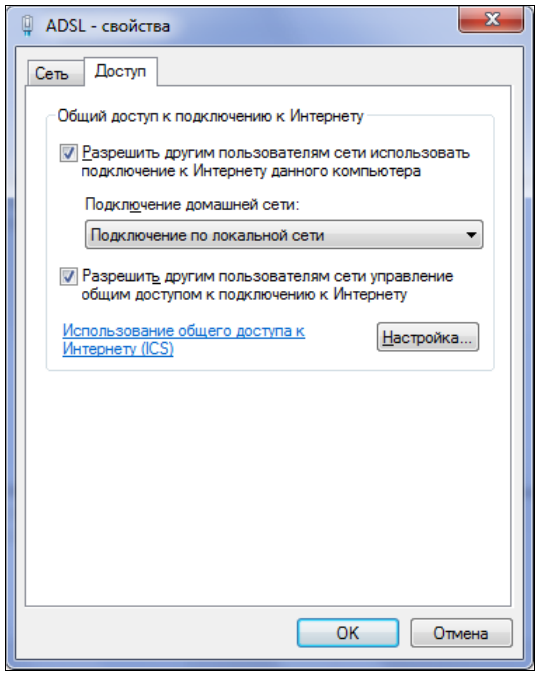

Рис. 2.28. Включение общего доступа к Интернету на выбранном сетевом подключении

При включении общего доступа появляется предупреждение об изменении сетевых настроек (рис. 2.29). Как можно видеть, перемены в сети достаточно серьезные. Если отказаться от продолжения операции, то никакие изменения вноситься не будут, и общий доступ включить не удастся.

Новые сетевые параметры на компьютере с ICS и клиентах сети легко увидеть с помощью команды `ipconfig /all`. В частности, она покажет, что центральный компьютер получил новый IP-адрес (рис. 2.30) (он всегда одинаковый при включении ICS!):

[1] Данная процедура выполняется одинаково для *любых* коммутируемых и VPN-подключений.

```
IPv4-адрес. . . . . . . . . . . . : 192.168.137.1(Основной)
Маска подсети . . . . . . . . . . : 255.255.255.0
```

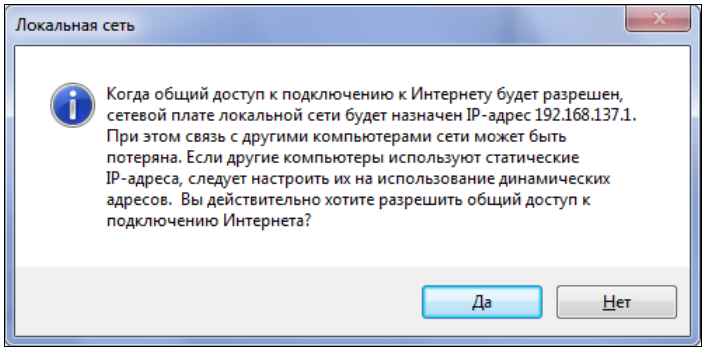

Рис. 2.29. Предупреждение об изменении сетевых настроек при включении общего доступа к Интернету

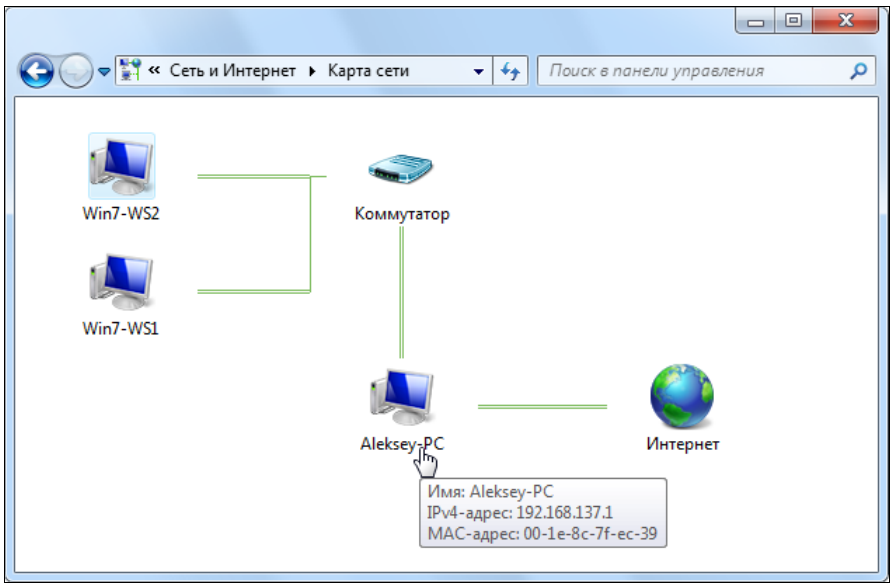

Рис. 2.30. Карта сети для клиента, подключенного к Интернету через компьютер с ICS

Клиенты получают настройки автоматически и имеют следующие параметры:

```
Ethernet adapter Подключение по локальной сети:
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   IPv4-адрес. . . . . . . . . . . . : 192.168.137.140(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.137.1
   DHCP-сервер. . . . . . . . . . . : 192.168.137.1
   DNS-серверы. . . . . . . . . . . : 192.168.137.1
```

Обратите внимание на то, что в качестве адреса шлюза, DHCP-сервера и DNS-сервера указан один и тот же адрес — IP-адрес центрального компьютера. Теперь все клиенты также получают доступ к Интернету через этот компьютер, что видно на карте сети (см. рис. 2.30).

По состоянию ADSL-подключения в окне сетевых подключений (см. рис. 1.13) сразу видно, что для него разрешен общий доступ к Интернету — на это указывает метка "Общедоступно" (Shared) (рис. 2.31).

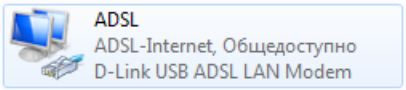

Рис. 2.31. Значок сетевого подключения ADSL-модема при разрешении общего доступа к Интернету

Внимание!

Напомним, что после перезагрузки компьютера с ICS для внутреннего (LAN) подключения опять будет установлено размещение *общественная сеть*, и компьютер не будет виден в сети. Поэтому сетевое обнаружение и общий доступ нужно снова включать вручную. При этом клиенты сразу получают нормальный доступ к Интернету и могут работать друг с другом — их сетевое размещение не затрагивается и сохраняется таким, как было задано ранее. Автоматическое изменение размещений можно ограничить с помощью политик безопасности, описанных *в предыдущем разделе*.

Дополнительные настройки

Если требуется, чтобы выбранное подключение автоматически активизировалось, когда другой компьютер локальной сети пытается обратиться к внешним ресурсам (а это, в первую очередь, имеет смысл для коммутируемых и VPN-подключений), в окне свойств подключения на вкладке **Доступ** (Sharing) (см. рис. 2.28) установите также флажок **Устанавливать телефонное подключение при попытке доступа к Интернету** (Establish a dial-up connection...). Этот флажок появляется только у подключений, устанавливаемых по запросу (коммутируемых и VPN).

При разрешении общего доступа к Интернету можно указать конкретные приложения и службы, к которым смогут обращаться пользователи из Интернета или из внешней сети (если такие службы имеются). Например, если в локальной сети на центральном или другом компьютере имеется FTP-или веб-сервер, то для того, чтобы с ним могли работать извне, нужно на совместно используемом подключении разрешить соответствующую службу. Для этого на вкладке **Доступ** (Sharing) (см. рис. 2.28) следует нажать кнопку **Настройка** (Settings) и в открывшемся окне (рис. 2.32) установить флажки рядом с именами служб, которые должны быть доступны. (Это можно делать сразу при разрешении доступа или в процессе дальнейшей работы.)

При установке флажка появляется дополнительное окно с параметрами службы (см. рис. 2.32), где можно указать имя или адрес компьютера, на котором установлены эти службы. Если какой-то службы в списке нет (например, для входящих

VPN-подключений нужно открыть TCP-порт 1723), то ее можно добавить вручную, указав имя, адрес компьютера и используемые порты TCP/UDP[1].

Примечание

Если включен доступ к домашней библиотеке мультимедиа через Интернет, то в списке разрешенных служб появляются также записи для служб потокового вещания.

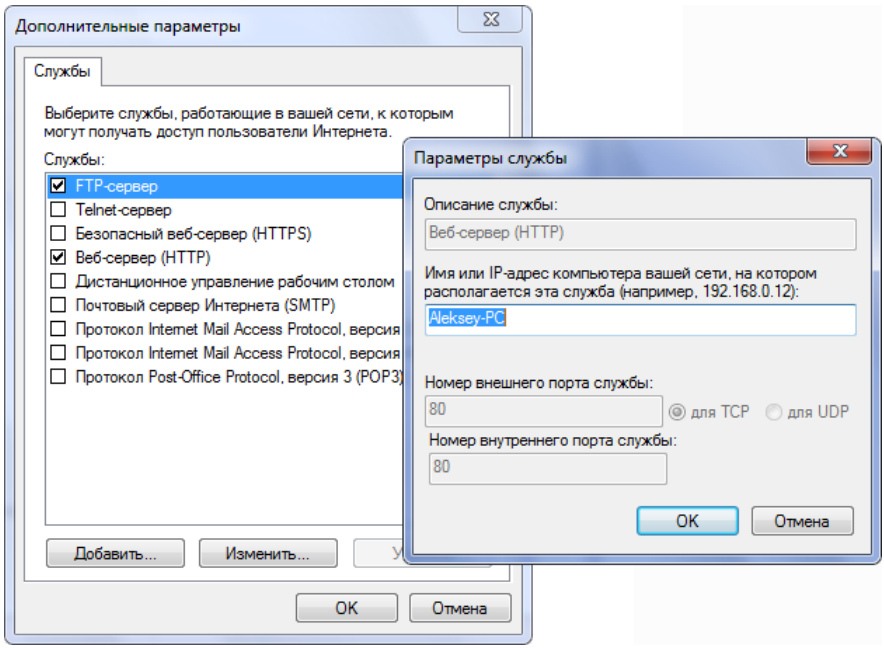

Рис. 2.32. Выбор сервисов, к которым будет разрешен доступ для пользователей Интернета

[1] См. первое примечание в *разд. "Виртуальные частные сети (VPN)"*.

ГЛАВА 3

Организация беспроводной сети

В предыдущей главе рассказывалось о том, как создать саму основу любой сети — соединения между компьютерами, а также о особенностях использования нескольких сетевых подключений. По сути, в настоящей главе эта тема будет продолжена, и мы рассмотрим все многообразие беспроводных сетей, которые используются как для создания домашней сети, так и для временного подключения электронных устройств или переносных компьютеров. Для работы с некоторыми видами беспроводной связи (Bluetooth, передача через ИК-порты и т. д.) используются свои, нестандартные средства с особым пользовательским интерфейсом.

Последующие главы уже никак не будут связаны с конкретными технологиями и используемым оборудованием, и в них будут рассматриваться средства, работающие уже "поверх" существующей сетевой инфраструктуры.

Типы беспроводных сетей Wi-Fi и аппаратные средства

Для работы с беспроводными сетями Wi-Fi необходимо познакомиться с некоторыми терминами, характеристиками и принципами, без которых сложно будет ориентировать в реальной ситуации. Таких сведений больше, чем при работе с обычными кабельными сетями[1] (там LAN-порт (адаптер), коммутатор, кабели — практически все оборудование), поэтому из этой неисчерпаемой темы мы выберем самую важную информацию, необходимую для работы и дальнейшего изложения.

Общие понятия. Типы безопасности и шифрования

Базовые стандарты для беспроводных сетей, получивших название *wireless fidelity* (Wi-Fi), были разработаны Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) и имеют общее название

[1] Если требуются более подробные сведения, то их легко можно найти в книгах, указанных в *списке литературы*, а также в Интернете.

802.11. О беспроводных сетях можно говорить долго и много, но с практической точки зрения наиболее важны два вопроса:

- методы проверки подлинности и шифрования;
- используемые стандарты сетей.

Любое сетевое соединение должно быть защищено и устанавливаться с тем лицом, который имеет на это право и может подтвердить свою идентичность.

Устаревшим и не рекомендуемым протоколом является *WEP* (Wired Equivalent Privacy). Его можно применять только в крайнем случае для связи со старыми устройствами.

Предпочтительнее использовать *Wi-Fi Protected Access* (WPA и WPA2), и чем выше уровень защиты (WPA2), тем лучше.

Протокол *802.1x (RADIUS)* требует наличия сервера для проверки подлинности, поэтому применяется только в корпоративных сетях, как и методы WPA-Enterprise и WPA2-Enterprise. Для домашних сетей достаточно использовать WPA-Personal и WPA2-Personal, где всем пользователям сети дается одинаковый *ключ* (security key).

Для шифрования каналов связи используются два метода:

- *Advanced Encryption Standard* (AES), который пришел на смену стандарту Data Encryption Standard (DES);
- стандарт *Temporal Key Integrity Protocol* (TKIP), используемый в беспроводных сетях 802.11.

При создании профилей сетей и подключений "компьютер-компьютер" *(см. далее)* можно пользоваться параметрами безопасности и шифрования, предлагаемыми по умолчанию. Настройка параметров необходима лишь в тех случаях, когда требуется их согласование с другим оборудованием или связь с устаревшими устройствами (например, предлагаемый по умолчанию WPA2-Personal для создания прямых подключений может не поддерживаться клиентами, пытающимися подключиться к компьютеру, и тогда уровень шифрования нужно понижать).

Команда `netsh wlan show drivers` покажет возможности используемого драйвера беспроводного соединения (обратите внимание на то, что в режиме прямого подключения (ad-hoc) методы проверки подлинности и шифрования слабее!), а команда `netsh wlan show all` позволит увидеть параметры безопасности доступных сетей. Эту информацию можно учитывать в дальнейшем для настройки подключений.

Имя сети (SSID)

Ключевым понятием для беспроводных сетей стандарта 802.11 является *имя сети*, или Service Set Identifier (SSID), которое может иметь длину до 32 символов. Каждая *точка доступа* или активное соединение сети "компьютер-компьютер", ожидающее входящих подключений, посылает широковещательные посылки, сообщающие ее имя. Клиенты могут по имени выбирать нужную точку доступа или

хотспот (hotspot — точка доступа в общественных местах, таких как кафе, гостиницы, вокзалы и т. п.) и подключаться к ней. Для подключения используется *ключевое слово* (security key), а в открытых сетях достаточно лишь выбрать сеть и подключение осуществляется сразу же.

Принцип *широковещания имени*, SSID (SSID Broadcast) создает определенные проблемы, связанные с безопасностью сети. Некоторые точки доступа не выполняют широковещания имени, поэтому не могут быть обнаружены путем сканирования — к ним можно подключиться, только зная точное имя. Эти соображения также важны при настройке точки доступа и подключений (профилей сети).

Стандарты сетей Wi-Fi

В настоящее время используются четыре основных стандарта: 802.11a, 802.11b, 802.11g и 802.11n. Каждый из них рассчитан на определенное допустимое расстояние между соединяемыми точками и на определенную максимальную скорость. Устройства сетей Wi-Fi обычно поддерживают несколько стандартов и могут работать на разных скоростях, в зависимости от реальной ситуации и имеющегося оборудования. Старые устройства работали со стандартами 802.11a и 802.11b, современные обычно поддерживают 802.11b и 802.11g и нередко к ним добавляется 802.11n. Информация о реализованных в устройствах стандартах важна при выборе оборудования (для обеспечения совместимости); кроме того, более скоростные устройства обычно дороже, и это также следует учитывать.

802.11b

Исходный стандарт 802.11, опубликованный институтом IEEE в 1997 году, предполагал максимальную скорость всего 2 Мбит/с. В 1999 году были разработаны два новых стандарта 802.11a и 802.11b, из которых второй получил наибольшее распространение. Он обеспечивает скорости передачи данных до 11 Мбит/с и удаленность для помещений порядка 35 м. Рабочая частота — 2,4 ГГц.

802.11a

Имеет скорость передачи до 54 Мбит/с и использует радиочастоту 5,0 ГГц. Допустимое расстояние около 22 м, при этом возникает большое затухание сигнала в помещениях, обусловленное высокой рабочей частотой. По этим причинам и из-за значительной стоимости оборудования, несмотря на большую скорость, данный стандарт уступил в популярности стандарту 802.11b.

802.11g

Предложен в 2003 году и объединяет в себе лучшие стороны стандартов 802.11b и 802.11a. Имеет теоретическую максимальную скорость передачи 54 Мбит/с и работает на расстояниях до 35 м (в помещениях). Рабочая частота — 2,4 ГГц, что позволило удешевить производство оборудования, но означает возможность помех со стороны устройств бытовой электроники, работающих на этой же частоте. Несмотря на это, данный стандарт стал одним из самых распространенных и практически все современные устройства Wi-Fi его поддерживают.

802.11n

Утвержден в 2009 году. Ориентирован на значительное повышение полосы пропускания — до 248[1] Мбит/с — за счет технологии мультиплексирования, одновременно использующей несколько приемников и передатчиков в каждом устройстве. Это позволяет организовать в одном устройстве несколько каналов передачи данных, за счет чего значительно повысить его производительность. Такие устройства уже позволят передавать по беспроводной сети видео высокого качества. Необходимо помнить о том, что реальная скорость передачи данных в 2 и более раз меньше, чем рабочая полоса пропускания[2], однако тесты показывают, что устройства 802.11n почти в 5 раз быстрее устройств стандарта 802.11g. Предполагается увеличение зоны охвата до 70 м. Для работы подобных устройств необходимо уже несколько передающих/приемных антенн. Пока этот стандарт только внедряется в широкую практику.

Устройства для сетей Wi-Fi

В настоящее время выпускается множество устройств различного назначения для работы в сетях Wi-Fi — от адаптеров до маршрутизаторов и принт-серверов. Конечно, рассматривать их все вряд ли целесообразно в рамках этой книги, однако *базовые* типы устройств следует упомянуть, тем более что они постоянно и часто упоминаются далее в этой главе и в других разделах книги.

Центральным связующим звеном сети Wi-Fi обычно является аппаратная *точка доступа* или *маршрутизатор*[3] с поддержкой Wi-Fi (рис. 3.1). (Точку доступа также можно создать и программно, используя адаптер Wi-Fi, поддерживающий эту функцию, и встроенные средства Windows 7 или специальные программы — *см. далее разд. "Виртуальные сети Wi-Fi"*.) Строго говоря, различие между точкой доступа и маршрутизатором скорее маркетинговое/организационное, нежели принципиальное/техническое. (Тем более что сейчас самыми продаваемыми устройствами являются маршрутизаторы, и особенно они удобны для организации домашней сети — *см. далее*.)

Точка доступа, как и маршрутизатор, выполняет передачу (маршрутизацию) трафика между компьютерами, подключенными по беспроводному каналу, и разъемом локальной сети Ethernet (LAN). (Вообще, компьютеры могут работать друг с другом через точку доступа и не подключаясь к проводной сети.) Разница лишь в том, что у точки доступа один LAN-порт, а у маршрутизаторов обычно четыре, по-

---

[1] По другим сведениям — до 600 Мбит/с.

[2] Это легко увидеть, просматривая диаграммы и числовые параметры в окне диспетчера задач, если включить столбцы "Пропускная способность отправки/получения", "Отправлено/получено байт в интервале" и др.

[3] Оба этих названия в немалой степени можно считать не техническими, а "коммерческими". У разных производителей маршрутизаторы с дополнительными портами могут называться по-разному; к тому же, точка доступа *всегда* является маршрутизатором. Поэтому здесь важнее понимать суть функций и возможности устройств.

скольку они еще выполняют функцию коммутатора пакетов в локальной сети (для проводного соединения нескольких компьютеров). Точки доступа могут иметь так называемую функцию автоопределения MDI/MDI-X, позволяющую подключать ее к сетевому коммутатору с помощью обычного "прямого" кабеля (патч-корда), а также напрямую соединять с компьютером через специальный кросс-кабель с "перевернутыми" парами сигналов. Прямое подключение необходимо и удобно при начальном конфигурировании точки доступа *(см. далее)*, его можно использовать и в обычной работе.

Маршрутизатор, точка доступа

Внутренний PCI-адаптер Wi-Fi

Переносной USB-адаптер Wi-Fi

Рис. 3.1. Основные типы устройств, используемых для построения сетей Wi-Fi

К особенностям маршрутизаторов можно отнести наличие у многих моделей дополнительных портов связи, помимо канала Wi-Fi (который у некоторых моделей вообще отсутствует). Например, комбинированное устройство помимо нескольких LAN-портов может иметь встроенный ADSL-модем (см. пример на рис. 3.2) или WAN-порт для подключения к кабельному (Ethernet) Интернету. Есть модели, обеспечивающие подключение радио (3G) модема. Между всеми имеющимися портами выполняется пересылка пакетов и маршрутизация связей между подключенными компьютерами или внешними линиями.

Ноутбуки и другие мобильные компьютерные устройства обычно имеют встроенный адаптер Wi-Fi, а в настольных компьютерах применяются внутренние *PCI-адаптеры Wi-Fi* (см. рис. 3.1). С любыми компьютерами и устройствами можно

применять компактные портативные *USB-адаптеры Wi-Fi* (см. рис. 3.1), которые подключаются к обычному USB-порту и выполняются все те же функции, что и другие адаптеры Wi-Fi[1]. Настройка сетевого подключения всегда выполняется одинаково и не зависит от типа используемого устройства. USB-адаптеры нередко применяются для работы с медиасерверами *(см. главу 6)*.

Конфигурация сети Wi-Fi и организация связи между компьютерами

Конфигураций (топологий) локальных сетей может быть довольно много: это объясняется использованием разных типов связи (кабельной и беспроводной), а также наличием (и способом) выхода в Интернет. Мы рассмотрим несколько характерных примеров сетей, где обязательно используется сеть Wi-Fi.

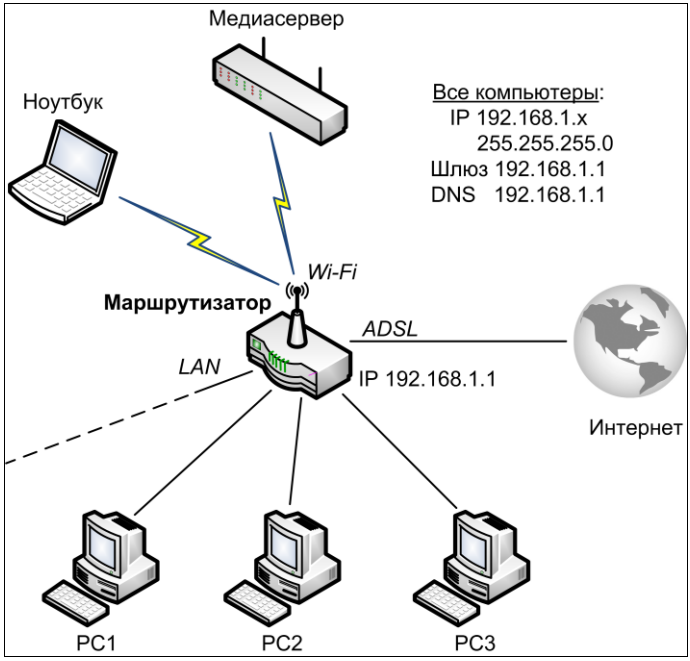

Рис. 3.2. Конфигурация сети с выходом в Интернет

Проще всего построить домашнюю сеть с использованием многофункционального устройства, выполняющего роль маршрутизатора, точки доступа сети Wi-Fi и ADSL-модема для подключения к Интернету. На рис. 3.2 такое устройство названо обобщенно — "маршрутизатор", и оно является центром сетевой инфраструктуры[2]. Вместо ADSL-модема может использоваться WAN-порт для Ethernet-подключения

[1] И все настройки для них будут точно такими же, никакой особой разницы в работе не будет.

[2] Можно сказать, что это классическая *звездообразная топология* сети, где к центральному узлу подключаются все периферийные узлы.

к Интернету или кабельный модем. Маршрутизатор обслуживает компьютеры, подключенные по кабелю (с помощью коммутаторов число клиентов можно увеличивать), а также разнообразные устройства, поддерживающие сети Wi-Fi.

Показанная на рис. 3.2 конфигурация легко настраивается, поскольку все параметры задаются в маршрутизаторе (получаемые значения перечислены на рисунке), а остальные устройства получают сетевые параметры автоматически. Все компьютеры и устройства постоянно связаны между собой и имеют доступ ко всем общим ресурсам и выход в Интернет. Благодаря тому, что все подключения относятся к частной сети ("замыкаются" на маршрутизаторе), не возникает проблем с определением сетевого размещения, и легко организовать домашнюю группу (HomeGroup). Отключение любого компьютера никак не сказывается на коммуникационных возможностях других членов сети.

Примечание

Пример полностью беспроводной сети, использующей общее подключение к Интернету, рассматривался на рис. 2.19. Этот вариант простой и дешевый, и вполне годится для тех случаев, когда выполняется сеансовый доступ к Интернету, а устройства подключаются на непродолжительное время. Центральный компьютер является связующим звеном и должен быть всегда включен для обеспечения коммуникаций между остальными устройствами.

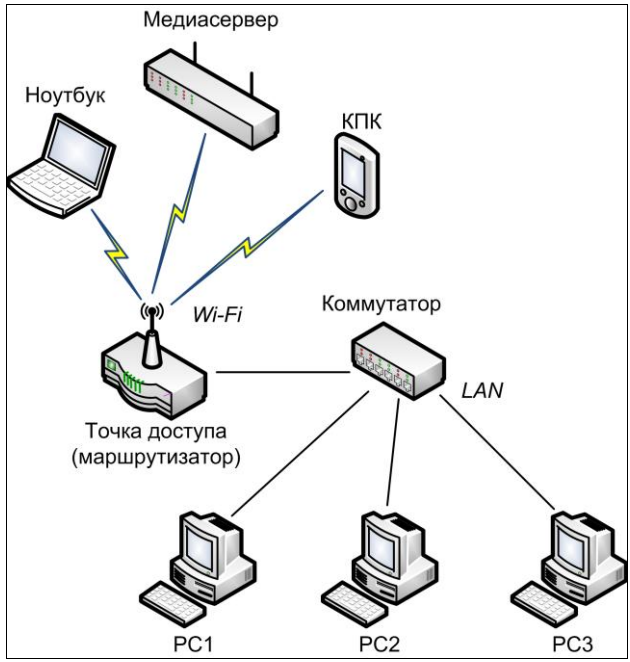

Рис. 3.3. "Закрытая" сеть, имеющая кабельные и беспроводные каналы связи

Для построения простой "замкнутой" (не имеющей выхода в Интернет) сети достаточно взять точку доступа и коммутатор (рис. 3.3). Несложно заметить, что в предыдущем примере (см. рис. 3.2) обе функции выполнял один маршрутизатор, а если

разорвать связь между точкой доступа и коммутатором, то сеть распадется на две подсети: беспроводную и кабельную. Такая конфигурация может быть примером "эволюционного развития" сети из нескольких компьютеров, к которой добавлялись новые устройства и каналы связи. Ее можно развивать дальше, подключив, к примеру, ADSL-модем к одному из компьютеров и сделав это подключение общим для остальной сети. Все члены сети получат, таким образом, доступ к Интернету.

Простым вариантом беспроводного соединения компьютеров и устройств является использование прямых подключений "точка-точка"[1] (рис. 3.4). В терминологии Wi-Fi такие связи называются *ad hoc*[2] *подключениями* или сетями *"компьютер-компьютер"*. Компьютеры на непродолжительное время устанавливают связи друг с другом и на это время могут работать с общими ресурсами или обмениваться данными. Через промежуточный узел возможна связь и между устройствами, не связанными друг с другом напрямую. Например, если показанные на рисунке *Ноутбук* и *Медиасервер* подключены к *Компьютеру*, то они будут "видеть" друг друга, даже если прямой связи между этими устройствами и не будет. Прямые подключения нужно устанавливать вручную, поэтому такая сеть может образовываться только для решения каких-то частных задач.

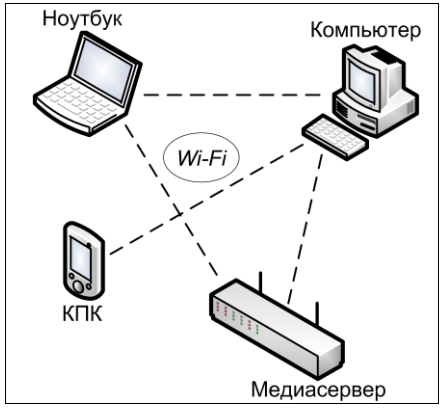

Рис. 3.4. Сеть на основе прямых соединений между устройствами

Конфигурирование точки доступа или маршрутизатора

Устройства могут настраиваться автоматически или вручную. В первом случае нужно следовать инструкциям производителя, и при связи устройства и компьютера все параметры будут выбраны без участия пользователя. Ручная настройка обычно выполняется с помощью веб-браузера, запущенного на компьютере, кото-

[1] Такая топология называется *смешанной*.

[2] Ad hoc — в переводе с латыни "специальный, устроенный для данной цели".

рый нужно напрямую или через коммутатор соединить с LAN-портом устройства. В браузере указывается IP-адрес устройства (например, 192.168.0.1) и вводятся стандартное имя и пароль, указанные в инструкции. После этого выполняется подключение к устройству, и на веб-страницах административного интерфейса можно задавать все нужные параметры.

Для настройки точки доступа обычно необходимо определить следующие основные характеристики (см. также рис. 3.2):

- IP-адрес и маску локальной сети (при изменении стандартного адреса потребуется повторное подключение по новому адресу), IP-адрес шлюза для выхода во внешнюю сеть;
- параметры беспроводной сети:
  - имя точки доступа (сети, SSID) и разрешение/запрет широковещания SSID (SSID Broadcast);
  - способ проверки подлинности (WPA-PSK, WPA2-PSK и т. д.[1]; сеть можно — хотя и не рекомендуется это делать! — оставить открытой: без проверки подлинности и шифрования);
  - ключевое слово (пароль);
- параметры DHCP-сервера (обычно используется):
  - пул IP-адресов и маска;
  - шлюз по умолчанию;
  - DNS-адрес.

На маршрутизаторе адрес внешнего шлюза не указывается, поскольку задаются параметры порта или устройства для подключения к Интернету, а статические маршруты формируются автоматически. Настройки определяются типом дополнительного устройства, и для их выбора нужно использовать программу (мастера) настройки, предлагаемую производителем, или задавать их вручную в соответствии с инструкциями интернет-провайдера. Параметры для беспроводной сети перечислены выше.

Подключение к Wi-Fi-сети или другому компьютеру

Если на компьютере имеется беспроводной адаптер Wi-Fi, то при инсталляции операционной системы для него будут установлены драйверы и создано "Беспроводное сетевое подключение". Как и подключение по локальной сети (для LAN-адаптера)

[1] Чем выше уровень защиты (чем более сложные протоколы), тем лучше; лишь бы эти методы поддерживались используемыми устройствами. Нередко встречающаяся аббревиатура PSK означает Pre-Shared Key — общее название метода шифрования с использованием ключа, известного обеим сторонам. Этот способ чаще всего и используется для доступа к беспроводной сети.

оно сразу же активизируется и готово к работе. Все имеющиеся на компьютере сетевые соединения доступны в окне сетевых подключений, пример которого показан на рис. 3.5. Вид окна, сортировку и группировку значков можно менять по своему вкусу и в соответствии с выполняемыми задачами. На панели задач имеются команды, наиболее употребительные для выбранного подключения (в зависимости от его типа набор команд несколько меняется). Здесь легко видеть состояние подключения и название устройства, с которым оно связано.

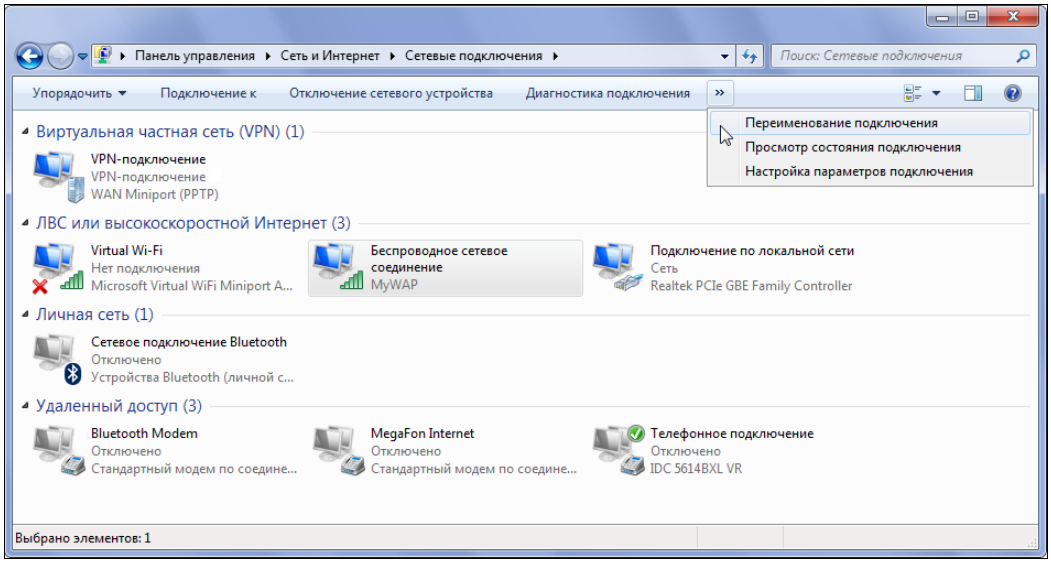

Рис. 3.5. Окно сетевых подключений компьютера, сгруппированных по *типу*

Подключаться к беспроводной сети можно *вручную* или с помощью *профиля сети*. При ручном подключении необходимую информацию нужно каждый раз вводить заново, а при наличии профиля подключение может устанавливаться автоматически или с помощью командного файла *(см. далее)*. Сначала рассмотрим первый вариант, а работе с профилями позже будет посвящен отдельный раздел.

Поскольку беспроводное сетевое соединение по умолчанию активно (включено), то подключение к беспроводной сети (хотспоту) или другому компьютеру с адаптером Wi-Fi (ad hoc подключение или связь "компьютер-компьютер") установить очень просто, буквально в три приема: нужно открыть окно доступных подключений, выбрать сеть и ввести пароль.

Доступные сети и компьютеры представлены в окне активных сетей (см. рис. 1.1) именем (SSID) и значком, отображающим качество принимаемого сигнала и тип безопасности. Отличный сигнал — это пять зеленых "столбиков", чем слабее сигнал, тем зеленого цвета меньше. Если сеть незащищенная, т. е. доступна без пароля, то на значке появляется изображение оранжевого щита с восклицательным знаком  .

Наведя курсор на имя сети, можно получить более подробную информацию о ней. Если выбрать сеть (рис. 3.6) и нажать кнопку **Подключение** (Connect), то для за-

щищенной сети на следующем шаге необходимо будет ввести ключ (security key) для доступа к сети (для открытой сети достаточно лишь нажать кнопку!). Если пароль правильный, то выполняется подключение и новое состояние сети видно в окне сетей ("Подключено").

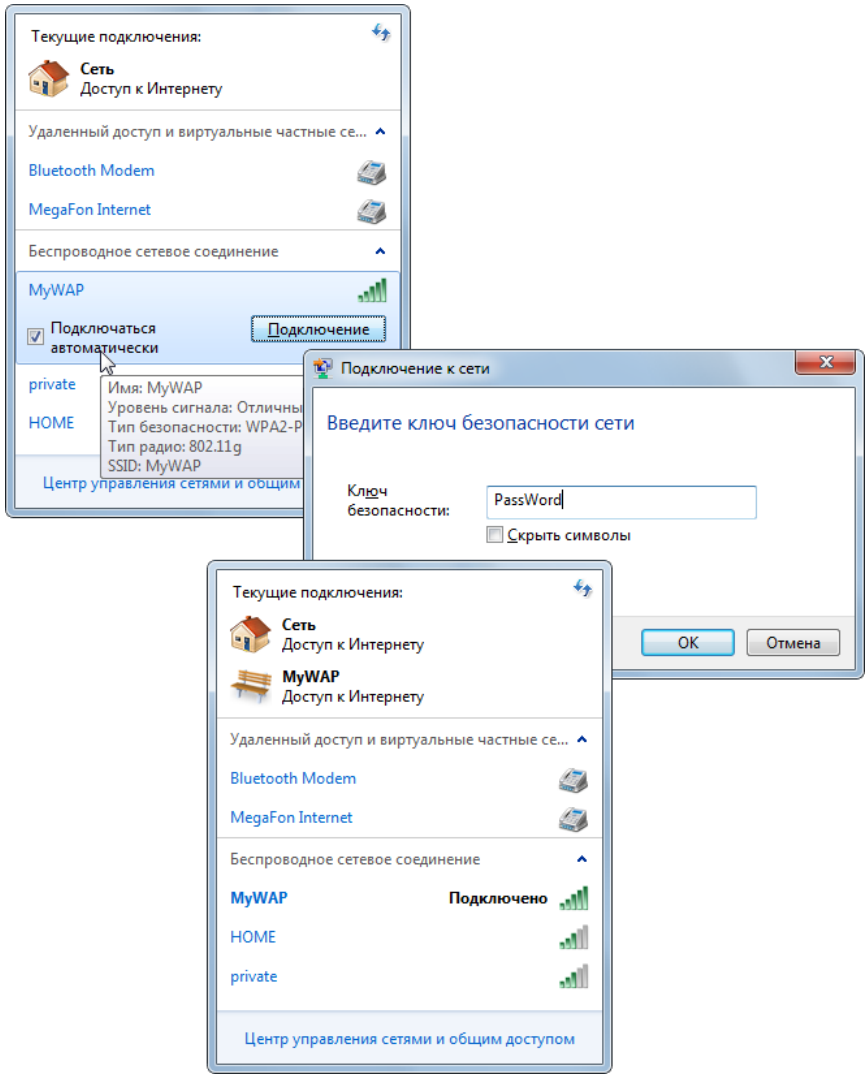

Рис. 3.6. Процедура подключения к доступной беспроводной сети

Первыми в списке доступных сетей всегда идут предпочитаемые сети, т. е. те, для которых имеется профиль и которые в списке сетей (см. рис. 3.13) идут первыми сверху.

"Другие сети" (скрытые сети)

Если точка доступа или хотспот не выполняют широковещания своего SSID, то в списке сетей можно видеть значок с именем "Другие сети" (см. пример на рис. 1.1, *справа*).

В этом случае для подключения к такой сети нужно будет перед вводом пароля (см. рис. 3.6) указать сначала имя (SSID) этой сети или использовать заранее настроенный профиль *(см. далее)*. Имя сети вводится ***с учетом регистра строчных и заглавных букв***!

Наличие флажка **Подключаться автоматически** (Connect automatically) около имени выбранной сети (см. рис. 3.6) означает, что данная сеть работает в режиме инфраструктуры (т. е. это точка доступа — аппаратная или программная) и к ней можно подключаться сразу же, когда эта сеть становится доступной; при этом соединение будет автоматически восстанавливаться в случае прерывания сеанса связи. (Режимы работы *всех* доступных сетей и тип шифрования легко увидеть сразу с помощью команды `netsh wlan show networks` — *см. далее*.) Если значок автоматического подключения не сбросить (а по умолчанию он всегда установлен для точек доступа), то в случае успешного подключения к сети в системе автоматически создается профиль для данной сети (см. рис. 3.13). Поэтому при подключении следует помнить об этом моменте.

Если для некоторой сети значок автоматического подключения отсутствует, то это означает одно из двух: либо для данной сети имеется профиль с сохраненными параметрами и достаточно нажать кнопку **Подключение** (Connect), либо будет выполняться ad hoc соединение с удаленным компьютером (профиль для такого соединения сохраняться не может и последующие подключения нужно будет каждый раз выполнять вручную; автоматическое восстановление прерванного сеанса связи также будет невозможным).

Для новой сети, связанной с установленным подключением, работают все правила выбора сетевого размещения, подробно рассмотренные в *главе 2*. Беспроводное сетевое подключение по умолчанию имеет режим автонастройки, поэтому от точки доступа оно обычно получает параметры рабочей подсети и, как следствие, по этому подключению сразу можно получить доступ к общим ресурсам той сети, к которой подключена точка доступа, и/или выход в Интернет. При установлении соединения "компьютер-компьютер" клиент может получить APIPA-адрес, поэтому сеть определится как *Неопознанная*, и сетевое обнаружение нужно включать вручную *(см. главу 2)*. Если сетевая конфигурация постоянная, то для устранения таких ситуаций можно попробовать задавать статические адреса (исходя из имеющихся параметров подсети).

Настройка соединения между двумя компьютерами (ad hoc подключение)

По сравнению с прямыми подключениями, использование точки доступа (маршрутизатора) дает два преимущества:

- профиль сети можно сохранить или создать заранее и использовать для подключения к сети (вручную или из командного файла);

- возможность автоматического подключения удобна для установки соединения при доступности сети без участия пользователя, а также для восстановления соединения при прерывании сеанса связи.

Прямые соединения между компьютерами — *соединения "компьютер-компьютер"* или *ad hoc подключения* — такими качествами не обладают, их нужно каждый раз устанавливать вручную *(см. предыдущий разд.)*.

Чтобы прямое соединение стало возможным, необходимо сначала настроить *принимающую сторону* — т. е. создать подключение на компьютере, ***к которому*** будут подключаться другие. Для этого используется опция **Настройка беспроводной сети компьютер-компьютер** (Set up a wireless ad hoc (computer-to-computer) network) в окне мастера сетевых подключений (см. рис. 2.1) или кнопка **Добавить** (Add) в окне сетевых профилей (см. рис. 3.13), после нажатия которой следует выбрать опцию **Создать сеть "компьютер-компьютер"** (Create an ad hoc network) (см. рис. 3.11).

В окне настройки сети "компьютер-компьютер" (рис. 3.7) необходимо указать имя сети (строчные и заглавные буквы будут различаться при обращении к этой сети!), тип безопасности (WEP, WPA2-Personal или "Нет проверки подлинности (Open)") и соответствующий выбранному типу ключа (security key). Подсказка для формата пароля появляется при наведении курсора на соответствующее поле. Если сеть не сохраняется, то входящее подключение будет существовать только на время сеанса работы пользователя в системе; если выбираются опции сохранения, то для данной сети создается профиль, который можно использовать в дальнейшем для быстрой установки входящих подключений.

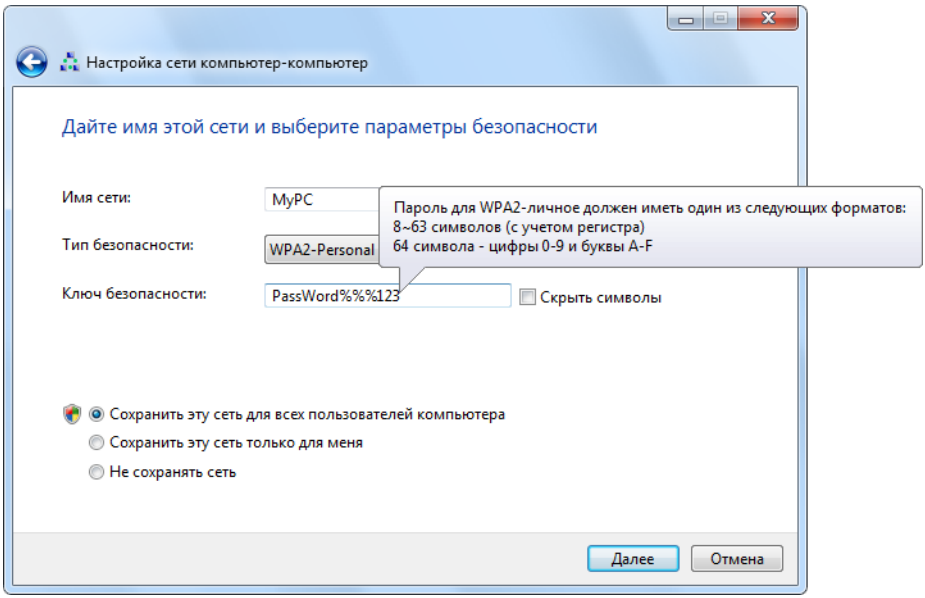

Рис. 3.7. Ввод параметров прямого подключения "компьютер-компьютер"

После выполнения проверок и создания новой сети появляется сообщение о готовности сети к работе (рис. 3.8). Если разрешается общий доступ к подключению к Интернету (сообщение о включении доступа появляется в отдельном окне), то входящие клиенты смогут использовать имеющееся подключение (коммутируемое или по локальной сети) для выхода в Интернет.

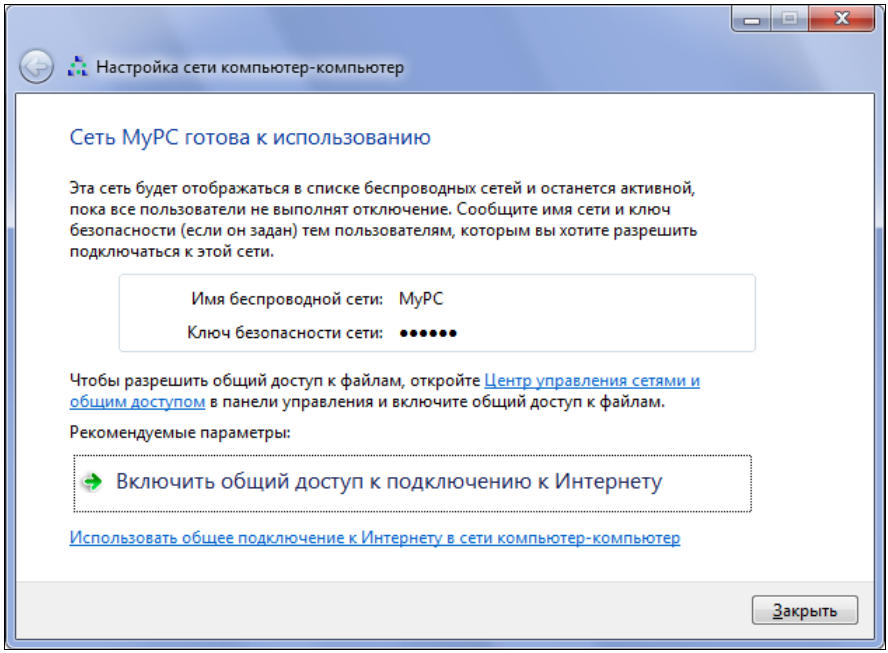

Рис. 3.8. Сообщение о создании сети "компьютер-компьютер" и опция разрешения подключения к Интернету

Вновь созданная сеть появляется в списке активных сетей (рис. 3.9) (обратите внимание на особый значок для таких сетей в виде "связки" трех экранов), и начинается ожидание входящих подключений. Теперь удаленные клиенты смогут подключаться к локальному компьютеру (эта стандартная процедура описывалась в предыдущем разделе). При установке соединения статус сети меняется на "Подключено" (Connected). При нажатии кнопки **Отключение** (Disconnect) сеть переходит в пассивное состояние (хотя и остается в данном окне), но внешние пользователи ее уже не видят. С помощью кнопки **Подключение** (Connect) сеть можно снова активировать, и к ней смогут подключаться другие компьютеры и устройства.

Если профиль сети "компьютер-компьютер" (*входящего* подключения) сохранен, то после включения системы имя сети всегда будет появляться в окне активных сетей. Однако всякий раз ее нужно будет явно переводить в активное состояние (подключать) — вручную или из командного файла. Только тогда она будет становиться видимой для клиентов. Подключения к такой сети всегда выполняются вручную, т. к. профиль для таких подключений сохранить нельзя (в отличие от подключений к точкам доступа и хотспотам).

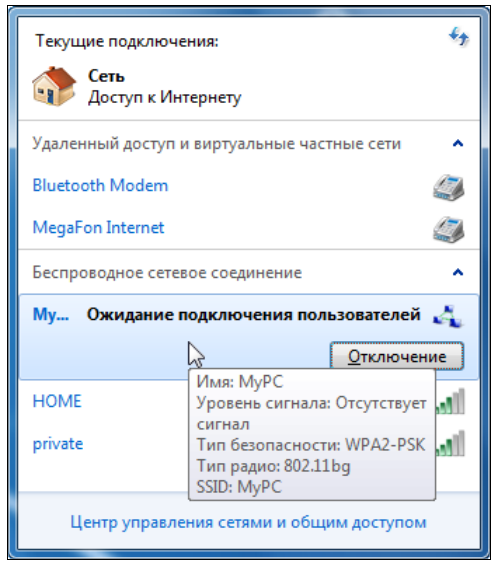

Рис. 3.9. Сеть "компьютер-компьютер", ожидающая внешних подключений, в окне активных сетей

Если выполняется прямое подключение к компьютеру, на котором отсутствует общее интернет-подключение, то клиент получает APIPA-адрес *(см. главу 2)*, и связанная с этим подключением сеть обозначается как *неопознанная общественная сеть*. Поэтому для разрешения доступа к ресурсам необходимо применять способы, описанные в *разд. "Особенности работы с несколькими сетевыми подключениями" главы 2*. Наличие общего интернет-подключения избавляет от такой проблемы, поскольку в таком случае клиенты будут получать "нормальные" адреса хостов и шлюза из подсети 192.168.137.0 (см. рис. 2.18 и рис. 2.19), и сеть будет распознаваться как частная (где сетевое обнаружение и общий доступ всегда включены). В любом случае, если в известной и четко определенной сетевой конфигурации возникает постоянно неопределенность с распознаванием сетей, имеет смысл пробовать статические адреса.

К одному входящему подключению "компьютер-компьютер" могут подключаться несколько клиентов: в этом случае они имеют доступ к центральному компьютеру и могут "видеть" друг друга. Если разрешен общий доступ к интернет-подключению, то они также получают выход в Интернет. На рис. 3.10 показана карта сети, полученная на одном из клиентов, входящих в такую сетевую конфигурацию.

Если обозначить буквами компьютеры, показанные на рис. 3.10, то можно предположить немного другую последовательность подключений "компьютер-компьютер": компьютер А подключается к компьютеру Б, а компьютер Б подключается к компьютеру В. В этом случае компьютер А также будет видеть компьютер В и его ресурсы (и наоборот). Соответственно, если связь от Б к В будет разорвана, то и компьютер А перестанет видеть компьютер В.

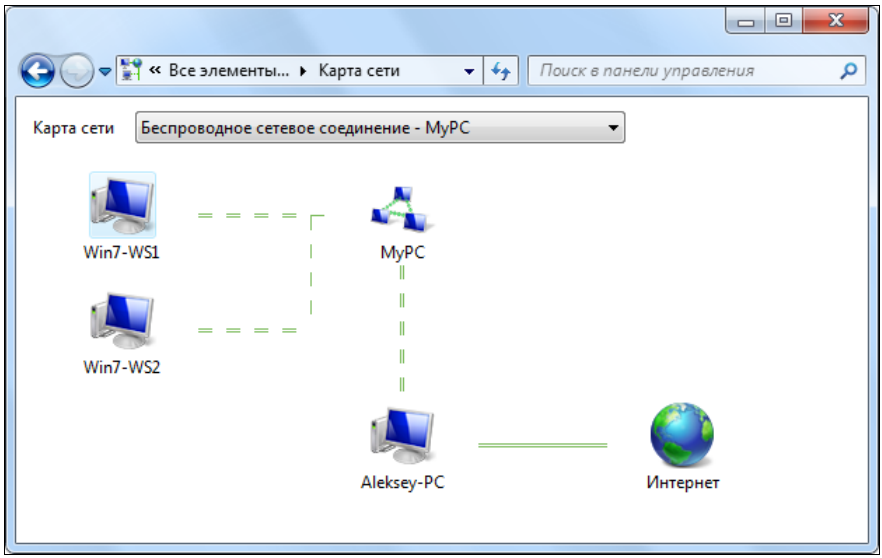

Рис. 3.10. Подключение двух удаленных компьютеров к сети MyPC, обеспечивающей доступ к локальному компьютеру и далее — к Интернету

Управление профилями Wi-Fi сетей

Профиль сети представляет собой набор параметров, сохраненных для дальнейшего использования и быстрой установки подключения — при его использовании не нужно каждый раз вводить имя сети и ключевое слово. Для сетей типа "инфраструктура" возможно автоматическое подключение: если сеть находится в радиусе действия, то компьютер сразу же к ней подключается без участия пользователя. Если имеется несколько профилей с автоподключением, то они рассматриваются с учетом приоритетов — первая в списке сеть выбирается в первую очередь при одновременной доступности нескольких сетей.

Некоторые сохраненные профили постоянно присутствуют в списке активных сетей (см. рис. 3.9): это относится к профилям для сетей "компьютер-компьютер" (поскольку входящее подключение можно в любой момент разрешить или же оно уже активно) и к профилям для точек доступа, подключение к которым *в ручном режиме* возможно даже в том случае, если они *не ведут вещания своего имени* (если подключение автоматическое, то профиль не присутствует в списке).

Профиль для точки доступа проще всего создать при первом подключении к ней: поскольку флажок **Подключаться автоматически** (Connect automatically) по умолчанию установлен, то при установке соединения создается и соответствующий профиль.

Для ручного создания профиля сети нужно воспользоваться ссылкой **Управление беспроводными сетями** (Manage wireless networks), имеющейся в окне Центра управления сетями и общим доступом (Network and Sharing Center) (см. рис. 1.7) (эта ссылка появляется в окне только в том случае, если на компьютере имеется

беспроводной адаптер). По этой ссылке открывается окно, где перечислены все имеющиеся в системе профили беспроводных сетей (см. рис. 3.13). Для создания нового профиля нажмите в этом окне кнопку **Добавить** (Add) на панели задач. На следующем этапе выберите *тип* профиля (рис. 3.11): можно создать профиль для сети типа "инфраструктура" или профиль для входящего подключения сети "компьютер-компьютер" (он описывался в предыдущем разделе, поэтому далее будет рассматриваться первая опция).

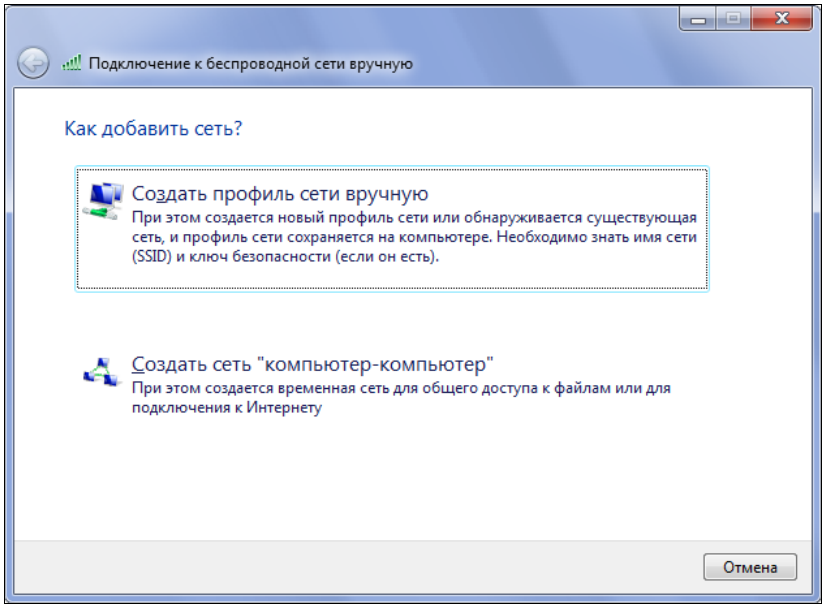

Рис. 3.11. Выбор типа профиля сети

Далее укажите имя сети, выберите тип безопасности и шифрования и задайте ключевое слово (security key) (рис. 3.12). Типов безопасности в данном случае много больше, чем при создании сети "компьютер-компьютер" (см. рис. 3.7), весь список показан на врезке. Для точек доступа желательно выбрать самый защищенный вариант — "связку" WPA2-Personal/AES (если эти спецификации поддерживаются устройством). Состояние флажков автоматического запуска и подключения к скрытой сети устанавливается в зависимости от конкретных рабочих условий.

После нажатия кнопки **Далее** (Next) профиль создается, и в окне сообщения о завершении операции можно выбрать опцию просмотра параметров профиля *(см. далее)* или просто закрыть окно.

Все созданные профили — для сетей типа "инфраструктура" и для входящих подключений сетей "компьютер-компьютер" — появляются в окне **Управление беспроводными сетями** (Manage Wireless Networks) (рис. 3.13). Здесь можно задать приоритеты подключения к сетям: если одновременно будут доступны несколько сетей, то выбираться будет первая (верхняя) в списке сеть. Обычно профили создаются для всех пользователей компьютера, но тип профилей можно и изменить,

разрешив создание общих и личных профилей. Если на компьютере имеется несколько беспроводных адаптеров, то профили задаются для каждого из них индивидуально. Окно свойств адаптера можно быстро открыть, нажав соответствующую кнопку на панели задач в окне профилей.

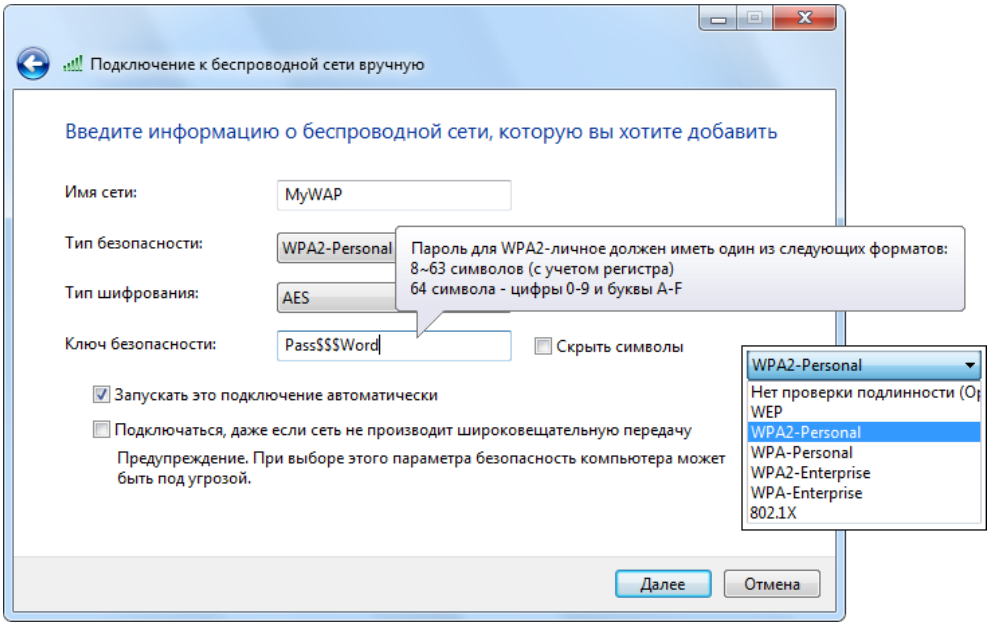

Рис. 3.12. Ввод параметров сети, к которой будет выполняться подключение

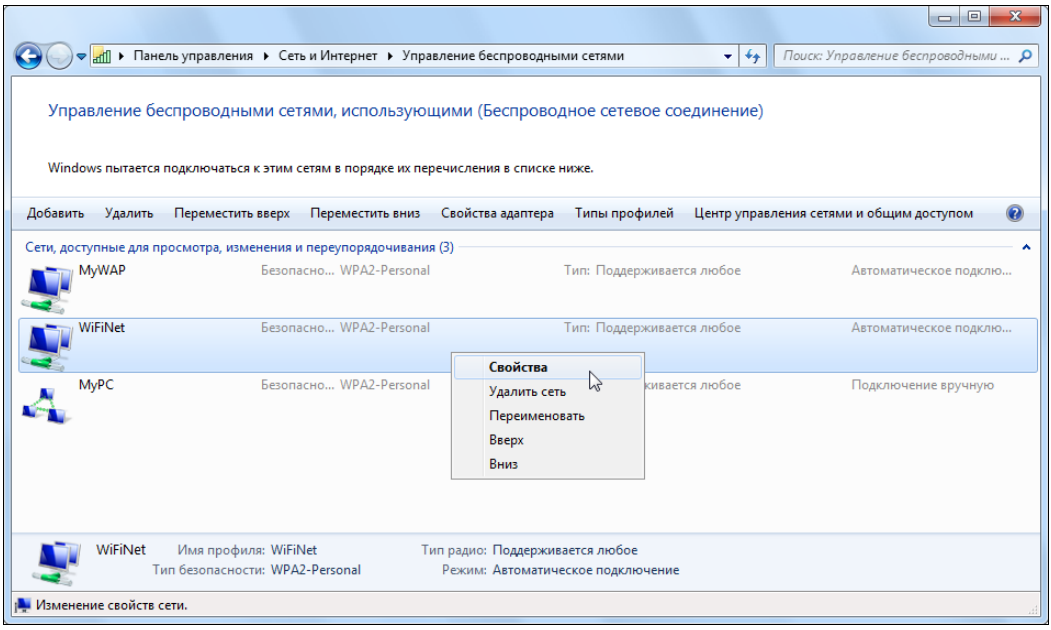

Рис. 3.13. Имеющиеся в системе профили беспроводных сетей

Важной возможностью окна профилей (см. рис. 3.13) является то, что здесь можно открыть окно свойств для каждого профиля, где сохраненные параметры профиля можно просматривать и менять (необходимость в этом возникает в реальной работе). Измененные параметры начинают действовать при следующем же подключении. На рис. 3.14 показана основная вкладка окна свойств профиля для сети "компьютер-компьютер" *(слева)* и для сети типа "инфраструктура" (здесь она названа "Точка доступа") *(справа)*. Как можно видеть, здесь присутствуют все параметры, заданные при создании профиля; на вкладке **Безопасность** (Security) указаны тип безопасности и шифрования, а также ключевое слово (которое можно посмотреть, если оно забылось, или изменить, если его поменяли на точке доступа).

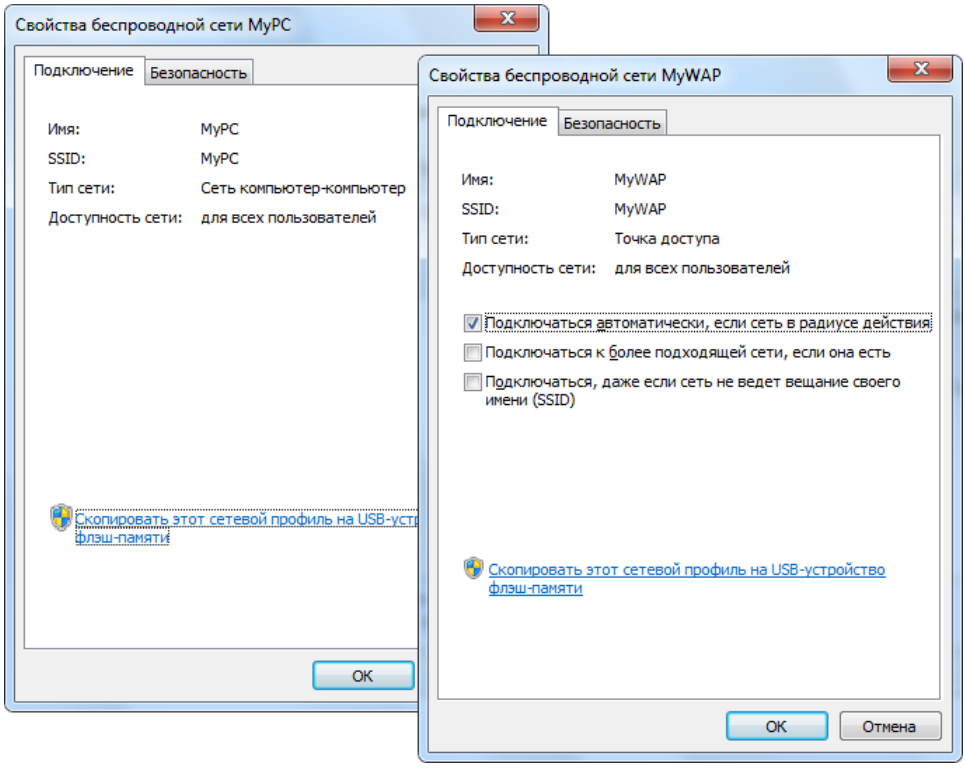

Рис. 3.14. Свойства профилей беспроводных сетей

Любой имеющийся профиль можно записать на флэш-устройство, которое затем можно использовать для быстрой установки подключения на других компьютерах. Для этого нужно подключить накопитель и щелкнуть по ссылке в нижней части окна свойств профиля (см. рис. 3.14). На флэшке будет создана папка SMRTNTKY и записан файл setupSNK.exe. Этот файл может запускаться автоматически при подключении накопителя к другому компьютеру или его можно запустить вручную. Подключение с заданными параметрами будет создано на компьютере, и пользователи смогут сразу подключаться к заданному устройству или устанавливать входящее подключение для своего компьютера.

В окно свойств профиля сети (см. рис. 3.14) также можно попасть из окна состояния беспроводного сетевого подключения (см. рис. 1.15), нажав кнопку **Свойства беспроводной сети** (Wireless Properties).

Профили сетей типа "инфраструктура" как таковые не видны в окне активных сетей (см. рис. 3.9): пользователь просто видит нужную сеть и может к ней сразу подключиться, не вводя никаких параметров — достаточно лишь нажать кнопку **Подключение** (Connect). Аналогичным образом активизируется и входящее подключение сети "компьютер-компьютер", после чего к компьютеру смогут подключаться удаленные клиенты.

Управление беспроводными подключениями из командной строки

В *разд. "Автоматическая установка подключения по запросу" главы 2* рассматривались причины, по которым может быть полезным управление сетевыми подключениями с помощью командных файлов. Аналогичные задачи могут возникнуть и при использовании беспроводных сетевых подключений. Кроме того, имеются различные параметры беспроводных сетей, которые удобнее (или возможно лишь) просматривать с помощью команд в окне консоли (командной строки).

Подключение к сетям или установка входящих подключений

Для работы с беспроводными подключениями используется стандартная утилита `Netsh.exe`, обеспечивающая доступ почти ко всем сетевым компонентам и параметрам.

Следующая команда позволяет запустить профиль с именем MyPC для подключения "Беспроводное сетевое соединение" (если такое подключение единственное, то имя интерфейса можно опустить; имя профиля обязательно и указывается ***с учетом строчных и заглавных букв***):

```
C:\>netsh wlan connect name=MyPC interface="Беспроводное сетевое соединение"
Запрос на подключение успешно завершен.
```

Данная команда устанавливает соединение с той точкой доступа, имя которой и другие параметры были сохранены в указанном профиле.

Для разрыва соединения используется команда:

```
C:\>netsh wlan disconnect interface="Беспроводное сетевое соединение"
Запрос на отключение для интерфейса "Беспроводное сетевое соединение" успешно
завершен.
```

Имя профиля может быть связано с сетью "компьютер-компьютер" или с сетью типа "инфраструктура" — в первом случае будет активизироваться входящее подключение, во втором случае будет выполняться подключение к заданной точке доступа.

Просмотр параметров и состояния беспроводных сетей

Команда `netsh wlan show settings` показывает общие параметры беспроводных сетей, в частности — разрешен ли режим размещенной сети (эта информация понадобится при работе с виртуальными сетями, описываемыми в следующем разделе).

С помощью следующей команды легко увидеть список всех доступных беспроводных сетей, включающий их имена (SSID) и параметры безопасности:

```
C:\>netsh wlan show networks
Имя интерфейса: Беспроводное сетевое соединение
В данный момент видны 5 сетей.
SSID 1: MyPC
    Тип сети:                 Прямое соединение
    Проверка подлинности:     WPA2-Personal
    Шифрование:               CCMP
SSID 2: MyWAP
    Тип сети:                 Инфраструктура
    Проверка подлинности:     WPA2-Personal
    Шифрование:               CCMP
SSID 3: td1534
    Тип сети:                 Инфраструктура
    Проверка подлинности:     Открыть
    Шифрование:               WEP
SSID 4: HOME
    Тип сети:                 Инфраструктура
    Проверка подлинности:     Открыть
    Шифрование:               Нет
SSID 5: private
    Тип сети:                 Инфраструктура
    Проверка подлинности:     WPA-Personal
    Шифрование:               TKIP
```

В показанном примере можно видеть разные типы сетей (прямое соединение и инфраструктура), различные способы проверки подлинности и шифрования. Две сети из перечисленных — *открытые*, без проверки подлинности, причем в одной используется шифрование WEP, а в другой (HOME) никаких механизмов защиты вовсе нет — такая небезопасная сеть помечается в окне активных сетей особым значком (изображением щита с восклицательным знаком — *см. ранее*).

Команда `netsh wlan show all` позволяет увидеть сводные данные по конфигурации беспроводной связи в системе. Информации очень много, поэтому ее нужно просматривать постранично или перенаправить в файл для последующего просмотра.

С помощью этой команды можно получить весьма ценные сведения, необходимые в работе, особенно при согласовании устройств или возникновении ошибок соединения. Например, в разделе "Показать драйверы" (Show Drivers) (команда `netsh`

`wlan show drivers` показывает только этот раздел) подробно расписаны все параметры, касающиеся используемого драйвера беспроводного сетевого соединения. В частности, среди прочей информации здесь указаны поддерживаемые стандарты Wi-Fi (802.11), возможность использования размещенной сети *(см. далее)*, методы проверки подлинности и шифрования, поддерживаемые в режиме инфраструктуры (infrastructure) и в режиме прямого подключения (ad-hoc) (можно увидеть, что для инфраструктуры возможностей намного больше).

В разделе "Показать интерфейсы" (Show Interfaces) (аналогичная команда `netsh wlan show interfaces`) видны активные соединения для данного подключения, с указанием типа и имени сети, используемого стандарта (типа радио, 802.11) и канала связи, скорости приема/передачи и т. д. Также указывается состояние размещенной сети.

Специальный раздел "Показать размещенную сеть" (Show Hosted Network) (команда `netsh wlan show hostednetwork`) описывает параметры виртуальной сети: поддерживается ли этот режим, настроена ли сеть (и ее свойства) и ее статус.

Далее подробно перечисляются имеющиеся в системе профили сетей (`netsh wlan show profiles`) и их параметры, а в завершении приводится список активных сетей *(см. выше)*, однако указываются также дополнительные параметры, например, тип радио, базовые и другие скорости передачи, уровень сигнала и используемый канал (это позволяет увидеть, нет ли сетей, работающих на одном канале).

Виртуальные (размещенные) сети Wi-Fi

О преимуществах использования точки доступа по сравнению с сетями "компьютер-компьютер" уже говорилось ранее в *разд. "Настройка соединения между двумя компьютерами (ad hoc подключение)"*. Обычно сетевые адаптеры работают в режиме подключения к внешним сетям (компьютерам) (режим инфраструктуры) и могут принимать входящие подключения для соединений "компьютер-компьютер". Однако в системах Windows 7 имеются стандартные возможности организации программной точки доступа[1]. Эта возможность связана с понятием *виртуальных*, или *размещенных* (hosted), сетей Wi-Fi. Более подробную информацию о "виртуальных сетях" в Windows 7 легко при необходимости найти в Интернете, мы же будем пользоваться термином "размещенная сеть", поскольку оно принято в интерфейсе команд и утилит, описываемых далее.

> ***Примечание***
>
> В системах Windows 7 вся работа с виртуальными сетями выполняется с помощью утилит командной строки, какой-либо графический интерфейс отсутствует. В Интернете можно найти программы, позволяющие реализовать данную возможность и использовать окно программы для настройки сетей и работы с ними. Примеры таких программ — Connectify и Virtual Router Manager.

[1] К рассмотренным ранее достоинствам нужно еще добавить, что на практике виртуальная сеть (программная точка доступа) работает быстрее, чем обычное соединение "компьютер-компьютер".

Создание размещенной сети

Для работы с размещенной сетью используется специальный драйвер виртуальной сети *Microsoft Virtual WiFi Miniport Adapter*, который нужно установить в системе. Это осуществляется одновременно с созданием размещенной сети с помощью следующей команды (в кавычках указаны частные параметры, которые выбираются индивидуально):

```
netsh wlan set hostednetwork mode=allow ssid="MyViAP" key="Pass$$$Word123"
keyUsage=persistent
```

После выполнения данной команды можно открыть окно диспетчера устройств (Device Manager), где в разделе сетевых адаптеров должен появиться новый адаптер. Для него в окне сетевых подключений (см. рис. 3.5) создается стандартное беспроводное сетевое соединение, которое в нашем примере для наглядности переименовано в "Virtual Wi-Fi". На рисунке можно видеть название адаптера, связанного с этим подключением.

В дальнейшем *поменять* имя сети (SSID) и/или ключ (security key) можно с помощью следующей команды:

```
netsh wlan set hostednetwork ssid=MyViAP key=NewPSW
keyUsage=[persistent|temporary]
```

Если последний параметр не указывается, то ключ сохраняется и используется постоянно.

Управление размещенной сетью

Чтобы размещенная сеть стала активной, ее нужно *запустить*; изменение параметров выполняется только для *остановленной* сети. Для этого используются две следующие команды:

```
netsh wlan start hostednetwork
netsh wlan stop hostednetwork
```

При запуске сети соответствующее беспроводное соединение становится активным и получает адрес 192.168.173.1. Теперь клиенты могут подключаться к размещенной сети с заданным именем и получать доступ к ресурсам компьютера. Если компьютер имеет доступ к Интернету, то соответствующее подключение можно сделать общим — в этом случае размещенная сеть также получит адрес 192.168.137.1 и выход в Интернет (рис. 3.15); при этом она будет раздавать адреса из подсети 192.168.137.0 всем подключающимся клиентам, которые также смогут подключаться к Интернету. В показанном примере общим является подключение по локальной сети.

Состояние и текущие параметры (в частности — используемый канал) размещенной сети можно увидеть в окне консоли с помощью следующей команды:

```
C:\>netsh wlan show hostednetwork
Параметры размещенной сети
-----------------------
    Режим                   : разрешен
```

```
    Имя идентификатора SSID : "MyViAP"
    Максимальное количество клиентов  : 100
    Проверка подлинности: WPA2-Personal
    Шифр:                    CCMP
Состояние размещенной сети
-------------------------
    Состояние               : Запущено
    BSSID                   : 00:1e:58:9a:e4:b6
    Тип радиомодуля          : 802.11b
    Канал                 : 13
    Число клиентов       : 1
        1c:af:f7:05:8f:1b        Проверка подлинности выполнена
```

В данном примере видно, что к сети подключен один клиент, и он прошел проверку подлинности.

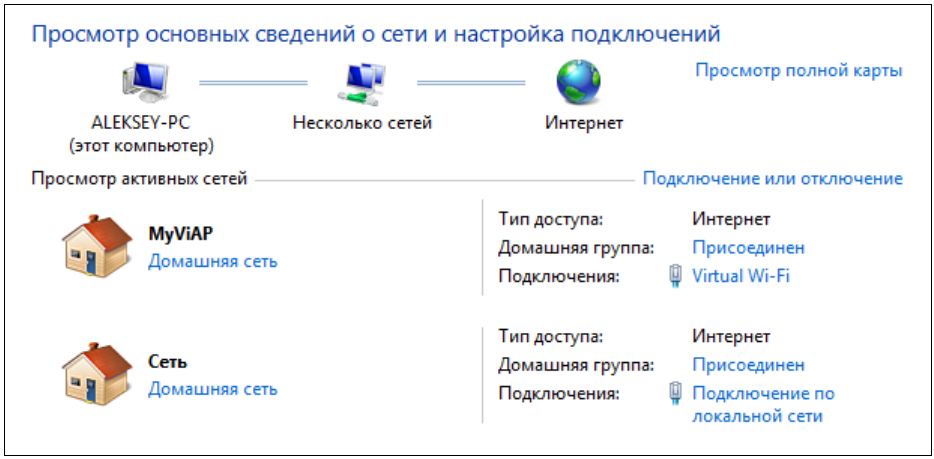

Рис. 3.15. Локальная и размещенная сети, имеющие выход в Интернет

Подключение других устройств беспроводной связи

Помимо беспроводных сетей Wi-Fi (стандарта 802.11), вместе с персональными компьютерами и многочисленными цифровыми устройствами используются и другие беспроводные технологии, некоторые из которых уже готовятся уйти в историю (как связь через ИК-порты), а некоторые получают все большее распространение (например, телефонные 3G-модемы). Три таких технологии и используемые для них устройства будут рассматриваться в оставшейся части главы.

Познакомимся сразу с устройствами, представляющими три типа беспроводной компьютерной связи (рис. 3.16) и подключающимися к любому компьютеру через USB-порт:

- Bluetooth-адаптер;
- IrDA-адаптер для связи через инфракрасный (ИК) порт;
- 3G-модем[1].

Bluetooth-адаптер

IrDA-адаптер

3G-модем

Рис. 3.16. Различные беспроводные устройства, используемые для обмена информацией и подключения к Интернету

Встроенные Bluetooth-адаптеры повсеместно встречаются в переносных компьютерах и КПК, мобильных телефонах и других электронных устройствах, также до сих пор нередко можно встретить и IrDA-адаптеры (чаще их можно найти в бытовых устройствах).

Технология *Bluetooth* обеспечивает скорость передачи данных порядка 1—3 Мбит/с на расстояниях от 10 до 100 м. Это в значительной степени зависит от используемых устройств, которые делятся на три класса (распространены Class 1 и Class 2). В реальных условиях для помещения можно рассчитывать на 1 Мбит/с и 10 м. Компьютерные Bluetooth-адаптеры обычно поддерживают работу в *личных сетях устройств Bluetooth* (Personal Area Network, PAN), что позволяет работать с общими ресурсами нескольких компьютеров так же, как в обычной локальной сети Ethernet.

Связь через инфракрасный (ИК) порт (Infrared Data Association, IrDA) работает в пределах прямой видимости на минимальных расстояниях: от 0,2 до 1 м. Скорости могут быть очень разные: от нескольких Кбит/с до 1 Гбит/с; обычно скорость работы сравнима с телефонным модемным соединением — несколько Кбайт/с. Обычно связь через ИК-порт используется для кратковременных соединений устройств с целью передачи отдельных файлов.

Различные *USB-модемы для телефонных сотовых сетей* получают широкое распространение по нескольким причинам: достаточно высокие скорости работы

[1] Напомним, что мы так называем *любой* цифровой модем для телефонной сотовой связи. Суть изложения от выбранного стандарта и оператора связи меняться не будет.

(3 Мбит/с в городе — достижимо и удобно), большая зона охвата, доступная стоимость (цены стремительно упали от нескольких тысяч рублей до одной тысячи[1]) и удобные тарифы (рубль за мегабайт — вполне приемлемые деньги, если не качать музыку, а работать с почтой или веб-сайтами).

Все перечисленные выше устройства в системах Windows используются одинаково: при подключении устройства устанавливаются стандартные драйверы модема, для которого затем создается обычное коммутируемое (телефонное) подключение. Первые два типа устройств позволяют также связываться или передавать файлы напрямую. Первый подход удобен, если есть намерение через устройство (например, мобильный телефон) подключиться к Интернету, второй — для связи между устройствами любого типа и назначения.

Устройства Bluetooth

Системы Windows 7 имеют стандартные компоненты для работы с Bluetooth-адаптерами. На ноутбуках адаптеры обычно встроенные, и драйверы для них устанавливаются при инсталляции операционной системы, но имеются и подключаемые адаптеры, которые можно вставить в USB-порт любого компьютера. Если такой адаптер (см. рис. 3.16) подключается к порту, то автоматически устанавливаются стандартные драйверы (рис. 3.17), и компоненты для работы с Bluetooth появляются в окне диспетчера устройств (Device Manager) в соответствующих разделах (показано на врезке).

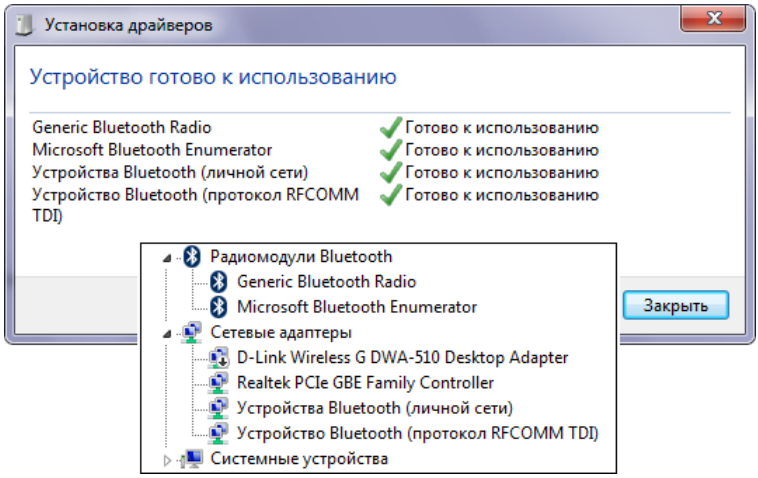

Рис. 3.17. Установка драйверов для Bluetooth-адаптера и перечень стандартных компонентов для работы с устройствами Bluetooth

После установки адаптера в окне сетевых соединений (см. рис. 3.5) должен появиться значок для нового подключения (рис. 3.18, *слева*), а значок самого адаптера

[1] Речь идет о крупных городах, но тут важна общая тенденция!

появляется в окне **Устройства и принтеры** (Devices and Printers) (см. рис. 3.24). Теперь можно устанавливать связь с Bluetooth-устройствами и/или подключаться к *личным сетям* (Personal Area Network, PAN).

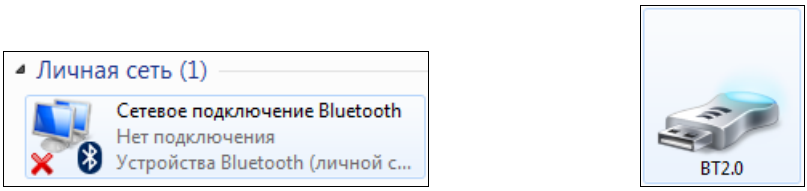

Рис. 3.18. Значок подключения Bluetooth в папке сетевых подключений *(слева)* и значок адаптера в окне устройств *(справа)*

Если адаптер устанавливается первый раз, то необходимо проследить за наличием всех компонентов и правильностью установки драйверов для них. Если отключить компонент **Generic Bluetooth Radio** (см. рис. 3.17), то работа Bluetooth-адаптера будет запрещена, и соответствующее сетевое подключение исчезнет. Если компонент снова задействовать, то вся функциональность будет полностью восстановлена.

При щелчке по значку устройств Bluetooth в области уведомлений на панели задач открывается меню команд для управления такими устройствами и передачи файлов (рис. 3.19). Использование некоторых команд будет рассмотрено далее, сейчас отметим лишь команду **Открыть параметры** (Open Settings). С ее помощью открывается окно (рис. 3.20), где указаны основные параметры, определяющие работу с Bluetooth-устройствами (показаны значения по умолчанию). Команда **Показать устройства Bluetooth** (Show Bluetooth Devices) открывает окно, где перечислены все устройства данного типа, ранее подключавшиеся к компьютеру.

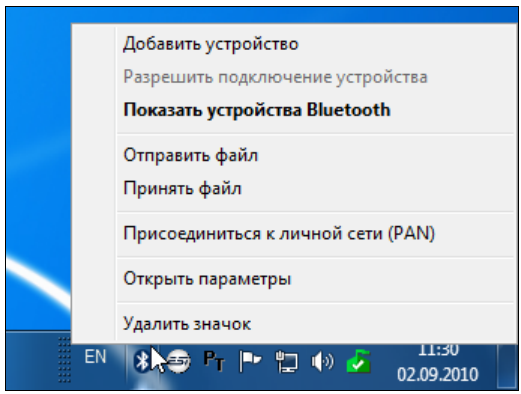

Рис. 3.19. Меню общих команд управления устройствами Bluetooth и команд передачи файлов

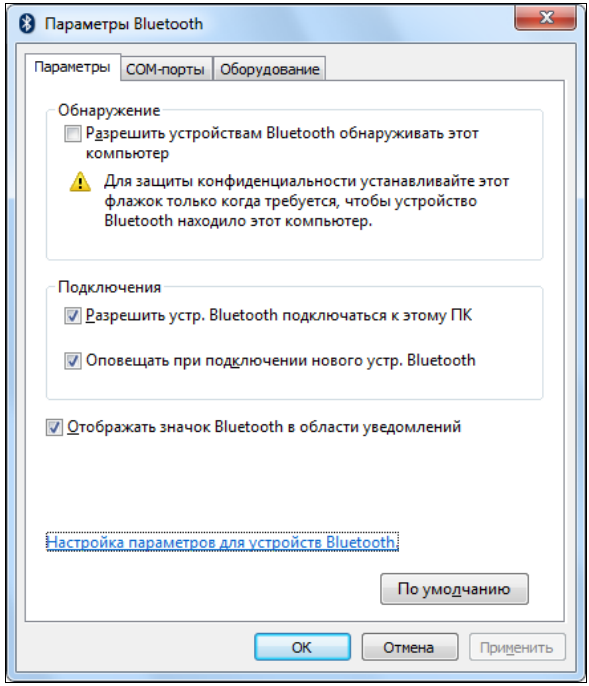

Рис. 3.20. Основные параметры работы устройств Bluetooth

Подключения устройства или компьютера по Bluetooth

Если Bluetooth-устройство или другой компьютер (настольный, ноутбук, КПК и т. п.) находятся в пределах рабочей зоны, то для подключения нужно выполнить команду **Добавить устройство** (Add a Device) в меню значка Bluetooth (см. рис. 3.19) или нажать кнопку **Добавление устройства** (Add a device) в окне устройств Bluetooth. При этом начнется поиск устройств, поэтому необходимо включить сами устройства и режим Bluetooth, если он не постоянен (на мобильных телефонах, например, для этого имеются соответствующие команды).

Обнаруженные устройства отображаются в специальном окне (см. рис. 3.21), где видны тип устройства и его имя (если таковое задано). Выберите устройство и нажмите кнопку **Далее** (Next) — начнется подключение к устройству, и для установки связи на нем появится предложение ввести так называемый *код образования пары*. При добавлении Bluetooth-устройств возможны три варианта использования кода (рис. 3.21): ввести один и тот же код на устройстве и на компьютере, ввести заранее известный фиксированный код или обойтись вообще без кода. Если запрашивается числовой код, то его нужно ввести на устройстве (произвольные цифры) и, выбрав первую опцию, повторить на компьютере.

После установки дополнительных драйверов (для модема и стандартных портов по соединению Bluetooth) (рис. 3.22) должно появиться сообщение об успешном добавлении устройства на компьютер. Теперь пиктограмму подключенного устройства можно увидеть в окне **Устройства и принтеры** (Devices and Printers) (см.

рис. 3.24) или в специальном окне, которое открывается по команде **Показать устройства Bluetooth** (Show Bluetooth Devices) в меню значка Bluetooth (см. рис. 3.19). В контекстном меню значка устройства (см. рис. 3.24) имеются следующие опции: команда перехода в окно модемов (см. рис. 2.2), где теперь появляется "Стандартный модем по соединению Bluetooth", команды управления модемом и создания коммутируемых подключений *(см. далее)*, а также традиционная команда **Свойства** (Properties).

Примечание

Если в параметрах Bluetooth (см. рис. 3.20) разрешено обнаружение компьютера, то подключение устройства можно инициализировать и с него самого, выполнив соответствующую команду и введя код образования пары. Разницы с описанным выше вариантом никакой не будет.

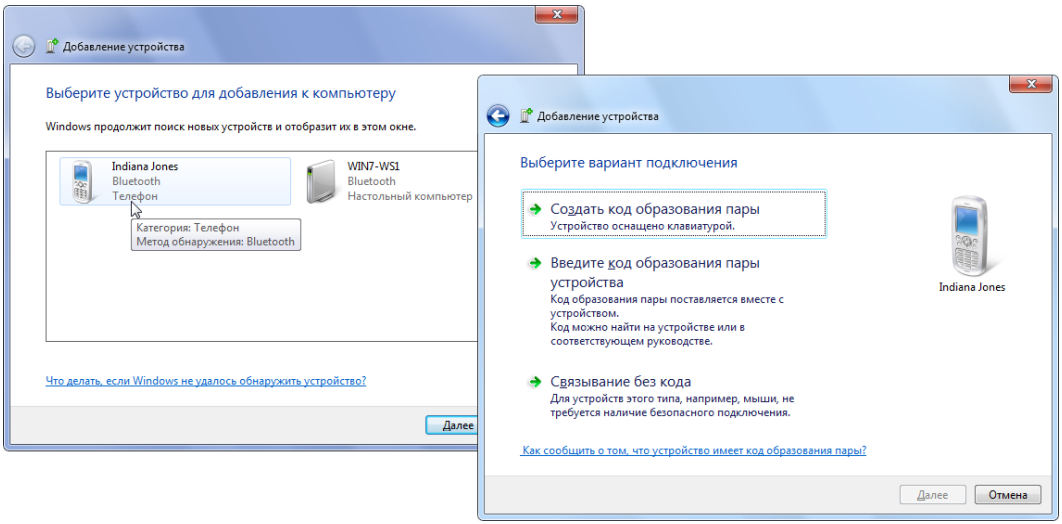

Рис. 3.21. Выбор подключаемого устройства и способа связывания

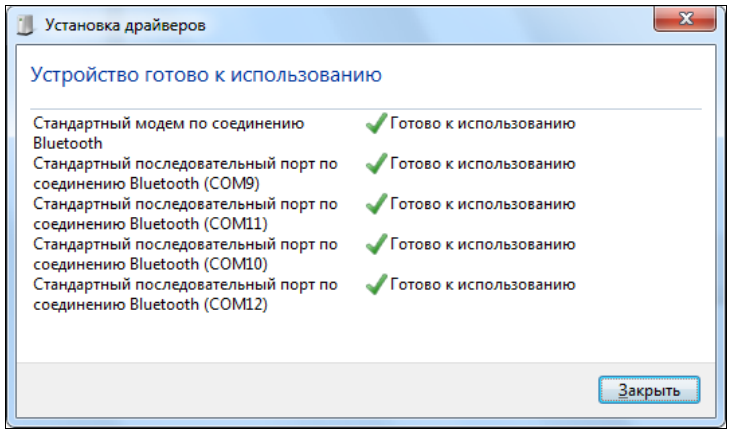

Рис. 3.22. Установка дополнительных драйверов для стандартного модема и портов по соединению Bluetooth

Если подключается компьютер или любое другое устройство, поддерживающее личную сеть (PAN) (см. значок настольного компьютера на рис. 3.21), то автоматически формируется код из восьми цифр, который после подтверждения подключения нужно ввести на другом компьютере. После этого выполняется настройка соединения и должно появиться сообщение об успешном завершении операции. Никакие дополнительные драйверы при этом не ставятся. Значок подключенного устройства автоматически помещается в окне личной сети (рис. 3.23), где можно просматривать имеющиеся устройства и подключаться к ним и принтерам (подключение к личной сети описывается *далее*).

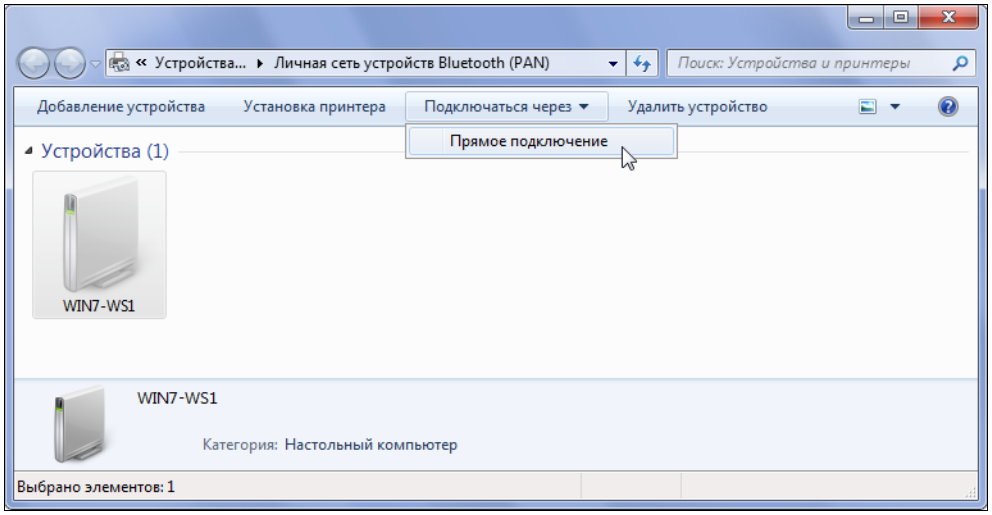

Рис. 3.23. Окно устройств личной сети (PAN)

На этом подключение устройства Bluetooth или компьютера можно считать полностью законченным, теперь можно обмениваться с ним информацией или создавать коммутируемое подключение, если мы хотим через это устройство (например, при помощи мобильного телефона) выходить в Интернет.

Все устройства, когда-либо подключенные к компьютеру, отображаются в окне **Устройства и принтеры** (Devices and Printers) (рис. 3.24). При этом используемые для связи протоколы и технологии могут быть самыми разными. Значки устройств (по умолчанию выбраны крупные значки) можно сортировать и группировать по классам и категориям. Устройства, недоступные в данный момент, но позволяющие просматривать свои параметры, имеют значки приглушенных цветов. В этом окне можно настраивать доступные параметры устройств и выполнять разрешенные для них команды. Также можно запускать операции добавления новых устройств и подключения принтеров (соответствующие кнопки видны на панели задач).

В окне свойств подключенного устройства Bluetooth важными для работы сведениями являются список оборудования, реализуемого с помощью данного устройства (функции устройства), и перечень служб, поддерживаемых данным устройством (рис. 3.25). Для нас здесь важно наличие последовательного порта, через который будет работать модем по соединению Bluetooth (COM4; см. также рис. 2.2).

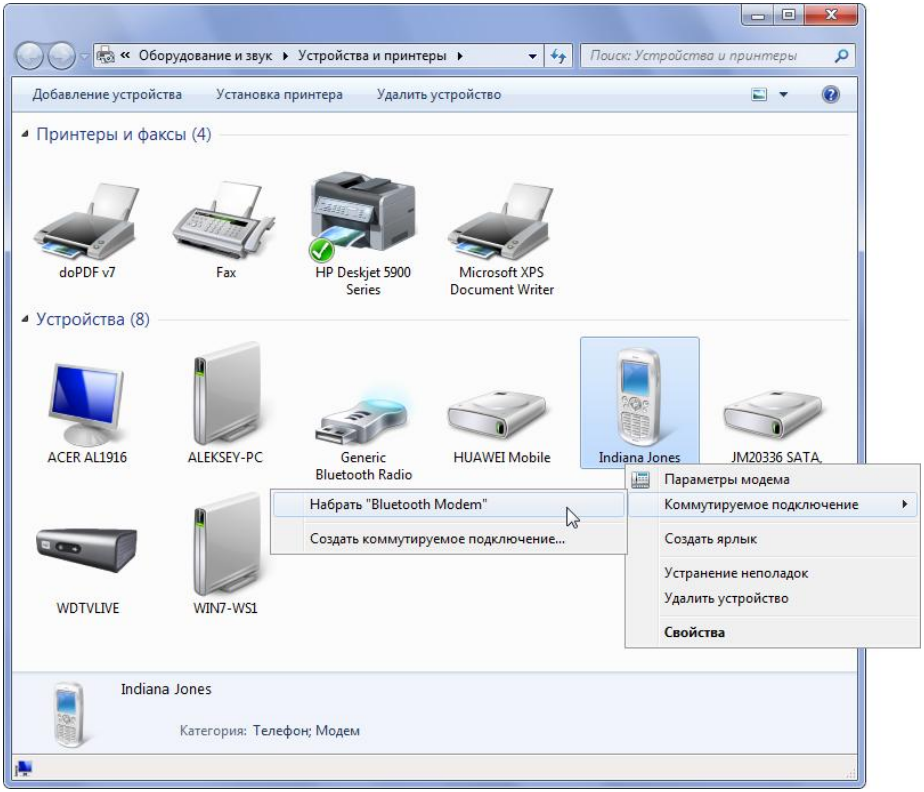

Рис. 3.24. Окно принтеров и различных устройств, подключенных к компьютеру — от монитора и дисковых накопителей до Bluetooth-устройств и медиаплеера

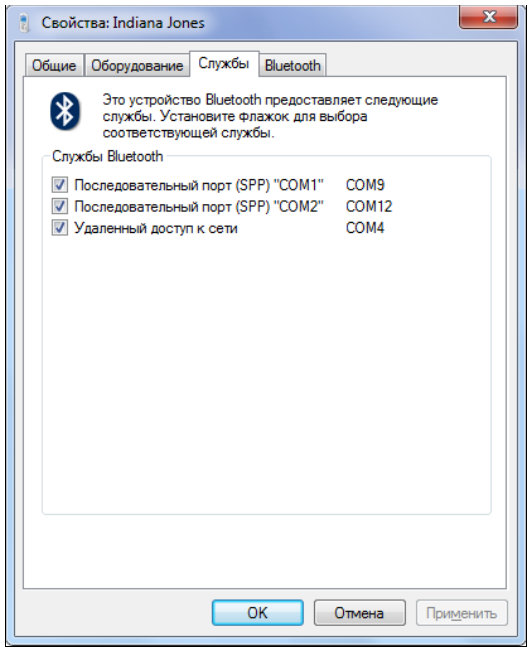

Рис. 3.25. Список служб, поддерживаемых подключенным устройством Bluetooth

Передача файлов

Передачу файлов между подключенным устройством Bluetooth и компьютером можно инициировать с любой стороны. Сама процедура простая и не вызывает никаких вопросов.

- Если файл передается ***с*** устройства, то необходимо выбрать файл и выполнить команду передачи через Bluetooth. Чтобы разрешить обмен данными, на компьютере выполните команду **Принять файл** (Receive a File) — после этого устройство "увидит" компьютер и можно запускать передачу. В окне передачи файлов можно видеть имя файла и его размер, а также указать папку для хранения полученного файла (по умолчанию файлы копируются в личную библиотеку **Документы** (Documents)). Эту процедуру необходимо повторять для каждого передаваемого файла.
- Если необходимо скопировать файл ***на*** устройство, то выполните команду **Отправить файл** (Send a File), выберите устройство Bluetooth и укажите файл для передачи. На устройстве появится запрос на прием информации, и необходимо подтвердить операцию.

> ***Внимание!***
>
> Передавать файлы описанным выше способом можно и между компьютерами (устройствами), связанными личной сетью (PAN). Однако при передаче файла на удаленный компьютер необходимо сначала с помощью команды **Принять файл** (Receive a File) включить режим ожидания, а только потом запускать пересылку данных.

Подключение к личной сети (PAN)

Личная сеть устройств Bluetooth (Personal Area Network, PAN) позволяет им общаться по протоколу Ethernet и получать доступ к общим ресурсам по тем же принципам, как это делается в обычных локальных сетях. Понятно, что не все Bluetooth-устройства могут поддерживать этот режим, и в первую очередь он используется обычными настольными компьютерами, ноутбуками, КПК и другими устройствами со встроенной операционной системой.

После того как было выполнено подключение к удаленному компьютеру (показанному на рис. 3.21), в окне мастера сетевых подключений (см. рис. 2.1) становится возможным выполнение команды **Подключение к личной локальной сети Bluetooth (PAN)** (Connect to a Bluetooth personal area network (PAN)) (иначе подключаться просто к не чему). В окне личной сети (см. рис. 3.23) можно видеть уже подключенные устройства; здесь же имеется команда **Добавление устройства** (Add a device) для поиска новых устройств (эта процедура уже рассматривалась *ранее*). Фактически для связи с другим компьютером или устройством личной сети имеется только две команды: подключение и отключение — необходимо выбрать устройство и нажать соответствующую кнопку на панели задач. Инициализировать подключение можно с любого компьютера, входящего в личную сеть.

Подключенный компьютер становится видимым в Проводнике в папке **Сеть** (Network) (см. рис. 1.4), и с его общими ресурсами можно работать так же, как и

с любым компьютером локальной сети. В папке сетевых соединений (см. рис. 3.5) для подключения Bluetooth видно, с каким компьютером произошло соединение (рис. 3.26). По умолчанию параметры TCP/IP получаются автоматически, поэтому при установке соединения выполняется автонастройка, и подключение получает APIPA-адрес *(см. главу 2)*. Из этого следует, что сеть идентифицируется как *Неопознанная*, и нужно искать способ изменения сетевого профиля, чтобы компьютеры могли видеть общие ресурсы *(см. разд. "Особенности работы с несколькими сетевыми подключениями" главы 2)*.

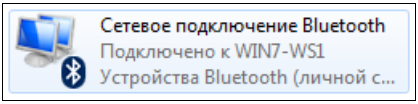

Рис. 3.26. Значок подключения Bluetooth при соединении с компьютером или устройством личной сети

Подключение через ИК-порт (IrDA)

Связь через инфракрасный порт ***автоматически*** инициализируется между компьютером и устройством при наличии у них ИК-порта (нужно проверить, что этот порт включен на устройстве![1]) и *при сближении на достаточно близкое расстояние* (обычно до 30—100 см). В этом случае в области уведомлений на панели задач компьютера активизируется значок ИК-порта, и начинается установка стандартного драйвера по инфракрасному соединению (рис. 3.27). После этого при приближении устройства к компьютеру появляется всплывающее сообщение о наличии "соседнего компьютера" (рис. 3.28), а при наведении курсора мыши на значок порта сообщается о том, что некий компьютер "находится в радиусе действия".

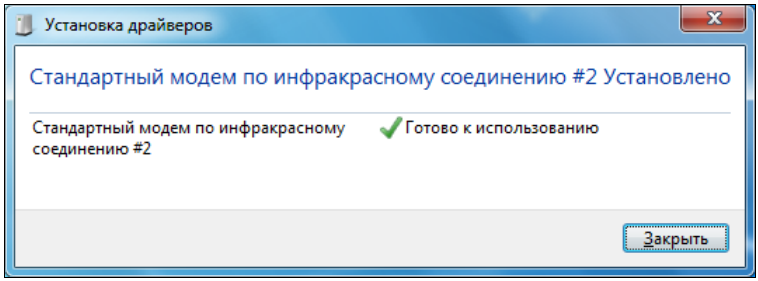

Рис. 3.27. Установка модема для создания коммутируемого подключения с использованием устройства, подключенного через ИК-порт

В контекстном меню значка ИК-порта имеются только две команды: **Передача файлов** (File Transfer) и **Свойства** (Properties). Перед началом работы с портом имеет смысл просмотреть и настроить параметры (рис. 3.29) — чтобы все события

[1] ИК-порт в устройствах обычно нужно включать с помощью специальной команды, а в случае бездействия он через короткое время (десятки секунд) автоматически отключается.

были понятными и предсказуемыми. Как можно видеть на рисунке, по умолчанию все полученные файлы сохраняются на рабочем столе, а переданные изображения — в соответствующей библиотеке (этот параметр задается на второй вкладке). Изображения (например, с фотокамер) могут передаваться без запроса на передачу каждого файла. Возможно, другие значения параметров будут удобнее, поэтому их предварительно нужно выбрать.

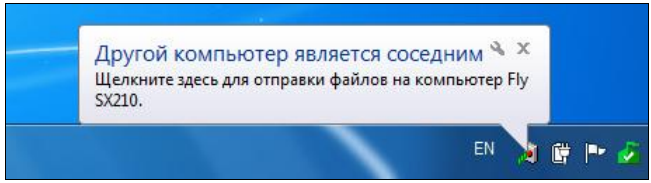

Рис. 3.28. Сообщение о наличии устройства, с которым можно связаться через ИК-порт

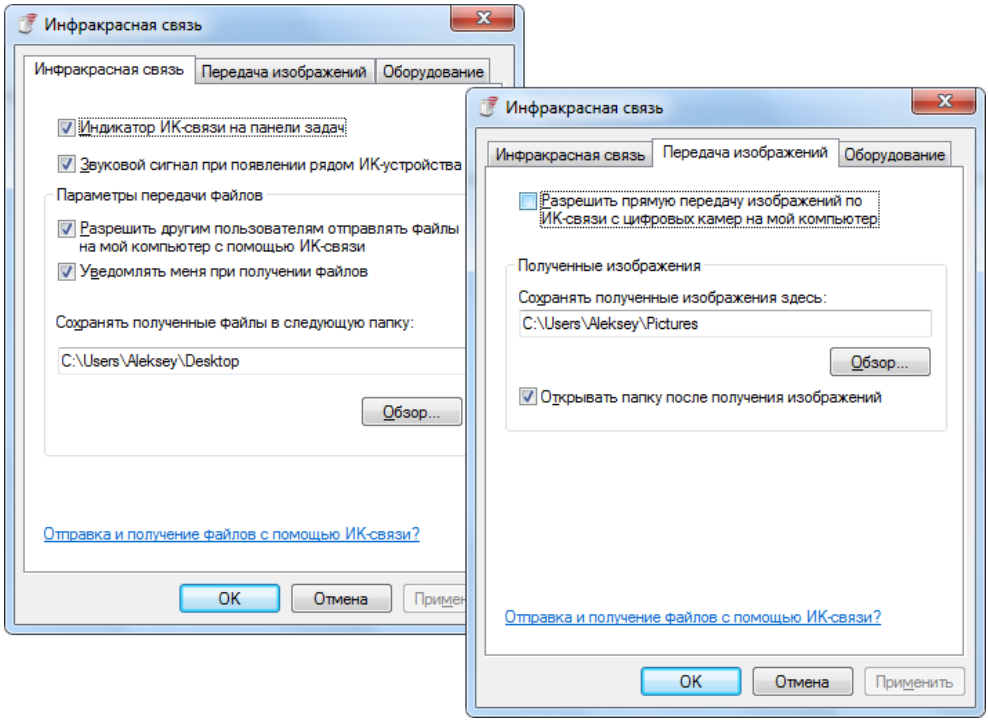

Рис. 3.29. Параметры работы ИК-порта и настройки, используемые при передаче файлов и изображений

Передача файлов на устройство инициализируется с помощью соответствующей команды в контекстном меню значка ИК-порта. Открывается окно выбора файлов, и после того как объекты для передачи указаны и принимающая сторона подтвердила операцию, запускается отправка данных. За ходом процесса можно следить в специальном окне (рис. 3.30); значок порта при передаче файлов динамически меняется и имеет вид .

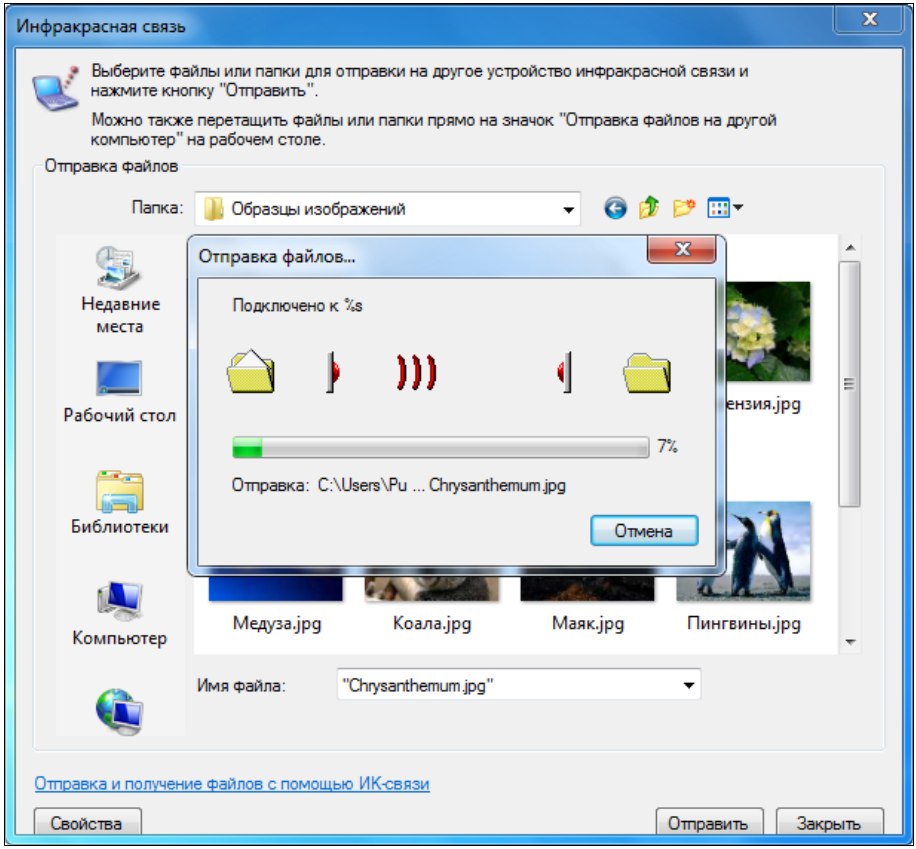

Рис. 3.30. Процесс передачи файла с компьютера на устройство через ИК-порт

Если данные передаются с устройства на компьютер, то нужно выбрать файл для передачи и выполнить команды, предписанные инструкцией по работе с устройством. На компьютере появится окно с запросом на передачу файла (рис. 3.31, *слева*) — если разрешение на прием будет дано, то начинается пересылка и за ее ходом можно следить в окне (рис. 3.31, *справа*).

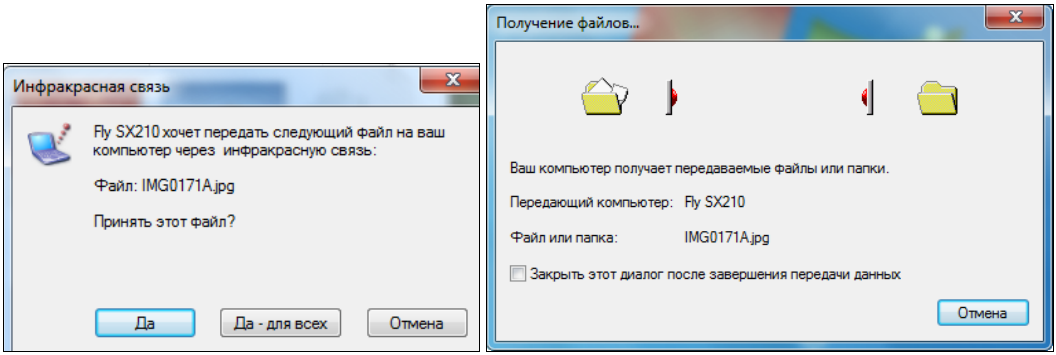

Рис. 3.31. Получение разрешения на прием файла и отображение хода процесса его получения

Как можно видеть, набор операций при работе через ИК-порт минимален и не требует специального освоения.

Настройка устройств для работы с коммутируемыми подключениями. Подключение к Интернету

Если устройство, подключенное к компьютеру по каналу Bluetooth, через ИК-порт или просто с помощью кабеля[1], может эмулировать модем, работающий по последовательному порту, и обеспечивает передачу данных по протоколам GPRS, EDGE[2] и т. п. для связи с Интернетом[3], то несложно создать подключение удаленного доступа и использовать его для выхода в Интернет компьютера или локальной сети (включив совместный доступ к подключению).

Процедура создания коммутируемого (телефонного) подключения во всех случаях совершенно стандартная (она описана в *главе 2*), и различие будет лишь в выбранном модеме. Например, для связи может использоваться "Стандартный модем по соединению Bluetooth" (см. рис. 2.2 и рис. 2.5), "Стандартный модем по инфракрасному соединению" и т. п. Набираемый номер, имя пользователя и пароль зависят от оператора связи, эту информацию лучше уточнить в салоне связи (для телефона может потребоваться дополнительная строка инициализации модема). Например, для некоторых популярных операторов связи используются следующие параметры:

	Набираемый номер	**Имя пользователя**	**Пароль**
"Билайн"	*99#	beeline	beeline
"Мегафон"	*99#	gdata	gdata
МТС	*99#	mts	mts

Нужны ли дополнительные параметры — это лучше уточнить у оператора связи (как не мешает узнать и тариф за подключение[4]) или найти информацию в Интернете (для начала можно попробовать указанные параметры).

Все созданные коммутируемые подключения постоянно отображаются в окне активных сетей (см. рис. 3.6), где любое подключение можно выбрать и активизировать, нажав кнопку **Подключение** (Connect). Для просмотра Интернета не забудьте проверить или настроить предпочитаемое подключение (см. рис. 2.11).

---

[1] Если для устройства имеется кабель передачи данных (data-кабель) для подключения к компьютеру.

[2] Тип телефона и применяемые протоколы могут повлиять только на скорость подключения; процедура подключения будет оставаться стандартной (даже если вместо связи через Bluetooth будет использоваться ИК-порт).

[3] То есть если такая возможность имеется технически, и используемый тарифный план включает эту возможность.

[4] Использование 3G-модема со специальным тарифом, скорее всего, обойдется заметно дешевле.

Любое такое подключение можно сделать общим и использовать совместно для подключения к Интернету *(см. главу 2)*.

Телефонные 3G-модемы

В настоящее время USB-модемы для подключения к Интернету и специальные тарифные планы предлагают все ведущие операторы сотовой связи, начиная с "большой тройки": МТС, "Билайн" и "Мегафон". Не будем говорить об используемых ими стандартах и перспективных стандартах 4-го поколения, а для обозначения таких модемов воспользуемся (как это делают в коммерческих целях некоторые продавцы устройств) "обобщенной" аббревиатурой 3G (3-е поколение). Нас интересуют общие принципы подключения и использования таких устройств в системах Windows 7. Чтобы разговор был конкретным, рассмотрим все операции на примере одного из предлагаемых модемов[1].

По сути 3G-модем является специализированным мобильным телефоном, подключаемым к USB-порту и ориентированным на передачу данных; он имеет свой номер[2] и связан с определенным тарифным планом (стандартным или специально выбранным). Пополнение счета осуществляется через платежные терминалы, как и для обычных телефонов.

Все необходимые программы и драйверы модем имеет внутри. При его подключении к USB-порту компьютера появляется окно автозапуска программы установки (рис. 3.32), и в нем нужно запустить файл AutoRun.exe. Впоследствии это же окно будет снова появляться при подключении модема, но ничего уже устанавливаться не будет, а будет запускаться программа управления модемом (см. рис. 3.34). Если

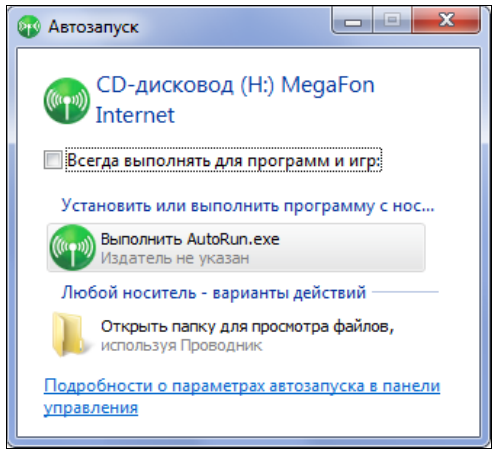

Рис. 3.32. Запуск установки драйверов и программы управления модемом

[1] Просим поверить, что этот выбор случайный (никакой рекламы!).

[2] На него можно даже отправлять смски и получать ответы.

программа установки не стартует автоматически, то файл AutoRun.exe следует вручную запустить с CD-дисковода, который эмулируется модемом[1].

При установке драйверов не следует спешить, нужно дождаться готовности всех используемых драйверов (рис. 3.33). Здесь особенно важны компоненты самого модема (3G Modem) и пользовательского интерфейса (3G PC UI Interface). После установки необходимо проверить в диспетчере устройств (Device Manager), что все драйверы установлены без ошибок.

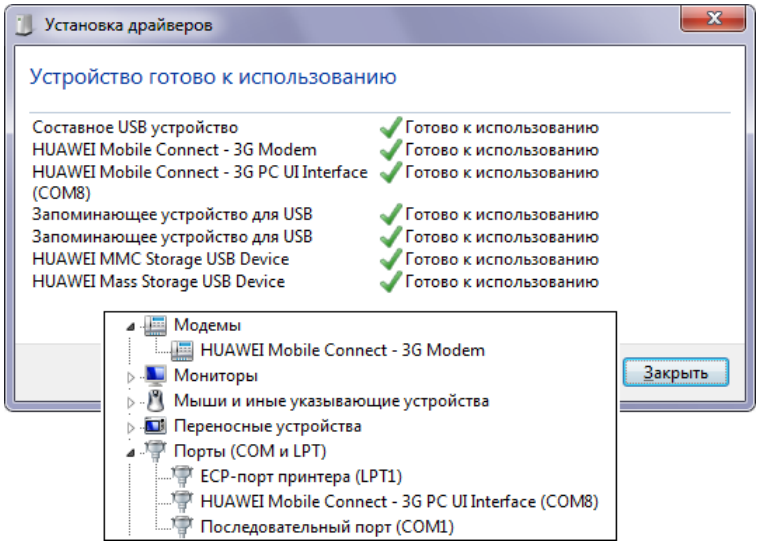

Рис. 3.33. Установка драйверов и программные компоненты 3G-модема

Ярлык для запуска программы управления модемом создается на рабочем столе, а значок модема появляется в области уведомлений на панели задач. В окне сетевых подключений автоматически создается подключение удаленного доступа (вполне стандартное телефонное подключение, соответствующее всем "правилам": оно отображается в списке активных сетей (см. рис. 1.1, *справа*) и его можно сделать общим подключением к Интернету). Для установления соединения можно использовать и стандартные методы системы Windows (об этом всегда следует помнить, особенно при настройке автоматического запуска подключения, а также при включении общего доступа к интернет-подключению), однако вручную удобнее работать со специальной программой управления модемом (рис. 3.34). При ее запуске необходимо каждый раз вводить ID-код модема, который идет в комплекте (если модем используется только на своем компьютере и нет опасения его потерять, то проверку этого кода можно и отключить).

Главным элементом окна программы управления модемом является команда включения и отключения (установки связи с Интернетом и разрыва связи). В процессе

[1] Если на модеме установлена дополнительная карта памяти (обычно microSD), то его можно также рассматривать и как внешний накопитель.

работы можно открыть окно статистики (см. рис. 3.34) и контролировать весь трафик (скорость и количество переданной информации) и время работы.

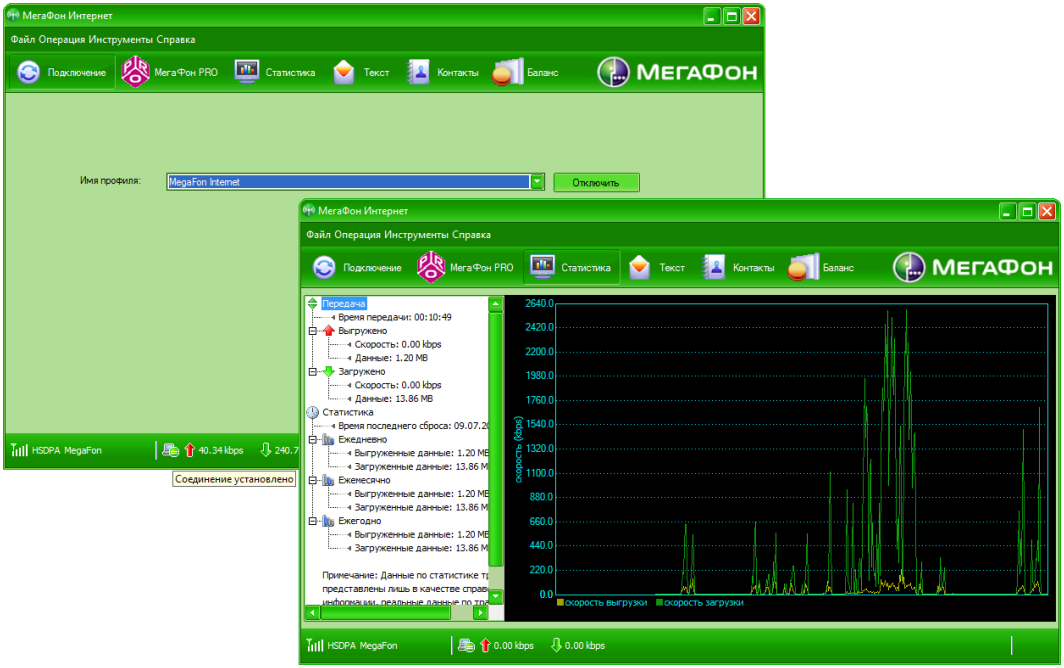

Рис. 3.34. Окно запуска модема и окно статистики

Кнопка **Текст** позволяет посылать текстовые сообщения ("смски") на любой мобильный номер (на них, соответственно, можно и отвечать). Кнопка **Баланс** служит (и это не удивительно!) для проверки текущего баланса счета. Обе операции, как и *получение* текстовых сообщений, не требуют подключения к сети!

При установке 3G-модема не забудьте проверить настройки браузера *(см. главу 2)*, поскольку в системе появляется новое коммутируемое подключение и возможна смена предпочитаемого соединения.

Таким образом, как можно видеть из сказанного, 3G-модем является устройством с оригинальными функциями, но для операционной системы — это обычный модем для коммутируемых телефонных подключений, со всеми вытекающими особенностями и требованиями *(см. главу 2)*. Поскольку с его помощью осуществляется подключение к внешней сети, то в целях безопасности необходимо помнить о правильном выборе профиля (сетевого размещения) и его настройках для специфических служб.

Примечание

Если говорить о конкретном модеме, описанном выше, то нужно добавить, что с помощью несложной программы (поставляемой вместе с модемом) и при наличии телефонной гарнитуры (или аналогичного оборудования) модем можно превратить в полноценный мобильный телефон для связи с любыми абонентами или с абонентами своей группы.

ГЛАВА 4

Обеспечение сетевой безопасности

Вопросы безопасности всегда являются одними из важнейших при работе на компьютере, а при работе в сети — локальной или в Интернете — появляются дополнительные требования. В этой главе описываются некоторые общие соображения, о которых необходимо помнить, а также средства Windows 7, обеспечивающие защиту сетевого трафика и самой системы.

Общие требования безопасности

Некоторые механизмы безопасности, используемые в Windows 7, появились более десятка лет назад, но ничуть не утратили актуальности. Поэтому следует вспомнить некоторые базовые принципы.

Каждый пользователь, работающий в системе, имеет *учетную запись* (account), для которой крайне желательно иметь пароль. По умолчанию невозможно подключиться к удаленной системе Windows 7, если применяется учетная запись ***без*** пароля, поэтому и доступ к удаленным общим ресурсам будет невозможен. Это справедливо, даже если компьютеры работают в составе домашней группы.

С учетными записями пользователей связаны их права (полномочия) в системе, а также разрешения доступа к различным локальным и общим сетевым ресурсам. Таким образом, учетные записи являются ключевым элементом системы безопасности Windows и требуются при работе в сети.

> ***Совет***
>
> Если необходимо, чтобы система загружалась сразу и не запрашивала каждый раз пароль, достаточно выполнить команду `control userpasswords2` и настроить автозагрузку для конкретной учетной записи.

Для организации доступа к другим компьютерам рабочей или домашней группы и их общим ресурсам можно использовать два подхода:

- создать *одинаковые учетные записи* с одинаковыми паролями на всех компьютерах. В этом случае пользователь, войдя в систему на одном компьютере, будет сразу получать доступ ко всем ресурсам, выделенным для совместного использования на других компьютерах;

- использовать для доступа к общим папкам *определенную учетную запись* и раздать другим клиентам сети ее имя и пароль. При обращении к общему ресурсу или при подключении сетевого диска (см. рис. 5.16) пользователи смогут указывать эти данные и сохранять их для последующих сеансов работы. При входе на удаленный компьютер имя учетной записи необходимо задавать в формате `COMPNAME\userName` (где `COMPNAME` — имя того компьютера), поскольку по умолчанию подставляется имя локального компьютера.

> ***Примечание***
>
> Для управления именами и паролями, использованными при входе на другие компьютеры, применяется *Диспетчер учетных данных* (Credential Manager), запускаемый из окна учетных записей по ссылке **Администрирование учетных записей** (Manage your credentials). Чтобы открыть это окно, достаточно щелкнуть по значку пользователя в верхней части меню **Пуск** (Start).

На этом с общими принципами обеспечения безопасности работы в системе можно закончить; в других главах книги рассматриваются конкретные случаи использования учетных записей и связанные с ними настройки.

Защита сетевых подключений с помощью встроенного брандмауэра (Windows Firewall)

В системах Windows 7 имеется встроенный *Брандмауэр Windows*[1] (Windows Firewall; сервис MpsSvc), позволяющий фильтровать всю информацию, поступающую из внешней сети (из Интернета) и обратно, пропуская только разрешенные TCP/UDP-пакеты и отбрасывая все остальные (таким образом, возможна фильтрация входящих и исходящих пакетов). По сравнению с предыдущими версиями, интерфейс для настройки заметно изменился; кроме того, все настройки правил фильтрации теперь выполняются только с помощью специальной оснастки *(см. далее)*.

Окно брандмауэра Windows Firewall открывается с панели управления (категория **Система и безопасность** (System and Security)) или из окна Центра управления сетями и общим доступом (Network and Sharing Center). (Также можно использовать команду `firewall.cpl`.) На рис. 4.1 показано главное окно брандмауэра, где одновременно можно видеть его состояние для домашних, рабочих (доменных) и общественных сетей. По умолчанию брандмауэр включен для всех сетей, и в конкретный момент времени для каждой сети активен *свой* профиль[2]. Возможна ситуация и наоборот — когда один профиль одновременно применяется к *нескольким* сетям.

---

[1] Даже если сравнить с версией, включенной в Windows Vista, интерфейс брандмауэра значительно изменился, а возможности расширились.

[2] Это одно из главных отличий данной версии брандмауэра, поскольку в Windows Vista, к примеру, один профиль применяется для *всех* подключений, причем выбираются самые "строгие" ограничения.

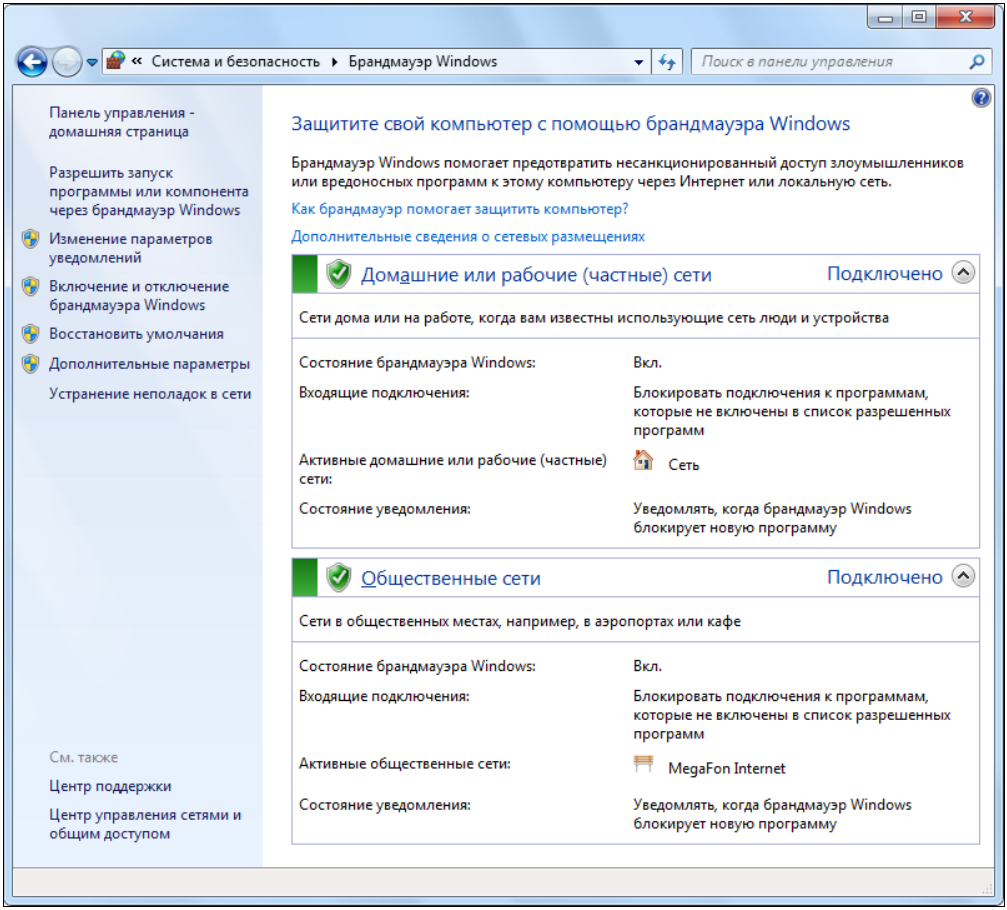

Рис. 4.1. Главное окно брандмауэра Windows

На панели задач слева (см. рис. 4.1) представлены ссылки для настройки сетевого доступа к программам и компонентам *(см. далее)*, а также для управления уведомлениями для каждого типа сетей, включения и выключения брандмауэра *(см. далее)*. Специальная ссылка позволяет восстановить все исходные параметры.

Для изменения состояния брандмауэра используется ссылка **Включение и отключение брандмауэра Windows** (Turn Windows Firewall on or off). В окне параметров (рис. 4.2) выбирается состояние программы и указывается необходимость уведомлений при блокировке. Здесь можно быстро отключать ***все*** входящие соединения, если работа в сети предъявляет повышенные требования к безопасности компьютера.

> ***Внимание!***
>
> При необходимости отключать брандмауэр рекомендуется именно с помощью показанных опций (см. рис. 4.2), а не путем остановки и запрета сервиса брандмауэра MpsSvc! Отключение данного сервиса может повлечь за собой трудно диагностируемые ошибки или потери в функциональности других сетевых средств.

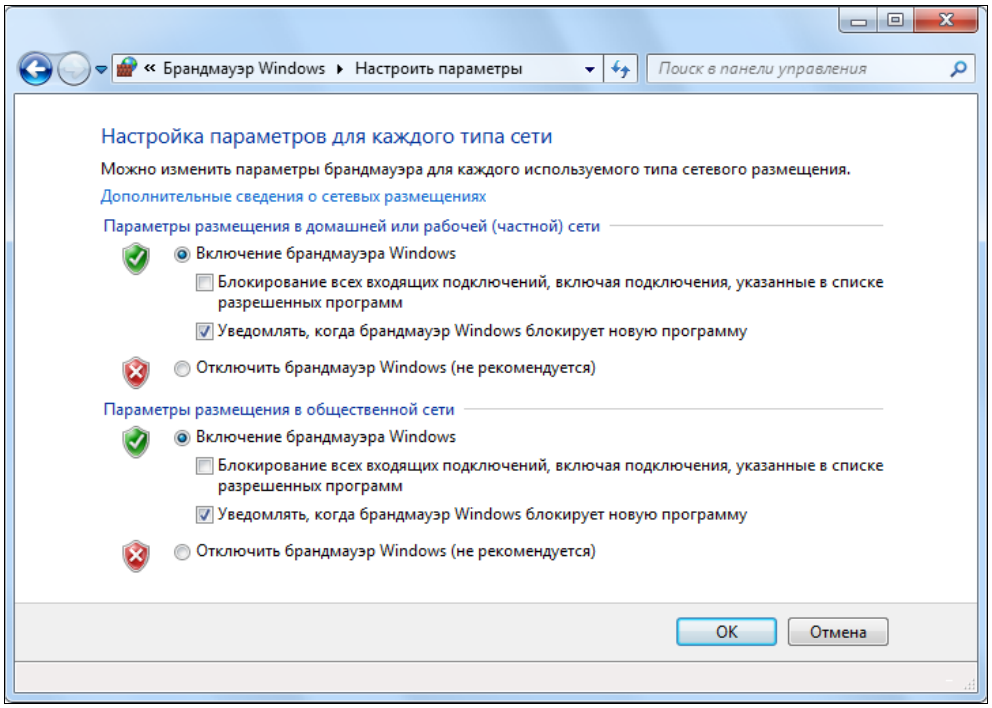

Рис. 4.2. Управление состоянием брандмауэра Windows для разных сетевых размещений

Для доступа к основным параметрам брандмауэра (правилам фильтрации) служит ссылка **Дополнительные параметры** (Advanced settings) (см. рис. 4.1), запускающая специальную оснастку *(см. далее)*.

Ссылка **Разрешить запуск программы или компонента через брандмауэр Windows** (Allow a program of feature through Windows Firewall) позволяет открыть окно (рис. 4.3), где указывается — каким программам и компонентам Windows разрешено работать через брандмауэр. Стандартные компоненты можно просто отмечать флажками; кнопка **Сведения** (Details) позволяет получить дополнительную информацию об используемых функциях и протоколах. Нажав кнопку **Разрешить другую программу** (Allow another program), можно выбрать приложение, отсутствующее в списке, и включить его в число разрешенных — при этом следует указать тип размещения, в котором это приложение сможет работать.

> ***Примечание***
>
> Фактически список разрешенных программ (см. рис. 4.3) — это упрощенный интерфейс для управления стандартными, уже настроенными правилами фильтрации, представленными в окне оснастки **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security) (см. рис. 4.4). В этом легко убедиться, разрешая и запрещая программы и просматривая разрешенные правила для соответствующей группы в окне оснастки. Это значительно упрощает работу и позволяет избегать ошибок в выборе правил.

За списком разрешенных компонентов особенно нужно следить при удаленном администрировании и доступе к рабочему столу, при использовании удаленного по-

мощника *(см. главу 7)*, при работе со службами IIS *(см. главу 8)* и т. д. — во всех тех случаях, когда программы и функции требуют индивидуальной разблокировки. Однако некоторые функции или программы (например, Windows Live Messenger, Virtual PC, Skype и т. п.) автоматически указываются в списке разрешенных компонентов при их установке или активации (разрешении пользователем необходимых соединений).

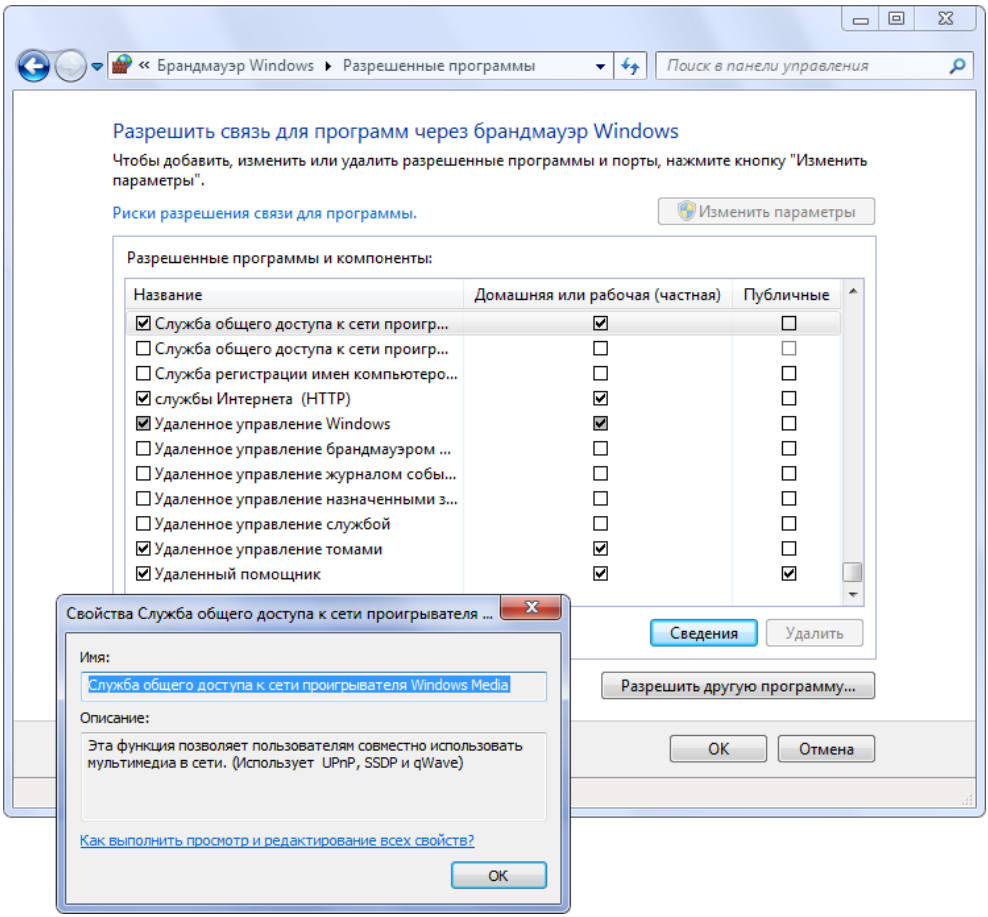

Рис. 4.3. Разрешение программам и компонентам доступа через брандмауэр Windows

Средства расширенного конфигурирования брандмауэра

В отличие от Windows Vista, какая-либо настройка конкретных правил фильтрации (rules) для встроенного брандмауэра в системах Windows 7 осуществляется только с помощью оснастки **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security) (рис. 4.4). Эта оснастка запускается из главного окна брандмауэра (см. рис. 4.1) по ссылке **Дополнительные параметры**

(Advanced settings) или непосредственно из программной группы **Администрирование** (Administrative Tools).

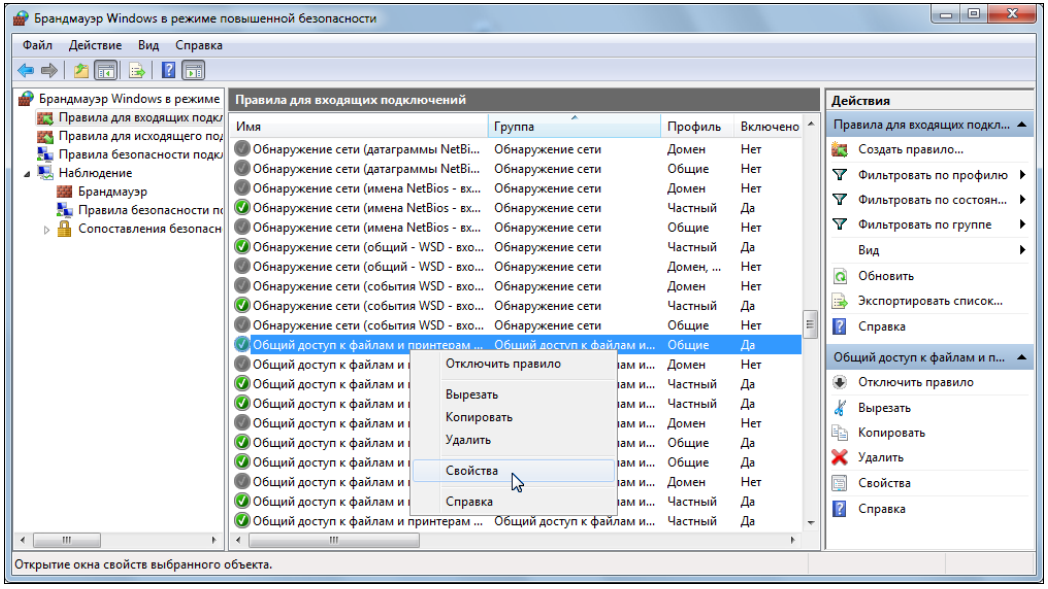

Рис. 4.4. Главное окно оснастки **Брандмауэр Windows в режиме повышенной безопасности**

Примечание

Просмотрите внимательно все многочисленные столбцы параметров в окне оснастки (см. рис. 4.4). Многие интересные и нужные параметры — например, имя программы или сервиса, связанного с правилом, название протокола и номер порта и т. п. — не помещаются на панели, и требуется ее прокрутка. Набор и порядок отображаемых столбцов[1] можно изменить с помощью команды **Вид | Добавить или удалить столбцы** (View | Add/Remove Columns), открывающей специальное окно для выполнения этой операции. В нем имеется также кнопка **По умолчанию** (Restore Defaults), восстанавливающая исходный вид окна и набор столбцов.

Правила для входящих и исходящих подключений группируются в окне оснастки в отдельных папках — это вполне очевидно. Специально следует объяснить назначение папки **Брандмауэр** (Firewall), входящей в область **Наблюдение** (Monitoring), — здесь отображаются только *активные* правила брандмауэра, т. е. правила, связанные со всеми используемыми в данный момент профилями сети (выбранными сетевыми размещениями). Поэтому для анализа текущей ситуации можно обращаться именно к этой папке. Неудобством является то, что на эту папку не распространяется действие фильтров *(см. далее)*.

Оснастка **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security) позволяет включать и отключать стандартные, предопределенные правила, а также создавать и конфигурировать дополнительные правила для каждого входящего и исходящего пакета "с точностью" до порта (TCP

[1] Столбцы можно перетаскивать в окне просто с помощью мыши, захватывая и перемещая заголовок столбца.

или UDP). Включенные правила в окне оснастки отмечены значком зеленого цвета с галочкой; выключенные правила имеют аналогичный серый значок, а запрещения помечаются специальным значком красного цвета.

Брандмауэр Windows работает с тремя сетевыми профилями:

- *доменный* профиль (Domain Profile);
- *частный* профиль (Private Profile);
- *общий* профиль (Public Profile).

С каждым профилем, которому соответствует сетевое размещение *(см. главу 1)*, связаны определенные правила, и эти правила можно индивидуально настраивать в соответствии со своими представлениями о требованиях безопасности (в данном случае речь идет о наборе разрешенных портов), предъявляемых к каждой категории сети.

Работу с многочисленными правилами (rules) значительно упрощают *фильтры*, включаемые на панели **Действия** (Actions) (см. рис. 4.4). С их помощью легко выбрать в окне программы только нужные группы правил, сортируя их по *сетевому профилю* (одному из трех), *состоянию* (включенные/выключенные (Enabled/Disabled)) и *группе*. Выбранные фильтры сохраняются и при последующих запусках, поэтому сбрасывать их нужно с помощью специальной команды (**Сброс всех фильтров** (Clear All Filters)). Если, например, выбрать частный профиль и включенные правила, то легко увидеть, какие подключения в данный момент разрешены к компьютеру, находящемуся в домашней сети, и для каких программ (компонентов). Включив фильтр для группы[1], можно увидеть правила, связанные с некоторым приложением, сетевой функцией или системным компонентом.

Помимо множества предустановленных правил, можно создавать и собственные — для этого используется специальный мастер, упрощающий эту операцию. В окне свойств правила приводятся подробные сведения обо всех заданных параметрах, здесь же изменяется состояние правила. На примере предустановленного правила (рис. 4.5) можно видеть, что эти параметры позволяют контролировать все аспекты сетевого взаимодействия (протоколы, порты, диапазоны разрешенных адресов, приложения, сервисы и т. д.).

Каждое правило брандмауэра (для входящего или для исходящего трафика) выполняет одно из трех действий для всех подключений, соответствующих заданным условиям (можно указывать компьютеры, пользователей, программы, службы, порты и протоколы):

- *разрешить* подключение;
- *разрешить* только *безопасное* подключение (т. е. подключение, защищенное протоколом IPsec);
- *блокировать* подключение.

---

[1] Обязательно посмотрите сами, какие группы имеются! Это позволит заметно упростить настройку брандмауэра или анализ текущих параметров.

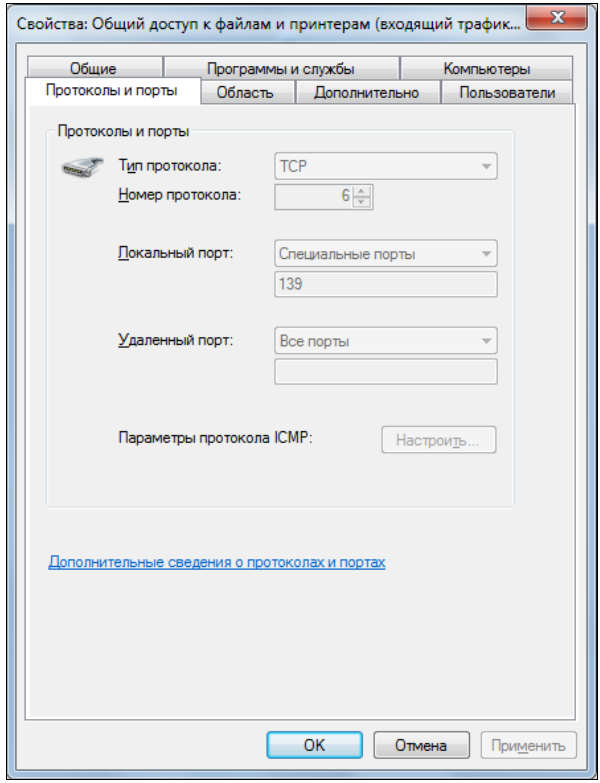

Рис. 4.5. Окно свойств правила фильтрации — выбранные протокол и порт

Последнее действие стоит прокомментировать. Зачем блокировать подключение, если по умолчанию и так запрещен весь входной трафик, не подпадающий под правила, разрешающие соединения? Причина простая. С помощью правила блокировки во всем *разрешенном* трафике легко выбрать отдельные "объекты" (IP-адреса, компьютеры, пользователей и т. д.), для которых соединение будет *запрещено*.

В правиле можно указывать, к какому типу интерфейса будет применимо это правило: к локальной сети, беспроводной сети, сети удаленного доступа (например, к VPN-подключениям) или ко всем типам. Каждое правило может применяться ко всем профилям или только к указанным явно.

Настройка сетевых параметров и брандмауэра из командной строки

Утилита командной строки `Netsh.exe` предназначена для настройки параметров сетевых подключений и может использоваться в любых версиях Windows 7 (как и во многих других версиях Windows). Утилита запускается в интерактивном или командном режиме. В первом случае администратор пошагово выбирает нужный *контекст* (набор сетевых параметров, относящихся к определенному компоненту или протоколу) и выполняет имеющиеся команды. Во втором — все параметры за-

даются утилите при запуске, и она выполняет конкретную задачу (этот режим можно использовать и из командных файлов). Для каждого контекста легко получить набор допустимых команд, введя слово `help` или просто символ вопроса.

Рассмотрим на примерах некоторые возможности утилиты `netsh`. В первую очередь она может пригодиться при настройке многочисленных правил брандмауэра Windows, поскольку вряд ли на домашних компьютерах возникнет необходимость в настройке параметров TCP/IP из командной строки (обычно используются окна свойств протоколов — см. рис. 1.18) — однако для полноты картины приведем и несколько примеров управления IP-адресами. Иногда утилиты командной строки (`netsh` и `ipconfig`) много удобнее графического интерфейса, поскольку позволяют увидеть весь набор параметров *сразу*, а не искать их по разным окнам (например, при анализе параметров нескольких сетевых подключений).

Назначение IP-адресов

Для просмотра текущих параметров стека TCP/IP используются команды `netsh interface ipv4 show config` и `netsh interface ipv6 show addresses`.

Они позволяют увидеть назначенные адреса и названия интерфейсов, которые во многих командах необходимо использовать в качестве параметра[1]: например, стандартное название локального подключения для русских версий системы — "Подключение по локальной сети" (для английских — "Local Area Connection"). Также имена интерфейсов можно получить с помощью команды `netsh interface ipv4 show interfaces`.

Имя интерфейса важно знать при изменении параметров стека. Например, следующая команда назначает подключению по локальной сети статический IP-адрес (192.168.0.2 с маской 255.255.255.0) и адрес шлюза (192.168.0.1 с метрикой 1):

```
netsh interface ipv4 set address "Подключение по локальной сети" static
192.168.0.2 255.255.255.0 192.168.0.1 1
```

Чтобы включить получение адреса от сервера DHCP, используется команда **`netsh interface`** `ipv4` **`set address name=`**`"Подключение по локальной сети"` **`source=dhcp`**.

Для назначения подключению статического адреса предпочитаемого (preferred) DNS-сервера (192.168.0.1) можно выполнить такую команду:

```
netsh interface ipv4 set dnsserver "Подключение по локальной сети" static
192.168.0.1 primary
```

Дополнительный адрес DNS-сервера задается с помощью параметра `add dnsserver`.

Управление брандмауэром

Многочисленные возможности утилиты `netsh` можно использовать и для управления брандмауэром Windows. Иногда текущие значения сетевых параметров проще получить с ее помощью, нежели в результате просмотра многочисленных диалоговых окон или списков исключений (правил).

---

[1] Например, см. команды автоматической установки подключений по запросу в *главе 2*.

С помощью команды[1] `netsh firewall show state` можно увидеть текущее состояние брандмауэра Windows (включая выбранный сетевой профиль); также удобна команда `netsh firewall show opmode`. Для просмотра параметров, установленных для всех профилей, служит команда `netsh firewall show config`.

Группы параметров брандмауэра можно просматривать индивидуально, например:

- `netsh firewall show allowedprogram` — показывает список разрешенных программ для используемых профилей;
- `netsh firewall show portopening` — перечисляет порты, вручную добавленные к списку исключений;
- `netsh firewall show icmpsetting` — показывает разрешенные ICMP-сообщения.

Команда `netsh firewall set opmode mode = DISABLE` позволяет полностью ***выключить*** брандмауэр (сервис MpsSvc при этом не останавливается!); при использовании параметра `ENABLE` брандмауэр ***активизируется***.

Для работы с брандмауэром Windows в режиме повышенной безопасности используется контекст `netsh advfirewall`. В этом контексте для просмотра текущих параметров интересны команды `show currentprofile` и `show allprofiles`.

Для отключения всех профилей (что эквивалентно выключению брандмауэра — см. команду `netsh firewall set opmode mode = DISABLE`) используется команда `set allprofiles state off`.

> ***Внимание!***
>
> Как уже говорилось ранее, в случае необходимости отключать брандмауэр рекомендуется с помощью соответствующих опций в графическом интерфейсе или приведенных выше команд выключения всех профилей, а не путем остановки сервиса брандмауэра MpsSvc.

С помощью команды `state on` можно включить все профили или один конкретный: например, для включения частного профиля для домашней сети используется команда `set privateprofile state on`.

Следующая команда позволяет увидеть параметры всех правил (список очень длинный!) для входящих (`in`) или исходящих (`out`) соединений (если параметр `dir` отсутствует, то отображаются все имеющиеся правила):

```
netsh advfirewall firewall show rule name=all dir=in
```

Можно указать имя конкретного правила[2], например (регистр букв в имени значения не имеет):

```
netsh advfirewall firewall show rule name="Общий доступ к файлам и принтерам
(эхо-запрос — входящий трафик ICMPv4)" dir=in
```

---

[1] Все перечисленные ниже команды успешно работают в Windows 7, хотя большинство из них система считает устаревшими и вместо них рекомендует применять команды из контекста `netsh advfirewall firewall`. Однако приведенные команды короче, поэтому мы и предлагаем познакомиться с ними.

[2] Названия правил вводятся буквально — так, как они отображаются в окне оснастки брандмауэра.

Названия правил можно также видеть на панели правил входящих и исходящих соединений в окне оснастки **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security) (см. рис. 4.4). Здесь же отображаются названия *групп* правил. (Название правила легко скопировать из окна его свойств и вставить в нужную команду в окне консоли.)

Включать и выключать правила можно как для отдельного имени (параметр `name`), так и для группы имен (параметр `group`). Например, следующая команда позволяет запретить эхо-ответы (File and Printer Sharing (Echo Request – ICMPv4-In)) для всех профилей (при использовании параметра `profile` можно назначить операцию для конкретного профиля):

```
C:\>netsh advfirewall firewall set rule name="Общий доступ к файлам и принтерам (эхо-запрос — входящий трафик ICMPv4)" new enable=no
Обновлены правила: 3.
OK.
```

Следующая команда разрешает все правила, входящие в группу "Удаленное управление Windows" (Windows Remote Management), для всех профилей:

```
C:>netsh advfirewall firewall set rule group="Удаленное управление Windows" new enable=yes
Обновлены правила: 4.
OK.
```

Защита компьютера от шпионских программ

Говоря о работе в сети (в первую очередь, конечно, подразумевая Интернет), нельзя обойти вниманием вопросы защиты системы и пользовательских файлов от вирусов, троянов и прочей "нечисти", с которой легко столкнуться даже на вполне проверенных публичных сайтах[1]. В табл. 4.1, взятой из одного блога на сайте **http://blogs.technet.com**, перечислены функциональные возможности нескольких поколений программ, выпускаемых компанией Microsoft для защиты систем Windows от шпионских (spyware) программ и вредоносных приложений, которые могут нарушить работоспособность и безопасность системы.

Средство удаления вредоносных программ распространяется через Windows Update. *Защитник Windows* является стандартным компонентом систем Windows Vista и Windows 7, его можно свободно скачать и установить и на предыдущие версии Windows, как и более поздний продукт — программу *Microsoft Security Essentials*[2].

---

[1] Например, если на сайте используется баннерная реклама, то в нее запросто может попасть ссылка с вредоносным или опасным кодом. Во всяком случае, автор сталкивался несколько раз с подобным на давно известных сайтах, и программа Microsoft Security Essentials мгновенно и успешно блокировала такие страницы.

[2] Центр поддержки (Action Center) рассматривает эту программу как защиту от вирусов и программ-шпионов и в случае ее установки не выдает предупреждений о наличии "дыр" в безопасности системы.

Forefront Client Security является клиентской частью набора программ Microsoft Forefront, используемых для обеспечения безопасности корпоративных сетей (**http://www.microsoft.com/forefront/ru/ru/default.aspx**).

Таблица 4.1. *Сравнительные характеристики программ защиты Windows от компании Microsoft*

	Средство удаления вредоносных программ (Malicious Software Removal Tool)	**Защитник Windows** (Windows Defender)	**Microsoft Security Essentials**	**Forefront Client Security**
Удаление распространенных видов вредоносного кода	Да	Нет	Да	Да
Удаление известных вирусов	Нет	Нет	Да	Да
Антивирус реального времени	Нет	Нет	Да	Да
Удаление известных программ-шпионов	Нет	Да	Да	Да
Защита от программ-шпионов в реальном времени	Нет	Да	Да	Да
Защита от rootkit	Нет	Нет	Да	Да
Контроль наличия потенциальных уязвимостей (пропущенные обновления безопасности ОС и т. д.)	Нет	Нет	Нет	Да
Интеграция с Network Access Protection (NAP)	Нет	Нет	Нет	Да
Централизованное управление	Нет	Да (групповые политики)	Нет	Да
Централизованный мониторинг и отчетность	Нет	Нет	Нет	Да

Защитник Windows

Одним из стандартных компонентов систем Windows 7 для обеспечения безопасности системы является программа *Защитник Windows* (Windows Defender, сервис WinDefend). Пиктограмму программы можно найти на панели управления, открытой в режиме представления всех задач. Значок программы  может постоянно отображаться в области уведомлений на панели задач, в этом случае программа запускается после двойного щелчка по этому значку. Обычно значок программы появляется только тогда, когда программа обнаруживает активность, требующую от нее определенных действий.

На рис. 4.6 показано главное окно программы. В нем отображаются информация о состоянии компьютера, время последнего сканирования, расписание запуска, статус онлайновой защиты и версия описаний программ (файлы описаний могут загружаться из Интернета автоматически, по мере регулярного обновления на вебсайте Microsoft). В меню **Проверить** (Scan) можно выбрать операции быстрого и полного сканирования, а также определить свои параметры сканирования компьютера. Ссылка **Журнал** (History) позволяет просмотреть список действий, выполненных с потенциально опасными элементами.

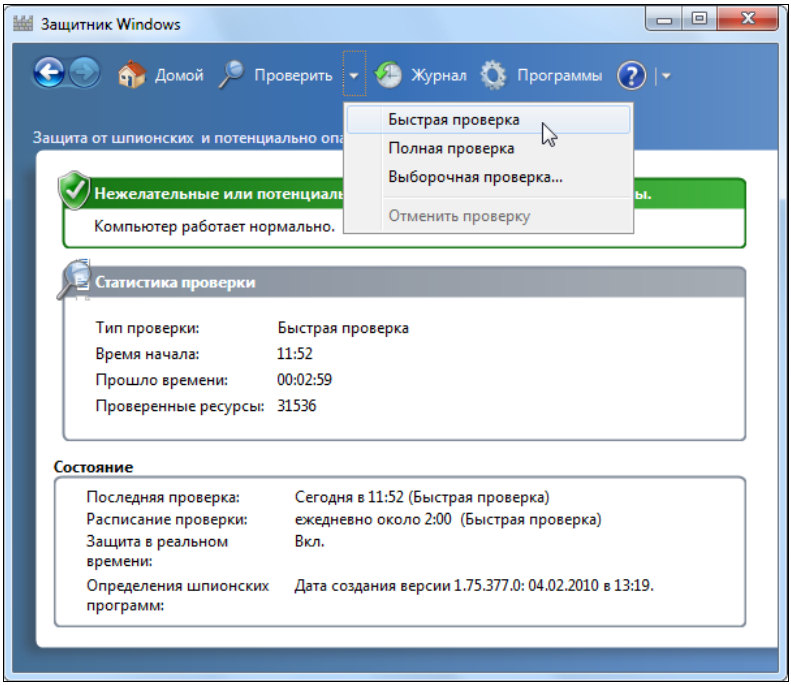

Рис. 4.6. Главное окно программы Защитник Windows

Защитник Windows обеспечивает два режима работы, минимально нагружающих систему и не мешающих работе пользователя:

- программа постоянно находится в памяти и следит за появлением нежелательных запущенных процессов, выдавая оперативное предупреждение пользователю (это стандартное состояние программы);
- Защитник может сканировать систему (память и жесткие диски) по запросу пользователя или по расписанию.

По ссылке **Программы** (Tools) можно попасть в окно параметров программы и дополнительных средств (рис. 4.7). Ссылка **Объекты в карантине** (Quarantined items) позволяет увидеть список приложений, которые были заблокированы по той причине, что представляли угрозу безопасности компьютера.

Если удаление было ошибочным, то программу можно восстановить и разрешить ее работу. Если Защитник Windows не смог принять решение о блокировке про-

граммы, то он запрашивает подтверждение на работу приложения и разрешенные программы помещает в раздел **Разрешенные объекты** (Allowed items).

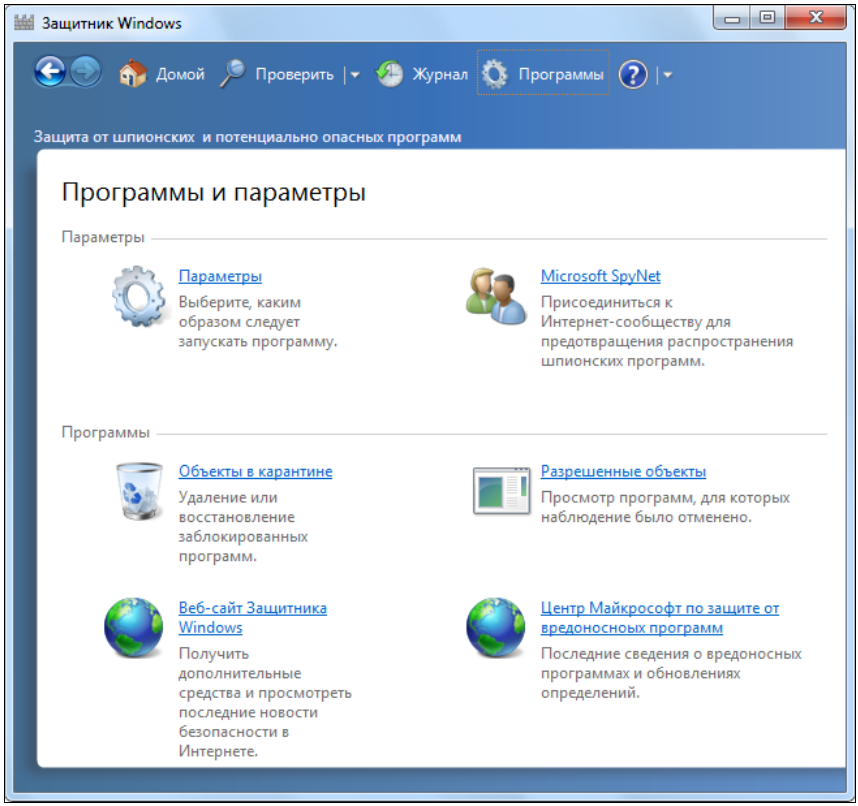

Рис. 4.7. Окно параметров и программ

Примечание

В системах Windows Vista в составе Защитника Windows также имеется *Проводник программного обеспечения* (Software Exporer), позволяющий получать подробную информацию обо всех программах, работающих в системе. В версии Windows 7 эта программа отсутствует, поскольку многие ее функции выполняет Монитор ресурсов (Resource Monitor) *(см. главу 1)*.

По ссылке **Параметры** (Options) можно попасть в окно многочисленных параметров программы Защитник Windows (рис. 4.8). В нем определяется расписание запуска программы (автоматической проверки), разрешается загрузка обновленных описаний сигнатур, выбираются параметры защиты в реальном времени (real-time) и т. д. В конце списка параметров в группе "Администратор" находятся два флажка, первый из которых включает и выключает сам Защитник Windows (при этом будет остановлен и сервис WinDefend, тип запуска которого меняется на ручной), а второй — разрешает просматривать результаты проверок, выполненных другими пользователями компьютера.

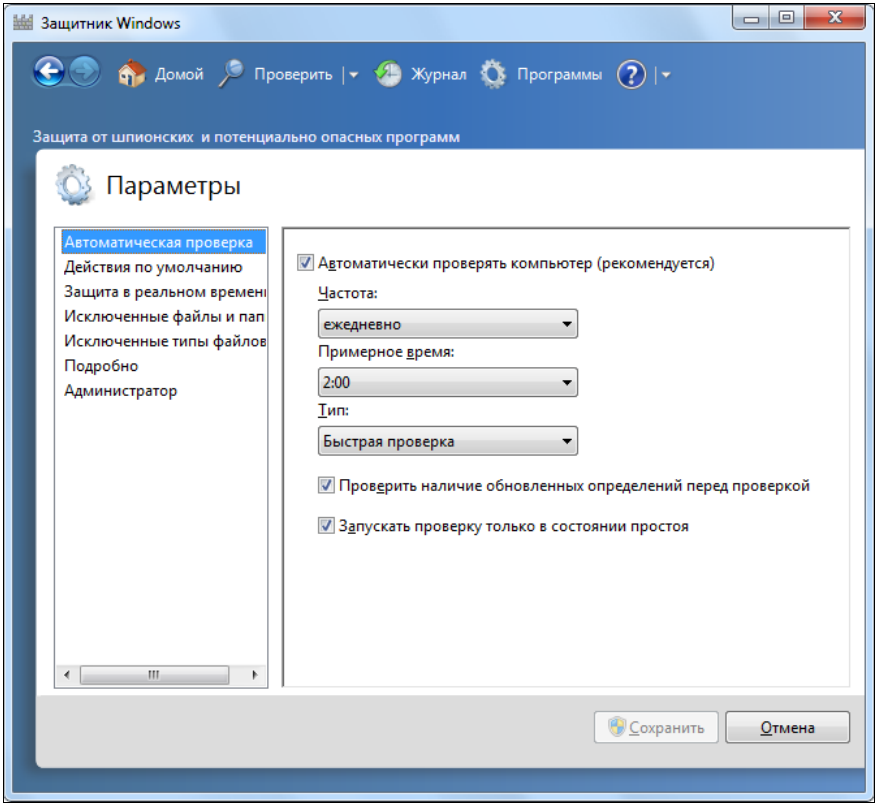

Рис. 4.8. Окно параметров Защитника Windows

Примечание

Если в системе устанавливается программа Microsoft Security Essentials *(см. далее)*, то Защитник Windows отключается. При попытке обращения к нему появляется окно предупреждения (рис. 4.9), в котором программу можно временно включить (после перезагрузки системы она снова будет выключена).

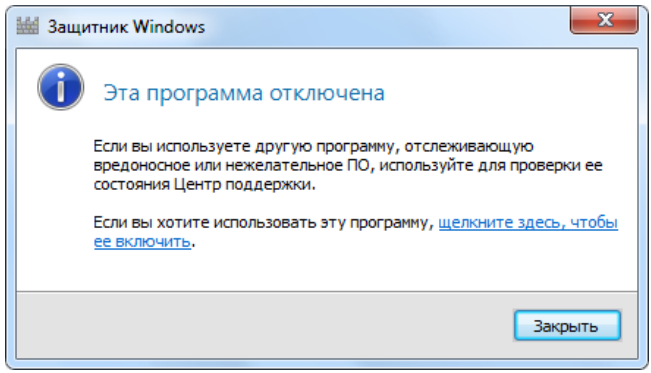

Рис. 4.9. Окно запуска отключенного Защитника Windows

Microsoft Security Essentials

Программа *Microsoft Security Essentials* может работать[1] на операционных системах Windows XP SP2 или SP3, Windows Vista SP1 или SP2 и Windows 7. Программа размером 8,16 Мбайт свободно скачивается с веб-сайта **http://www.microsoft.com/security_essentials/**. Имеются варианты для множества языков, включая русский. После установки программы ее значок  постоянно отображается в области уведомлений на панели задач. Дважды щелкнув по значку, легко открыть окно программы; также это можно сделать из меню **Пуск | Все программы** (Start | All Programs).

На рис. 4.10 показано главное окно программы. В нем легко увидеть текущее состояние и запустить быструю или полную проверку локальных дисков компьютера. На вкладке **Параметры**, похожей на соответствующее окно Защитника Windows (см. рис. 4.8), располагаются многочисленные настройки программы, управляющие запуском по расписанию, загрузкой обновлений, действиями при обнаружении зловредных программ и т. д.

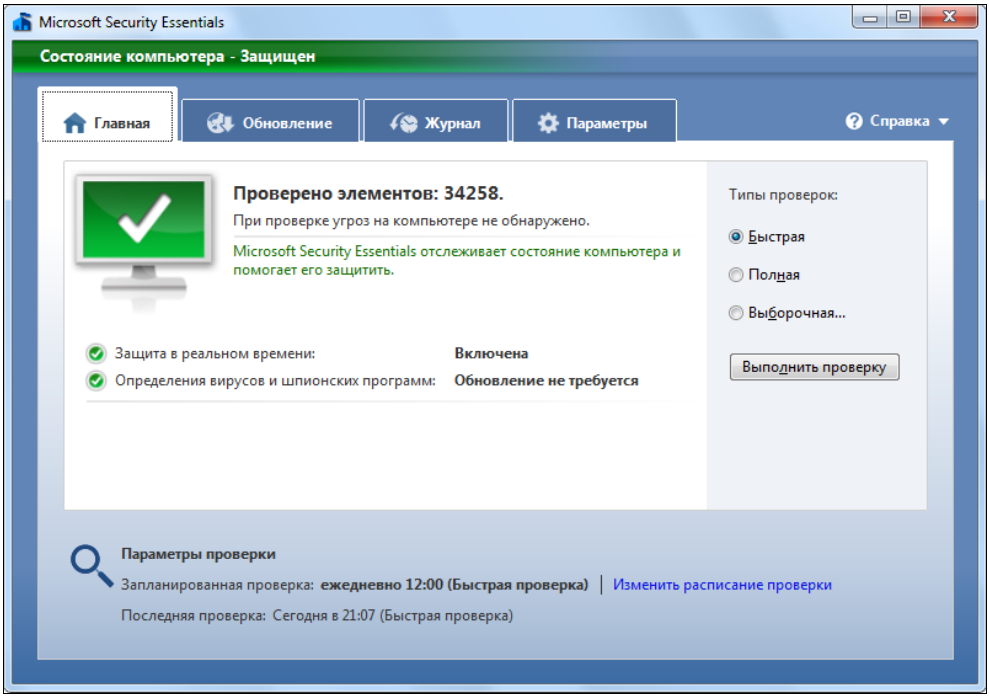

Рис. 4.10. Главное окно программы Microsoft Security Essentials

После установки программы в контекстном меню каждого файла и папки появляется команда **Проверка с помощью Microsoft Security Essentials**[2] (Scan with ...)

[1] При условии проверки на подлинность!

[2] Вид команды определяется языком установленной программы.

(см. рис. 5.15) — с ее помощью легко протестировать выбранный объект. Особенно это рекомендуется делать с новыми файлами, скачанными из Интернета или переписанными со съемных носителей и оптических дисков.

При обнаружении угроз в главном окне программы появляются соответствующее предупреждение и красная кнопка с предложением очистить компьютер (рис. 4.11).

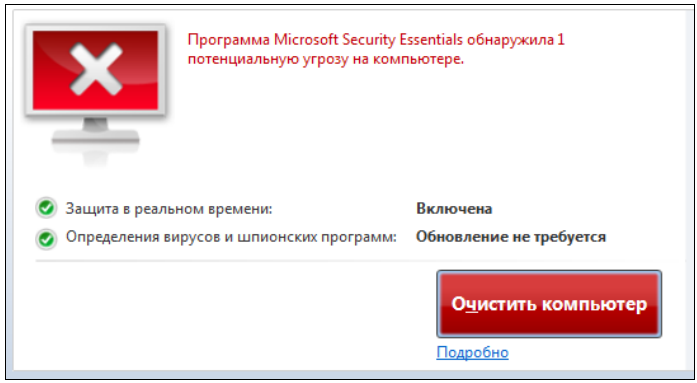

Рис. 4.11. Предупреждение об обнаружении вируса или шпионской программы

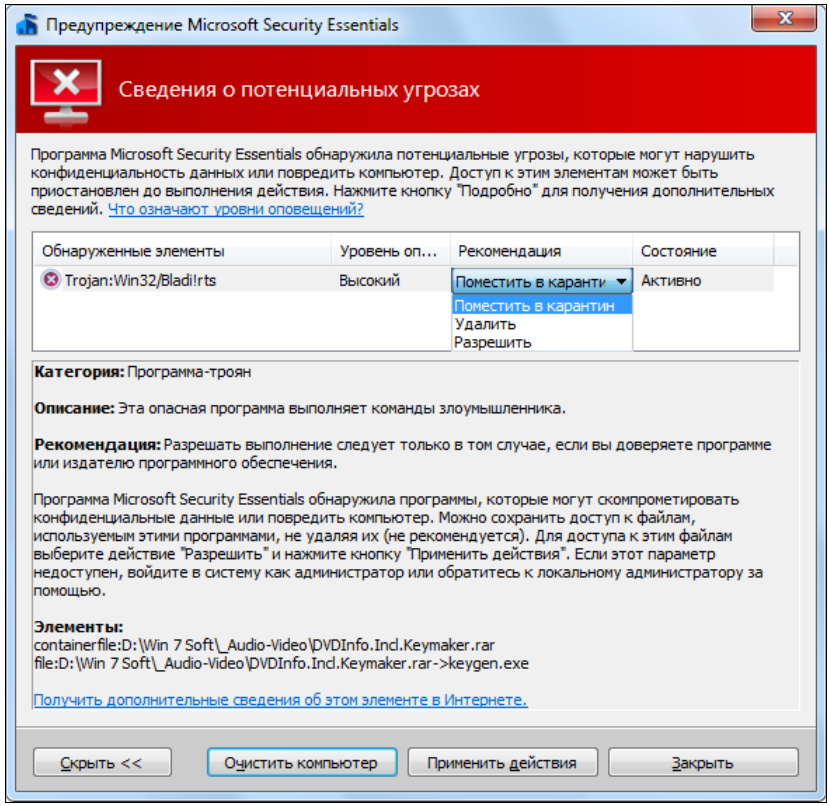

Рис. 4.12. Подробная информация, касающаяся обнаруженной угрозы

Щелкнув по ссылке **Подробно**, можно в специальном окне (рис. 4.12) увидеть детальную информацию, включающую название обнаруженного элемента, уровень угрозы и выполняемое действие. Также указывается имя файла (он может находиться в кэше браузера).

Предупреждение будет действовать до тех пор, пока пользователь не выберет действие и не выполнит указанную операцию (или пока эта операция не будет выполнена автоматически, если разрешено настройками программы). После успешного выполнения действий появится соответствующее сообщение, и окно программы сменит цвет на зеленый.

Сведения обо всех обнаруженных угрозах и выполненных действиях хранятся в **Журнале** (рис. 4.13). Файлы, помещенные в карантин, можно восстановить (если они не представляют опасности) или удалить окончательно. Как можно видеть, все действия программы и необходимые ответы пользователя интуитивно понятны и не требуют особого изучения.

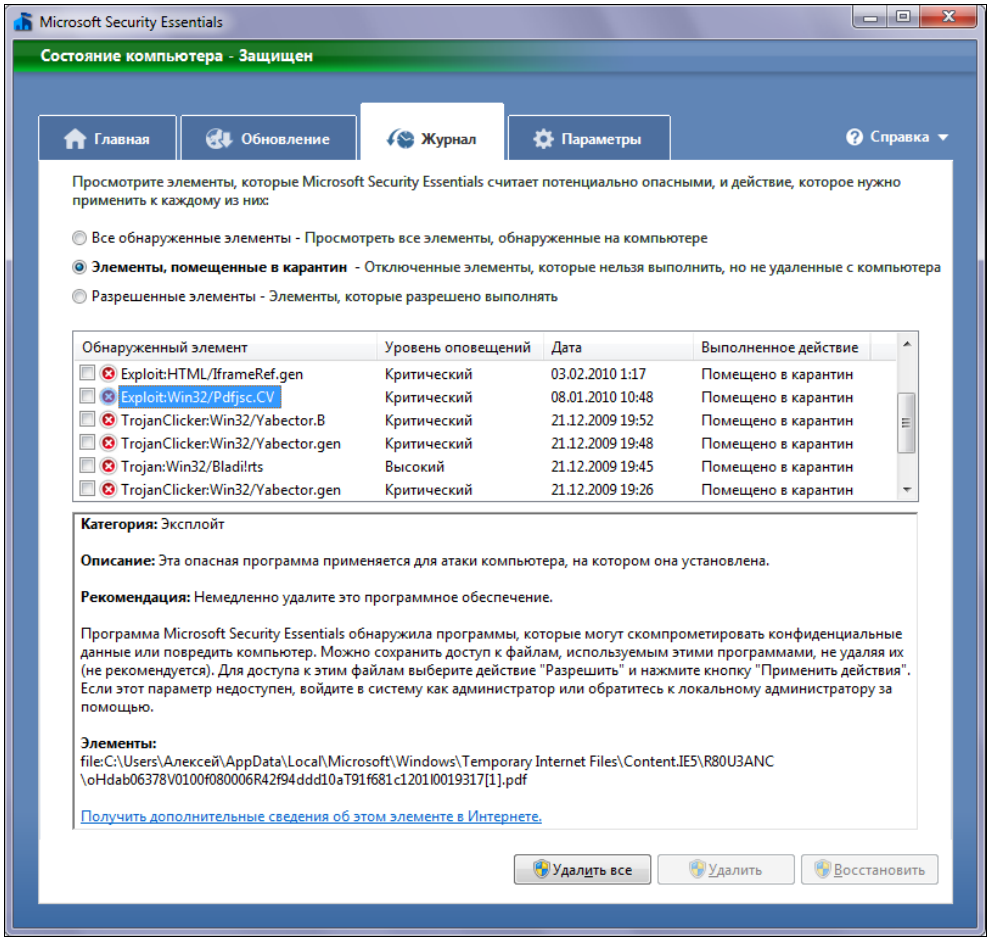

Рис. 4.13. Журнал обнаруженных угроз и файлов, помещенных в карантин

Совет

После установки программы Microsoft Security Essentials рекомендуется хотя бы один раз выполнить *полное* сканирование системы и проверить все хранящиеся файлы. Возможно, что будут обнаружены принесенные ранее извне опасные элементы, пропущенные другими средствами проверки.

Настройка параметров безопасности при взаимодействии разных систем

Если в локальной сети используются компьютеры, работающие только под управлением одинаково установленных и настроенных операционных систем (ОС) Windows Vista или Windows 7, то проблем сетевого взаимодействия между этими компьютерами быть не должно, и пользователи могут входить в любые системы и подключаться к любым общим ресурсам. Однако если в сети также используются компьютеры с другими ОС (более ранних версий или других производителей), а также сетевые устройства с внутренними накопителями (например, медиасерверы), работающие со своими ОС, то можно столкнуться с проблемами доступа — скажем, при входе в удаленную систему или при обращении к общим ресурсам (папкам). Если уж такая проблема возможна и встречается, то необходимо рассказать о том, чем она вызвана и как ее решать.

Для нормального взаимодействия компьютеров с разными операционными системами Windows (для простоты будем рассматривать только их) необходимо, чтобы в этих системах были согласованы параметры безопасности сетевых каналов — т. е. требования должны быть одинаковыми. В более ранних версиях Windows использовались менее защищенные связи, а в Windows 7 применяются более строгие правила взаимодействия. Соответственно нужно либо повысить уровень защиты в других системах, либо понизить (в допустимых пределах!) требования в системах Windows 7.

Далее рассматриваются основные параметры (политики безопасности), определяющие защищенность сетевого трафика. Для их настройки необходимо использовать стандартную оснастку **Локальная политика безопасности** (Local Security Policy, secpol.msc) или оснастку **Редактор объектов групповой политики** (Group Policy Object Editor, вызывается только по имени gpedit.msc).

Примечание

Все описываемые ниже политики безопасности находятся в папке **Параметры безопасности | Локальные политики | Параметры безопасности** (Security Settings | Local Policies | Security Options). Они конфигурируются для всего компьютера. Дополнительные политики безопасности, применяемые на компьютерах, включенных в домен Active Directory, мы рассматривать не будем.

При недоступности указанный выше оснасток можно использовать редактор системного реестра (`Regedit.exe`) и менять параметры непосредственно в реестре. Для этого требуется знать имена ключей реестра и нужные значения. Необходимые сведения можно найти в статье Базы знаний Microsoft "Проблемы с совместимостью клиентов, программ и служб, которые могут возникнуть при изменении параметров безопасности и назначенных прав пользователей" (KB823659), которую легко найти по номеру.

По умолчанию системы Windows требуют цифровую подпись (с *согласия сервера*, но не *всегда*) для пакетов SMB (Server Message Block — Блок серверных сообщений). Эти условия задаются политиками **Клиент сети Microsoft: использовать цифровую подпись...** (Microsoft network client: Digitally sign communications (always/if server agrees)), а соответственно для ответов — с серверной стороны — регламентируются политиками **Сервер сети Microsoft: использовать цифровую подпись (всегда/с согласия клиента)** (Microsoft network server: Digitally sign communications (always/fi client agrees)), которые по умолчанию отключены (Disabled).

Протокол аутентификации клиентов определяется политикой **Сетевая безопасность: уровень проверки подлинности LAN Manager** (Network security: LAN Manager authentication level). По умолчанию системы Windows Vista и Windows 7 отправляют только ответы NTLMv2 (Windows XP отправляет ответы LM и NTLM).

Следует помнить о том, что в Windows 7 для защиты подключений общего доступа используется 128-битное шифрование (см. окно дополнительных параметров общего доступа на рис. 1.23). Этот уровень шифрования может не поддерживаться другими клиентами сети, и тогда в указанном окне необходимо выбрать 40- или 56-битное шифрование. (Уровень шифрования определяется политиками **Сетевая безопасность: минимальная сеансовая безопасность...** (для клиентов/для серверов) (Network security: Minimum session security...(for clients/for servers)).)

ГЛАВА 5

Подключение к общим ресурсам

Совместное использование общих ресурсов является одной из важнейших целей, определяющих необходимость создания локальной сети. В этой главе подробно описываются все вопросы, возникающие при общем доступе к папкам и принтерам, имеющимся на компьютерах локальной сети, а также способы управления общими ресурсами и организация безопасной работы.

Профили пользователей. Личные и общие папки

Может возникнуть вопрос: а какое отношение к общим ресурсам имеет то, как в Windows 7 организованы и где располагаются личные пользовательские папки и общие папки, доступные для других локальных пользователей компьютера? Связь между этими вопросами не так очевидна. Для начала необходимо разобраться со спецификой личных и общих папок в Windows 7[1], а также с тесно связанным с ними понятием *профиля пользователя*. В системе имеются механизмы, обеспечивающие другим пользователям компьютера доступ к личным папкам пользователя (в первую очередь это касается участников домашней группы (HomeGroup)), а также позволяющие обращаться к локальным папкам (личным и общим) с других компьютеров, входящих в домашнюю или рабочую группу (об этом шла речь в *разд. "Настройка сетевого доступа к общим папкам и принтерам" главы 1*). Поэтому важно понимать: к *каким* же конкретно папкам, *кому* и с помощью *каких настроек* будет разрешен доступ. И как можно разрешить доступ к *любой* папке, имеющейся на диске. При этом нужно помнить о вопросах безопасности и конфиденциальности данных — следовательно, уметь настраивать *права доступа* для различных пользователей.

> ***Примечание***
>
> В этой главе мы будем говорить только об "обычных" файлах и папках — доступ к библиотекам мультимедиа может также осуществляться с помощью специальных механизмов, которые рассматриваются в *главе 6*.

[1] Это особенно важно для пользователей Windows XP, которые "пропустили" версию Windows Vista и начинают работу сразу в Windows 7.

Профили пользователей

Рабочая среда пользователя определяется настройками рабочего стола (например, цвета экрана, курсора мыши, размера и расположения окон), параметрами подключенных сетевых устройств и принтеров, переменными среды, параметрами реестра, наборов доступных приложений и т. д.

Все настройки рабочей среды хранятся в *профиле пользователя* (user profile) и определяются самим пользователем; они автоматически сохраняются в служебных файлах, хранящихся в папке, имя которой по умолчанию выглядит следующим образом: *%SystemDrive%*\Users*%USERNAME%* (*%SystemDrive%* — имя загрузочного диска, на котором находятся файлы системы; для Windows 7 это почти всегда диск C:\). В профиле пользователя также располагаются и интересующие нас многочисленные личные папки, предназначенные для хранения информации определенных форматов или специфических файлов.

> ***Внимание!***
>
> Папка **Documents and Settings** присутствует в системах Windows Vista и Windows 7 для совместимости, но не представляет собой реальную папку файловой системы.
>
> В окне Проводника русских версий Windows 7 папка **Users** *отображается* как **Пользователи**, но ее физическое имя (*см. далее*) не изменяется. В процессе изложения будет использоваться русскоязычное название папки (т. е. то имя, которое мы видим в Проводнике), чтобы не было расхождений с иллюстрациями.
>
> При переименовании учетной записи пользователя (%USERNAME%) имя папки его профиля (%USERPROFILE%) не изменяется!

Локальный профиль и набор стандартных личных папок создаются автоматически для каждого пользователя в процессе его первой регистрации на компьютере. Благодаря сохраненному профилю при последующем входе пользователя в систему рабочая среда имеет ту же конфигурацию, какая существовала в момент окончания предыдущего сеанса работы. Благодаря наличию профилей несколько пользователей могут работать (даже одновременно) на одном и том же компьютере в индивидуальных средах, не влияя друг на друга.

На рис. 5.1 показан пример папки **Пользователи** (Users) (для случая, если на компьютере работают несколько пользователей). Как можно видеть, помимо папок профилей администратора компьютера[1] и пользователя, созданного в момент начального конфигурирования системы, имеется также папка еще одного локального пользователя (User), а также папка **Общие** (Public), которая предназначается для хранения информации, доступной как всем локальным пользователям, так и пользователям удаленных компьютеров (к этой папке по умолчанию разрешен общий доступ[2]). Подробнее назначение и применение этой папки мы рассмотрим *далее*.

---

[1] Этот профиль появляется, если только учетная запись Администратор (Administrator) была разблокирована и использовалась для входа в систему!

[2] В этом легко убедиться с помощью команды `net share`.

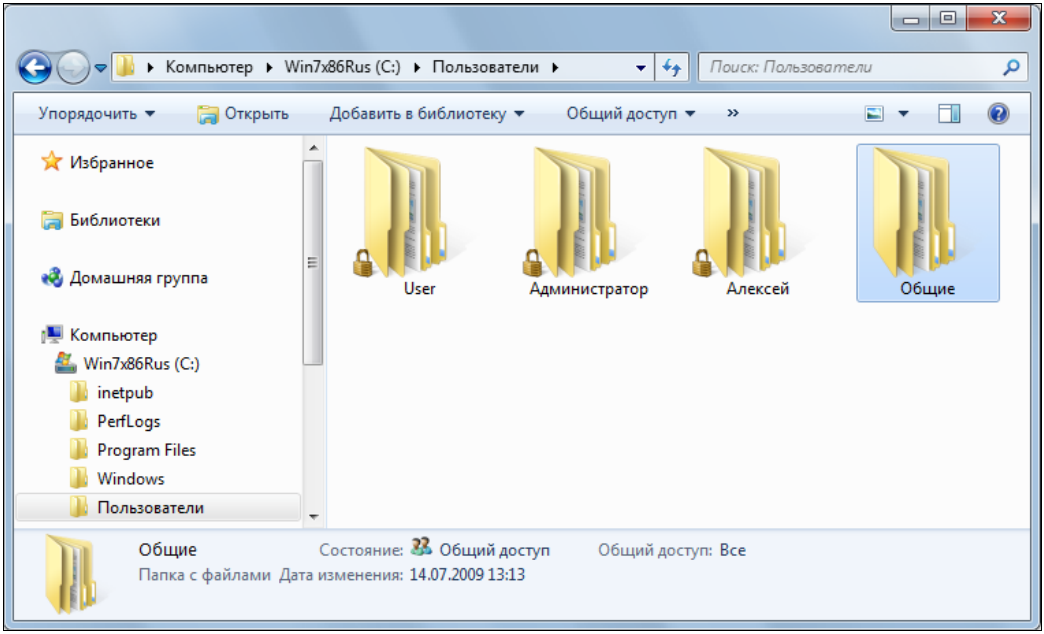

Рис. 5.1. Папка **Пользователи**, в которой хранятся профили пользователей

Примечание

Строго говоря, папки "Пользователи" вообще физически не существует[1]. В этом легко убедиться, выполнив в окне консоли команды `dir C:\users` и `dir C:\Пользователи` (результаты сравните сами). "Подмена" имен происходит в программе Проводник (Windows Explorer), в чем можно также убедиться, взглянув на пример, показанный на рис. 5.4. Локализованное название реальной папки Users определяется содержимым хранящегося в ней скрытого файла desktop.ini. В этом файле имеются только две строки:

```
[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21813
```

Достаточно переместить этот файл на другой диск или в другую папку — и русское название папки "потеряется". Иногда ошибки с этим файлом возникают при переносе данных между системами, при установке некоторых программ и т. п. Если такая неприятность случилась, то достаточно вручную создать файл с указанным содержимым и поместить его внутрь папки.

Структура профиля пользователя

Профиль пользователя создается на основе профиля, назначенного по умолчанию. Имеются скрытые системные папки **Default** и **All Users**, используемые для определения параметров стандартного профиля и представляющие собой реальные папки файловой системы. Папка **Default User** оставлена для совместимости и является

[1] Это относится и ко многим другим "локализованным" папкам.

ссылкой. Эти папки, как и папки пользовательских профилей, также хранятся в папке **Пользователи** (Users) корневого каталога загрузочного диска.

На рис. 5.2 показана структура папок локального профиля пользователя (для наглядности изображены *все* имеющиеся стандартные папки). Многие папки являются скрытыми и по умолчанию не видны в окне Проводника (если же включить отображение скрытых папок, то в окне программы папки будут более светлыми и не имеют особой пиктограммы — например, папка **AppData**). Некоторые из объектов на самом деле представляют собой не файловые папки, а ссылки (junction point) (что видно по изображению стрелки на значке папки — например, папка **Local Settings**) и доступ к ним невозможен (их имена используются для совместимости только прикладными программами).

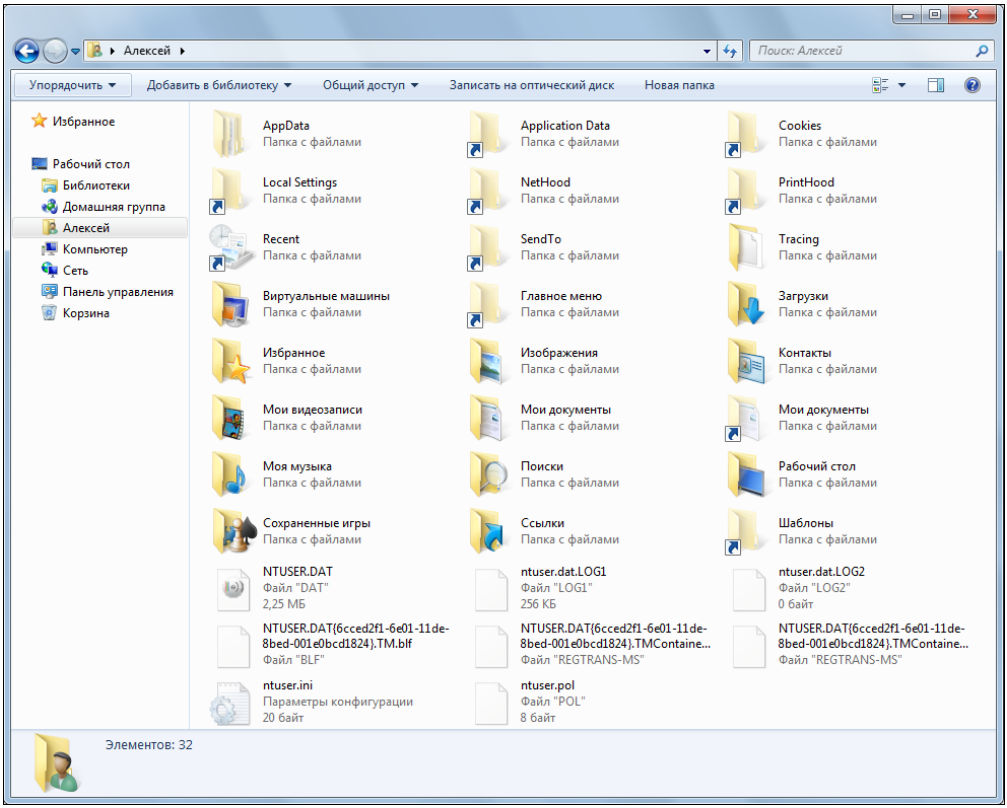

Рис. 5.2. Структура подпапок локального профиля пользователя

Папки, представляющие собой *точки повторной обработки* (junction points), а не реальные физические папки, можно увидеть в окне консоли с помощью команд `dir /A` или `dir /AL`. Вот примеры таких папок (строки, не имеющие отношения к делу, не показаны):

```
C:\>dir /AL
Содержимое папки C:\
14.07.2010  08:53    <JUNCTION>     Documents and Settings [C:\Users]
```

```
C:\>cd users
C:\Users>dir /AL
Содержимое папки C:\Users
14.07.2010  08:53    <SYMLINKD>     All Users [C:\ProgramData]
14.07.2010  08:53    <JUNCTION>     Default User [C:\Users\Default]
29.08.2010  13:28    <SYMLINKD>     Все пользователи [C:\ProgramData]
```

В приведенных строках можно видеть имя, которое фигурирует в окне Проводника и доступно прикладным программам, а в квадратных скобках — имя физической папки, связанной с данным объектом.

> ***Внимание!***
> Ссылки невозможно удалить с помощью обычных операций удаления в окне Проводника или в командной строке. В случае такой необходимости следует использовать утилиту `fsutil` с параметрами `reparsepoint delete`.

Некоторые папки пользовательского профиля, традиционные для Windows XP, довольно сложно с непривычки найти в системах Windows Vista и Windows 7 — многие из них находятся внутри папки C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows. В табл. 5.1 перечислены некоторые из этих папок и указано их полное имя в файловой системе.

Таблица 5.1. *Специальные папки, входящие в профиль пользователя*

Application Data	Настройки прикладных программ, входящие в перемещаемый профиль C:\Users*%USERNAME%*\AppData\Roaming
Cookies	Служебные файлы, получаемые с просматриваемых веб-серверов C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows\Cookies
Local Settings	Локальные и временные файлы прикладных программ C:\Users*%USERNAME%*\AppData\Local
Recent	Данные о документах и графических файлах, открытых пользователем в течение последнего времени C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows\Recent
SendTo	Ярлыки объектов, куда могут посылаться документы C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows\SendTo В эту папку можно поместить ярлыки программы, которые будут открываться при вызове контекстного меню для файла или папки и выборе команды **Отправить** (Send To)
Главное меню (Start Menu)	Ярлыки программ C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows\Start Menu
Мои документы	Личные документы пользователя C:\Users*%USERNAME%*\Documents
Шаблоны	Шаблоны документов, создаваемых приложениями C:\Users*%USERNAME%*\AppData\Roaming\Microsoft\Windows\Templates

Личные папки и папка *Общие* (Public)

Внутри папки пользовательского профиля имеется множество специализированных папок для хранения разного рода данных (рис. 5.3). Назначение папок понятно из их названия. Все показанные на рисунке папки являются реальными папками файловой системы. Можно обеспечить доступ к этим папкам со стороны удаленных пользователей, в том числе и для компьютеров, входящих в домашнюю группу (см. параметры в нижней части окна на рисунке).

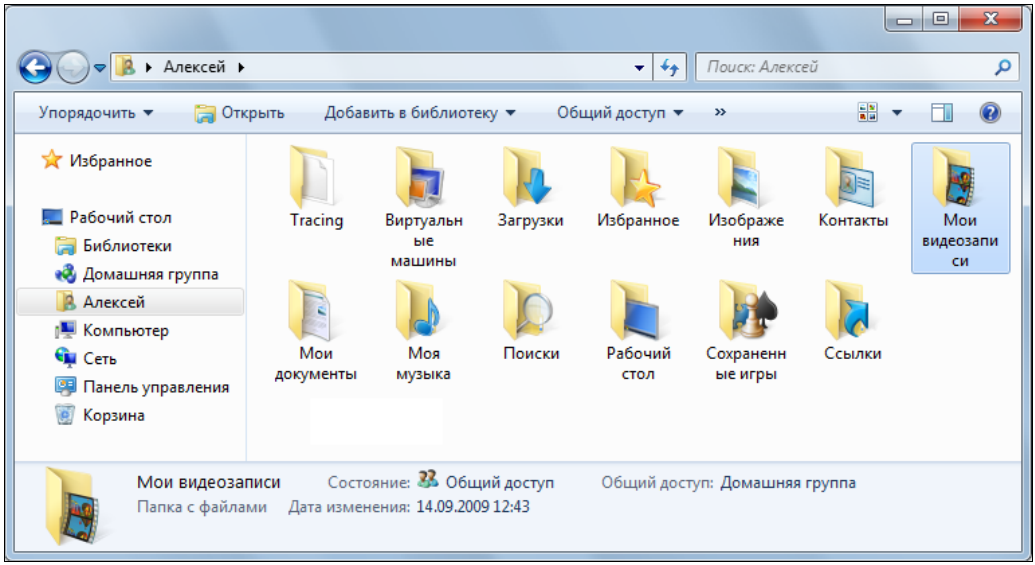

Рис. 5.3. Личные папки пользователя

> ***Примечание***
>
> Личные папки (библиотеки), разрешенные для просмотра другим участникам домашней группы (см. рис. 1.22), доступны только для чтения. При попытке *записи* в эти библиотеки создаваемые файлы фактически будут помещаться не в личные, а в общие папки (входящие в папку **Общие** (Public) — см. рис. 5.5).

При работе с папками следует учитывать тот факт, что их полные имена "маскируются" в поле адреса окна Проводника. Если требуется увидеть реальное имя папки, щелкните мышью по полю адреса — после этого будет отображаться физический путь к папке (иногда именно он нужен для работы). Это проиллюстрировано на рис. 5.4: вверху показано представление по умолчанию, внизу — реальное имя папки.

> ***Примечание***
>
> Проигрыватель Windows Media может получать доступ к папкам библиотеки мультимедиа, находящимся на другом компьютере. Для этого используется не обычный доступ к общим ресурсам, а специальная сетевая служба *(см. главу 6)*.

Как уже говорилось, внутри папки **Пользователи** (Users) имеется папка **Общие** (Public), в которой пользователи компьютера могут сохранять информацию, дос-

тупную другим пользователям (локальным или пользователям удаленных компьютеров, если им разрешен доступ). Подкаталоги этой папки показаны на рис. 5.5 (обратите внимание на строку "Общий доступ: Все" (Shared with: Everyone)). Пользователь может с помощью несложной операции (см. рис. 1.23) разрешить удаленный доступ на чтение и запись к подкаталогам папки **Общие** (Public). Мы обращаем на это внимание, поскольку настройка доступа к данной папке осуществляется иначе и намного проще, чем организация обычного общего доступа к произвольным папкам, который будет рассматриваться *далее* в этой главе.

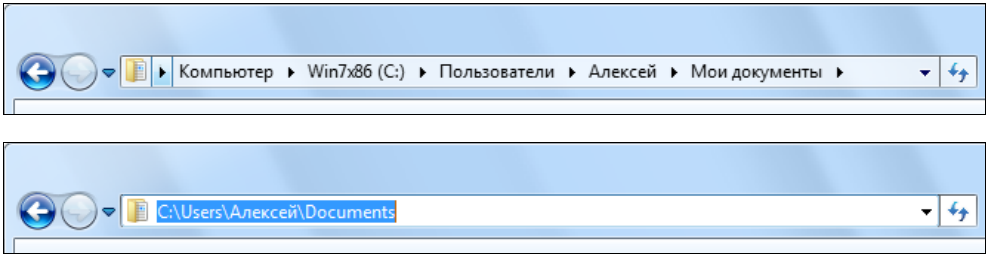

Рис. 5.4. Представление адреса папки в окне Проводника и ее реальное физическое имя

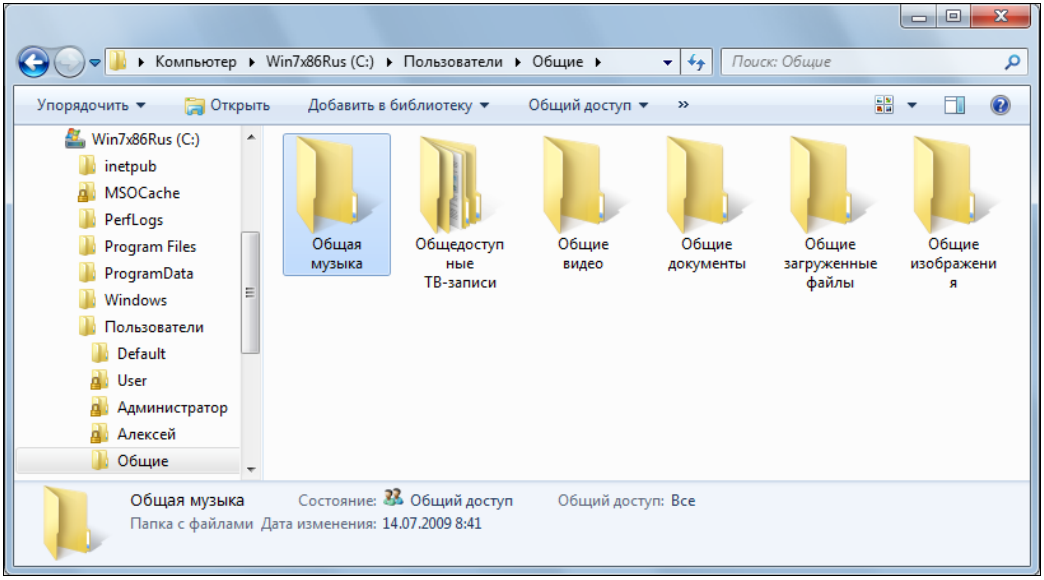

Рис. 5.5. Стандартные папки для общего доступа

В заключение — если уж речь зашла о папках с пользовательскими файлами — можно отметить, что местоположение этих папок не "привязано" к диску C: и при необходимости стандартное местоположение любой личной (см. рис. 5.3) или общей (см. рис. 5.5) папки можно изменить: например, перенести ее на другой логический диск. Для этого нужно открыть окно свойств этой папки, перейти на вкладку **Расположение** (Location) (рис. 5.6), нажать кнопку **Переместить** (Move) и выбрать новое местоположение для папки. Система предложит перенести файлы из

старой папки в новую. Нажав кнопку **По умолчанию** (Restore Default), легко в любой момент вернуть все в исходное состояние.

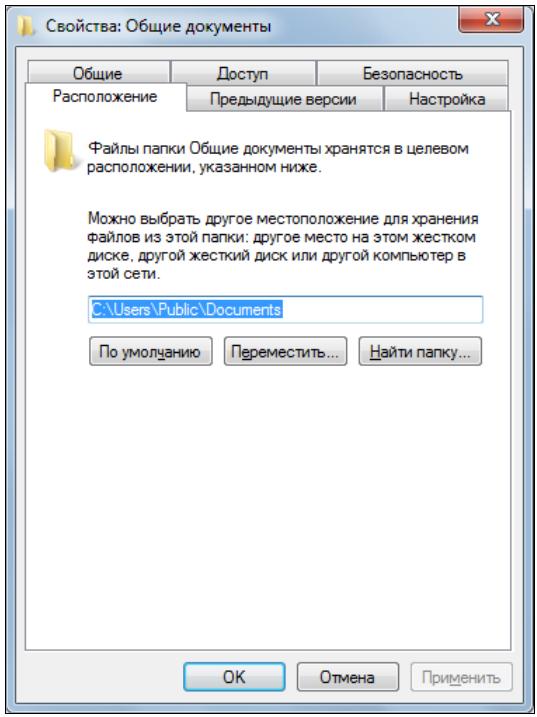

Рис. 5.6. Окно выбора местоположения для личной или общей папки

Внимание!

При изменении местоположения личных папок проверьте, сохранились ли разрешения на уровне файловой системы. Изначально доступ к таким папкам — помимо самого пользователя — имеют только система и группа Администраторы (Administrators). Можно проверить это *перед* перемещением папки и при необходимости задать нужные разрешения *после* выполнения операции.

Управление доступом к файлам и папкам

Если разрешается доступ к дисковым ресурсам со стороны других локальных пользователей или пользователей других компьютеров в сети, то неизбежно возникает задача управления этим доступом. Назначение прав доступа имеет смысл рассматривать *в совокупности* — для локального доступа (разрешения на уровне файловой системы) и для общего (сетевого), поскольку методы выбора этих прав тесно взаимосвязаны.

Примечание

Личные папки пользователей по умолчанию закрыты для других пользователей компьютера (кроме администраторов). Доступ для членов домашней группы регламенти-

рован и возможен только к строго определенным папкам (см. рис. 1.22), при этом по умолчанию права доступа задаются автоматически через встроенную учетную запись HomeUsers. Поэтому отдельно можно говорить только о папках, создаваемых пользователями в *произвольных* местах файловой системы и предоставляемых для совместного доступа. В этом случае применяются специальные функции, имеющиеся для управления разрешениями и общими ресурсами. О них и пойдет речь *далее*.

Общие принципы назначения разрешений на доступ

Для общих папок разрешения на доступ к ресурсу определяются на двух уровнях:

- *на уровне общей папки* (т. е. ресурса, выделенного для общего сетевого доступа); эти разрешения распространяются на ***все*** вложенные папки и файлы, содержащиеся в общей папке, и действуют только при доступе к папке через сеть;
- *на уровне файловой системы NTFS* (если общая папка расположена на FAT-томе, то такие разрешения для нее невозможны); эти разрешения можно назначать как всей папке, так и ***конкретным*** вложенным папкам и файлам внутри общей папки; они действуют всегда, независимо от способа доступа к папке (т. е. распространяются и на локальных пользователей, и на удаленный доступ).

При выборе разрешений доступа обычно руководствуются следующими правилами:

- на уровне общего ресурса рекомендуется задавать наиболее "широкие" права (если позволяют требования безопасности — полный доступ для всех);
- на уровне файловой системы NTFS определяются более "узкие" разрешения на конкретные папки и файлы для отдельных групп или пользователей.

Такой подход упрощает администрирование полномочий пользователей. Результирующие права доступа ***определяются наиболее "строгими" разрешениями, установленными либо на уровне общего ресурса, либо на уровне файловой системы*** (при этом самыми приоритетными являются *запреты* каких-либо разрешений — когда установлен флажок **Запретить** (Deny)).

Предположим, на уровне общей папки установлено разрешение Чтение (Read) для группы Все (Everyone). Если теперь нужно какой-то группе или пользователю дать более широкие права, например разрешение на запись в какую-то папку, то это сделать невозможно, поскольку права доступа ограничены на уровне общей папки более "узким" разрешением Чтение (Read).

Кроме того, разрешения на уровне общей папки не позволяют детализировать права доступа, поскольку они распространяются на *весь* общий ресурс и представляют собой достаточно обобщенные возможности (чтение, изменение или полный доступ). Разрешения, заданные на уровне файловой системы, более "универсальны": они не зависят от того, зарегистрирован ли пользователь на компьютере локально или обращается к нему через сеть.

Внимание!

Обычно разрешения предоставляются не отдельным пользователям, а группам (в соответствии с функциональными задачами, возлагаемыми на эти группы). Пользователи же получают права опосредованно, через членство в определенной группе. Глав-

ным образом это связано с тем, что членство пользователя в группе поменять значительно легче, чем все разрешения, если бы они были назначены *непосредственно* этому пользователю. Кроме того, групп обычно значительно меньше, чем пользователей. В первую очередь это правило актуально при работе в больших сетях, имеющих множество компьютеров и пользователей, а в домашней сети вполне можно ограничиться отдельными учетными записями пользователей.

Разрешения, заданные "внутри" каждого уровня (т. е. на уровне общей папки или на уровне файловой системы), являются *аддитивными*, т. е. результирующие права будут *складываться* из всех разрешений, явно или косвенно распространяющихся на пользователя (в первую очередь это правило применимо к разрешениям, задаваемым на уровне файловой системы, поскольку различных разрешений там больше). Если, например, пользователь имеет разрешение на чтение, а группе, в которую он входит, дано разрешение на запись, то в результате этот пользователь будет иметь возможность *и* читать, *и* записывать.

Внимание!

Пользователи клиентских компьютеров, имеющие учетные записи без пароля, не могут обращаться по сети к общим папкам систем Windows 7, поскольку в этих системах по умолчанию действует политика безопасности **Учетные записи: разрешить использование пустых паролей только при консольном входе** (Accounts: Limit local account use of blank passwords to console logon only) — т. е. пустые пароли допускаются только при локальном входе в систему, а при обращении по сети аутентификация пользователя без пароля не производится. Поэтому для обеспечения доступа к общим папкам нужно либо дать пользователям пароли, либо отключить эту политику.

Разрешения доступа на уровне файловой системы NTFS

Для защиты конфиденциальной информации от несанкционированного доступа (от прочтения или только от внесения изменений) пользователь может установить определенные *разрешения* (permissions) на доступ к своим файлам и папкам. (Это необходимо в особых ситуациях, поскольку в простейшем случае локальные пользователи могут обращаться только к файлам в личных папках, а также видеть и изменять информацию, помещенную другими пользователями в общие папки).

Все операции с разрешениями доступа к файлам и папкам выполняются в окне программы Проводник (Windows Explorer). Интерфейс, используемый при работе с разрешениями в системах Windows 7, достаточно традиционен, хотя несколько и отличается от предыдущих версий Windows (набор и смысл операций при этом не изменился). Порядок выполнения операций с *файлами* и с *папками* одинаковый, меняются лишь некоторые частные разрешения доступа.

Примечание

В окне Проводника на некоторых папках можно увидеть изображение замка. Причины его появления достаточно просты — см. первое примечание далее в *разд. "Включение общего доступа к папкам"*.

Необходимые разрешения доступа (помимо стандартных, задаваемых при создании файла или папки) устанавливаются в окне свойств файла или папки на вкладке

Безопасность (Security) (рис. 5.7). Здесь разрешения для имеющихся в списке групп и пользователей можно только просматривать без возможности модификации. Для того чтобы добавить или удалить пользователей и группы, а также для того, чтобы изменить установленные разрешения, следует нажать кнопку **Изменить** (Edit) и в специальном окне разрешений выбрать новые параметры.

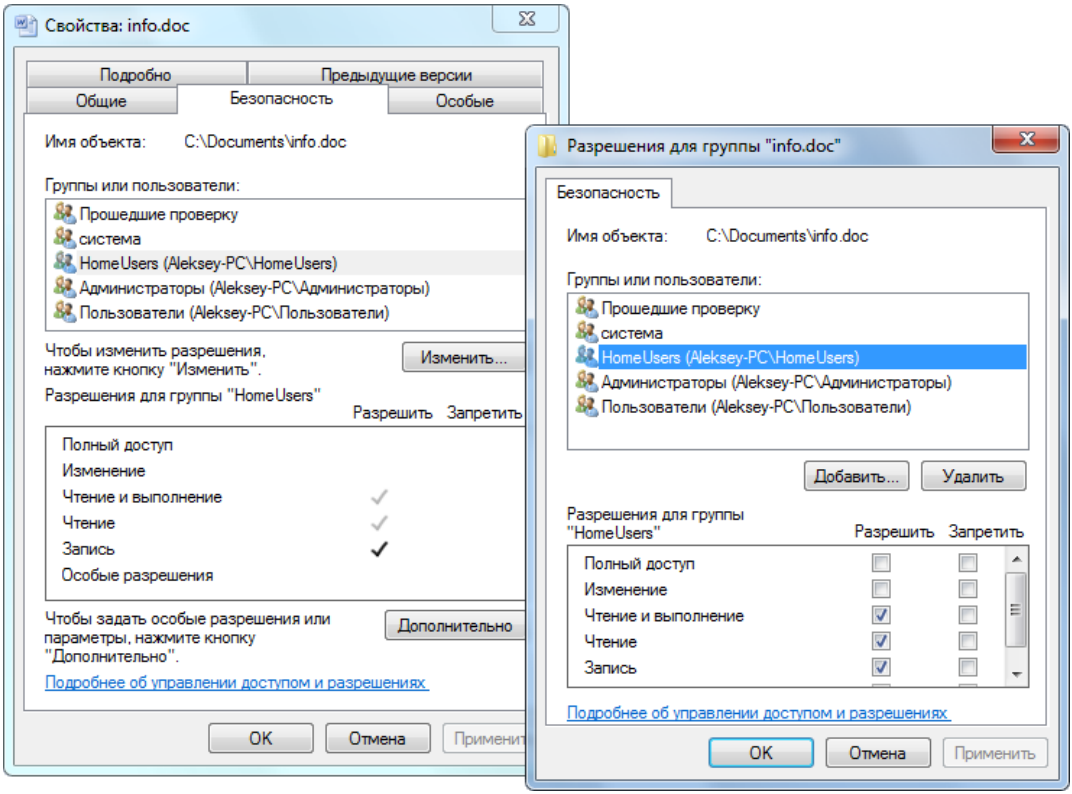

Рис. 5.7. Вкладка **Безопасность** окна свойств файла

Кнопка **Дополнительно** (Advanced) (см. рис. 5.7) позволяет получить доступ к тонкой настройке, на уровне специальных разрешений. В окне дополнительных параметров безопасности (рис. 5.8) можно видеть, от какой папки унаследованы разрешения, действующие на выбранный файл (папку). Здесь можно запретить наследование разрешений, сбросив флажок **Добавить разрешения, наследуемые от родительский объектов** (Include inheritable permissions from this object's parent) и задав индивидуальные (или дополнительные) разрешения для выбранного файла или папки. (Для папок также можно *распространить* выбранные разрешения на все дочерние объекты.)

Внимание!

В принципе, администраторы компьютера имеют неограниченные права доступа к объектам файловой системы. Если даже доступ администратору закрыт, он может

сделать себя владельцем файла или папки[1] (см. вкладку **Владелец** (Owner) на рис. 5.8) и назначить себе любые права. Такая операция может потребоваться в тех случаях, когда после краха или переустановки системы на диске появляются ненужные, но недоступные файлы, которые невозможно удалить.

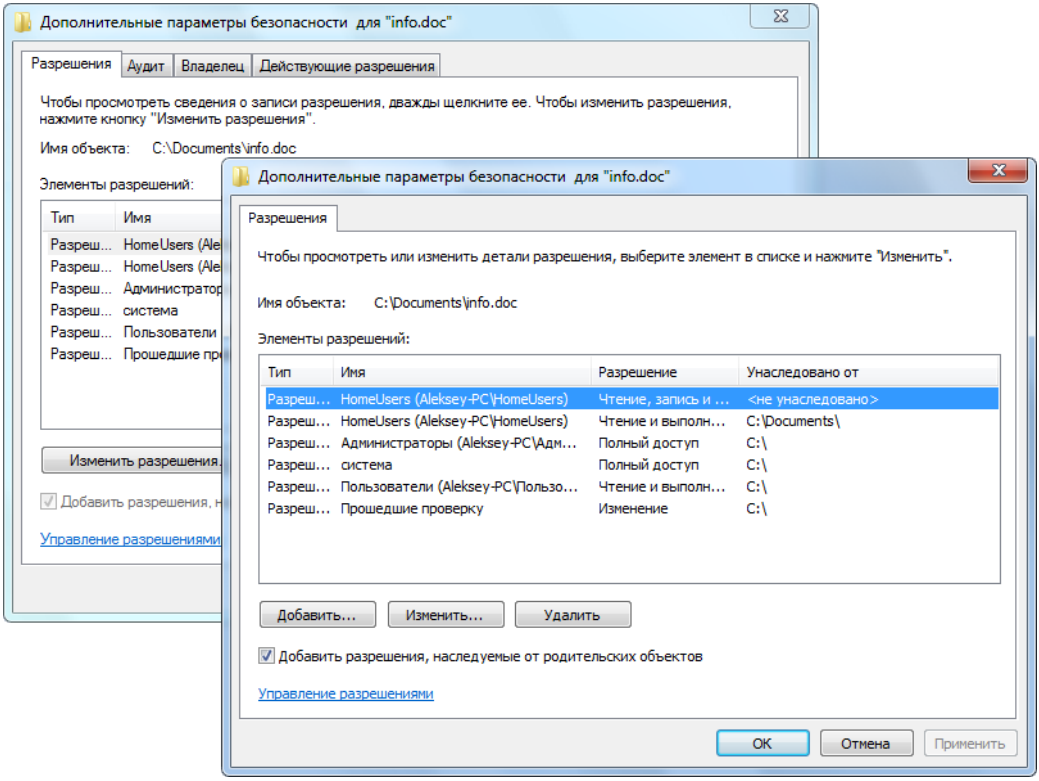

Рис. 5.8. Окно редактирования дополнительных параметров безопасности

Разрешение общего доступа к папкам

При разрешении общего доступа к дискам и отдельным папкам информация, хранящаяся на компьютере, будет доступна по сети для пользователей других компьютеров. Обычно для создания общих ресурсов (папок или принтеров) и управления доступом используется Проводник (Windows Explorer). В системах Windows 7 для выполнения этой задачи достаточно щелкнуть правой кнопкой мыши по любой нужной папке и в контекстном меню выполнить команду **Общий доступ** (Share with) (рис. 5.9, *сверху*) (можно также нажать одноименную кнопку на панели задач — рис. 5.9, *снизу*): в этом случае следует указать, кому разрешается доступ, и подтвердить операцию. (Обратите внимание на наличие в этих меню опций для

[1] При выполнении операций смены владельца папки или назначения прав можно также распространить изменения на все вложенные объекты (иногда это просто необходимо).

домашней группы.) Выбранной папке сразу же будут назначены соответствующие разрешения, которые можно увидеть в окне свойств папки на вкладке **Безопасность** (Security) (см. рис. 5.7).

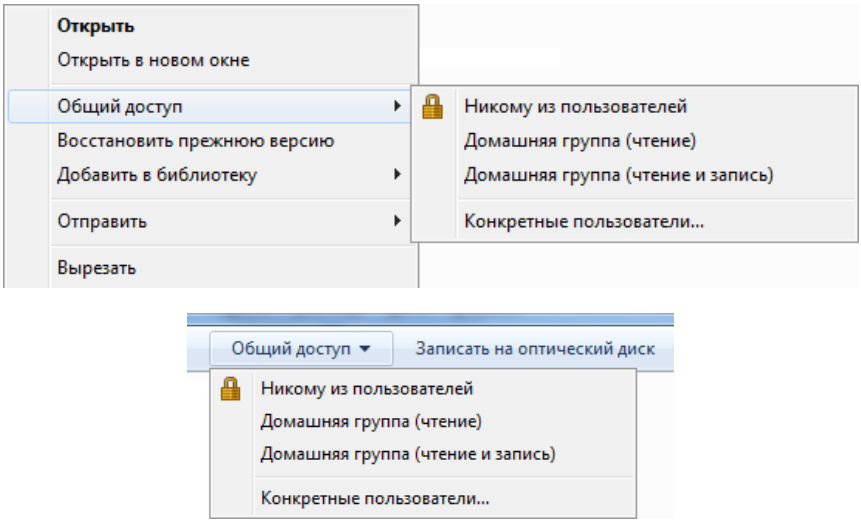

Рис. 5.9. Команды управления общим доступом к папке

Все операции разрешения общего доступа к папкам и принтерам — с помощью каких бы средств они ни выполнялись — должны быть согласованы с настройками сетевого профиля (см. рис. 1.3 и рис. 1.23). Если общий доступ не разрешен в профиле, то ресурсы не будут видны в сети, даже если все настройки и разрешения выполнены правильно.

> ***Внимание!***
>
> Необходимо отдельно пояснить действие опции **Никому из пользователей** (Nobody). При выборе этой опции общий доступ отключается, если был разрешен, и кроме того, меняются разрешения на уровне NTFS: доступ к папке получает только сам пользователь, система и группа Администраторы (Administrators). Таким образом, папка "закрывается" от других пользователей, о чем и свидетельствует появляющийся замок на ее значке. Наличие замка на любой папке означает, что доступ к ней имеет *только* система и администраторы, а также пользователь-создатель папки. Если добавить разрешение хотя бы еще для одной учетной записи — замок исчезнет.

> ***Примечание***
>
> К сожалению, в системах Windows 7 значок папки, к которой разрешен общий доступ, никак не изменяется в окне Проводника. О наличии доступа к выбранной папке можно судить только по состоянию "Общий доступ" и пиктограмме на панели сведений в нижней части окна (см. рис. 5.5).

Действия, выполняемые с помощью команды **Общий доступ** (Share with), зависят от того, включен или нет *Мастер общего доступа* (Sharing Wizard). По умолчанию он используется, поскольку в окне свойств папок (открывается с помощью задачи **Параметры папок** (Folder Options) на панели управления) на вкладке **Вид** (View)

установлен флажок **Использовать мастер общего доступа** (Use Sharing Wizard). Если флажок сброшен, то мастер не задействуется в работе, и кнопка **Общий доступ** (Share) на вкладке **Доступ** (Sharing) (см. рис. 5.10) будет недоступна. Кроме этого, в контекстном меню папки (см. рис. 5.9) и при нажатии кнопки **Общий доступ** (Share with) на панели задач Проводника будет доступна только одна команда — **Расширенная настройка общего доступа** (Advanced sharing) *(см. далее разд. "Традиционный «классический» подход").*

Управлять общим доступом можно также в окне свойств выбранной папки на вкладке **Доступ** (Sharing) (рис. 5.10). Для разрешения/запрета на доступ к папке используется кнопка **Общий доступ** (Share) (в этом случае будет задействован мастер общего доступа) или кнопка **Расширенная настройка** (Advanced Sharing) (использование второй кнопки требует административных привилегий). Далее эти две возможности рассматриваются подробнее.

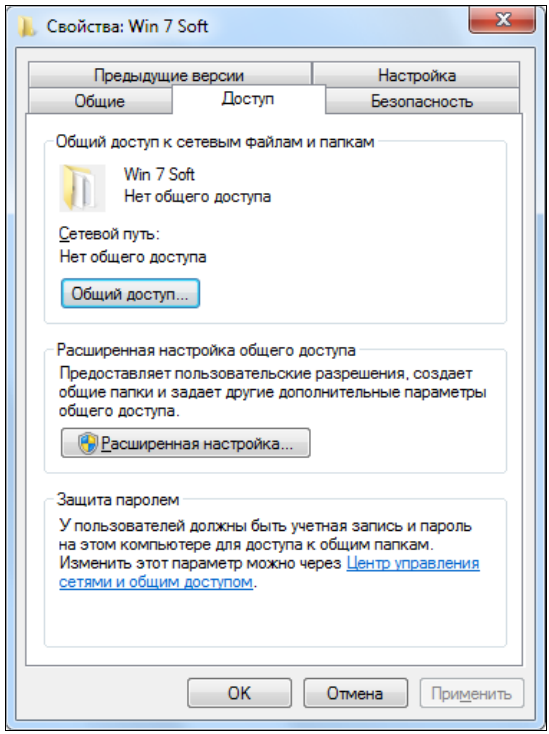

Рис. 5.10. Вкладка окна свойств папки, на которой можно выбирать способы настройки общего доступа к данной папке

Внимание!

Если Мастер общего доступа (Sharing Wizard) *(см. далее)* не используется, то изначально при разрешении общего доступа к папке всегда предоставляется разрешение Чтение (Read) для группы Все (Everyone). В случае его применения учетные записи и их права выбираются сразу, по индивидуальному принципу, и при этом автоматически устанавливаются аналогичные разрешения на уровне файловой системы.

Примечание

Помимо описанных здесь и ниже средств, управлять общими ресурсами можно с помощью традиционных команд `net share`, `net use` и `net view`, запускающихся в окне консоли. Примеры их использования приведены *далее* в заключительном разделе главы.

Мастер общего доступа

Если на вкладке **Доступ** (Sharing) в окне свойств папки нажать кнопку **Общий доступ** (Share) (см. рис. 5.10), то вызывается *Мастер общего доступа* (Sharing Wizard) (см. рис. 5.11). Также для запуска этого мастера можно использовать команду **Общий доступ** (Share with) (см. рис. 5.14), указав опцию **Конкретные пользователи** (Specific people).

По умолчанию в списке пользователей, которым разрешен доступ к папке (рис. 5.11), указан только владелец (owner) папки. Если щелкнуть по стрелочке, отмеченной на рисунке, и раскрыть список, располагающийся слева от кнопки **Добавить** (Add), то в нем можно выбрать учетную запись пользователя из числа имеющихся на компьютере, опцию **Все** (Everyone) или опцию **Домашняя группа** (Homegroup) и добавить ее в список разрешенных пользователей. В результате указанный пользователь или члены выбранной группы получат доступ к папке.

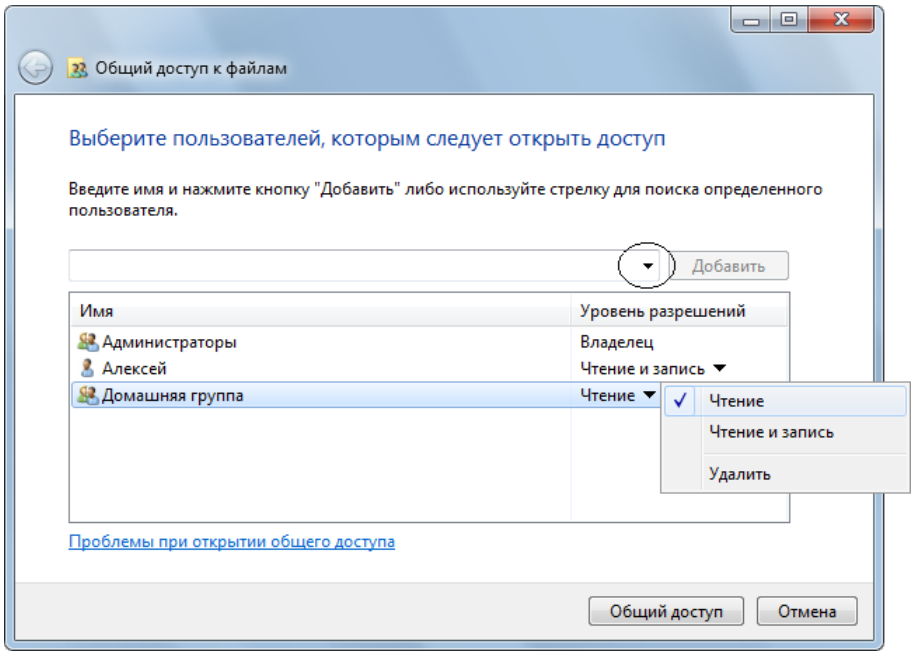

Рис. 5.11. Выбор разрешений с помощью Мастера общего доступа

По умолчанию вновь добавленному пользователю дается разрешение **Чтение** (Read), позволяющее только читать данные. Опция **Чтение и запись** (Read/Write) разрешает также изменение и создание файлов, а опция **Владелец** (Owner) разре-

шает полный (Full) доступ. После того как все пользователи и уровни разрешений выбраны, можно нажать кнопку **Общий доступ** (Share), и операция будет выполнена. Мастер сообщит о создании новой общей папки, и в результирующем окне можно выбрать ссылку просмотра всех общих ресурсов компьютера. К мастеру общих ресурсов можно обращаться и позднее — для изменения разрешений доступа или для отмены общего доступа к папке.

Внимание!

При работе Мастера общего доступа пользователю или группе, которым предоставляется доступ к выбранной папке, одновременно даются соответствующие ***разрешения на уровне файловой системы*** (это легко проверить в окне свойств папки на вкладке **Безопасность** (Security)). Таким образом, мастер задействует всю триаду параметров общего доступа — учетную запись, разрешения доступа и разрешения файловой системы NTFS. Если применяется так называемый "классический подход", то каждый из этих трех параметров нужно выбирать индивидуально: сначала разрешается сам общий доступ, затем уточняются разрешения доступа с указанием учетных записей, а потом определяются разрешения на уровне NTFS. Поскольку операций больше, легче допустить ошибку или неточность.

Традиционный "классический" подход

Для более детальной настройки параметров доступа к папке (или же если мастер общего доступа отключен) необходимо на вкладке **Доступ** (Sharing) в окне свойств папки нажать кнопку **Расширенная настройка** (Advanced Sharing) (см. рис. 5.10). Откроется окно, где для разрешения общего доступа установите флажок **Открыть общий доступ к этой папке** (Share this folder) (рис. 5.12).

В поле **Имя общего ресурса** (Share name) указывается произвольное название общей папки (впоследствии это поле может стать списком, поскольку имен у общей папки может быть несколько — нажав кнопку **Добавить** (Add), можно определить дополнительное имя; при этом для каждого имени может быть свой набор разрешений). Чтобы задать разрешения доступа, нажмите кнопку **Разрешения** (Permissions) и в открывшемся окне (см. рис. 5.12) выберите требуемые параметры доступа (обратите внимание, что для всех пользователей по умолчанию разрешено только чтение). Кнопка **Кэширование** (Caching) позволяет перейти к настройкам режима использования папки в *автономном режиме*[1].

После того как все параметры выбраны, закройте все окна — с этого момента общий доступ к папке включен.

Оснастка *Общие папки*

Для локального и удаленного администрирования общих ресурсов может использоваться оснастка **Общие папки** (Shared Folders, fsmgmt.msc), входящая в стандарт-

[1] Это специальный режим использования папок при отключении от удаленного компьютера (или при его временной недоступности). Механизм автономных файлов позволяет продолжить их использования в таких случаях, а затем синхронизировать изменения файлов при восстановлении доступа.

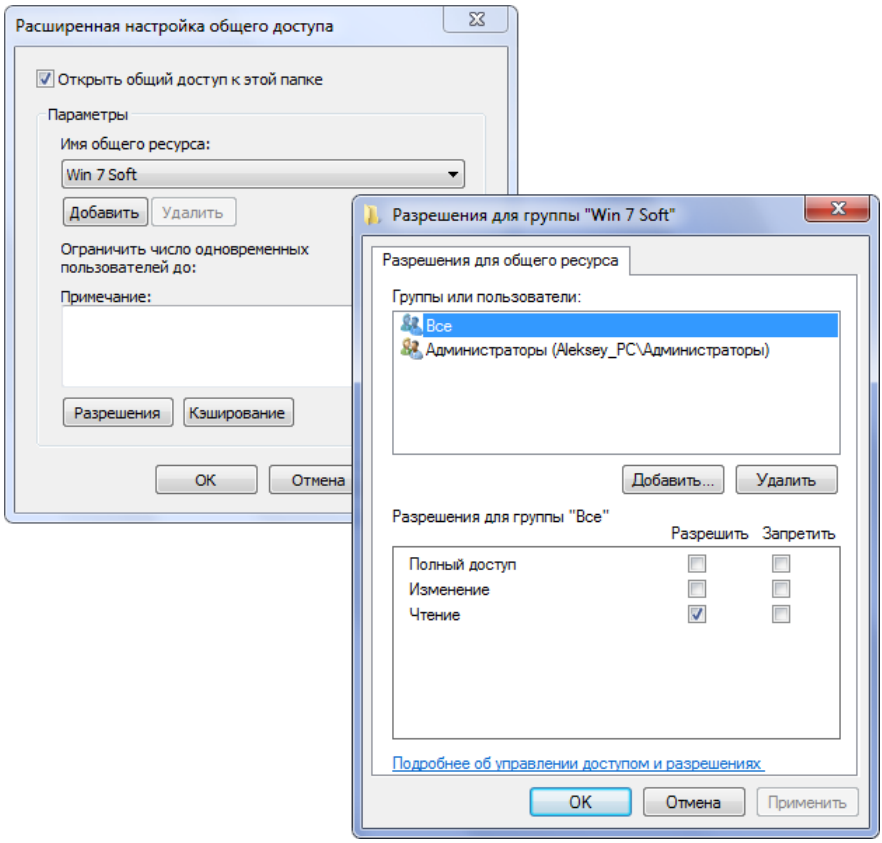

Рис. 5.12. Окна расширенной настройки общего доступа к папке

ный инструмент администрирования — **Управление компьютером** (Computer Management) (рис. 5.13). С ее помощью можно также управлять сеансами и открытыми файлами. Данная оснастка удобна тем, что позволяет увидеть все общие ресурсы сразу, что важно при их большом количестве. В других случаях вполне достаточно средств, описанных ранее.

С помощью узла **Общие ресурсы** (Shares) оснастки **Общие папки** (Shared Folders) можно разрешать и запрещать общий доступ к локальным папкам, а также видеть количество пользователей, подключенных к той или иной папке.

Для создания новой общей папки достаточно выбрать в окне пустое место и щелкнуть правой кнопкой мыши, после чего в контекстном меню нужно выбрать команду **Новый общий ресурс** (New Share). Запустится мастер, с помощью которого легко можно выполнить все действия, нужные для обеспечения общего доступа к заданной папке.

В окне свойств выбранной в окне оснастки общей папки можно менять все ее параметры, включая имя, описание, опции кэширования, разрешения доступа и разрешения, заданные на уровне файловой системы.

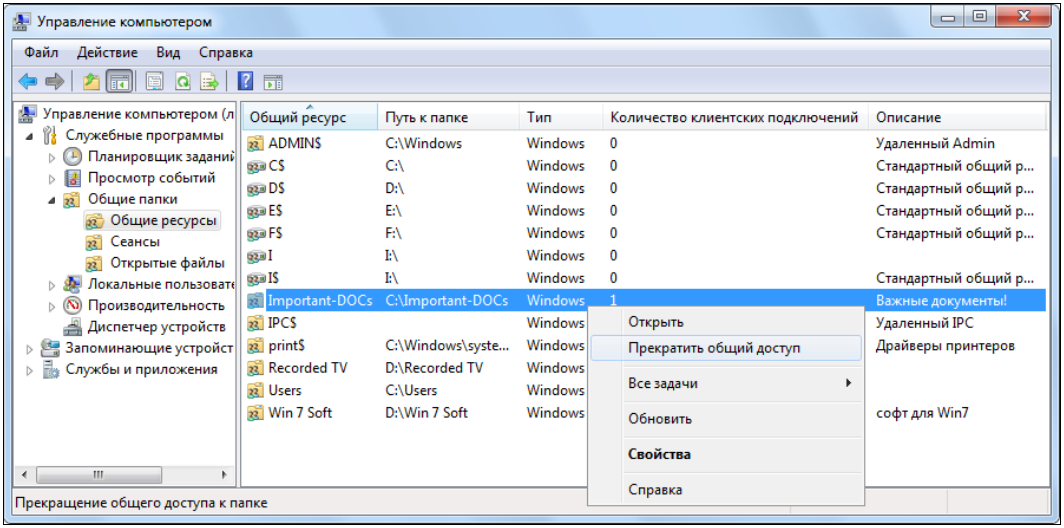

Рис. 5.13. Окно оснастки **Общие папки**
в составе инструмента **Управление компьютером**

Разрешение общего доступа к локальным принтерам

Для того чтобы сделать локальный принтер доступным другим клиентам сети, необходимо после его установки открыть окно **Устройства и принтеры** (Devices and Printers) (см. рис. 3.2) — соответствующая опция имеется в меню **Пуск** (Start). Все принтеры — локальные или удаленные — отображаются в разделе принтеров и факсов. Щелкните по значку принтера правой кнопкой мыши и в контекстном меню выберите команду **Свойства принтера** (Printer properties). На вкладке **Доступ** (Sharing) (рис. 5.14) установите флажок, разрешающий доступ, и укажите сетевое имя принтера (длинные имена могут не распознаваться некоторыми системами, но для Windows XP/Vista/7 можно оставить имя, предлагаемое по умолчанию). После нажатия кнопки **ОК** общий доступ будет разрешен, и принтер станет видимым для других пользователей сети.

Доступ к принтерам на компьютерах, входящих в домашнюю группу, осуществляется еще проще: достаточно установить соответствующий флажок в окне параметров домашней группы (см. рис. 1.22).

Во всех случаях следует помнить о том, что другие компьютеры сети смогут реально увидеть общий принтер (и общие папки) только в том случае, если на локальном компьютере включен доступ в настройках используемого сетевого профиля (см. рис. 1.23).

Примечание

Кнопка **Дополнительные драйверы** (Additional Drivers) (см. рис. 5.14) позволит установить драйверы для других платформ: например, если удаленные компьютеры с 32-раз-

рядной версией Windows захотят подключиться к принтеру, установленному в 64-разрядной редакции Windows 7, или наоборот. При этом потребуется драйвер для соответствующей платформы. Если все версии Windows одной разрядности, об этой проблеме можно забыть.

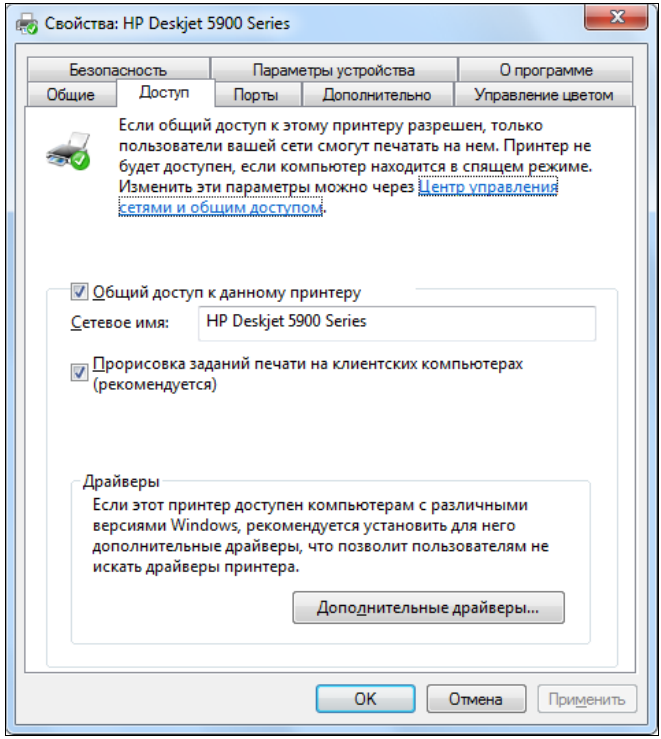

Рис. 5.14. Включение общего доступа к локальному принтеру

Работа с общими папками и принтерами

Компьютеры, входящие в домашнюю или рабочую группу, отображаются в окне Проводника (Windows Explorer) внутри папки **Сеть** (Network) (см. рис. 1.4). Если выбрать конкретный компьютер, то можно увидеть его общие папки и принтеры (рис. 5.15). Любую такую папку можно раскрыть дальше и работать с ее содержимым как с локальной папкой (с учетом разрешений, предоставленных владельцем папки). Если щелкнуть по папке правой кнопкой мыши, то можно увидеть список дополнительных команд, которые можно выполнить для данной папки — отметим здесь команду добавления общей папки в локальную библиотеку (она имеется не для всех общих папок!). Если выполнить эту операцию, то содержимое папки удаленного компьютера можно просматривать в общем пространстве своей библиотеки, не обращаясь каждый раз к папке **Сеть** (Network).

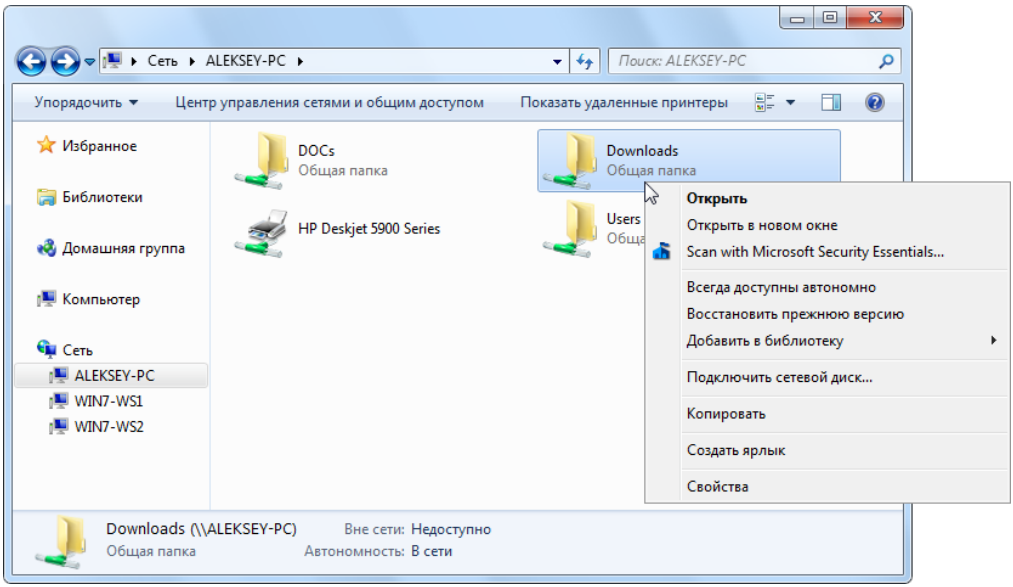

Рис. 5.15. Просмотр общих ресурсов на удаленном компьютере и меню команд для работы с общими папками

Примечание

Для участников домашней группы имеется еще один способ просмотра общих папок — непосредственно в папке **Домашняя группа** (HomeGroup) (см. рис. 1.6); он подробно рассматривался в *разд. "Компьютеры в составе домашней группы" главы 1*. В этом случае реализован только просмотр содержимого папок, без возможности подключения сетевых дисков.

Внимание!

Напомним, что для систем Windows 7 по умолчанию невозможен доступ к общим папкам, если используется учетная запись без пароля (даже в домашней группе).

Подключение сетевых дисков

Пользователи сети могут подключить любую общую папку в виде *сетевого диска*, который появится в списке устройств компьютера в окне Проводника. Иногда это необходимо для работы прикладных программ, обращающихся к данным на удаленных компьютерах. Подключения к сетевым дискам могут сохраняться и восстанавливаться при входе пользователя в систему.

Для того чтобы общая папка на удаленном компьютере стала доступной в виде диска, достаточно в окне программы в папке **Сеть** (Network) выбрать компьютер и папку, щелкнуть правой кнопкой и выполнить в контекстном меню команду **Подключить сетевой диск** (Map network drive) (см. рис. 5.15). (Эту команду можно вызвать и из контекстного меню опции **Компьютер** (Computer), имеющейся в меню **Пуск** (Start)[1].) Диску можно назначить любую свободную букву устройства

[1] В этом случае общую папку (см. рис. 5.16) можно задавать *произвольно*, вручную, или же выбрать после просмотра общих ресурсов сети.

(рис. 5.16) и указать, нужно ли восстанавливать подключение при последующих входах в систему. Установив нижний флажок, можно выбрать для подключения учетную запись, отличную от текущей (например, если для доступа к удаленному компьютеру требуются другие имя и пароль). В этом случае после нажатия кнопки **Готово** (Finish) система попросит указать эти дополнительные данные.

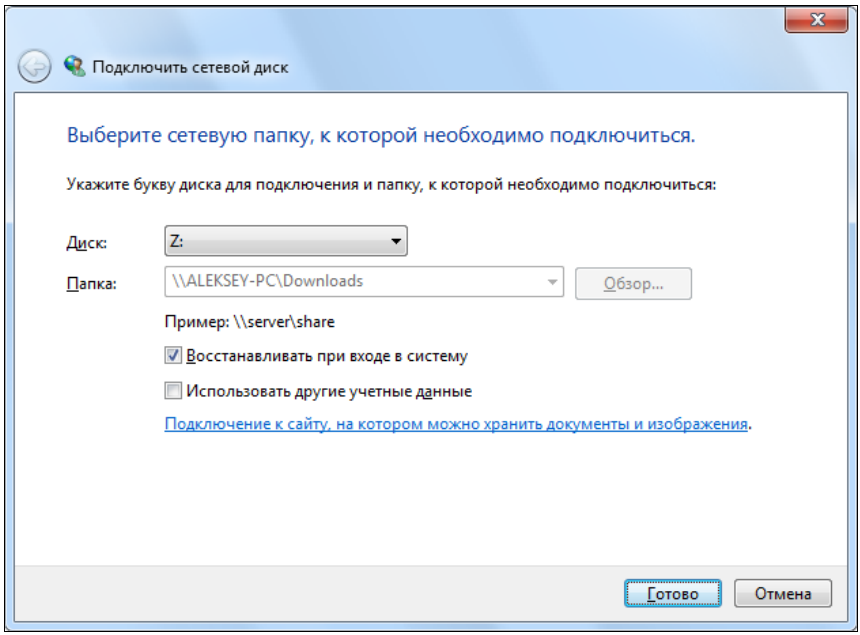

Рис. 5.16. Окно подключения к общей сетевой папке, расположенной на другом компьютере

Для удаления сетевого диска используется команда **Отключить** (Disconnect) в его контекстном меню или аналогичная команда в контекстном меню опции **Компьютер** (Computer).

Подключение к общему сетевому принтеру

Чтобы подключиться к принтеру, установленному на удаленном компьютере (входящем в домашнюю или в рабочую группу), достаточно выбрать принтер в папке **Сеть** (Network) (см. рис. 5.15), щелкнуть по нему правой кнопкой мыши и выполнить команду **Подключить** (Connect) в контекстном меню. Необходимые драйверы автоматически установятся на локальный компьютер, и устройство печати будет готово к работе.

Примечание

В данном разделе речь идет о принтерах, физически подключенных к компьютеру, т. е. о *локальных* принтерах удаленного компьютера, разрешенных для общего пользования *(см. ранее разд. "Включение общего доступа к локальным принтерам")*. При работе с сетевыми принтерами или принт-серверами (т. е. с устройствами печати, имеющими собственный сетевой адаптер и подключающимися непосредственно к сети) используются другие процедуры подключения, описанные в инструкциях произво-

дителя. Обычно к таким устройствам каждый компьютер сети подключается индивидуально, и операционная система рассматривает такое устройство как локальный принтер, с которым можно работать напрямую.

Подключенный удаленный принтер появляется в окне **Устройства и принтеры** (Devices and Printers) (см. рис. 3.24). Отсюда можно управлять принтером, просматривать очередь печати и свойства принтера. Здесь же, с помощью соответствующей команды из контекстного меню, сетевой принтер можно и отключить.

Подключение к принтеру можно инициализировать и из окна **Устройства и принтеры** (Devices and Printers), нажав кнопку **Установка принтера** (Add a printer) и в следующем окне выбрав опцию **Добавить сетевой, беспроводной или Bluetooth-принтер** (Add s network, wireless or Bluetooth printer). Система выполнит в сети поиск доступных принтеров, после чего следует выбрать принтер в списке и нажать кнопку **Далее** (Next). Выполнится подключение к удаленному принтеру и установка драйверов для него. Затем можно распечатать тестовую страницу и/или закончить работу мастера, нажав кнопку **Готово** (Finish). Установленный принтер становится устройством печати по умолчанию (отмечен зеленым кружком с галочкой).

Использование утилит командной строки

Все операции по управлению общими папками и сетевыми дисками можно выполнять и в окне консоли (командной строки). Перечислим основные команды и приведем примеры их использования. Подробное описание параметров каждой команды и ее дополнительных опций можно получить из встроенной справки, запустив конкретную команду с ключом `/?`.

Команда `net share` может применяться для просмотра списка общих папок и принтеров, имеющихся на локальном компьютере — для этого ее нужно запустить без параметров, например:

```
C:\>net share
Общее имя   Ресурс                        Заметки
-------------------------------------------------------------------
ADMIN$      C:\Windows                    Удаленный Admin
C$          C:\                           Стандартный общий ресурс
D$          D:\                           Стандартный общий ресурс
print$      C:\Windows\system32\spool\drivers
                                          Драйверы принтеров
IPC$                                      Удаленный IPC
DOCs        C:\Documents
Downloads   D:\Downloads
Users       C:\Users
HP Deskjet 5900 Series
            USB001              Очередь   HP Deskjet 5900 Series
Команда выполнена успешно.
```

Если выполнить команду, указав имя общей папки, то можно увидеть параметры использования этой папки, включая описание, имена подключившихся пользователей, разрешения на доступ и т. д.

С помощью команды `net share` также можно добавлять или изменять разрешения общего доступа, а также редактировать другие параметры общей папки.

Команда `net view` позволяет просматривать список общих папок на удаленном компьютере (работающем под управлением Windows или других систем). Если ее запустить без параметров, то она отображает список видимых в сети компьютеров, имеющих общие ресурсы:

```
C:\net view
Имя сервера            Заметки
-------------------------------------------------------------------
\\ALEKSEY-PC
\\WIN7-WS2
\\XPRUS
Команда выполнена успешно.
```

Если при запуске команды указывается имя компьютера, то перечисляются все его общие ресурсы:

```
C:\net view \\WIN7-WS2
Общие ресурсы на \\WIN7-WS2
Имя общего ресурса  Тип   Используется как  Комментарий
-------------------------------------------------------------------
Sys                 Диск
New                 Диск
Archive             Диск
Команда выполнена успешно.
```

Команда `net use` служит для подключения и отключения сетевых дисков[1], она позволяет подключить общую папку на удаленном компьютере в качестве сетевого диска и назначить ему букву устройства: например, после выполнения следующей команды в системе появится сетевой диск с именем Z:, который будет представлять собой общую папку Archive, хранящуюся на компьютере WIN7-WS2:

```
C:\>net use Z: \\WIN7-WS2\Archive
The command completed successfully.
```

При подключении сетевых дисков можно явно указывать учетную запись безопасности, используемую для доступа к удаленному компьютеру.

> ***ВНИМАНИЕ!***
>
> Важной особенностью команды `net use` является то, что она позволяет подключить в качестве сетевого диска папку, находящуюся *внутри* общего ресурса (программа Проводник такой возможности не предоставляет). Например, команда `net use X: \\WIN7-WS2\Archive\Docs` подключает папку Docs, находящуюся внутри общей папки Archive, как диск X:. Таким образом, пользователь получит доступ к конкретной папке и не сможет видеть другие (родительские) папки, также находящиеся в общей папке.

[1] Это может оказаться полезным, когда по каким-то причинам компьютер или сетевое устройство (например, медиаплеер) не видны в папке **Сеть** (Network) и нельзя подключиться к общей папке обычными способами, из окна Проводника.

ГЛАВА 6

Потоковое воспроизведение мультимедиа

Одной из интересных возможностей проигрывателя Windows Media Player версии 11.0, включенной в Windows Vista и работающей в Windows XP[1], и версии 12.0, входящей в состав Windows 7, является возможность потокового воспроизведения аудио- и видеофайлов, а также использование общих библиотек мультимедиа. Помимо этого, версия 12.0 позволяет воспроизводить файлы на удаленном компьютере или цифровом плеере — так называемый режим "Воспроизводить на" (Play To) — а также предоставлять доступ к домашней библиотеке мультимедиа через Интернет.

В режиме потокового воспроизведения файл не копируется целиком, а передается по частям, которые буферизируются и тут же проигрываются на конечном устройстве или компьютере. Благодаря этому не нужно клонировать файлы во все возможные места, а достаточно хранить в каком-то одном месте (централизованно или на разных компьютерах) и обращаться к ним по мере надобности. Кроме того, потоковый режим передачи не создает такой высокой нагрузки на сеть, как копирование файлов или воспроизведение файла из общей сетевой папки, и обычная беспроводная сеть Wi-Fi вполне справляется с передачей видеофайлов высокой четкости (до 1920×1088 пикселов), не говоря уж о передаче обычного видео и несжатого звука или использовании кабельных сетей.

В этой главе рассматриваются все сетевые возможности проигрывателя Windows Media 12.0 и его главные особенности, по сравнению с предыдущими версиями. Также описываются сетевые возможности Windows 7, касающиеся работы с устройствами мультимедиа.

Папка *Сеть* и устройства мультимедиа

Как уже говорилось в *главе 1*, все сетевые ресурсы в системах Windows просматриваются в папке **Сеть** (Network), отображаемой в окне Проводника (Windows

[1] При установке в Windows XP проигрыватель Windows Media 11.0 позволяет другим клиентам только обращаться к локальной библиотеке мультимедиа, т. е. использовать компьютер как медиасервер. В среде Windows Vista проигрыватель также позволяет просматривать общие библиотеки, хранящиеся на других компьютерах, и воспроизводить из них файлы.

Explorer). В предыдущих главах мы обращали внимание на компьютеры и общие ресурсы, а теперь подробно рассмотрим работу с устройствами мультимедиа, которые в упомянутом окне представлены как отдельная группа (категория) (рис. 6.1). Здесь присутствуют пиктограммы для всех устройств в сети, которые связаны с хранением или воспроизведением файлов мультимедиа (музыки, видео, изображений и ТВ-записей). Посмотрим, что означает вся имеющаяся информация, и начнем с бытовых устройств, подключаемых к локальной сети.

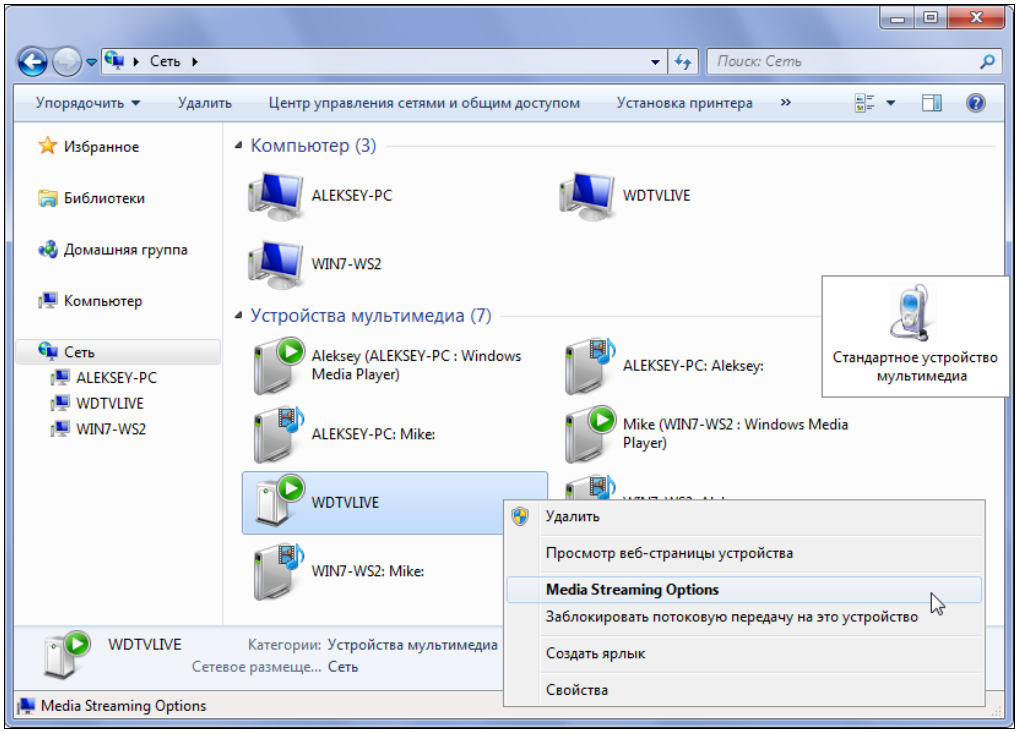

Рис. 6.1. Представление сетевых устройств мультимедиа в окне Проводника

Бытовые устройства мультимедиа при подключении к сети представляются в папке **Сеть** (Network) специальным значком, показанным на рис. 6.1 во врезке; помимо значка указывается имя устройства. Если щелкнуть по значку правой кнопкой мыши и в контекстном меню выполнить команду **Установить** (Install), то в системе будут установлены драйверы для выбранного устройства, и стандартный обобщенный значок поменяется на специализированный (см. выделенное устройство на рис. 6.1) — в нашем случае подключен медиасервер, он представлен как *модуль воспроизведения цифровых носителей*, Microsoft Digital Media Render Module[1]. Такой же значок для установленного устройства появляется и в окне **Устройства и принтеры** (Devices and Printers), где теперь можно просматривать свойства устрой-

[1] Назначение и возможности таких устройств будут понятными из дальнейшего текста.

ства и управлять его рабочими режимами. Если в системе разрешено скачивание из Интернета улучшенных значков устройств и замена стандартных пиктограмм, то при следующем обновлении в окне устройств появится новое изображение устройства (именно оно показано рис. 3.24), и этот же значок будет использоваться в пользовательском интерфейсе других функций мультимедиа (это можно видеть, например, на рис. 6.10). Кроме того, в этом случае в окне свойств устройства появятся сведения, предоставленные производителем.

> ***Внимание!***
>
> В *главе 1* говорилось о том, что для обнаружения мультимедийных устройств используется специальный протокол Simple Search and Discovery Protocol (SSDP). Поэтому специализированные цифровые устройства воспроизведения (медиаплееры) могут быть представлены только в категории устройств мультимедиа и никак не попадать в группу компьютеров, если у них нет собственных дисковых ресурсов с общим доступом.

Функционально устройства мультимедиа Windows 7 можно условно поделить на три типа (причем все три типа могут быть реализованы в одном устройстве или на одном компьютере):

- *медиасервер* — устройство или компьютер, имеющие локальную библиотеку мультимедиа (совместимую с проигрывателем Windows Media) и предоставившие к ней доступ другим пользователям компьютера или клиентам сети. Чем медиасервер отличается от обычного компьютера с общими папками — проще всего понять на примере бытового цифрового медиаплеера. Если плеер обращается к общей папке какого-то компьютера, то он может использовать определенную учетную запись этого компьютера и видеть обычный список файлов в выбранной папке, где ориентироваться можно только по именам файлов. Если плеер обращается к этому же компьютеру как к *медиасерверу*, то он сразу получает доступ к разрешенным библиотекам, причем их можно просматривать по жанрам, ключевым словам, оценкам, спискам воспроизведения и т. п. — т. е. по различным атрибутам, упрощающим поиск в библиотеке и ее организацию;
- *цифровой медиаприемник* или *медиаплеер* — устройство или компьютер, которые могут воспроизводить потоки мультимедиа с медиасерверов. Можно индивидуально управлять передачей потока на такое устройство, а также определять более конкретно параметры транслируемых файлов;
- *цифровой медиаплеер, поддерживающий функцию "Воспроизвести на"* (Play To) — то же, что и в предыдущем пункте, плюс возможность проигрывания файлов в тех случаях, когда сами файлы хранятся на другом компьютере и операция воспроизведения инициируется также с другого компьютера *(см. далее окончание главы)*. Для таких устройств к имени добавляется "суффикс" *Windows Media Player* (см. рис. 6.1). Применительно к компьютерам это означает, что на компьютере стоит Windows 7 и запущен проигрыватель Windows Media 12.0.

Дополнительная информация, касающаяся устройств мультимедиа и их значков, имеется *далее в разд. "Общий доступ к локальной библиотеке"*.

Проигрыватель Windows Media Player 12.0

Мультиформатный *Проигрыватель Windows Media* (Windows Media Player) является универсальным средством систем Windows для воспроизведения аудио-, видеофайлов и оптических носителей самых популярных форматов. В состав всех редакций Windows 7 входит проигрыватель версии 12.0[1].

Библиотеки мультимедиа являются одним из ключевых элементов проигрывателя Windows Media, поскольку к ним одновременно могут обращаться пользователи компьютера и локальной сети. Благодаря этому образуется доступная для всех, удобная для просмотра и поиска распределенная среда, в которую также могут интегрироваться различные цифровые плееры и бытовые медиасерверы, получающие все бóльшую популярность. Средствами воспроизведения мультимедиа по сети все чаще оснащаются даже обычные телевизоры[2], что позволяет передавать видео непосредственно от компьютера к экрану по проводной или беспроводной сети. Системы Windows 7 очень хорошо вписываются в такую инфраструктуру и могут быть основой для ее построения. Именно на "многопользовательские" и сетевые возможности проигрывателя Windows Media 12.0 мы и будем обращать основное внимание в дальнейших разделах этой главы. При этом речь пойдет и об особенностях и новых функциях данной версии проигрывателя.

> ***Внимание!***
>
> В редакциях Windows 7 Начальная (Starter) и Windows 7 Домашняя базовая (Home Basic) возможности проигрывателя Windows Media частично ограничены, поскольку в них отсутствует встроенный декодер MPEG-2 и не поддерживаются средства передачи потоков мультимедиа через Интернет (Remote Media Streaming).

Поддерживаемые форматы

Проигрыватель Windows Media 12.0 может воспроизводить аудио- и видеофайлы множества форматов, которые перечислены далее[3]. Помимо традиционных форматов, поддерживаемых предыдущими версиями программы, появилось множество новых — в первую очередь это касается видео высокой четкости и сжатых видеопотоков (которые новая версия воспроизводит без проблем и необходимости установки дополнительных кодеков), а также форматов, используемых компьютерами Apple и плеерами iTunes. Некоторые форматы на практике используются только для потокового вещания.

---

[1] В отличие от предыдущей, 11-й версии, эту программу нельзя скачивать отдельно и устанавливать на другие системы Windows.

[2] Конечно, не совсем "обычные", а, скорее, наоборот — "продвинутые" и новые модели. Но эта тенденция получает все большее распространение.

[3] По умолчанию некоторые из перечисленных форматов не ассоциированы с проигрывателем Windows Media, но могут нормально воспроизводиться, если открыть файлы из программы или задать соответствие.

Описание	Расширение файла
Аудио	
AU (UNIX)	.au и .snd
Сжатый звук AAC (стандарт для iPhone, iPod, iTunes, Sony PlayStation 3 и т. д.)	.m4a, .m4b, .m4p, .m4v, .m4r, .3gp, .mp4, .aac
Audio Interchange File Format (AIFF)	.aif, .aifc и .aiff
MPEG1 Audio Layer II (MP3)	.mp2, .mpa
MPEG1 Audio Layer III (MP3)	.mp3 и .m3u
Musical Instrument Digital Interface (MIDI)	.mid, .rmi и .midi
Аудио CD-диски	.cda
Несжатый поток Windows	.wav
Аудио Windows Media	.wma
Обложки Windows Media Player	.wmz и .wms
Списки воспроизведения Windows Media Player	.wpl
Видео	
Indeo video technology	.ivf
Видео высокой четкости AVCHD	.m2t, .mts и .m2ts
Записи цифрового телевидения MPEG-2 TS	.ts и .tts
Контейнерный формат для аудио- и видеопотоков, используемый в мобильных устройствах	.3gp
Контейнерный формат для файлов мультимедиа QuickTime	.mov и .qt
MPEG-1	mpeg, mpg, m1v
MPEG-2*	mpeg, mpg, mpe, mp2v и mpv2
Контейнерный формат для видеопотоков (AVI, H.264/MPEG-4 AVC, DivX и XviD)	avi
Видео Windows Media	asf, asx, wax, wm, wmd, wmv, wvx, wmp и wmx
Видео DVD	vob
Записанные телепередачи Microsoft (Microsoft Digital Video Recording) и Windows TV (WTV; Телепередача, записанная Windows)	dvr-ms и wtv

* Отсутствует в редакциях Windows 7 Starter и Windows 7 Home Basic.

Первые шаги при запуске проигрывателя

При первом запуске проигрывателя Windows Media из меню **Пуск** (Start) или при попытке воспроизведения какого-либо файла мультимедиа появляется окно приветствия программы, в котором пользователь может выбрать одну из двух опций настройки проигрывателя:

- **Рекомендуемые параметры** (Recommended settings) — принять стандартные параметры конфигурации, которые можно изменить позднее;
- **Настраиваемые параметры** (Custom settings) — настроить конфигурацию самостоятельно.

Первая опция позволяет быстро начать работу и поначалу не думать о настройках — любые параметры можно изменить в процессе работы. Если в системе уже имеется программный плеер и с ним связаны какие-то форматы файлов, то лучше выбирать ручную настройку.

При выборе второй опции пользователь имеет возможность указать, как проигрыватель будет взаимодействовать с различными интернет-сайтами, от которых можно получать информацию о названии треков аудиодисков, обновлять теги в файлах, уже хранящихся на компьютере, приобретать права для защищенного контента и т. д. По умолчанию проигрывателю разрешено получать из Интернета сведения о воспроизводимых файлах и дисках.

Далее можно указать — для воспроизведения каких файлов проигрыватель будет использоваться. По умолчанию выбраны все поддерживаемые типы файлов, но при необходимости можно задать и только конкретные форматы. Впоследствии эти ассоциации можно в любой момент переопределить через панель управления (категория **Программы по умолчанию** (Default Programs)).

Внимание!

Перед началом работы с проигрывателем Windows Media рекомендуется проверить состояние следующих важных флажков в окне параметров программы:

- **Добавлять воспроизводимые локальные файлы мультимедиа в библиотеку** (Add local media files to library when played) на вкладке **Проигрыватель** (Player);
- **Копировать компакт-диски автоматически** (Rip CD automatically) на вкладке **Копирование музыки с компакт-диска** (Rip Music);
- **Добавлять данные авторегулировки громкости в новые файлы** (Add volume leveling information values for new files) и **Удалять файлы с компьютера при удалении из библиотеки** (Delete files from computer when deleted from library) на вкладке **Библиотека** (Library);
- **Применять выравнивание громкости между дорожками** (Apply volume leveling across tracks) на вкладке **Запись** (Burn).

Используемые по умолчанию параметры разрешают операции, которые могут оказаться нежелательными (например, удаленный из библиотеки файл может физически удаляться с диска).

Кроме того, проверьте параметры копирования аудио-CD, поскольку по умолчанию эта операция запускается с текущими параметрами, которые могут оказаться неподходящими для вас.

Пользовательский интерфейс программы

После запуска проигрывателя Windows Media и первоначальной настройки можно увидеть главное окно программы, отображающее содержимое библиотеки мультимедиа. По умолчанию сразу же выполняется импорт файлов, имеющихся в стандартных личных папках пользователя, и в библиотеке появятся обложки альбомов для демонстрационных музыкальных клипов, имеющихся на диске после установки системы, а также сведения о других обнаруженных файлах.

Проигрыватель Windows Media 12.0 не сильно отличается от предыдущей версии функционально, однако пользовательский интерфейс для многих операций заметно переработан. Разработчики стремились минимизировать количество элементов управления, в результате чего некоторые решения могут показаться непривычными и к ним нужно привыкнуть.

> ***Внимание!***
>
> Заметным отличием версии 12.0 от предыдущих является отсутствие *Расширенного редактора тегов* (Advanced Tag Editor). Поскольку основную часть информации о треках можно получить из Интернета, данному факту можно не придавать большого значения. При необходимости удобные и бесплатные редакторы тегов легко найти в Сети.

Главное окно проигрывателя Windows Media, позволяющее работать с библиотеками мультимедиа разных пользователей и списками воспроизведения, используемыми в специальных рабочих режимах, показано на рис. 6.2. На примере этого окна рассмотрим главные элементы интерфейса программы.

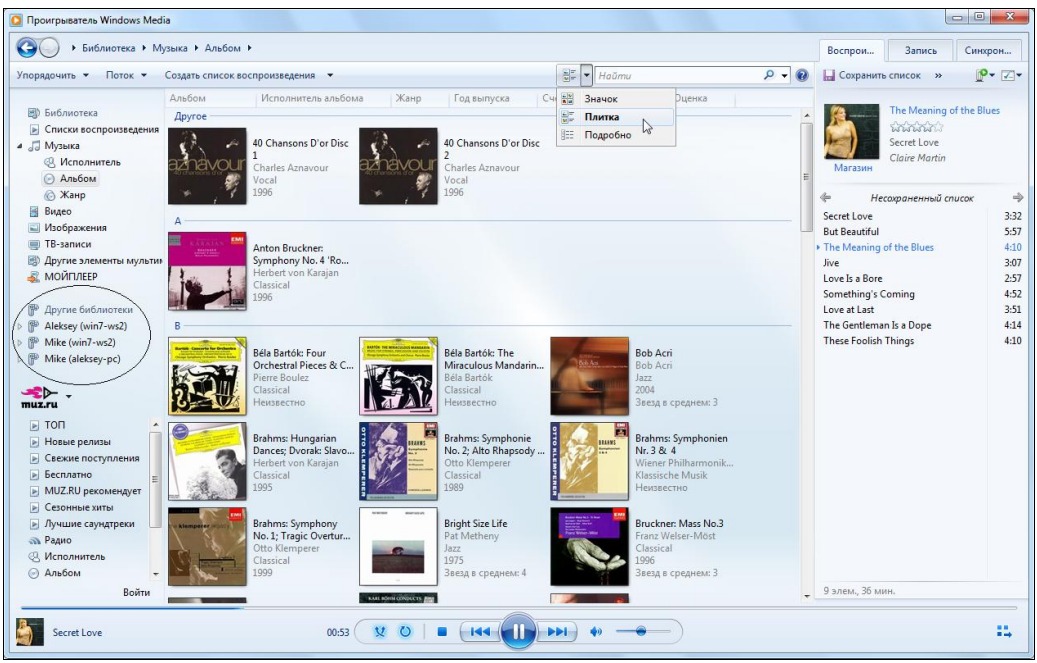

Рис. 6.2. Главное окно проигрывателя Windows Media 12.0 — один из многих вариантов отображения сведений о файлах, хранящихся в библиотеке мультимедиа

В верхней части окна программы (см. рис. 6.2) расположена *адресная строка* (address bar), где выбирается конкретная библиотека файлов мультимедиа (музыка, видео, ТВ-записи и т. д.) и списки воспроизведения (play lists). Правее находятся три кнопки (или названия вкладок), соответствующие *спискам* треков для основных режимов использования проигрывателя: **Воспроизведение** (Play), **Запись** (Burn), **Синхронизация** (Sync). Эти списки в виде вкладок появляются в правой части программы (см. рис. 6.2) при щелчке мышью по соответствующей кнопке и убираются при повторном щелчке.

Под адресной строкой находится *панель задач*, используемых для управления библиотеками мультимедиа, настройки окна программы и ее параметров (кнопка **Упорядочить** (Organize)), а также для конфигурирования потокового вещания и создания списков воспроизведения.

Левую часть окна программы занимает *область навигации*, где можно выбирать списки воспроизведения, разделы локальной библиотеки, подключаемые устройства и CD/DVD-приводы, содержащие диски. Здесь также можно выбирать разделы библиотек мультимедиа, предоставленных в общее пользование другими локальными пользователями или пользователями других компьютеров[1] (отмечены кружком на рис. 6.2). В левом нижнем углу находится кнопка перехода к страницам интернет-магазинов (Online Stores) или опции, предлагаемые конкретным магазином (см. рис. 6.2). Для настройки панели навигации используйте команду **Упорядочить | Настроить область переходов** (Organize | Customize navigation pane).

Центральную часть окна программы занимает панель содержимого библиотеки мультимедиа — *область сведений*. Эта панель отображается всегда (если не переключаться к текущему списку воспроизведения — *см. далее*), здесь же реализован и режим копирования треков с аудио-CD. В нижней части окна находится *панель элементов управления воспроизведением*. Также на ней отображаются сведения о текущем альбоме, а также могут появляться сообщения о ходе выполнения некоторых операций (например, копирования с аудио-CD, записи или синхронизации).

По умолчанию классическое меню команд (**Файл** (File), **Вид** (View)...) не отображается в окне программы (как и во многих встроенных приложениях Windows 7). Чтобы включить его *постоянно*, нужно либо нажать клавиши <Ctrl>+<M>, либо щелкнуть правой кнопкой мыши на панели адреса (или на панели управления воспроизведением) и в контекстном меню выполнить команду **Отображать меню** (Show menu bar). Для быстрого *временного* отображения меню команд достаточно нажать клавишу <Alt> — в этом случае всплывающее меню появляется в левом верхнем углу окна проигрывателя (рис. 6.3). При вызове меню щелчком правой кнопкой мыши список команд главного меню отображается в текущем местоположении курсора. С помощью этого меню можно получить доступ ко всем командам и параметрам проигрывателя.

[1] Здесь сразу следует отметить, что эти компьютеры могут входить как в домашнюю группу (HomeGroup), так и в обычную рабочую (при соблюдении прав доступа).

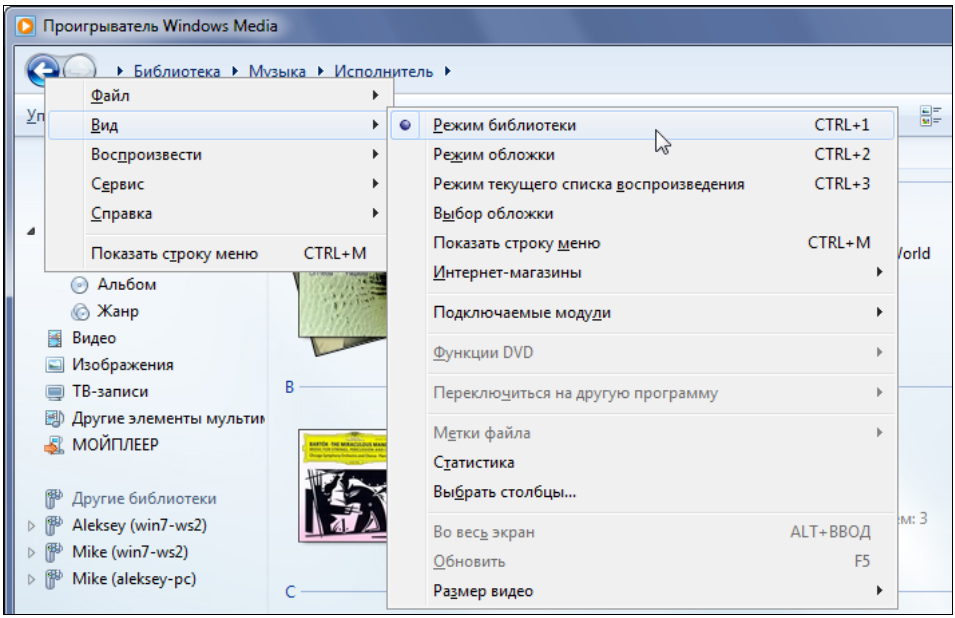

Рис. 6.3. Всплывающее меню команд программы

Библиотеки мультимедиа

Важнейший элемент проигрывателя Windows Media — это *библиотека мультимедиа* (Media Library), представляющая собой централизованное хранилище ссылок на аудио- и видеоматериалы, которые могут располагаться на компьютере в самых разных папках. Проигрыватель позволяет работать как с личной библиотекой пользователя (аудио, видео, изображения, ТВ-записи), так и с общими библиотеками других локальных или удаленных пользователей. Файлы мультимедиа (в любых поддерживаемых форматах) группируются по имени исполнителя (Artist), названию альбома (Album), жанру (Genre) (см. рис. 6.2) и другим атрибутам, которые можно выбрать в окне настройки области переходов. В библиотеке также хранятся списки файлов, отобранных для воспроизведения в определенном порядке (playlist), и списки файлов, подготовленных для записи на оптические диски или съемные носители. Возможность поиска по ключевым словам позволяет быстро находить записи по названиям произведений, именам исполнителей и т. д.

> ***Примечание***
>
> Библиотека мультимедиа является общей как для проигрывателя Windows Media 12.0, так и для программной оболочки Windows Media Center. Общими также являются и некоторые параметры, например формат копирования аудио-CD на жесткий диск или списки воспроизведения.

Обнаруженная на дисках компьютера информация заносится в библиотеку и сортируется в первую очередь не по местонахождению в определенных папках на диске, а по тематическим признакам, и ее элементы воспринимаются пользователем как

логически связанные объекты. Если даже файлы мультимедиа разбросаны по всему диску или между несколькими компьютерами, визуально все они могут быть собраны в одной библиотеке мультимедиа, и их не нужно всякий раз искать заново. Если требуется узнать, где физически находятся конкретные файлы, то можно обратиться к свойствам трека (*см. далее* команду **Открыть расположение файла** (Open file location) в контекстном меню — см. рис. 6.5).

Работать с библиотекой мультимедиа в проигрывателе Windows Media 12.0 очень удобно, поскольку отображается только выбранный раздел (музыка, видео и т. д.) и все элементы библиотеки представлены пиктограммами. Например, при просмотре музыкальных альбомов можно видеть обложки дисков (см. рис. 6.2) (переключение режимов осуществляется с помощью кнопки **Параметры просмотра** (View options), показанной слева от панели поиска). То же самое можно сказать и о других способах группировки содержимого библиотеки. В режиме группировки записей по песням (Songs) все треки очень удобно разбиты по альбомам, и в них легко ориентироваться.

Переключаться между разделами библиотеки, а также подразделами внутри любого выбранного подраздела, можно с помощью меню, появляющегося при щелчке по стрелке рядом с кнопкой выбора раздела на панели адреса, — в этом меню легко указать элемент для соответствующего подраздела (рис. 6.4).

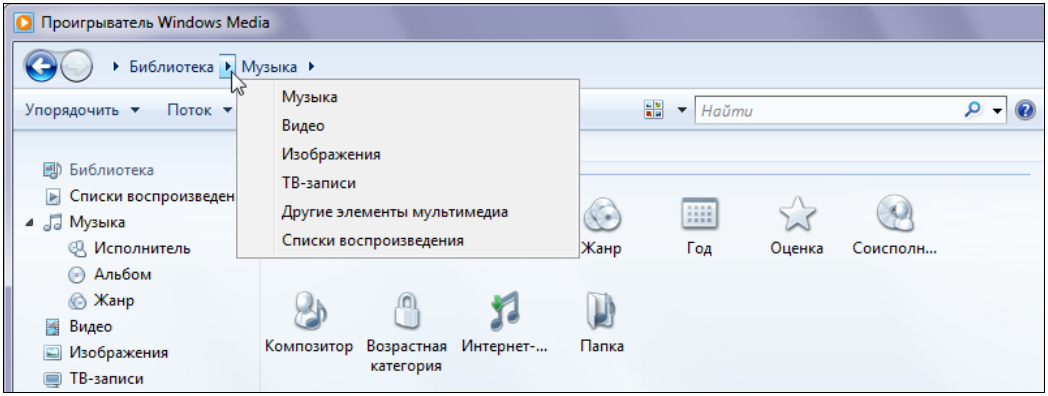

Рис. 6.4. Меню выбора раздела библиотеки мультимедиа

Щелкнув правой кнопкой на имени одной или нескольких выделенных дорожек в библиотеке музыкальных файлов или в некотором списке воспроизведения, можно получить доступ к контекстному меню (рис. 6.5), позволяющему выполнять манипуляции с этими записями. Здесь нужно обратить внимание на команды добавления в специальные списки *воспроизведения* (включая списки *записи* и *синхронизации*). Записи можно включить в любой из уже существующих списков воспроизведения (пример выделен на рисунке) или создать дополнительный. Кроме того, обратите внимание на команду **Воспроизвести на** (Play to), с помощью которой треки можно проигрывать на *удаленных* цифровых медиаплеерах.

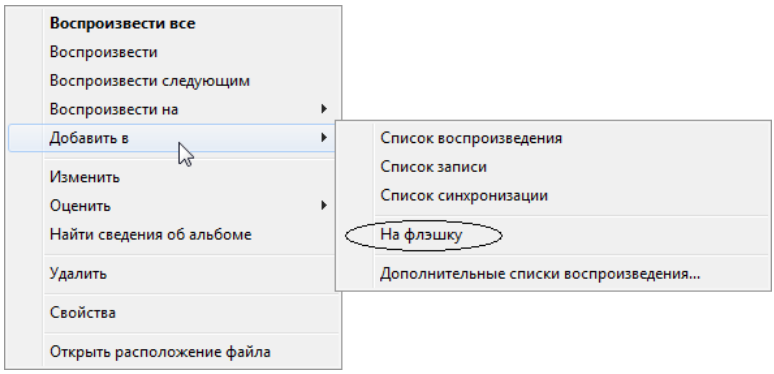

Рис. 6.5. Команды для треков, выбранных в окне библиотеки или в списке воспроизведения

Добавление файлов в библиотеку

При работе с проигрывателем Windows Media 12.0 ссылки на различные файлы мультимедиа могут появляться в библиотеке мультимедиа разными способами:

- по умолчанию файлы добавляются в библиотеку при их воспроизведении. Флажок, управляющий этой опцией, — **Добавлять воспроизводимые локальные файлы мультимедиа в библиотеку** (Add local media files to library when played) — находится на вкладке **Проигрыватель** (Player) (команда **Параметры** (Options) в меню кнопки **Упорядочить** (Organize)). По умолчанию он установлен;
- основной режим наполнения библиотеки мультимедиа — когда проигрывателю Windows Media явно указывается, за какими папками он должен следить, чтобы их содержимое автоматически отображалось в библиотеке. В этом случае все ссылки на новые или удаленные файлы будут сразу же регистрироваться или аннулироваться в библиотеке, и не нужно следить за обновлением ссылок.

Чтобы увидеть список просматриваемых папок и изменить его, нужно открыть меню кнопки **Упорядочить** (Organize), выполнить команду **Управление библиотеками** (Manage libraries) и выбрать нужную библиотеку (можно просто щелкнуть по библиотеке правой кнопкой мыши и выбрать команду **Управление...** (Manage ... library)). В окне настроек (рис. 6.6) задаются все папки (локальные или удаленные), за которыми проигрыватель будет следить в процессе своей работы. После сканирования указанных папок программа распределит все обнаруженные файлы по тематическим папкам, руководствуясь информацией, хранящейся в атрибутах файлов.

Удаление файлов и папок из библиотеки

Существуют два способа удаления файлов и папок: в первом случае из библиотеки мультимедиа удаляется только *ссылка* на объект файловой системы; во втором — вместе со ссылкой файлы и/или папки удаляются *физически*.

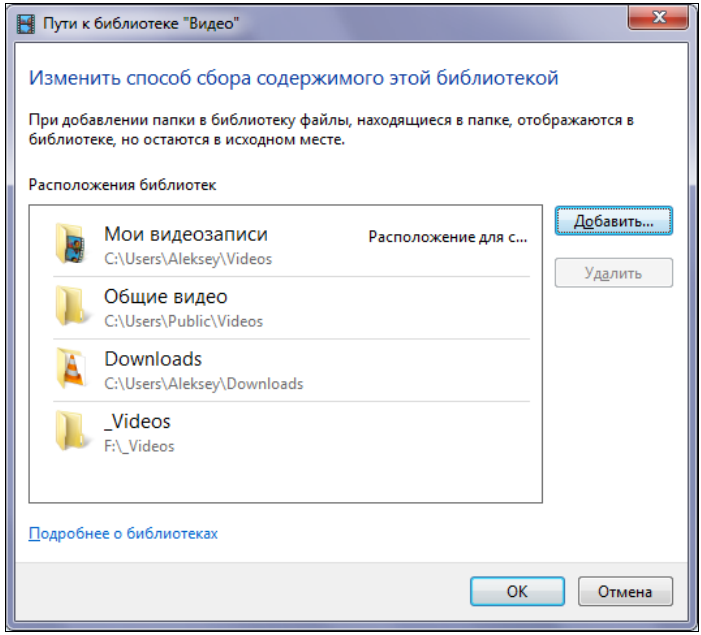

Рис. 6.6. Окно выбора папок, содержимое которых просматривается для создания библиотеки музыкальных файлов

Перед тем как работать с библиотекой, необходимо выбрать режим удаления элементов. Выполните команду **Параметры** (Options) в меню кнопки **Упорядочить** (Organize) и на вкладке **Библиотека** (Library) определите нужное состояние флажка **Удалять файлы с компьютера при удалении из библиотеки** (Delete files from computer when deleted from library). Лучше этот флажок не устанавливать, чтобы случайно не удалить файлы физически.

По умолчанию проигрыватель просит уточнить, какие объекты удалять (рис. 6.7). Пользователю лучше всего определить наиболее удобную для себя стратегию при выполнении операций удаления и впоследствии уже не менять ее.

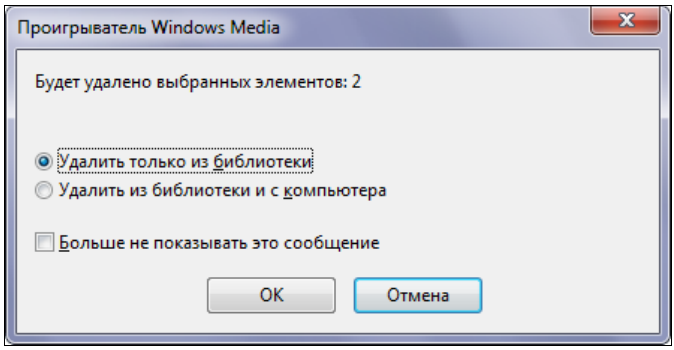

Рис. 6.7. Запрос на удаление файла из библиотеки

Списки воспроизведения

Для выборочного прослушивания треков, например произведений определенного жанра или исполнителя, используются *списки воспроизведения* (playlist). Такие списки также создаются в процессе подготовки файлов к копированию на компакт-диск или переносное устройство, а также для воспроизведения на удаленном цифровом медиаплеере *(см. далее)*. Для формирования списков можно пользоваться командами в контекстном меню треков (см. рис. 6.5) или просто перетаскивать мышью имена выбранных треков на открытую панель списка воспроизведения (записи или синхронизации). Если списку дается имя (в верхней части панели), то он считается сохраненным и его имя появляется в составе узла **Списки воспроизведения** (Playlists) (см. рис. 6.4).

Все созданные пользователем списки (с расширением .wpl) помещаются в подкаталог **Playlists**, создаваемый в личной папке **Моя музыка** (My Music).

Общий доступ к локальной библиотеке

Библиотеки мультимедиа можно использовать совместно несколькими пользователями (как локальными, работающими на одном компьютере, так и удаленными, обращающимися к компьютеру по сети и, даже, через Интернет). С помощью соответствующих параметров пользователь может разрешить удаленным компьютерам доступ к своей личной библиотеке или ее отдельным папкам (это распространяется и на других пользователей *данного* компьютера). При этом файлы мультимедиа остаются в стандартных пользовательских папках, и их не нужно никуда перемещать (в *общие* папки).

> ***Примечание***
>
> Для удаленного доступа к библиотеке мультимедиа используется специальная сетевая служба — *Служба общих сетевых ресурсов проигрывателя Windows Media* (Windows Media Player Network Sharing Service, сервис WMPNetworkSvc), поэтому общедоступные папки библиотеки не являются традиционными общими ресурсами, которые можно видеть в сетевом окружении (например, при помощи команды `net share`). Для работы данной службы брандмауэр Windows открывает специальные порты, а ее имя (учетная запись) используется в настройках безопасности для разрешенных папок.

Опции общего доступа к библиотеке мультимедиа можно изменять в любой момент (все эти опции доступны, если только имеется связь с сетью). Для этого используются команды кнопки **Поток** (Stream), имеющейся на панели задач (рис. 6.8). Первая опция (доступ через Интернет) будет описываться отдельно, в следующем разделе, пока рассмотрим другие команды. Если разрешается удаленное управление проигрывателем, то другие пользователи с помощью команды **Воспроизвести на** (Play To) смогут проигрывать файлы на данном экземпляре проигрывателя Windows Media. При этом название плеера появится после имени пользовательской библиотеки и имени компьютера (см. рис. 6.1). Для разрешения удаленного воспроизведения необходимо будет в специальном окне (рис. 6.9) подтвердить выполнение операции.

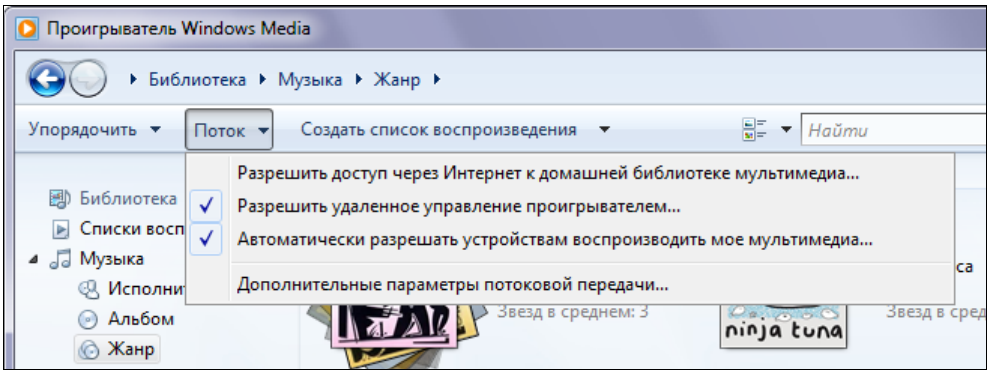

Рис. 6.8. Команды управления потоковым воспроизведением файлов мультимедиа

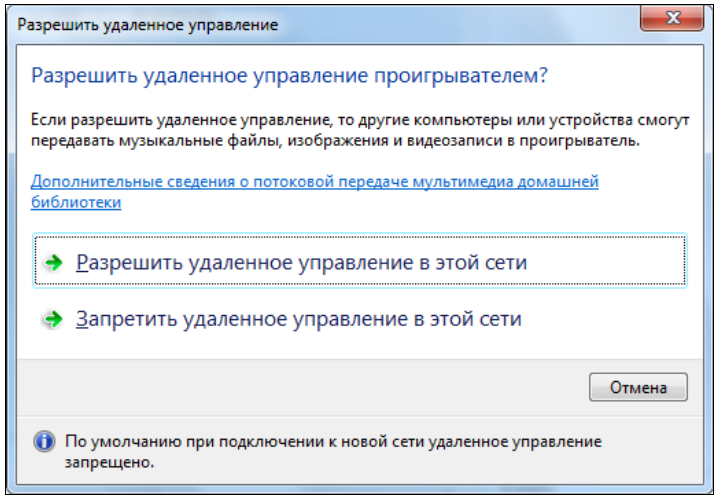

Рис. 6.9. Окно подтверждения операции разрешения удаленного управления плеером

Если флажок автоматического разрешения воспроизведения файлов (см. рис. 6.8) установлен, то все устройства сети могут обращаться к библиотекам мультимедиа данного пользователя и проигрывать его файлы; при этом в окне домашней группы (см. рис. 1.22) одновременно будет устанавливаться флажок **Потоковая передача изображений, музыки и видео на все устройства домашней сети** (Stream my pictures, music, and videos to all devices on my home network). Если какой-либо из названных флажков сбросить, то сбросится и другой флажок, при этом доступ от ***всех*** устройств сети будут сразу же заблокирован. Если меняется состояние флажка в окне проигрывателя, то появляется окно подтверждения операции, аналогичное тому, что показано на рис. 6.9, только меняется название функции.

Для тонкой (индивидуальной) настройки устройств сети необходимо в меню кнопки **Поток** (Stream) (см. рис. 6.8) выполнить команду **Дополнительные параметры потоковой передачи** (More streaming options). В специальном окне (рис. 6.10) перечисляются устройства и компьютеры, которым разрешен или запрещен доступ

к библиотечным файлам (при этом для разных устройств могут применяться *параметры по умолчанию* или *пользовательские параметры*). Даже на самом компьютере можно разрешить или запретить другим локальным пользователям доступ к своим файлам.

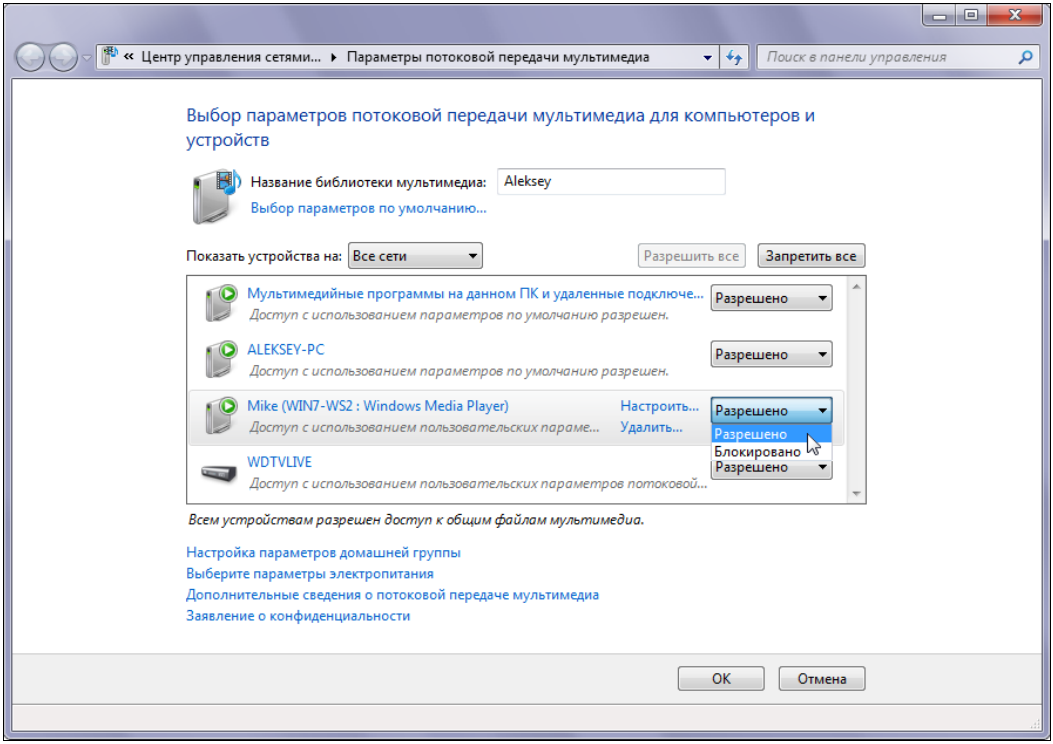

Рис. 6.10. Окно управления общим доступом к библиотечным файлам

Ссылка **Настройка параметров домашней группы** (Choose homegroup and sharing options) (см. рис. 6.10) позволяет открыть окно, где разрешается и запрещается доступ к локальным библиотекам в целом (флажок **Потоковая передача изображений, музыки и видео на все устройства домашней сети** (Stream my pictures, music, and videos to all devices on my home network)), а также отмечаются конкретные типы файлов, которые будут доступны другим пользователям (см. рис. 1.22).

Параметры доступа являются индивидуальными для каждого пользователя компьютера. Если нажать кнопку **Запретить все** (Block All), то передача потокового мультимедиа с данного компьютера будет полностью запрещена. Включить ее можно будет с помощью соответствующей команды в меню кнопки **Поток** (Stream) (см. рис. 6.8).

По умолчанию можно разрешить доступ другим пользователям локального компьютера, но если в сети имеются другие компьютеры, работающие под управлением Windows 7 в составе домашней группы, то можно указывать и пользователей других компьютеров.

После того как некоторый пользователь компьютера разрешил общий доступ к своей библиотеке мультимедиа, на других компьютерах домашней сети в папке **Сеть** (Network) программы Проводник (Windows Explorer) в разделе устройств мультимедиа (см. рис. 6.1) появится дополнительный значок (рис. 6.11) с именем компьютера — выступающего в данном случае в роли *медиасервера* — и названием пользовательской библиотеки, которое было указано при включении общего доступа (см. рис. 6.10).

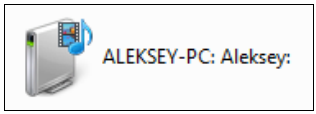

Рис. 6.11. Представление в окне Проводника общедоступной библиотеки мультимедиа, расположенной на локальном или удаленном компьютере — значок *медиасервера*

Если другие пользователи дважды щелкнут по такому значку, то запустится проигрыватель Windows Media, и они смогут воспроизводить файлы ***из*** выбранной библиотеки. В случае, когда на значке устройства имеется зеленый кружок с белым треугольником, это означает, что данное устройство потенциально может воспроизводить файлы из удаленных библиотек — т. е. выступает в роли цифрового *медиаплеера*, и ***на*** данное устройство возможна передача потоков мультимедиа с локального компьютера (разрешена она или нет фактически — это нужно смотреть в контекстном меню устройства или в окне параметров — см. рис. 6.10). Щелкнув по такому значку правой кнопкой мыши, можно выбрать параметры потокового вещания, а также запретить или разрешить передачу потока на это устройство (рис. 6.12) (это сразу отразится и в окне параметров потоковой передачи — см. рис. 6.10). Если же на другом компьютере запущен проигрыватель Windows Media, то помимо зеленого кружка после имени библиотеки и компьютера указывается "Windows Media Player", и это означает, что можно непосредственно ***воспроизводить*** файлы ***на*** тот компьютер[1] (с помощью функции Play To — *см. далее*).

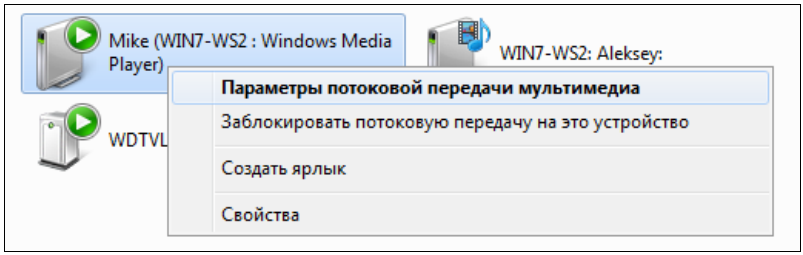

Рис. 6.12. Представление в окне Проводника компьютера или устройства, способного принимать потоки мультимедиа — значок *медиаплеера*

[1] По виду значка *бытовых* устройств или по наличию команд в контекстном меню нельзя судить о наличии у них такой возможности.

Разрешение доступа через Интернет

Новая возможность проигрывателя Windows Media 12.0 позволяет обратиться к домашнему архиву мультимедийных файлов из любой точки, где есть доступ к Интернету. Таким образом, многочисленные файлы не нужно носить с собой, а обращаться к ним можно точно так же, как и к любой библиотеке проигрывателя Windows Media.

Для использования данной функции необходимо, чтобы были соблюдены следующие условия:

- домашний компьютер, на котором хранятся файлы, должен располагаться в частной сети (т. е. не в публичной или доменной);
- оба компьютера — передающий и принимающий — должны работать под управлением Windows 7 (возможны редакции Домашняя расширенная (Home Premium) и старше);
- чтобы доступ стал возможным, необходимо сначала к каждому компьютеру "привязать" *сетевое удостоверение* Windows Live ID (одно удостоверение может работать не более чем с 10 компьютерами). С помощью такой операции пользователь как бы авторизует каждую систему и позволяет ей обращаться к одним и тем же файлам.

> ***Идентификатор Windows Live ID***
>
> Для доступа ко многим веб-ресурсам (онлайновым службам) компании Microsoft и для работы с компонентами Windows Live (например, с программой Messenger) необходим идентификатор *Windows Live ID*. Идентификатор Windows Live ID легко получить на сайте **http://home.live.com** — здесь необходимо лишь пройти простую регистрацию и получить новый почтовый адрес Hotmail.com или Live.com, который и будет являться идентификатором при дальнейших обращениях.

Операция разрешения доступа инициируется из окна проигрывателя Windows Media, где необходимо в меню кнопки **Поток** (Stream) на панели задач установить флажок **Разрешить доступ через Интернет к домашней библиотеке мультимедиа** (Allow Internet access to home media). При первом обращении к данной функции система попросит привязать к учетной записи пользователя сетевое удостоверение (рис. 6.13). Эту же операцию можно инициировать непосредственно, выбрав в окне учетной записи пользователя (в него легко попасть, щелкнув по значку пользователя в меню **Пуск** (Start)) ссылку **Подключение идентификаторов пользователей Интернета** (Link online IDs).

Изначально в окне **Сопоставление ИД интернет-служб** (Link Online IDs) (см. рис. 6.14) кроме значка и имени пользователя имеется только кнопка добавления поставщика сетевых удостоверений, который необходим для связи идентификатора (ИД) интернет-службы с учетной записью пользователя Windows. Фактически предлагается единственный поставщик — Windows Live ID. После выбора опции добавления поставщика выполняется переход на веб-страницу сайта Microsoft, откуда нужно загрузить программу "Помощник по входу Windows Live ID 6.5" (32- или 64-разрядную версию). Скачанный файл (размером 5—6 Мбайт) можно сохранить на диске и затем установить, а можно сразу запустить на выполнение.

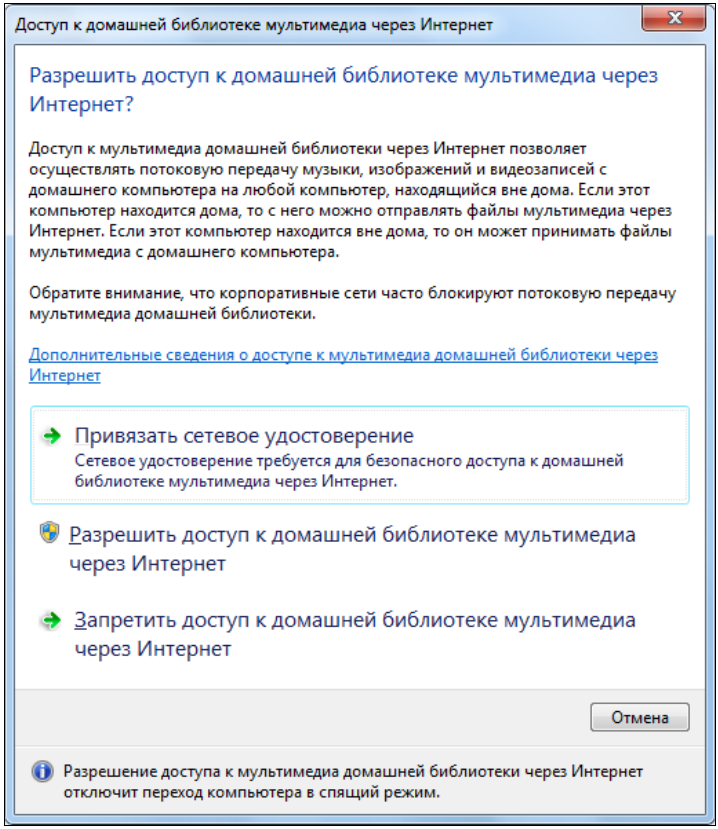

Рис. 6.13. Опции настройки доступа к библиотеке мультимедиа через Интернет

После того как программа будет установлена, в окне (рис. 6.14) появится логотип поставщика, и можно выполнять привязку сетевого удостоверения. Для этого щелкните по ссылке **Сопоставить подключенный ИД** (Link online ID) и войдите в службу Windows Live. В случае успешного входа будут выполнены необходимые привязки, и окно сопоставлений обновится — в нем можно будет видеть имя пользователя, зарегистрированное в интернет-службе (рис. 6.15). Теперь нужно нажать кнопку **ОК** и продолжить настройку доступа.

Вернувшись в окно доступа к домашней библиотеке мультимедиа (см. рис. 6.13), можно будет увидеть, что теперь опция разрешения доступа стала доступной. После ее выбора выполняются необходимые системные проверки и настройки, и по окончании операции появляется окно (рис. 6.16), сообщающее об успешном ее завершении — компьютер готов к воспроизведению мультимедиа через Интернет, и можно связываться с другими компьютерами. Перед этим, однако, выбранное сетевое удостоверение (***тот же самый*** Windows Live ID) должно быть привязано к учетной записи пользователя и на другом компьютере (или на нескольких компьютерах).

Если теперь в окне проигрывателя Windows Media снова щелкнуть по флажку **Разрешить доступ через Интернет к домашней библиотеке мультимедиа** (Allow

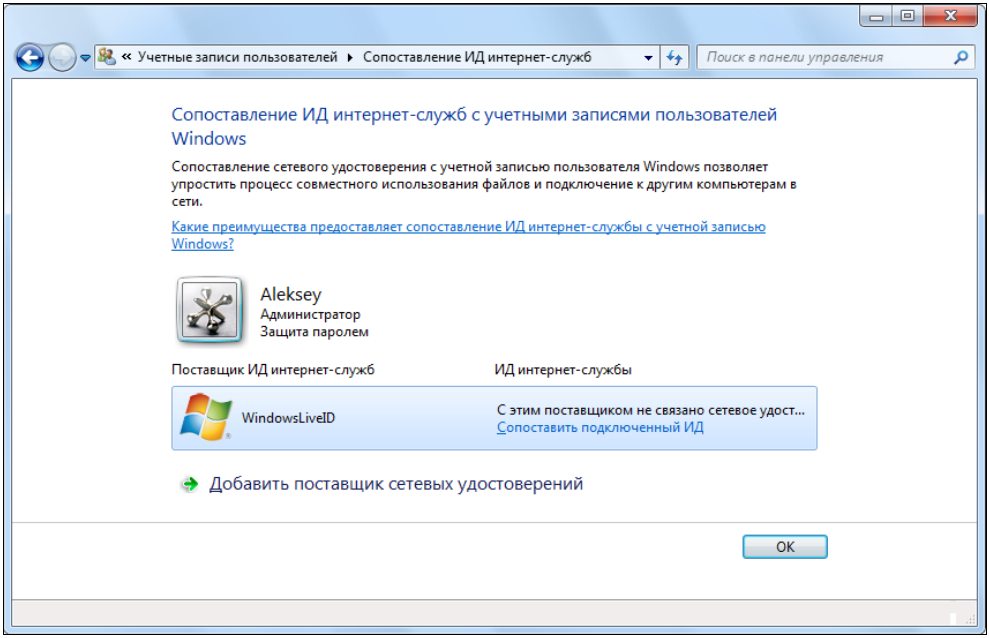

Рис. 6.14. Вид окна сопоставления ИД интернет-служб после установки поставщика сетевых удостоверений

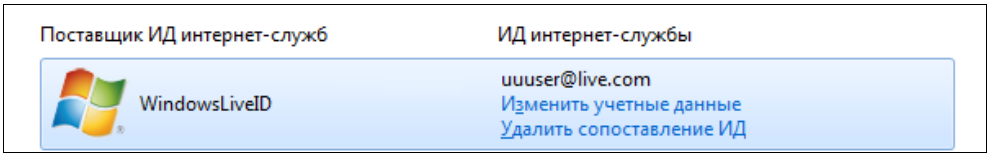

Рис. 6.15. Изменения в окне сопоставлений после подключения Windows Live ID

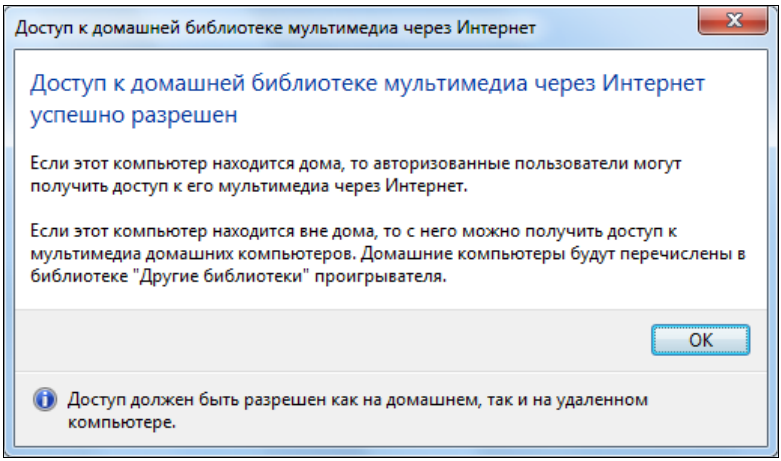

Рис. 6.16. Сообщение об успешном завершении настройки доступа к библиотеке мультимедиа через Интернет

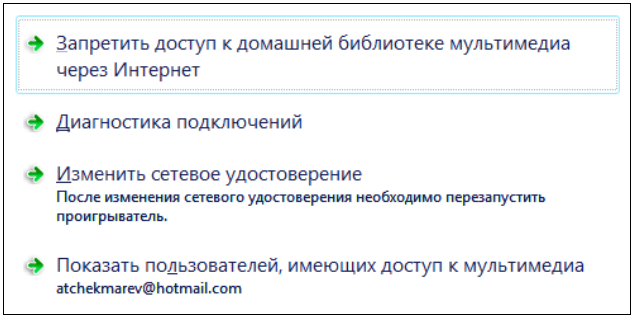

Рис. 6.17. Опции управления доступом к домашней библиотеке через Интернет

Internet access to home media) в меню кнопки **Поток** (Stream) (см. рис. 6.8), то в окне доступа будут отображаться новые опции (рис. 6.17) — их назначение понятно из названий, кроме опции диагностики, на которой мы остановимся подробнее.

Опция **Диагностика подключений** (Diagnose connections) позволяет проверить правильность выполнения операции разрешения доступа через Интернет, доступность компьютеров и наличие портов TCP, необходимых для дальнейшей работы. Все результаты тестов отображаются в специальном окне (рис. 6.18), где следует обратить внимание на ссылку **Сведения о перенаправлении портов** (Port forwarding information). Эту информацию следует обязательно учесть, если в сети используется маршрутизатор или другое подобное оборудование, фильтрующее трафик.

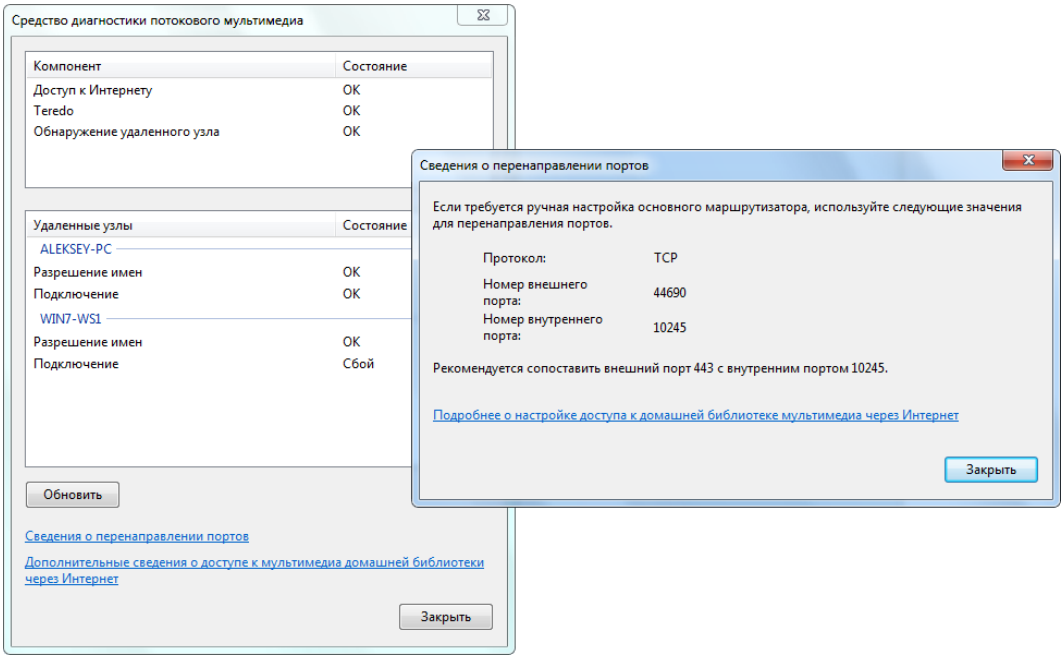

Рис. 6.18. Результаты проверки соединений для передачи файлов мультимедиа и сведения об используемых портах TCP

Для передачи мультимедиа через Интернет используется протокол TCP. Для каждого компьютера задается уникальный *номер внешнего порта*, который будет применяться для доступа к домашнему компьютеру извне. Этот номер следует учесть при настройке маршрутизатора. Один и тот же номер порта — 10245 — используется для доступа к файлам внутри домашней сети. Также рекомендуется добавить сопоставления между внешним портом 443 и внутренним 10245.

Воспроизведение файлов мультимедиа через Интернет

Просмотр файлов в удаленной библиотеке, доступной через Интернет, ничем не отличается от манипуляций с библиотекой локального пользователя, работающего на том же самом компьютере. Имя библиотеки и компьютера, где она находится, указывается в окне проигрывателя Windows Media в списке "Другие библиотеки" (Other Libraries) в области навигации (см. рис. 6.1). Единственное, что отличает библиотеку, доступ к которой выполняется через Интернет, это наличие крошечного значка глобуса на значке этой библиотеки.

Воспроизведение музыки и видео

Рассмотрим особенности основных рабочих режимов проигрывателя Windows Media 12.0, обращая внимание на отличия от предыдущих версий.

Воспроизведение музыки, DVD-диска или диска со смешанным содержимым может начинаться автоматически сразу после того, как диск оказывается в приводе. Пользователь сам выбирает программу для выполнения операций. По умолчанию в системах Windows 7 диски CD-аудио и фильмы на DVD-дисках автоматически начинают проигрываться с помощью проигрывателя Windows Media. Это определяется параметрами автозапуска (см. панель управления).

Если диск (аудио или видео) уже находится в приводе, то в окне проигрывателя его можно запустить на воспроизведение, выбрав имя диска или устройства в области навигации. Во время воспроизведения аудиофайлов или компакт-дисков можно продолжать просмотр разделов библиотеки. Щелкнув по названию вкладки **Воспроизведение** (Play), можно в любой момент увидеть содержание звучащего в данный момент альбома (при повторном щелчке список воспроизведения закрывается).

Одно из заметных отличий проигрывателя Windows Media Player 12.0 от предыдущих версий состоит в том, что он может воспроизводить музыкальные файлы в двух режимах:

- с отображением *главного окна* программы, где просматривается содержимое библиотеки мультимедиа (см. рис. 6.1);
- в специальном *окне списка воспроизведения*, где присутствует только информация, относящаяся к звучащему альбому или файлу (см. рис. 6.20).

Также в проигрывателе сохраняется возможность воспроизведения в режиме обложки (см. рис. 6.21).

Для управления проигрывателем Windows Media 12.0 можно использовать "быстрые клавиши" (hotkeys), список которых приведен в табл. П1.4 *приложения 1*.

Аудиофайлы и CD-диски

Во время воспроизведения выбранного файла или диска на *панели списка* (List pane) в правой части окна программы может отображаться разнообразная информация, относящаяся к данному файлу или диску: например, обложка диска, названия альбома и треков (для DVD-дисков — список разделов), длительность дорожек и т. д. (рис. 6.1). В списке проигрываемых файлов можно менять порядок их воспроизведения (перетаскивая названия мышью или пользуясь командами контекстного меню).

Одновременно с прослушиванием компакт-диска, альбома или списка воспроизведения можно осуществлять просмотр библиотеки мультимедиа — звучание музыки при этом не прекращается. В проигрывателе Windows Media 12.0 появилась новая интересная функция, названная *предпросмотром* (preview). Смысл ее описан ниже.

> ***Примечание***
>
> Функцией предпросмотра управляет флажок **Автоматически проигрывать фрагмент композиции при наведении курсора на заголовок дорожки** (Automatically preview songs on track title hover) на вкладке **Библиотека** (Library) в окне параметров проигрывателя. Если флажок установлен, то воспроизведение треков начинается автоматически всегда (даже если плеер остановлен), и можно лишь управлять прокруткой трека. Далее описано поведение программы для случая, когда этот флажок сброшен (по умолчанию).

Если при просмотре содержимого музыкального альбома задержать курсор мыши над каким-нибудь треком, то появляется окно с изображением альбома и названием трека (рис. 6.19, *сверху*). Если щелкнуть по ссылке **Предпросмотр**, то текущая музыка прерывается и начинает звучать с начала выбранный трек (рис. 6.19, *снизу*). Щелкая по ссылке **Пропустить**, можно "перескакивать" по треку на 15 секунд вперед. Если отвести курсор от изображения всплывающего окна, то возобновляется звучание прерванной дорожки — с того момента, когда произошла остановка.

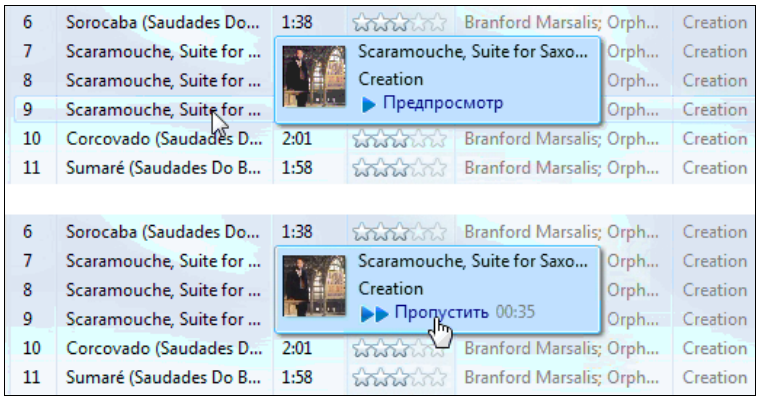

Рис. 6.19. Предпросмотр треков в просматриваемом альбоме

Если щелкнуть по кнопке, расположенной в правом нижнем углу окна программы, то проигрыватель переключается к *текущему списку воспроизведения*, который

отображается в небольшом окне. Здесь могут отображаться обложка альбома (рис. 6.20, *слева*), зрительные образы или список треков (рис. 6.20, *справа*).

Рис. 6.20. Окно текущего списка воспроизведения

Кроме того, присутствуют кнопки управления воспроизведением и регулятор громкости (они автоматически скрываются после небольшой паузы), а также кнопка перехода в окно библиотеки мультимедиа (в правом верхнем углу — отмечена на правом рисунке кружком). Если окно проигрывателя растянуть по горизонтали, то обложка (или образы) и список треков могут отображаться одновременно.

Для смены вида окна текущего списка воспроизведения нужно щелкнуть в окне правой кнопкой мыши и в контекстном меню в подменю **Зрительные образы** (Visualization) выбрать желаемый зрительный образ или изображение обложки диска (опция **Оформление альбома** (Album Art)). Список воспроизведения включается/выключается с помощью команд **Показать список/Скрыть список** (Show list/Hide list).

Режимы работы проигрывателя

Проигрыватель Windows Media Player 12.0, как и предыдущие версии, имеет возможность работы в режиме *обложки* (skin), который используется для компактного представления программы (рис. 6.21). В системах Windows 7 предлагается только две стандартных обложки, однако существует множество обложек, которые можно выбрать по своему вкусу и загрузить с веб-сайта Microsoft. Для выбора и смены обложки нужно в главном меню выполнить команду **Вид | Выбор обложки** (View | Skin Chooser).

Для возврата в окно библиотеки используется значок в верхнем правом углу программы (отмечен кружком на рис. 6.20, *справа*).

Однако проще всего для переключения режимов использовать комбинации клавиш:

- <Ctrl>+<1> — переход в окно библиотеки;
- <Ctrl>+<2> — работа в режиме обложки;
- <Ctrl>+<3> — отображение окна текущего списка воспроизведения.

Рис. 6.21. Работа проигрывателя Windows Media в режиме обложки

При сворачивании окна проигрывателя Windows Media Player 12.0 на панели задач остается кнопка с изображением значка программы. При наведении на нее курсора мыши появляется окно предварительного просмотра (рис. 6.22), где в миниатюре можно видеть окно программы — любой из описанных выше вариантов (в этом окне воспроизводится даже видео или фильм на DVD-диске). В окне присутствуют только кнопки воспроизведения/паузы и переходов вперед/назад. Воспроизведение аудио- и видеофайлов при свертывании/восстановлении и предварительном просмотре не нарушается.

Рис. 6.22. Вид проигрывателя Windows Media в окне предварительного просмотра на панели задач

DVD-диски

При воспроизведении диска DVD-видео на панели списка в окне библиотеки мультимедиа можно видеть структуру диска и переходить сразу к любому разделу, однако непосредственный *просмотр* диска возможен только в окне текущего списка воспроизведения. При движении мыши в нижней части этого окна появляется панель управления, где можно переключаться между главами, управлять громкостью

и вызвать меню параметров DVD. В меню параметров можно выбирать звуковую дорожку, субтитры, углы зрения камеры и обращаться к меню диска и разделов.

Проигрыватель Windows Media 12.0 позволяет просматривать DVD-диски, сохраненные на жестком диске. Для этого можно вручную переписать на локальный диск папку VIDEO_TS со всем содержимым или использовать для копирования DVD-диска специальную программу. Затем, запустив проигрыватель, нужно выполнить команду **Файл | Открыть** (File | Open) и выбрать в папке файл VIDEO_TS.IFO. После этого запустится фильм или появится меню DVD-диска.

> ***Примечание***
>
> Для просмотра DVD-диска можно открыть в проигрывателе любой файл *.VOB — обычно в этом случае воспроизведение диска начинается с начала (с заглавных титров или с меню), хотя это зависит от способа авторинга диска. *Отдельный* файл *.VOB в папке не всегда удается проиграть, поскольку программа автоматически пытается определить структуру диска и запустить его с начала. Поэтому при необходимости индивидуального просмотра VOB-файла его нужно предварительно скопировать в другое место, а только затем открывать. Если ситуация позволяет, то можно "прямо на месте" изменить расширение файла и поменять .VOB на .mpg — в этом случае файл без проблем запускается, а структура DVD-диска игнорируется.

Функция "Воспроизведение на" (Play To)

В системах Windows 7 имеется новая функция воспроизведения файлов мультимедиа поддерживаемых типов, которая может запускаться из окна Проводника или из окна проигрывателя Windows Media 12.0. Эта функция может применяться вместе с другими компьютерами, работающими под управлением Windows 7 (любых редакций), или с бытовыми мультимедийными устройствами (плеерами, телевизорами, медиасерверами и т. п.), поддерживающими стандарт *Digital Living Network Alliance* (DLNA) 1.5 (на сайте **http://www.dlna.org** можно найти перечень устройств, отвечающих этой спецификации).

Смысл функции состоит в том, что файл мультимедиа (аудио, видео, ТВ-запись, изображение), хранящийся на локальном компьютере, можно запустить на ***воспроизведение на*** другом компьютере или устройстве. Такая возможность дает несколько преимуществ. Во-первых, хотя практически все медиасерверы могут обращаться как к обычным общим папкам компьютеров, так и к их библиотекам мультимедиа, возможности компьютерной среды и проигрывателя Windows Media все же шире, чем у бытовых устройств, и пользователю с ними работать удобнее. К тому же не все устройства (цифровые плееры, телевизоры и т. д.) могут похвастаться "продвинутыми" функциями, имеющимися у медиасерверов. Во-вторых, иногда просто удобнее запустить выбранный файл или список воспроизведения там, где он хранится, а слушать или просматривать его совсем в другом месте. Так или иначе, описываемая функция — и любопытная, и полезная!

Запуск из окна проигрывателя Windows Media

Функция "Воспроизвести на" (Play To) работает ***только со списками воспроизведения*** и становится доступной, если в списке (временном или постоянном) имеется

хотя бы один трек (в принципе, любой файл мультимедиа — изображение, видеоклип или ТВ-запись). В этом случае при наличии в сети доступных цифровых плееров можно нажать кнопку **Воспроизвести на** (Play to) (рис. 6.23), и в списке появятся имена компьютеров или устройств, которые могут воспроизводить выбранные файлы.

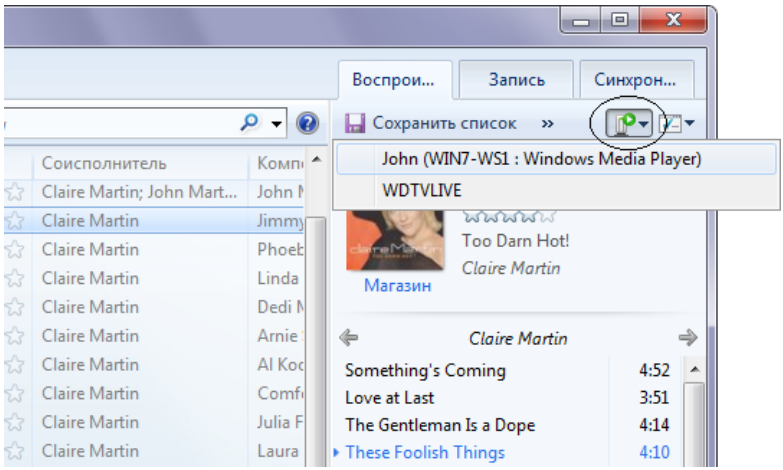

Рис. 6.23. Выбор удаленного компьютера
или устройства для воспроизведения текущего списка треков

Цифровые плееры обычно всегда готовы к работе, а в системах Windows 7 для того чтобы можно было воспроизводить файлы мультимедиа с другого компьютера, предварительно следует запустить проигрыватель Windows Media. (Как уже говорилось, в этом случае в папке **Сеть** (Network) рядом с его значком, именем библиотеки и самого компьютера появятся слова "Windows Media Player" — см. рис. 6.12).

После выбора устройства воспроизведения из окна проигрывателя Windows Media на экране появится новое окно (новое приложение), в котором будет видно имя выбранного устройства или компьютера, а также предложенный список воспроизведения, который начнет проигрываться на удаленном устройстве. На рис. 6.24 в качестве примера показано окно воспроизведения на бытовой медиаплеер *(слева)* и на обычный компьютер с Windows 7 *(справа)*. Каждое окно имеет свои кнопки управления и регулятор уровня громкости, такие же элементы управления имеет и "принимающая" сторона. Если такое окно открыто, то список воспроизведения можно формировать прямо в нем, очищая его и перетаскивая названия треков из окна проигрывателя в окно приложения.

Показанные на рис. 6.24 окна являются самостоятельными программами, которые в окне диспетчера задач называются *Приложение контроллера мультимедиа Windows Media* (Windows Media Player Digital Media Controller Application, процесс WMPDMC.exe). На панели задач это приложение представлено значком  .

Все запущенные программы, включая сам проигрыватель Windows Media, являются совершенно независимыми и могут воспроизводить совершенно разный контент со своими плейлистами: т. е., например, можно запустить музыку на удаленное уст-

ройство (или несколько устройств), а в проигрывателе просматривать фильм или же на одно устройство запустить набор фотографий, а на другое видеоклип.

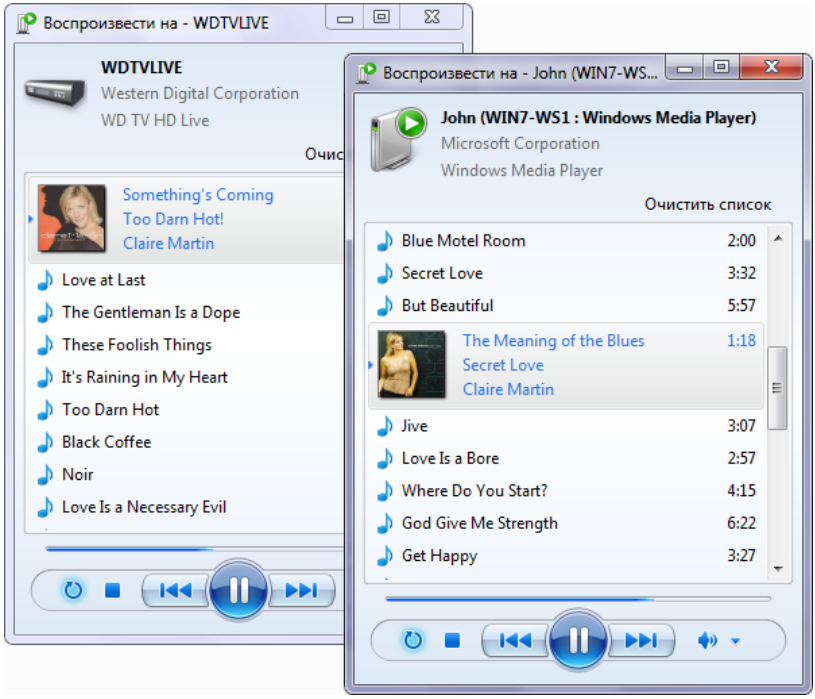

Рис. 6.24. Воспроизведение музыкальных треков на других устройствах и компьютерах локальной сети

Примечание

Аудио CD-диски нельзя сразу *воспроизводить на* удаленное устройство: сначала нужно скопировать треки на жесткий диск. Это связано с принципом работы сервиса воспроизведения файлов мультимедиа.

Запуск из окна Проводника

Если в сети имеются доступные цифровые плееры, то в окне Проводника (Windows Explorer) в контекстном меню файлов мультимедиа или папок, содержащих такие файлы, появляется дополнительная команда воспроизведения — **Воспроизвести на** (Play To) (рис. 6.25). Она запускает уже упомянутое выше Приложение контроллера мультимедиа Windows Media, которое управляет воспроизведением файлов на выбранном удаленном устройстве или компьютере. Все принципы использования данного средства были описаны в предыдущем разделе.

Названная команда имеет два положительных качества, создающих удобство в работе:

- она никак не связана с проигрывателем Windows Media;
- она позволяет воспроизводить файлы, расположенные в любых папках (кроме общих сетевых), не входящих в библиотеку мультимедиа. Как говорилось,

в проигрывателе Windows Media можно запустить *воспроизведение на* только тех файлов, которые включены в какой-нибудь список (пусть даже временный), и, следовательно, эти файлы должны быть включены в библиотеку. Иногда такое требование становится неудобным ограничением, которое легко снимается с помощью описываемой команды в окне Проводника.

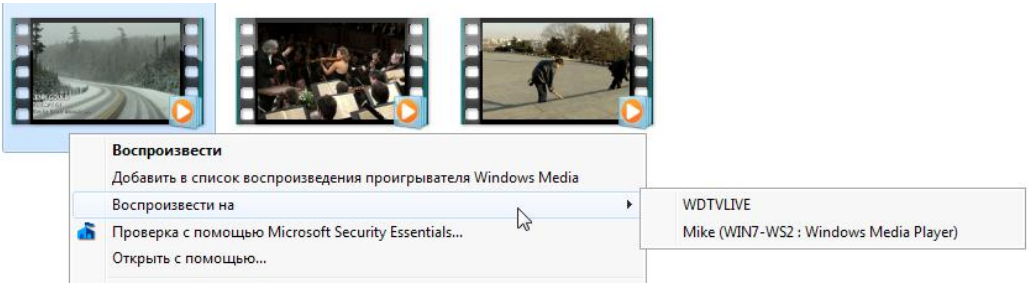

Рис. 6.25. Запуск воспроизведения выбранного файла на удаленном устройстве или компьютере

На стороне устройства воспроизведения выбранных файлов не имеет значения, каким способом (из числа двух описанных выше) была запущена операция. Доступные функции управления процессом проигрывания файла (с помощью команд прокрутки вперед и назад) зависят от конкретного устройства воспроизведения и формата файла. Команда паузы и продолжения всегда доступна, а переходы между треками на удаленных устройствах запрещены.

ГЛАВА 7

Доступ к рабочему столу и удаленный помощник

Уже в нескольких поколениях клиентских версий Windows имеется однопользовательская версия служб терминалов (Terminal Services), с помощью которой можно "войти" в систему с удаленного компьютера и работать на нем, как на локальной машине, — эта функция называется *Удаленный рабочий стол*[1] (Remote Desktop). Также имеется функция *Удаленный помощник* (Remote Assistance), позволяющая инициировать сеанс удаленного доступа со стороны пользователя, которому необходима помощь — в этом случае он разрешает доверенному лицу подключиться к своей системе.

Подключение к удаленному рабочему столу (Remote Desktop) возможно, если только компьютер, ***к*** которому выполняется обращение, работает под управлением редакций Windows 7 Professional, Windows 7 Enterprise, Windows 7 Ultimate. В других редакциях возможны только *исходящие* подключения, т. е. обращения к другим удаленным системам. По этой причине мы не будем подробно рассматривать данную функцию[2], а сосредоточим основное внимание на Удаленном помощнике (Remote Assistance), доступном во всех редакциях Windows 7.

Удаленный доступ к рабочему столу

Для включения режима удаленного доступа используется вкладка **Удаленный доступ** (Remote settings) окна **Свойства системы** (System Properties) (рис. 7.1). (Для быстрого доступа к этому окну введите команду `sysdm.cpl` или же нажмите клавиши <Win>+<Pause/Break>, а в открывшемся окне щелкните по ссылке **Настройка удаленного доступа** (Remote settings).) На рисунке показаны установки, заданные по умолчанию.

Чтобы пользователи могли с других компьютеров обратиться к локальной системе, установите флажок **Разрешить подключение от компьютеров с любой версией**

---

[1] По умолчанию она выключена, и пользователь может не беспокоиться об уязвимости своего компьютера с этой стороны.

[2] Те, кто работал с этой функцией, без труда разберутся в особенностях новой реализации. При необходимости можно обратиться за информацией к другим книгам — *см. список литературы*.

удаленного рабочего стола (Allow connections from computers running any version of Remote Desktop). Следующая опция (Allow connections only from computers running Remote Desktop with Network Level Authentication) разрешает подключение только от тех компьютеров, на которых используется новый метод сетевой аутентификации NLA, позволяющий повысить защищенность удаленного соединения. Этот метод используется в Windows Vista и Windows 7; при установке обновленной программы подключюючений его можно применять и на других версиях Windows.

Нажав кнопку **Выбрать пользователей** (Select Users), можно явно указать, каким пользователям разрешен удаленный доступ: эти пользователи будут включены в группу Пользователи удаленного рабочего стола (Remote Desktop Users). По умолчанию только администраторы имеют доступ к компьютеру. По умолчанию (без изменения политик безопасности) нельзя использовать для удаленного доступа ***учетные записи без пароля***.

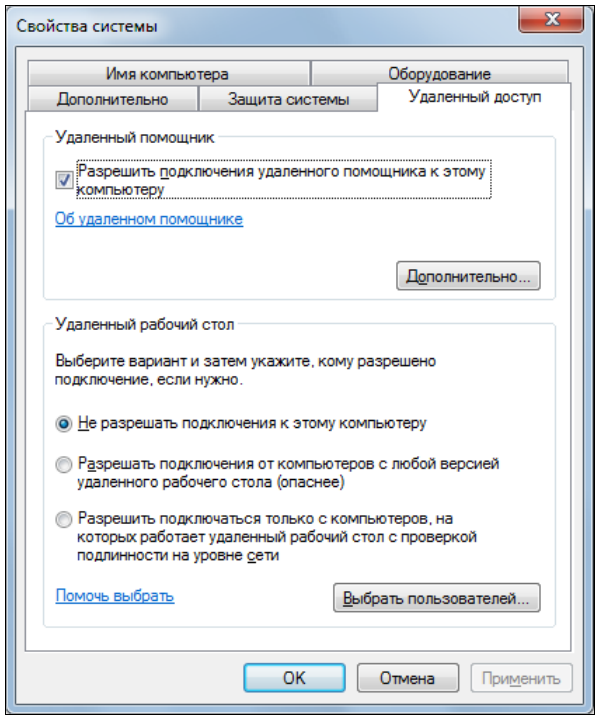

Рис. 7.1. Окно управления удаленным доступом и удаленным помощником

Подключение к удаленному компьютеру

Для инициализации сеанса удаленного доступа служит утилита *Подключение к удаленному рабочему столу* (Remote Desktop Connection; `mstsc.exe`) (она запускается из меню **Пуск | Все программы | Стандартные** (Start | All Programs | Accessories)). Чтобы инициировать соединение с удаленным компьютером, введите его имя или IP-адрес и нажмите кнопку **Подключить** (Connect) (рис. 7.2).

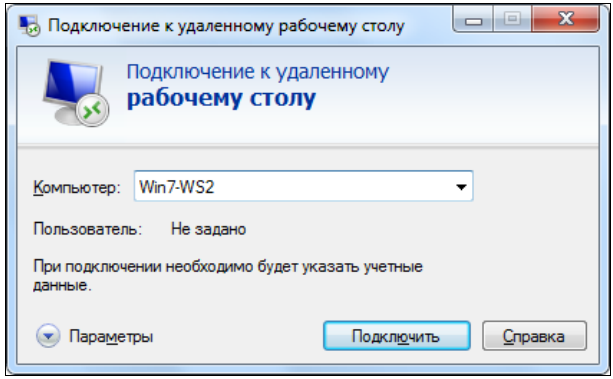

Рис. 7.2. Окно установки сеанса работы с удаленным компьютером

В следующем окне потребуется указать имя и пароль учетной записи, которая будет использоваться для регистрации на удаленном компьютере — введенные данные сразу проверяются. После выполнения нескольких проверок и при условии правильности всех параметров подключения появится окно регистрации в системе или же сразу рабочий стол удаленного компьютера (если учетные данные были введены заранее).

> ***Внимание!***
>
> При входе в локальную систему Windows 7 с использованием функции удаленного рабочего стола текущий пользователь "выталкивается" из системы, но при этом его текущий рабочий сеанс не закрывается. Если удаленный пользователь входит с именем уже зарегистрированного пользователя, то он получает рабочую среду — открытые окна, запущенные программы — этого пользователя, который в свою очередь может снова войти в систему и "вытолкнуть пришельца" (работа запущенных приложений при этом не нарушается). Только при использовании функции Удаленный помощник (Remote Assistance) возможна одновременная работа *двух* пользователей в одном сеансе.
>
> Если удаленный пользователь использует учетную запись, отличную от той, которая использована в данный момент для работы на компьютере, то после того как будут введены имя и пароль учетной записи, работающий пользователь получит предупреждение. В этом случае он может сразу прекратить работу (его программы и окна затрагиваться не будут), либо же он может отклонить запрос на подключение.

Подключение через Интернет

Для того чтобы к рабочему столу компьютера можно было подключиться через Интернет (т. е. с любого компьютера, имеющего подключение к Интернету), необходимо выполнение двух условий:

- наличие у компьютера или сетевого маршрутизатора фиксированного *внешнего (public) адреса*, который будет указываться при подключении (см. рис. 7.2);
- *свободный доступ к TCP-порту 3389*, открытому в брандмауэре[1] (см. рис. 4.3) и маршрутизаторе, и *маршруты* для входящих подключений по этому порту,

[1] В принципе, в брандмауэре Windows этот порт открывается автоматически при включении удаленного доступа, но только в частном профиле.

связывающие внешний адрес и адрес компьютера, к которому осуществляется доступ.

Если компьютер напрямую подключается к Интернету (например, через ADSL-модем), то достаточно проверить только брандмауэр. При использовании общего подключения к Интернету необходимо установить соответствующий флажок в окне дополнительных параметров (см. рис. 2.32). Наличие доступа к порту 3389 можно проверить с помощью специальных веб-сайтов (см. примечания в *разд. "Виртуальные частные сети (VPN)" главы 2* и *разд. "Начальный запуск" главы 8*).

Примечание

Требования касаются только *входящих* подключений, с *исходящими* никаких сложностей не возникает.

Само подключение через Интернет никаких особенностей не имеет и инициализируется стандартным образом (см. рис. 7.2), необходимо только правильно выбрать параметры отображения графических элементов, соответствующие скорости подключения.

Если по каким-то причинам доступ через порт 3389 невозможен, но есть другие свободные порты, можно изменить номер порта, по которому прослушиваются входящие подключения к рабочему столу. Для этого необходимо в реестре изменить значение параметра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber`. Новое значение необходимо будет при подключении указывать через двоеточие в строке адреса утилиты Подключение к удаленному рабочему столу (Remote Desktop Connection) (см. рис. 7.2). Например, формат адреса может быть таким: `194.130.55.133:3399`.

Удаленный помощник

Для использования *Удаленного помощника* (Remote Assistance) компьютеры должны работать под управлением операционных систем не ниже Windows XP (при этом следует учитывать некоторые проблемы совместимости из-за отличий в реализации этого средства в разных версиях Windows). Работа с применением всех имеющихся опций возможна только в однородной среде Windows 7.

Примечание

Для работы Удаленного помощника (Remote Assistance) статические маршруты не требуются, достаточно лишь того, чтобы в маршрутизаторе или на общем подключении к Интернету (см. рис. 2.32) был бы разблокирован TCP-порт 3389. Если компьютер пользователя, запрашивающего помощь, напрямую подключен к Интернету, то необходимо проверить, чтобы в брандмауэре стояло разрешение для публичного профиля (см. рис. 4.3), поскольку автоматически дается разрешение только для частного профиля.

Включить/выключить функцию Удаленный помощник (Remote Assistance) можно на вкладке **Удаленный доступ** (Remote settings) (см. рис. 7.1) (по умолчанию функ-

ция включена). Нажав на этой вкладке кнопку **Дополнительно** (Advanced), можно настроить параметры удаленного помощника (рис. 7.3).

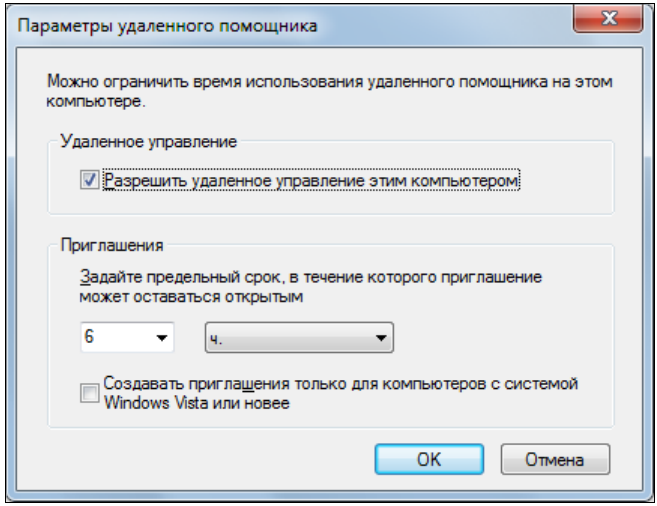

Рис. 7.3. Выбор параметров удаленного помощника

Обратите внимание на то, что по умолчанию разрешено и удаленное *управление* компьютером. Это не должно беспокоить, поскольку во время сеанса работы удаленного помощника для управления компьютером всегда требуется дополнительное, ***явное разрешение*** с запрашивающей помощь стороны.

Если не менять срок действия запроса (по умолчанию 6 часов), то в течение этого времени приглашение будет действительным, т. е. помощник сможет *запрашивать* доступ к локальному компьютеру. Всякий раз при этом потребуется давать ему отдельное разрешение на подключение.

Специальный флажок (см. рис. 7.3) позволяет ограничить круг систем, которые смогут принимать приглашения, и использовать более защищенные удаленные подключения *(см. пред. разд.)*.

Вызов функции удаленного помощника в Windows 7, а также способы передачи приглашения и связи с удаленным пользователем существенно отличаются от тех методов, которые реализованы в предыдущих версиях Windows. *Обратиться за помощью* (сделать запрос) или *ответить* удаленному пользователю можно двумя способами, которые описываются ниже. Сначала мы рассмотрим способы инициализации сеанса связи с запрашивающей и с отвечающей стороны, а затем опишем диалог, необходимый для установления подключения.

> ***Внимание!***
>
> Фактически сеанс связи должен начинаться сразу после отправки запроса помощи: в зависимости от способа инициализации запроса ответ может быть получен через секунды (в случае онлайнового контакта) или через минуты (при передаче запроса по электронной почте). В любом случае, сразу после запроса помощи начинается ожидание входящего подключения.

Инициализация запроса на оказание помощи

Во-первых, из меню **Пуск** (Start) можно открыть окно справки и, обратившись к дополнительным параметрам поддержки (ссылка в нижней части экрана), вызвать удаленного помощника. В этом случае открывается окно, показанное на рис. 7.4, и необходимо выбрать нужную опцию. (Предлагающий помощь человек будет выбирать здесь вторую опцию — *см. далее*.) В случае *запроса помощи* (первая опция) на следующем шаге требуется указать способ связи с удаленным пользователем (см. рис. 7.5).

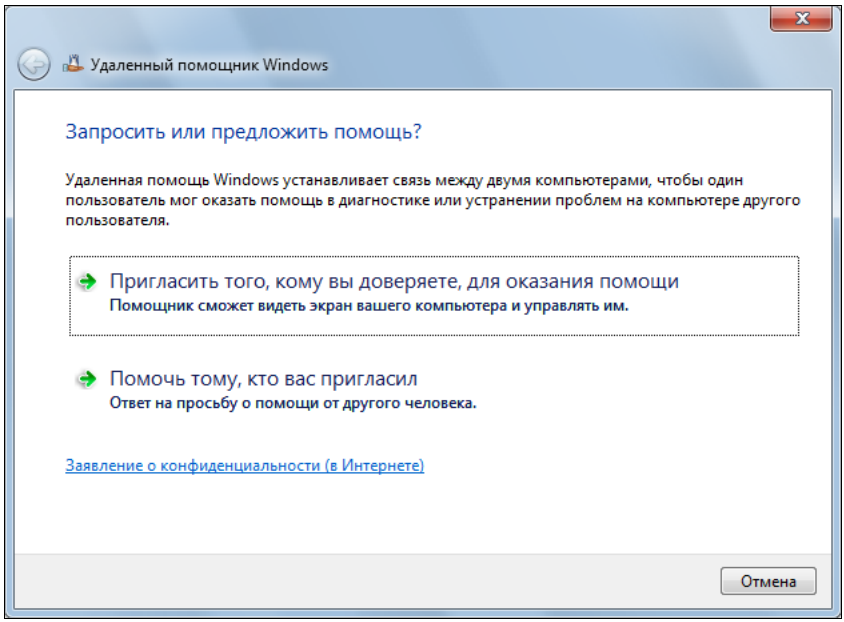

Рис. 7.4. Начальное окно запроса к удаленному помощнику

Приглашение на удаленную помощь (рис. 7.5) можно сохранить как *файл* на локальном диске (по умолчанию он имеет имя Приглашение.msrcIncident[1]), который нужно *немедленно*, любым возможным способом передать удаленному помощнику. При этом появляется окно Удаленного помощника (см. рис. 7.9), где будет задан пароль, который также необходимо сразу сообщить своему помощнику. При этом начинается ожидание входящего подключения. Это окно закрывать нельзя, поскольку в противном случае запрос будет нужно создавать заново.

Другой вариант — отослать приглашение *по электронной почте*, выбрав вторую опцию[2]. В этом случае автоматически формируется стандартное письмо запроса, а файл приглашения добавляется как вложение — достаточно лишь ввести адрес по-

[1] Если приглашение создавалось в русскоязычной версии Windows.

[2] Если в системе отсутствует используемый по умолчанию почтовый клиент, то эта опция будет заблокирована и недоступна.

мощника и отправить письма. Для пересылки используется любой настроенный почтовый клиент. При этом также появляется окно с паролем (см. рис. 7.9) и ожидается входящее подключение.

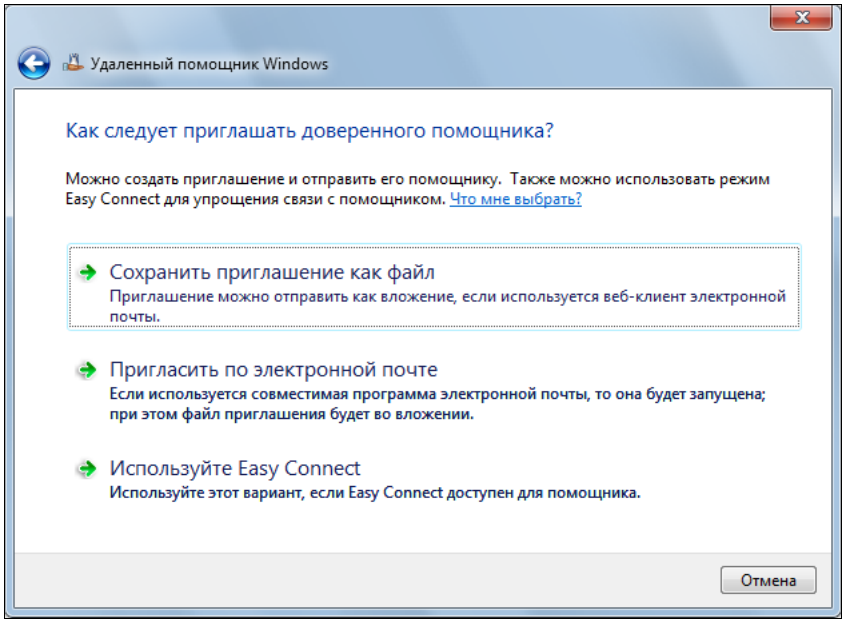

Рис. 7.5. Выбор способа передачи приглашения на оказание удаленной помощи или способа связи с помощником

Третий вариант — опция *Easy Connect* — доступна только пользователям Windows 7, если они одновременно находятся в сети. Этот вариант мы подробно рассмотрим позже.

Во-вторых, вызвать удаленного помощника можно с помощью имеющейся на панели управления задачи **Устранение неполадок** (Troubleshooting), в окне которой следует выбрать ссылку **Обратиться за помощью к другу** (Get help from a friend). В этом случае действия аналогичны описанным выше: можно либо сделать *запрос* для оказания помощи (верхняя кнопка), либо *предложить свою помощь* другому пользователю (ссылка ниже кнопок) (рис. 7.6). В том случае, если удаленный помощник уже отвечал на запрос и использовалось средство Easy Connect с сохранением контактов, то в данном окне отображается имя помощника — достаточно щелкнуть по нему и новый сеанс сразу будет инициирован. Если же выполняется обращение за помощью к другому пользователю, то после выбора соответствующей опции появляется окно, показанное на рис. 7.8, и выбирается способ передачи приглашения.

После отправки запроса удаленному помощнику и сообщения ему пароля сеанса можно ждать входящего подключения и продолжать работу.

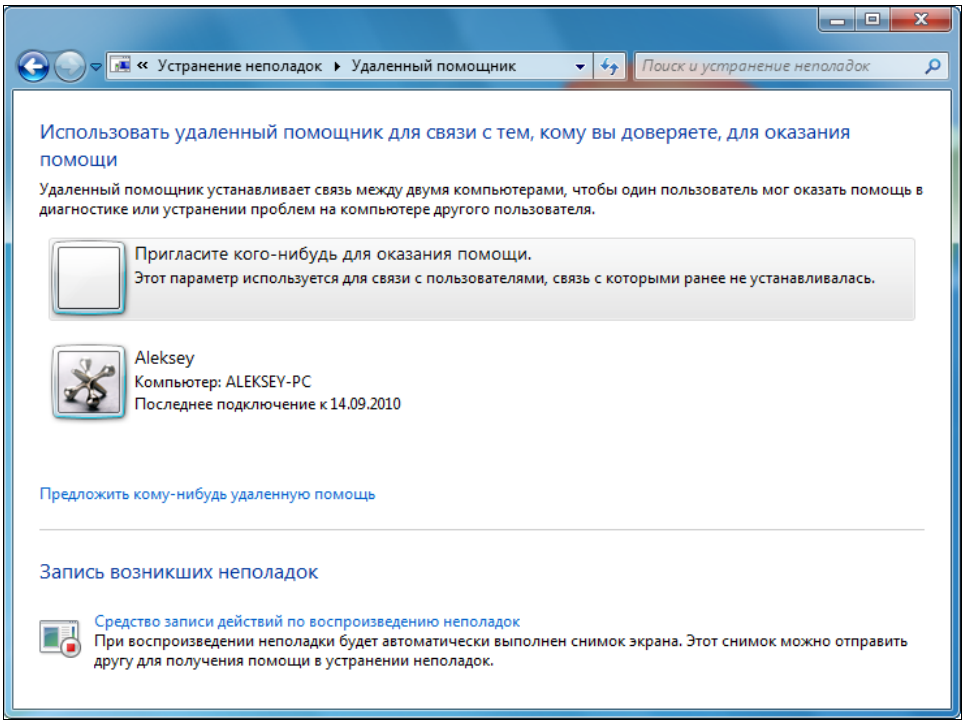

Рис. 7.6. Выбор режима использования удаленного помощника — *запрос* или *предложение* помощи

Средство записи действий по воспроизведению неполадок

Если уж выше зашла речь об удаленной помощи и упоминалась задача **Устранение неполадок** (Troubleshooting), то нельзя не упомянуть очень полезную функцию, которая вызывается по ссылке в нижней части окна вызова удаленного помощника (см. рис. 7.6).

Окно используемой программы (рис. 7.7) аскетично по набору операций, и все действия интуитивно понятны. Начав запись, пользователь должен выполнить операции, относящиеся к имеющейся проблеме, или какие-то действия, требующие разъяснений. Снимок каждого нового окна будет сохраняться, как и действия пользователя — нажатые кнопки, открытые меню, выполненные команды и т. п.

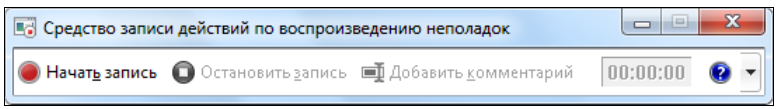

Рис. 7.7. Окно программы для записи действий пользователя, сохранения снимков экрана и комментариев

В любой момент можно приостановить запись и добавить комментарий. При этом на экране нужно выделить какую-то проблемную область и в специальном окне ввести свои замечания или вопросы. После этого запись возобновляется, и можно

продолжать выполнение операций. Такие шаги можно повторять многократно, после чего нужно, в конце концов, остановить запись и сохранить всю информацию в архиве с расширением .zip.

В этом архиве будет храниться файл с именем `Problem_yyyymmdd_hhmm.mht`, где `yyyy` — текущий год, `mm` — месяц, `dd` — день, `hh` — часы, `mm` — минуты. Данный файл представляет собой HTML-документ (веб-архив в одном файле), где зафиксированы снимки экрана компьютера, описаны все действия пользователя и вложены его комментарии[1].

Приведенная информация позволяет достаточно полно описать проблему (с иллюстрациями и замечаниями), причем для ее сбора и оформления требуется минимум времени. Файл можно отправить специалисту, знакомому или в службу поддержки, и такое детальное изложение ситуации в значительной мере поможет им быстрее разобраться в проблеме.

Предложение помощи другому пользователю

Если требуется *оказать помощь* удаленному пользователю, то нужно выбрать соответствующую опцию в окнах вызова удаленного помощника — см. рис. 7.4 либо рис. 7.6. При использовании любого из этих вариантов на следующем шаге появится одно и то же окно (рис. 7.8). Если же сеансы помощи ***с применением Easy Connect*** уже состоялись ранее и контакты сохранялись[2], то сначала появится дополнительное окно, в котором сразу можно выбрать имя пользователя, обращавшегося за помощью. В этом случае сразу инициализируется сеанс связи Easy Connect, и ничего больше вводить не нужно (пароль при этом не генерируется). Если же выбирается *новое* лицо, то всегда нужно выбрать способ подключения.

В первом случае (см. рис. 7.8) нужно открыть полученный каким-то способом файл приглашения, хранящийся на диске, и в окне удаленного помощника ввести пароль, переданный пользователем любым возможным образом, хоть по телефону (окно ввода пароля показано на рис. 7.11). Полученный файл можно открыть сразу, просто дважды щелкнув по нему в окне Проводника.

Во втором случае используется функция Easy Connect — если удаленный пользователь также работает в среде Windows 7 и выбрал эту опцию. И в этом случае также необходимо ввести полученный пароль.

Если приглашение на удаленную помощь было получено по электронной почте, то нужно открыть вложение (файл Invitation.msrcincident[3]) и запустить его на выполнение. После этого потребуется указать пароль и начать сеанс связи с удаленным пользователем.

При использовании любого способа ответа на запрос необходимо, чтобы в это время пользователь, запросивший помощь, находился на связи и ожидал входящего подключения (см. рис. 7.9).

---

[1] Одним словом — это нужно попробовать и увидеть самому.

[2] В других случаях контакты вообще не сохраняются!

[3] По электронной почте пересылается файл только с английским именем.

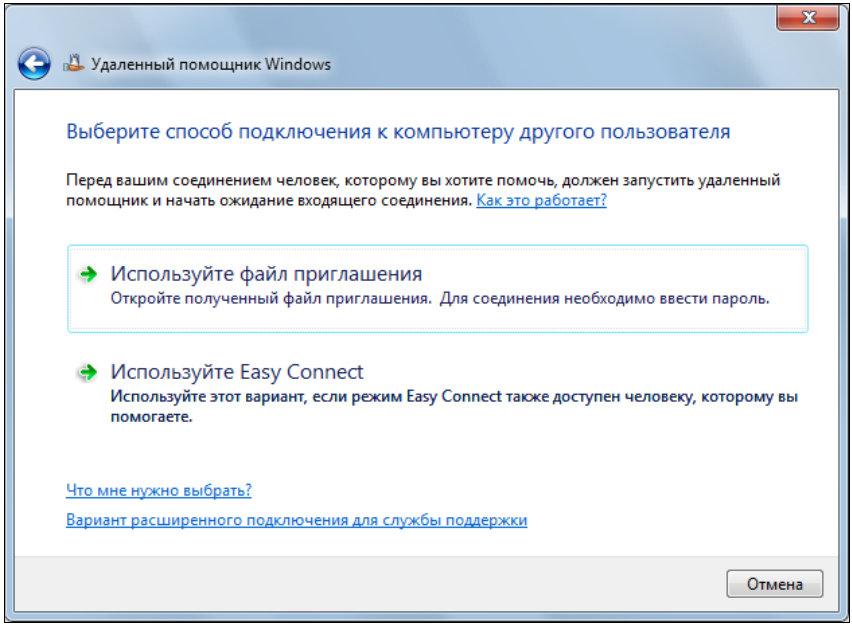

Рис. 7.8. Выбор способа связи с пользователем, запросившим удаленную помощь

Теперь рассмотрим процесс установления сеанса удаленной помощи до конца на примере использования функции Easy Connect.

Режим Easy Connect

При выборе опции Easy Connect (см. рис. 7.5) у пользователя, запросившего помощь, открывается окно Удаленного помощника (рис. 7.9), где виден пароль, который необходимо как-то передать удаленному эксперту. Кнопка **Параметры** (Settings) позволяет открыть окно (рис. 7.10), в котором по умолчанию задаются самые "щадящие" параметры использования сетевого подключения. Если скорость подключения велика, то качество отображения экрана пользователя можно повысить, передвинув ползунок выше. Как можно видеть, по умолчанию сохраняется журнал сеанса и контакты, которые можно впоследствии использовать для быстрого установления подключения (см. рис. 7.6).

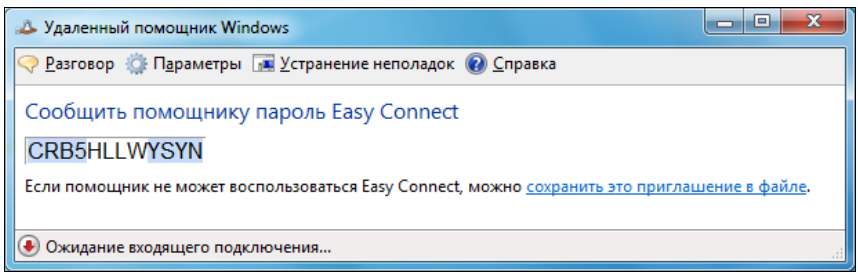

Рис. 7.9. Окно Удаленного помощника после создания запроса помощи и перехода в режим ожидания — этот пароль необходимо передать своему помощнику

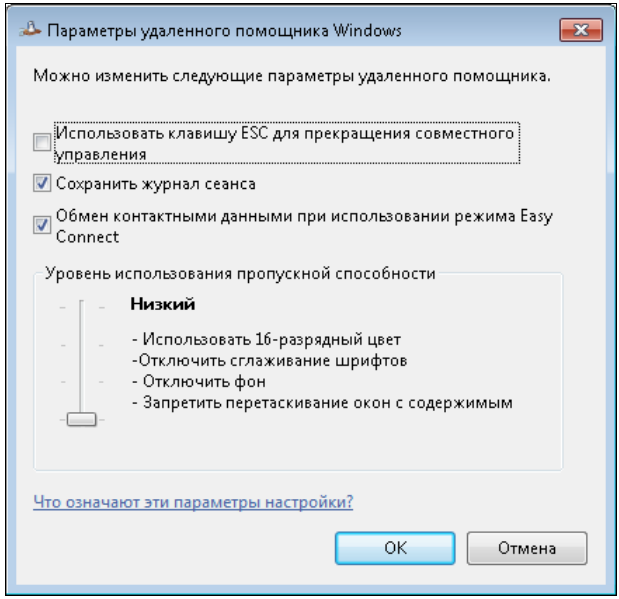

Рис. 7.10. Окно параметров удаленного помощника, определяющих качество отображения картинки и сохранение информации для последующих сеансов

Кнопка **Устранение неполадок** (Troubleshoot) (см. рис. 7.9) запускает мастер обнаружения неисправностей, которым может помочь в диагностике ошибок (например, при отсутствии сетевого подключения или открытого порта TCP).

После того как удаленный помощник — эксперт — выберет опцию оказания помощи (см. рис. 7.4 или рис. 7.6), у него на экране также появится окно Удаленного помощника, где в дополнительном окне (рис. 7.11) нужно ввести полученный ранее пароль, переданный пользователем, запросившим помощь.

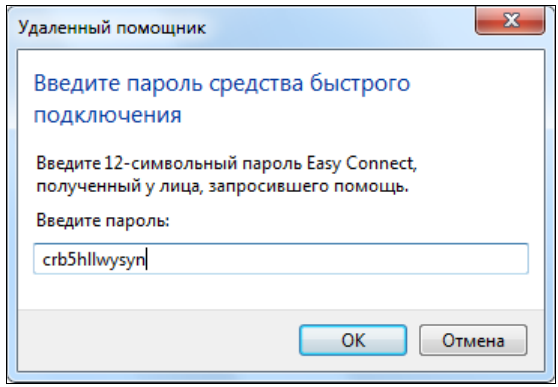

Рис. 7.11. Окно ввода пароля для установления подключения к компьютеру пользователя, обратившегося за помощью

После того как эксперт ввел пароль, начинается сеанс связи с удаленным компьютером, и у пользователя, запросившего помощь, на экране появится предупрежде-

ние о том, что к его компьютеру выполняется подключение (рис. 7.12). Теперь пользователь должен явно разрешить доступ к своему компьютеру. В противном случае сеанс связи завершается, и всю процедуру выполнения запроса нужно начинать заново.

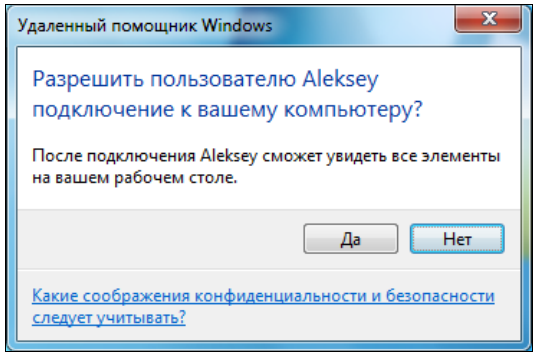

Рис. 7.12. Запрос на подключение к компьютеру со стороны удаленного помощника

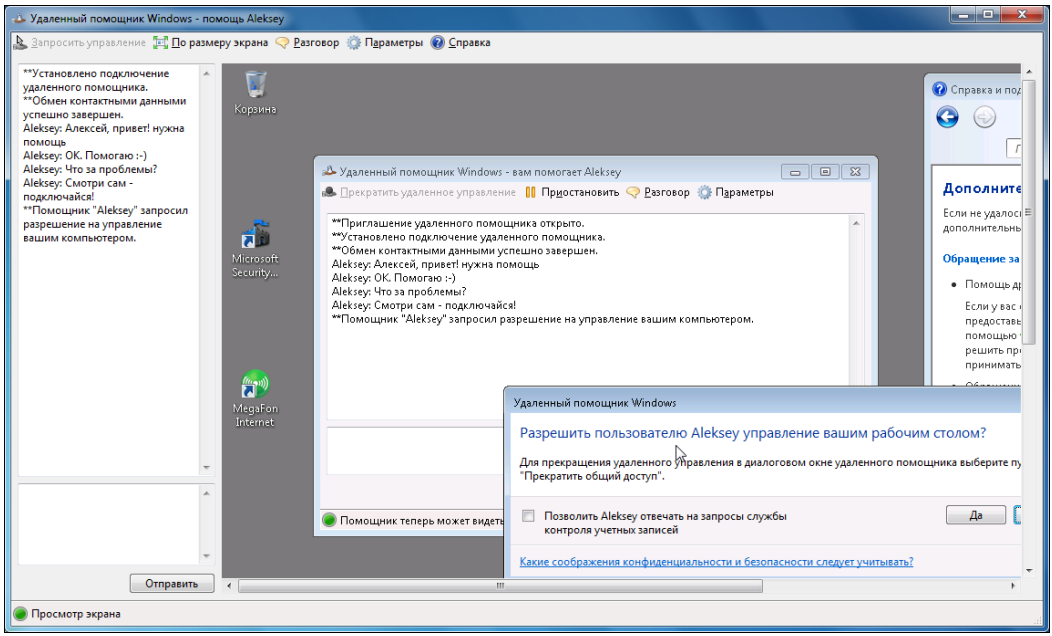

Рис. 7.13. Окно, в котором помощник видит рабочий стол на компьютере пользователя, обратившегося за помощью, и запрос управления этим компьютером

Если пользователь подтверждает доступ к своему компьютеру, то удаленный помощник начинает видеть рабочий стол своего "клиента" и вести с ним диалог (рис. 7.13). В заголовке окна удаленного помощника всегда указано имя: пользователь видит, *кто* ему помогает, эксперт всегда видит, *кому* он помогает. При установлении сеанса связи на компьютере пользователя всегда включается упрощенная цветовая схема (т. е. все эффекты Aero отключаются). Панель диалога включается

с помощью кнопки **Разговор** (Chat). В левом нижнем окне виден режим работы — в данном случае эксперт может лишь пассивно наблюдать за происходящим на компьютере пользователя и вести с ним диалог. Как можно видеть, эксперт *запросил управление* компьютером и на экране пользователя появился запрос на подтверждение операции (и его тоже эксперт видит у себя).

Если пользователь разрешает удаленному помощнику управлять своим компьютером, то они начинают совместную работу на компьютере (тут важно не торопиться и не забывать, что теперь мышью управляют два человека!) (рис. 7.14). На рисунке на панели диалога можно видеть, что помощник запросил и получил управление компьютером. Теперь эксперт может начать анализировать ситуацию или выполнять необходимые операции (в нашем примере он запустил оснастку **Управление компьютером** (Computer Management) и начал анализ журнала сообщений). Изменившийся режим работы указывается в левом нижнем углу программы.

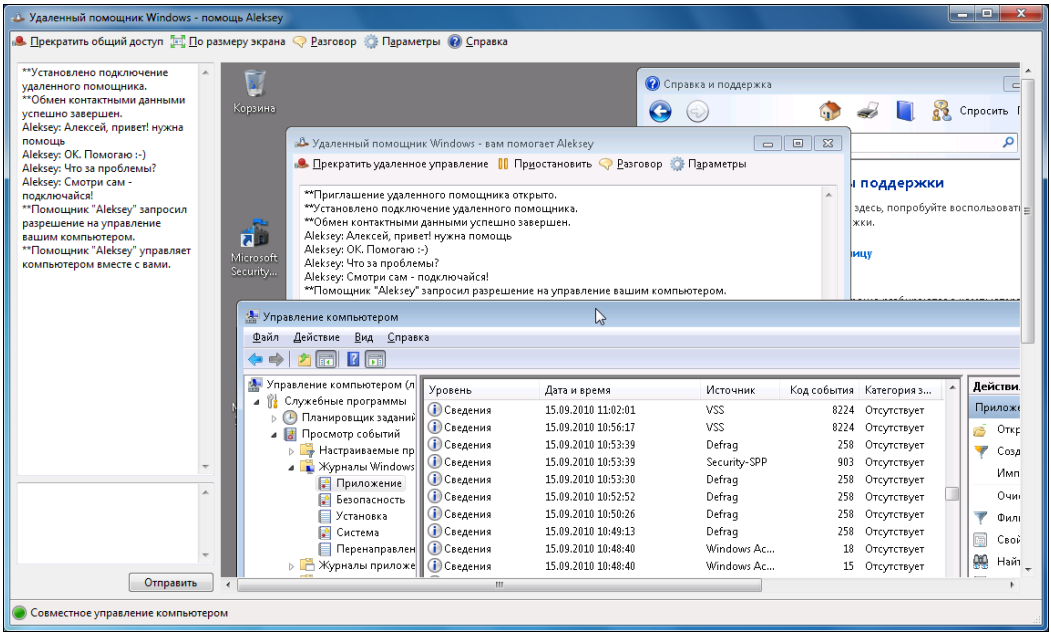

Рис. 7.14. Совместная работа на компьютере — пользователь и помощник могут одновременно выполнять операции и вести диалог

Удаленный помощник может видеть рабочий стол пользователя сжатым (по размеру своего окна программы) — чтобы изображение *полностью* умещалось на экране, или "один-к-одному", в реальном разрешении (чтобы не было искажений из-за масштабирования). Для переключения режима отображения служит кнопка **По размеру экрана/Истинный размер** (Fit to screen/Actual size).

Пользователь может в любой момент на время приостановить доступ к своему рабочему столу, нажав соответствующую кнопку (в этом случае помощник будет видеть черный экран), или вообще завершить сеанс работы, закрыв у себя окно Удаленного помощника. Аналогично может закончить работу и эксперт.

Любая сторона может инициализировать новый сеанс работы Удаленного помощника с использованием Easy Connect (новое подключение) и сохраненных контактов — все операции будут полностью соответствовать тем, что описаны выше.

Использование программы Windows Live Messenger

Помимо описанных выше способов передачи запроса на удаленную помощь, существует и третий — использование программы Windows Live Messenger (для связи с системами Windows XP SP3 применяется стандартная версия программы Windows Messenger). В этом случае пользователи, одновременно находящиеся в сети, могут инициализировать запрос и ответить на него, установив соединение с рабочим столом удаленного компьютера.

Чтобы запросить удаленную помощь у кого-то из контактов, находящихся в сети, можно поступить по-разному. Если в главном окне программы Windows Live Messenger (рис. 7.15) нажать клавишу <Alt>, то появится меню программы, где следует выбрать команду **Действия | Запросить удаленную помощь**. Появится дополнительное окно, в котором можно выбрать контакт и нажать кнопку **ОК**.

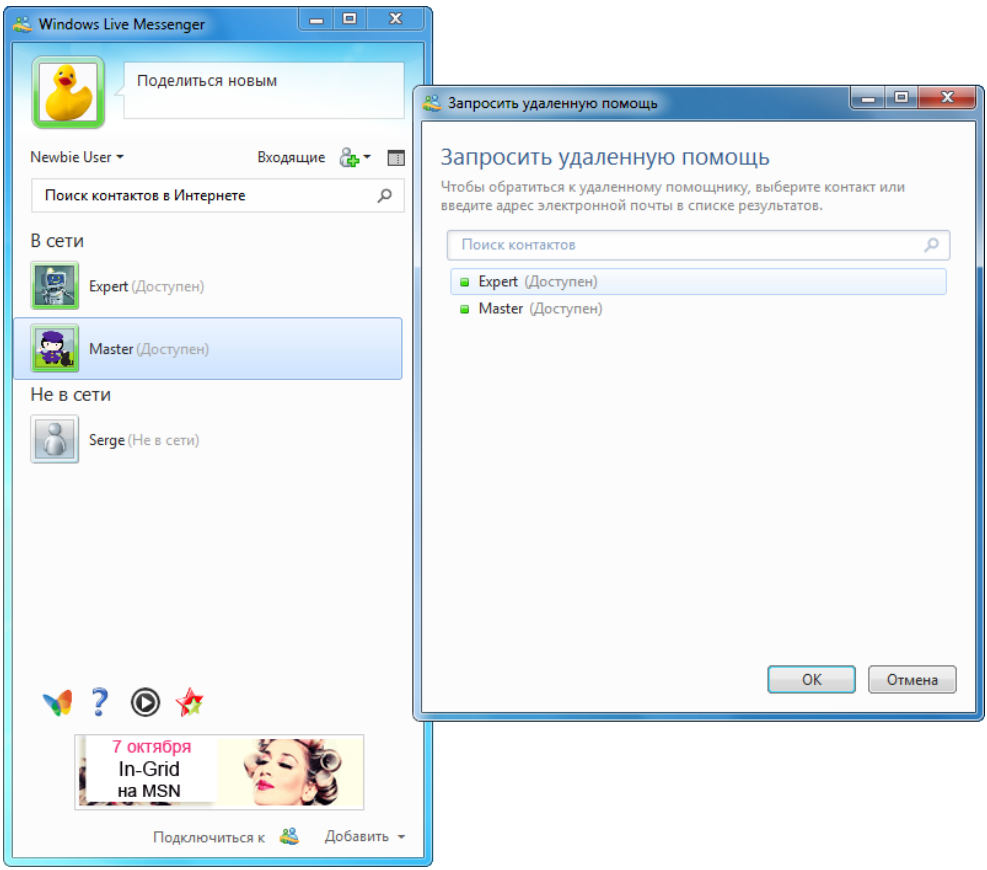

Рис. 7.15. Запрос удаленной помощи в главном окне программы Windows Live Messenger

Другой вариант — сначала выбрать контакт, открыть для него окно диалога, в нижней части окна щелкнуть по кнопке **Действие** и выбрать в меню опцию **Запросить удаленную помощь**.

При любой последовательности действий у запрошенного контакта (эксперта) активизируется окно диалога (рис. 7.16), в котором будет предложение запустить программу Удаленный помощник. Если эксперт принимает приглашение, то у пользователя появляется окно Удаленного помощника с паролем (см. рис. 7.9). Аналогичное окно появляется и у эксперта — только с окном, где нужно *ввести* пароль (см. рис. 7.11). Этот пароль можно, к примеру, скопировать (copy-paste) в окно чата, откуда эксперт, в свою очередь, может его скопировать в окно запроса.

После того как эксперт ввел полученный пароль, инициализируется подключение от него к удаленному компьютеру, и пользователь видит предупреждение о подключении к своему рабочему столу (см. рис. 7.12). Дальнейшие действия уже понятны, и были подробно описаны в предыдущем разделе.

Достоинством запроса удаленной помощи с помощью программы Windows Live Messenger является удобство и оперативность выполнения всех начальных действий, а кроме того — эта программа позволяет выполнять голосовые и видеозвонки, поэтому в процессе совместной работы можно свободно общаться, что существенно повышает ее эффективность.

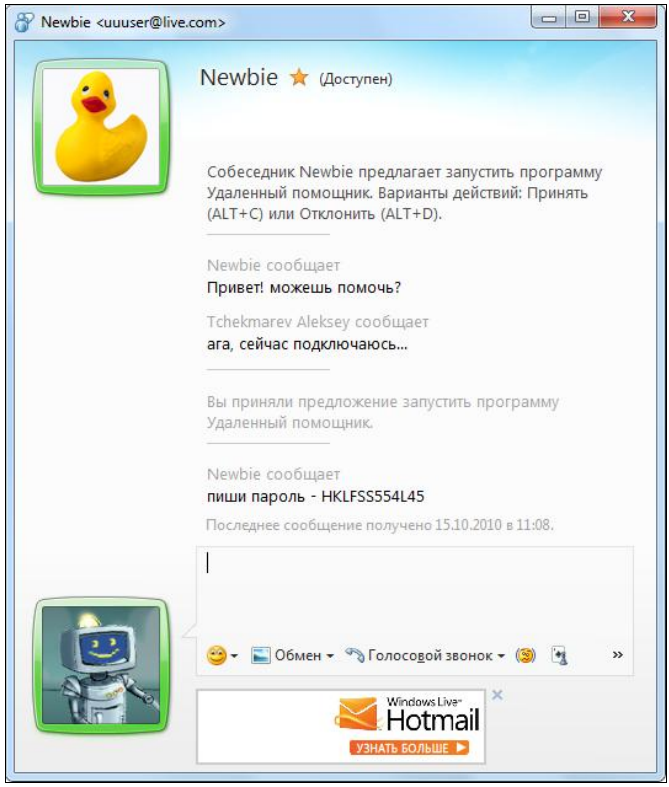

Рис. 7.16. Запрос удаленной помощи в окне диалога с выбранным контактом

ГЛАВА 8

Установка FTP- и веб-серверов

Системы Windows 7 позволяют создать на компьютере персональный веб-сервер и размещать на нем любую информацию, интересующую других пользователей локальной сети или Интернета. Также можно установить FTP-сервер для надежного скачивания файлов с использованием отказоустойчивого протокола FTP. Единственное, что требуется для доступности этих серверов из Интернета, это наличие фиксированного публичного (внешнего, public) IP-адреса, "видимого" в Интернете. Такая услуга иногда входит в стандартные тарифные планы интернет-провайдеров, чаще ее можно заказать за дополнительную оплату (ежемесячную и за подключение).

В данной главе рассмотрены все вопросы, возникающие у пользователя при установке и настройке веб- и FTP-сайтов в домашней сети.

Информационные службы Интернета (IIS версии 7.5)

В состав систем Windows 7 (начиная с редакции Домашней расширенной (Home Premium)) входят интернет-службы *Internet Information Services (IIS) 7.5*[1] (Version 7.5.7600.16385). К их числу относятся следующие компоненты:

- веб-сервер — *Служба веб-публикаций* (World Wide Web Publishing Service; сервис W3SVC);
- FTP-сервер — *Служба FTP (Майкрософт)* (Microsoft FTP Service; сервис ftpsvc);
- служба, поддерживающая администрирование метабазы IIS — *Служба IIS Admin* (IIS Admin Service; сервис IISADMIN);
- компоненты разработки приложений (ASP и ASP.NET, CGI, расширения ISAPI и т. д.);

[1] Эти службы имеются и в серверных версиях Windows, поэтому их возможности на порядок превышают потребности домашнего пользователя. Нам достаточно рассмотреть лишь способы развертывания сайтов и задачи начального конфигурирования.

- средства администрирования серверов;
- различные вспомогательные службы и средства обеспечения безопасности.

Все службы IIS 7.5 имеют единый стандартный интерфейс администрирования и общие методы управления.

Рассмотрим, как установить службы IIS на домашнем компьютере и подготовить к работе веб-сервер и FTP-сервер. Этой базовой информации будет достаточно для запуска серверов, их наполнения статическим содержимым и обеспечения доступа к ним со стороны клиентов локальной сети или Интернета (при наличии внешнего IP-адреса).

В простейшем случае запуск серверов, входящих в состав служб IIS 7.5, сводится к следующим простым этапам:

1. Установка служб IIS 7.5.
2. Разрешение доступа к сайтам через брандмауэр Windows (индивидуально для веб-сайтов и для FTP-сайтов), настройка маршрутизатора или общего подключения при доступе через Интернет.
3. Создание и конфигурирование FTP-сайта, если он требуется.
4. Наполнение серверов содержимым[1]. Этот этап, по сути, бесконечен, поскольку информационное наполнение обычно изменяется в течение всего срока службы серверов.

Установка компонентов служб IIS 7.5

Для установки служб IIS используется традиционная задача **Программы и компоненты** (Programs and Features), имеющаяся на панели управления. В ее окне нужно выбрать ссылку **Включение или отключение компонентов Windows** (Turn Windows features on or off) и в окне компонентов выбрать нужные элементы (рис. 8.1). Здесь имеются некоторые неочевидные моменты, требующие комментариев.

По умолчанию службы IIS не установлены и бокс (квадратик, где помещается отметка о выбранных элементах списка) около их имени не отмечен ☐. Если щелкнуть по нему мышью, то будут выбраны все базовые компоненты, необходимые для работы веб-сервера (см. рис. 8.1) и бокс станет синим ■ (такой значок означает, что некоторые компоненты выбраны, но ***не все***). Этого (даже с избытком) достаточно для установки и запуска веб-сервера, поэтому можно нажать кнопку OK — и начнется установка нужных средств. При этом будут установлены и автоматически запущены Служба веб-публикаций (World Wide Web Publishing Service), средства администрирования и вспомогательные модули.

---

[1] Мы будем говорить только о *статических* веб-страницах, т. к. вопросы использования скриптов, веб-приложений и других механизмов формирования динамического содержимого далеко выходят за рамки книги.

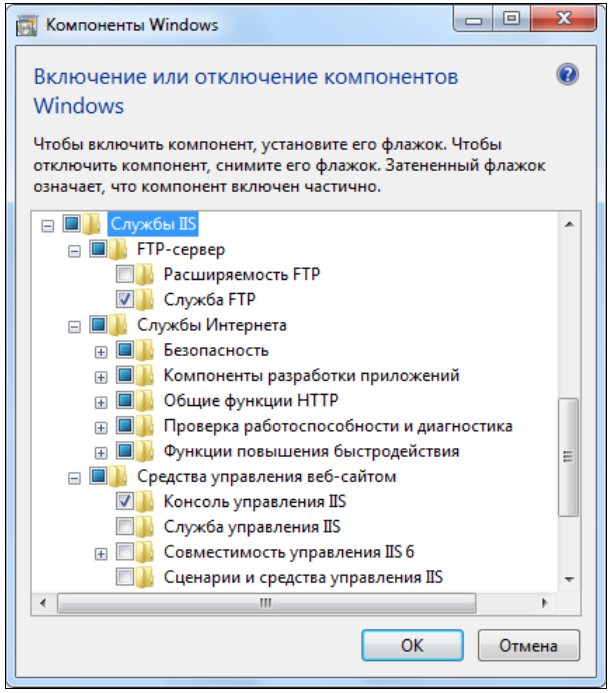

Рис. 8.1. Выбор устанавливаемых компонентов служб IIS

Если щелкнуть по значку ⊞, то список раскрывается и можно выбирать отдельные компоненты, входящие в данную группу. Для установки FTP-сервера именно таким способом следует раскрыть соответствующую группу и отметить в ней компонент **Служба FTP** (FTP Service) (см. рис. 8.1). В этом случае будет установлена и запущена Служба FTP (Майкрософт)[1] (Microsoft FTP Service).

Только в том случае, когда ***все*** входящие в группу компоненты будут выбраны, рядом с ее именем появится отметка ☑ (это требуется довольно редко).

Мы останавливаемся на этих нюансах только по трем причинам: 1) в списке компонентов отсутствует как таковой веб-сервер; 2) непонятно, что нужно выбрать "по минимуму", чтобы установить только веб-сервер и необходимые дополнительные средства (устанавливать все элементы без исключения вряд ли целесообразно!); 3) компонент FTP-сервера по умолчанию не выбирается и его следует отметить отдельно (как показано на рис. 8.1).

Если для работы каких-то средств требуются дополнительные обязательные компоненты, то они отмечаются автоматически при выборе базового элемента (например, при установке ASP.NET подключается ее множество компонентов).

Для обеспечения работы служб IIS на компьютерах с Windows 7 имеется встроенная группа IIS_IUSRS.

[1] Однако, хотя служба FTP и запускается сразу, для работы FTP-сервера требуется дополнительная настройка (в отличие от веб-сервера, который доступен сразу после установки).

Начальный запуск

После установки служб IIS в корне дискового тома, где находятся системные файлы (*%SystemDrive%*), создается каталог \inetpub, содержащий корневые папки для веб-сервера и FTP-сервера — \wwwroot (содержит страницу приветствия) и \ftproot (эта папка пустая) соответственно.

Веб-сервер (создаваемый по умолчанию веб-сайт — см. рис. 8.3) может работать сразу после установки служб IIS 7.5 и отвечать на обращения клиентов. Если в окне веб-браузера на любом компьютере локальной сети в поле адреса ввести строку `http://<имяСервераIIS>` (или просто указать IP-адрес; на локальном компьютере также можно использовать строку `http://localhost`[1]), то можно увидеть страницу-заставку веб-сервера, имеющуюся в каталоге \inetpub\wwwroot (рис. 8.2[2]). Эта операция может служить проверкой правильности установки служб и доступности сайта для клиентов сети. Поэтому практически сразу же после установки можно заниматься информационным наполнением веб-сервера.

Рис. 8.2. Домашняя страница веб-сервера, заданная по умолчанию при его установке

Внимание!

Чтобы установленные серверы были видны *в локальной сети*, настройки служб IIS должны быть скоординированы с параметрами встроенного брандмауэра Windows

[1] На локальном компьютере службы доступны, даже если не включены соответствующие разрешения в брандмауэре Windows; но для работы по сети настройка брандмауэра ***обязательна.***

[2] Для наглядности мы несколько отредактировали заголовок окна и добавили в него имя компьютера.

(Windows Firewall). Для выбранного профиля (сетевого размещения) необходимо разрешить все используемые службы и порты и проверить их доступность. В самом простом случае в окне разрешенных программ (см. рис. 4.3) необходимо установить флажки **FTP-сервер** (FTP Server) и **Службы Интернета (HTTP)** (World Wide Web Services (HTTP)) для используемых сетевых размещений.

Если в сети используется маршрутизатор (программный или аппаратный), то на нем необходимо настроить доступ к компьютеру, где расположены службы IIS, и разрешить соответствующие TCP-порты (80 для веб-сервера и 21 для FTP-сервера). (Фактически это создание статических маршрутов для связи шлюза и конкретного компьютера.) Данная операция аналогична выбору конкретных приложений и служб, к которым обращаются пользователи Интернета, при разрешении общего доступа к интернет-подключению (см. рис. 2.32). Описание конкретных операций нужно искать в инструкции производителя устройства. (Например, для маршрутизаторов D-Link для переназначения входящего внешнего трафика на конкретный внутренний компьютер используется понятие *Virtual Servers* (Виртуальные серверы) в разделе параметров NAT.)

При обращении к серверам из Интернета в браузере вводится строка адреса `http://<PublicIP>` или `ftp://<PublicIP>`, где *PublicIP* — внешний адрес, полученный от провайдера. Если заказать услугу DNS-хостинга и зарегистрировать домен[1], то к серверам можно будет обращаться и по доменному имени.

Если нужно немедленно опубликовать информацию на веб-сервере, не тратя времени на создание структуры каталогов веб-узла, можно просто скопировать публикуемые файлы в основной каталог по умолчанию. Пользователи сети смогут обращаться к этим файлам, вводя URL-адрес `http://<имяСервераIIS>/<имяФайла>`. Также можно создать HTML-файл с именем Default.htm и поместить его в домашний (корневой) каталог (см. рис. 8.12). В этом случае сервер по-прежнему будет "откликаться" на адрес `http://<имяСервераIIS>`, но теперь вместо страницы приветствия клиенты увидят предложенный HTML-документ.

Для FTP-сервера начальные шаги по наполнению него содержимым также очень простые: публикуемые файлы и папки достаточно скопировать в папку \ftproot. При обращении к серверу пользователь увидит их имена в окне браузера или своего FTP-клиента. Однако для ***FTP-сервера обязательно требуется начальная настройка*** *(см. далее)*.

Средства администрирования служб IIS и компонентов разработки приложений

Средства управления службами IIS 7.5 объединены с подсистемой конфигурирования компонентов приложений (ASP.NET) — это хорошо видно по интерфейсу диспетчера служб IIS, где в окне оснастки все группы параметров сгруппированы в так называемые *области* (areas) (см. рис. 8.3). Такой "задачно-ориентированный" подход позволяет быстро находить нужные группы параметров для каждой практической ситуации.

---

[1] В Интернете можно найти и бесплатные службы хостинга (при знании английского языка — поскольку требуется процедура регистрации, а русскоязычные сервисы отсутствуют). Для этого достаточно выполнить поиск по словам "DNS hosting" или "бесплатные DNS серверы".

После установки служб IIS оснастка **Диспетчер служб IIS** (Internet Information Services (IIS) Manager; `InetMgr.exe`) автоматически добавляется к оснастке **Управление компьютером** (Computer Management) и включается в меню **Администрирование** (Administrative Tools). При первом запуске диспетчера служб IIS можно видеть имя сервера[1], список задач, сгруппированных по областям, и основные команды управления серверов на панели **Действия** (Actions) (рис. 8.3). Например, с этой панели легко запустить или остановить веб-сайт, просмотреть список работающих на нем приложений или список его виртуальных каталогов. (Специальная область **ASP.NET** появляется только в случае установки соответствующего компонента, если таковой требуется для работы веб-приложений.)

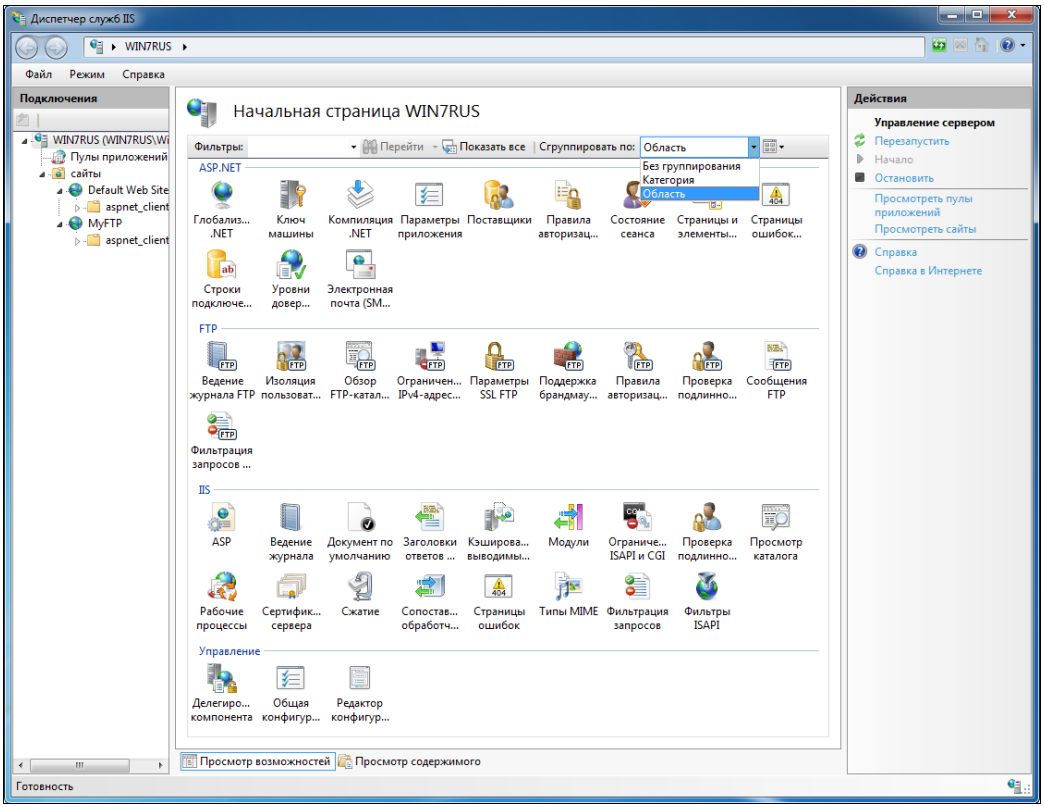

Рис. 8.3. Начальная страница оснастки управления службами IIS 7.5

Примечание

В предыдущих версиях служб IIS для управления FTP-сервером использовалась оснастка *Диспетчер служб IIS 6.0* (Internet Information Services (IIS) 6.0 Manager). Теперь она не требуется и устанавливается только в том случае, когда требуется управление удаленными серверами более ранних версий.

[1] Изначально создается только веб-сайт с именем *Default Web Site*. Сайты FTP необходимо настраивать вручную!

Как можно видеть на рис. 8.3, интерфейс диспетчера служб IIS весьма насыщенный, но, тем не менее, легко выбирать нужные параметры, относящиеся к определенной задаче (которая определяется *областью* управления (опция **Область** (Area)) или *категорией* (опция **Категория** (Category)). Некоторые задачи и действия, показанные в данном окне, будут описаны ниже.

Кнопка **Режимы** (Views) (отмечена кружком на рис. 8.4) позволяет переключать вид представления групп параметров (по умолчанию выбран режим **Значки** (Icons) (см. рис. 8.3), в данном примере — **Сведения** (Details)). Все относящиеся к выбранному объекту задачи отображаются справа на панели **Действия** (Actions).

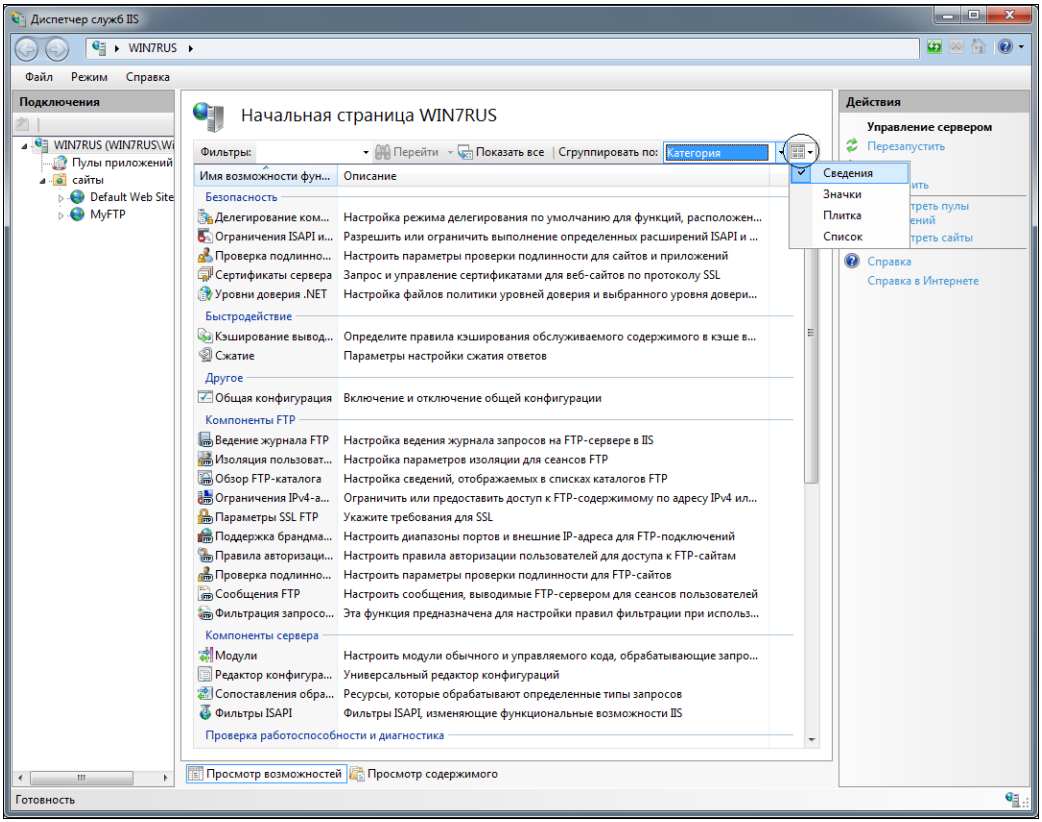

Рис. 8.4. Основные категории задач для компьютера с установленными службами IIS 7.5

Обратите внимание на кнопки **Просмотр возможностей** (Features View) и **Просмотр содержимого** (Content View) в нижней части окна оснастки — с их помощью можно быстро переключаться между режимами выбора задач и просмотра пулов приложений и сайтов (WWW и FTP).

Примечание

По умолчанию все операции доступа к веб- и FTP-серверам регистрируются в журнале, который располагается в папке C:\inetpub\logs\LogFiles.

Настройка FTP-сервера

Рассмотрим подробно базовый вариант создания FTP-сайта[1] с анонимным доступом (т. е. без указания имени и пароля). Создание сайта начинается с выполнения команды **Добавить FTP-сайт** (Add FTP Site) в контекстном меню корневого узла в окне диспетчера служб IIS. Другой путь — выбрать узел **Сайты** (Sites) и выполнить аналогичную команду на панели **Действия** (Actions).

На первом шаге определите имя сайта и местоположение физической папки, которая будет являться корневым каталогом сайта (рис. 8.5). Можно выбрать стандартную папку, создаваемую при установке служб IIS, или же любую другую. (Корневой каталог можно в дальнейшем менять.)

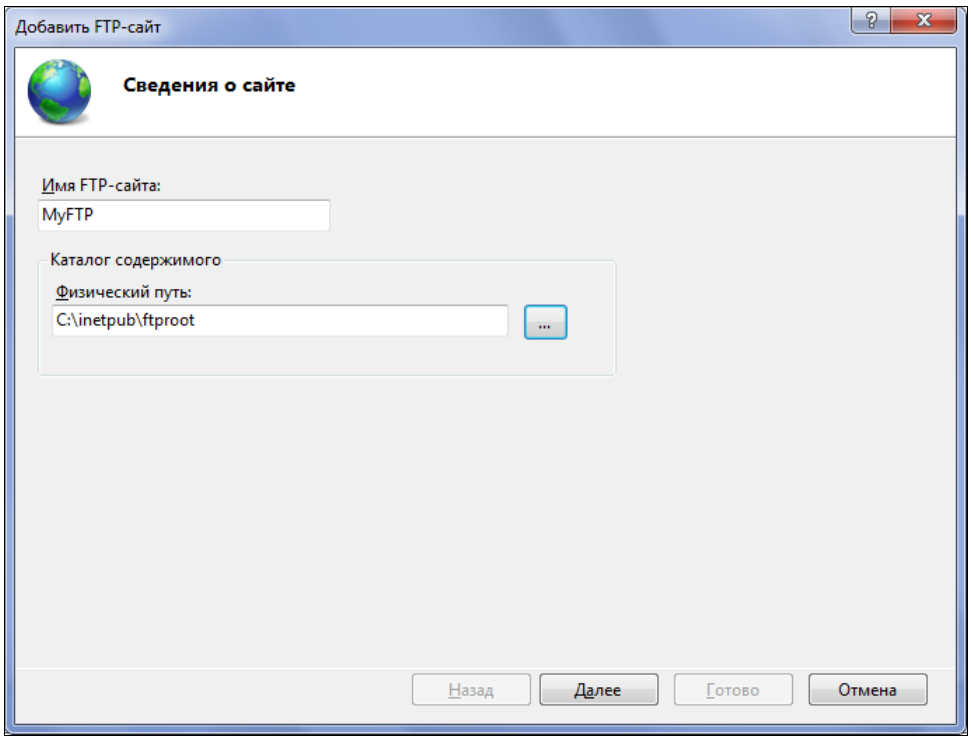

Рис. 8.5. Выбор имени FTP-сайта и местоположения корневого каталога

На следующем этапе (рис. 8.6) укажите IP-адрес сайта (в случае одного интерфейса можно оставить опцию, предлагаемую по умолчанию), номер порта (стандартный 21 или собственный), режим запуска и использование протокола безопасности SSL. В простейшем случае от него следует отказаться (опция **Без SSL** (No SSL)).

[1] Термин "сайт" используется потому, что на компьютере один веб- или FTP-сервер может поддерживать работу нескольких сайтов, каждый из которых имеет индивидуальные настройки. Понятие "сервер" применяется по отношение к веб-службе в целом.

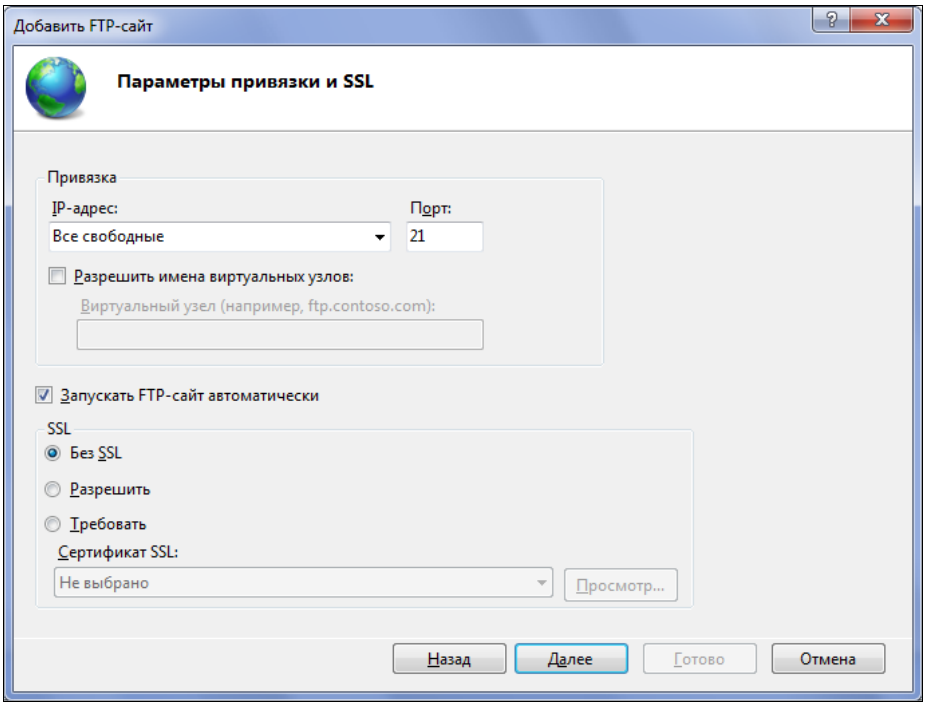

Рис. 8.6. Выбор основных сетевых параметров FTP-сайта

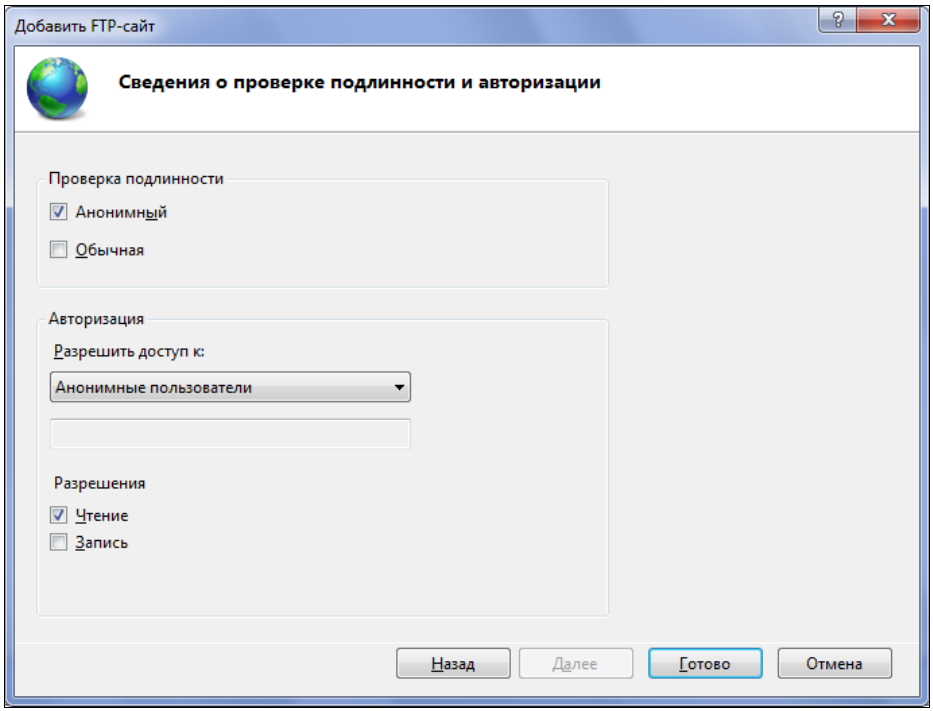

Рис. 8.7. Определение способа доступа к содержимому FTP-сайта и прав пользователей

На следующей странице программы-мастера для простейшего случая доступа — без проверки подлинности, т. е. без указания личных данных — установите флажок **Анонимный** (Anonymous) (рис. 8.7). В этом случае и авторизацию нужно разрешить для анонимных пользователей. (В качестве альтернативного варианта возможно указывать всех пользователей, конкретные группы или отдельных пользователей. Если анонимный доступ запрещен, то доступ к FTP-сайту получат только те клиенты, которые укажут при подключении имя локальной учетной записи и ее пароль.) Флажки разрешений чтения и записи определяют максимальные права клиентов на данном сайте (т. е. без учета разрешений, заданных на уровне файловой системы).

После нажатия кнопки **Готово** (Finish) новый FTP-сайт будет создан и станет доступным для клиентов сети (при соответствующих разрешениях в брандмауэре!), и его параметрами можно будет управлять в окне диспетчера служб IIS (рис. 8.8). На панели **Действия** (Actions) располагаются базовые команды настройки и управления сайтом: привязки, настройки, просмотр виртуальных каталогов, запуск и останов. Важную роль играет ссылка **Редактировать разрешения** (Edit Permissions), позволяющая в окне свойств базового каталога сайта на вкладке **Безопасность** (Security) настроить права доступа на уровне файловой системы NTFS.

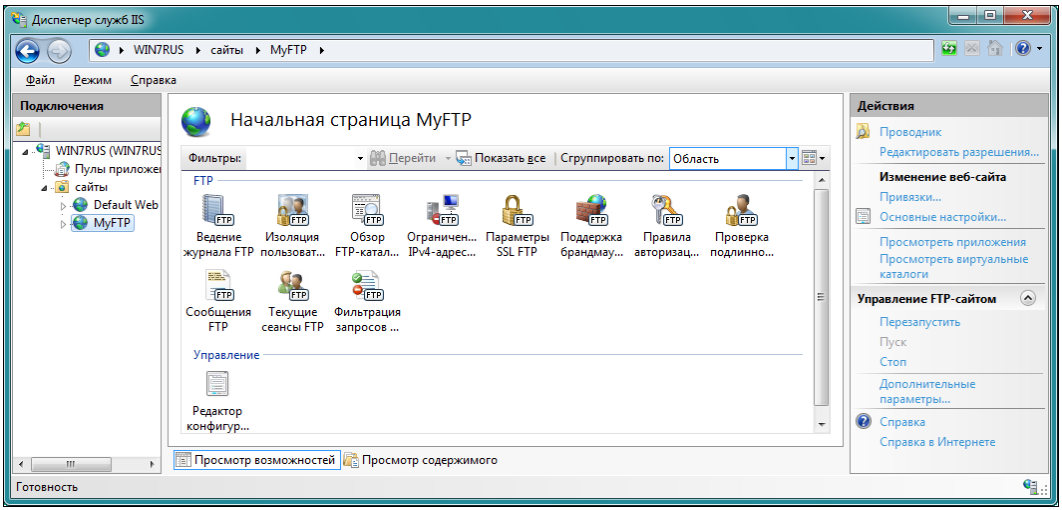

Рис. 8.8. Задачи управления выбранным сайтом

Назначение прав доступа к сайту

Для определения режимов авторизации на сайте и групп пользователей, которым разрешено обращение к сайту, в основном окне оснастки (см. рис. 8.8) имеются две важнейших задачи: **Правила авторизации** (FTP Authorization Rules) и **Проверка подлинности** (FTP Authentication). Они позволяют изменять настройки, заданные при создании сайта, а также вводить дополнительные режимы. Эти две задачи вместе с настройками разрешений NTFS и определяют основные возможности доступа

к сайту. Другие задачи требуются для обеспечения повышенной защиты сайта и его мониторинга во время работы.

Способы проверки подлинности и правила авторизации должны быть согласованы между собой. Если FTP-сайт создавался для анонимного доступа, а затем потребовалось включить доступ с указанием учетной записи и пароля, то соответствующие изменения должны быть выполнены с помощью соответствующих задач (рис. 8.9). Для этого требуются следующие операции (показанные на рисунке):

1. Включить *обычную проверку подлинности*[1] (для этого используется соответствующая команда на панели **Действия** (Actions)).
2. В правилах авторизации выбрать нужные учетные записи, которым разрешается доступ к сайту (рис. 8.10): "Все пользователи" (All Users), конкретные локальные или доменные группы, учетные записи отдельных пользователей. Правил авторизации может быть несколько, что позволяет для каждой учетной записи индивидуально задавать права на чтение и на запись.

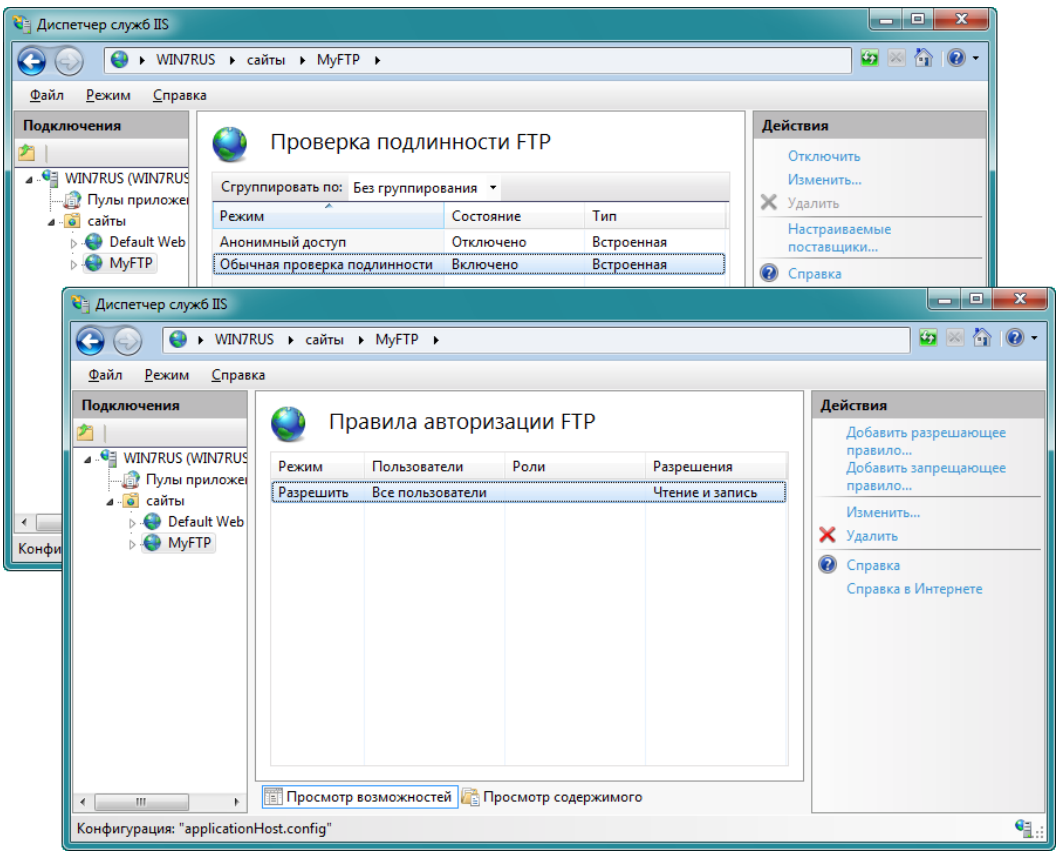

Рис. 8.9. Выбор способа проверки подлинности и правил авторизации на FTP-сайте

[1] Обратите внимание на рис. 8.9, что анонимный доступ отключен!

Если обычная проверка подлинности включена, то при обращении к сайту пользователи увидят окно запроса (рис. 8.11), где следует указать имя и пароль. Если при этом разрешен и анонимный вход, то достаточно будет установить флажок **Анонимный вход** (Lon on anonymously) и нажать кнопку **Вход** (Log on).

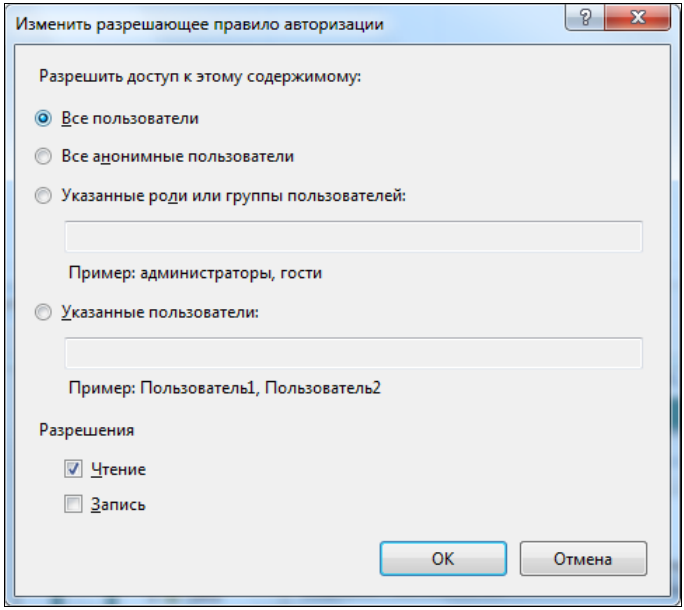

Рис. 8.10. Выбор учетных записей, которым разрешается доступ к FTP-сайту, и разрешений доступа

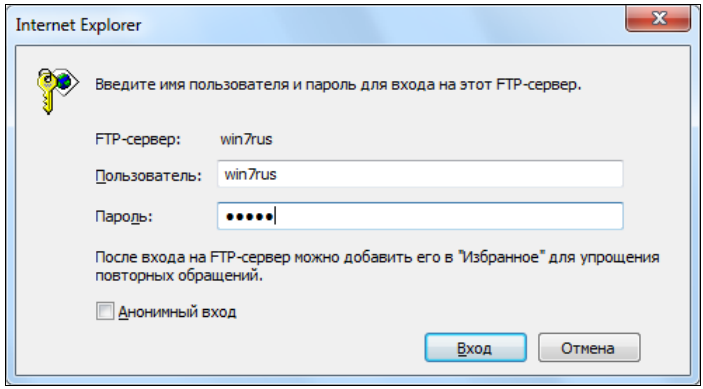

Рис. 8.11. Ввод учетных данных при обращении к FTP-сайту с проверкой подлинности

Выбранные для доступа имена учетных записей можно применять для установки разрешений на уровне файловой системы, например, для детализации прав пользователей, обращающихся к FTP-сайту. Операции записи или чтения, если они разрешены (см. рис. 8.10), распространяются на *весь* сайт, и только на уровне файловой системы NTFS можно определить персональные права доступа к конкретным файлам и каталогам.

Свойства веб- и FTP-сайтов

Выбирая задачи в нужной области или категории (см. рис. 8.3), пользователь настраивает параметры соответствующих компонентов, в том числе изменяет и свойства сайтов. (В предыдущих версиях служб IIS настройка параметров конкретного сайта выполнялась в *одном* окне свойств с множеством вкладок.) С каждой задачей связана какая-то группа параметров, объединенных по смыслу или назначению.

Например, когда при обращении к веб-сайту пользователь указывает только имя сайта (или имя компьютера), то должна открываться определенная страница — обычно это домашняя страница сайта. Если в главном окне диспетчера служб IIS в области **IIS** дважды щелкнуть по значку **Документ по умолчанию** (Default Document) (см. рис. 8.3), то появится панель, на которой задан список имен файлов, которые будут использоваться в этом случае (рис. 8.12). Имя, находящееся выше других, имеет более высокий приоритет, т. е. при наличии файла с таким именем будет отображаться только его содержимое. По умолчанию в папке \wwwroot имеется только файл iisstart.htm — он и выполняется при первом обращении к сайту, если нет других страниц. Можно удалить ненужные файлы, оставив в нем только одно имя.

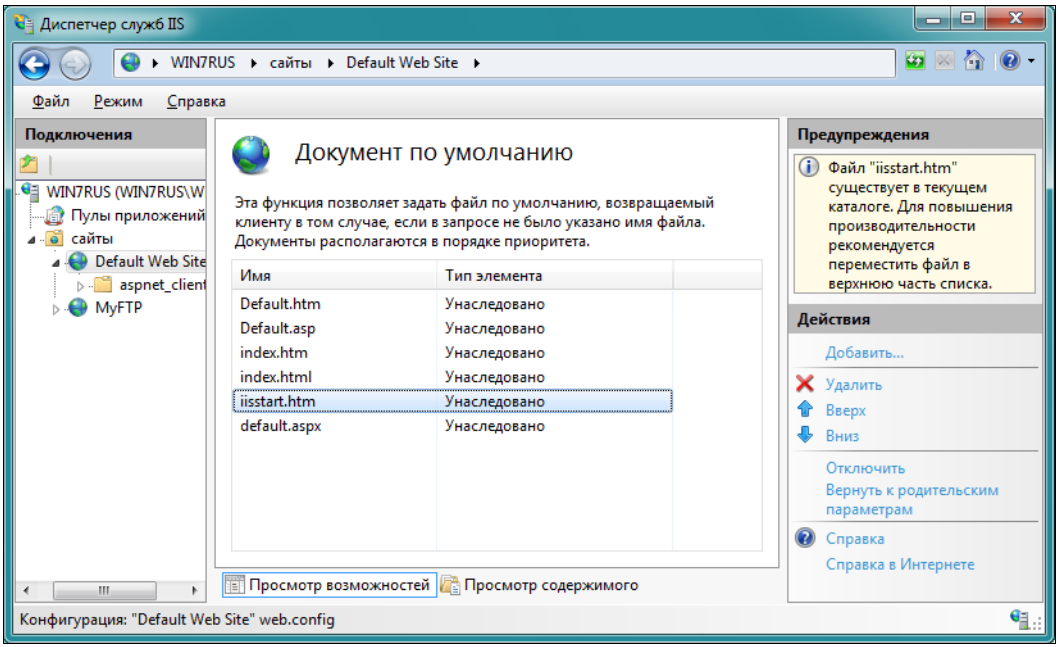

Рис. 8.12. На этой панели задаются файлы, открываемые при обращении к веб-сайту

Для FTP-сервера стандартная папка \ftproot сразу после установки служб IIS 7.5 пустая — поэтому при обращении по адресу `ftp://`*`<имяСервераIIS>`* или `ftp://localhost` пользователь увидит пустое окно браузера или пустой список в окне FTP-клиента.

Все параметры работы FTP-сайта определяются в области **FTP** (см. рис. 8.3 и рис. 8.8). Некоторые настройки расположены на панели **Действия** (Actions). Ссылка **Основные настройки** (Basic Settings) позволяет открыть окно, где задается домашний (корневой) каталог сайта (рис. 8.13), указанный при его создании. При выборе ссылки **Привязки** (Bindings) открывается окно, где перечислены прото-

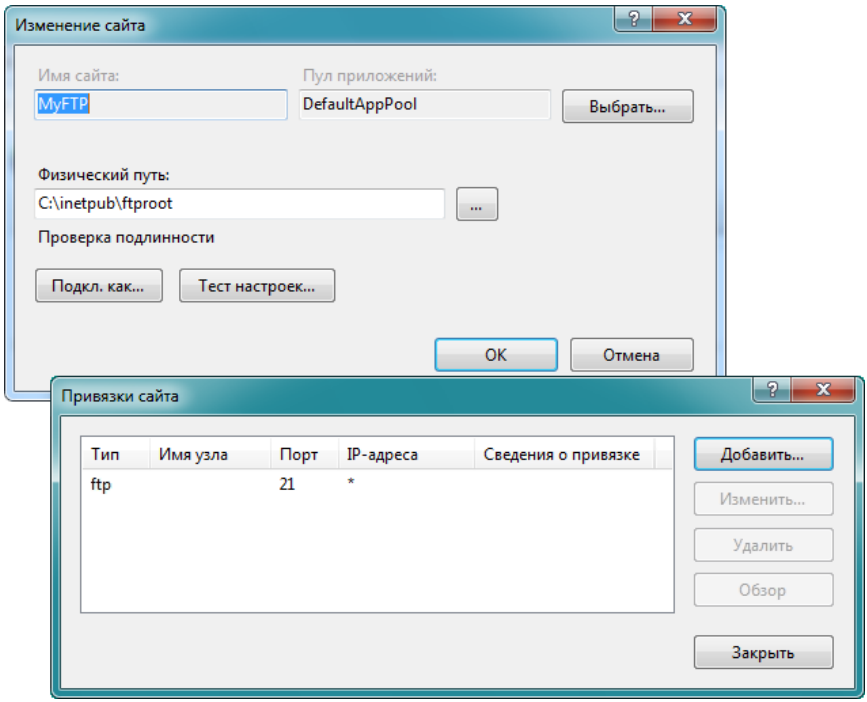

Рис. 8.13. Основные параметры FTP-сервера — домашний каталог и привязка к адресам и портам

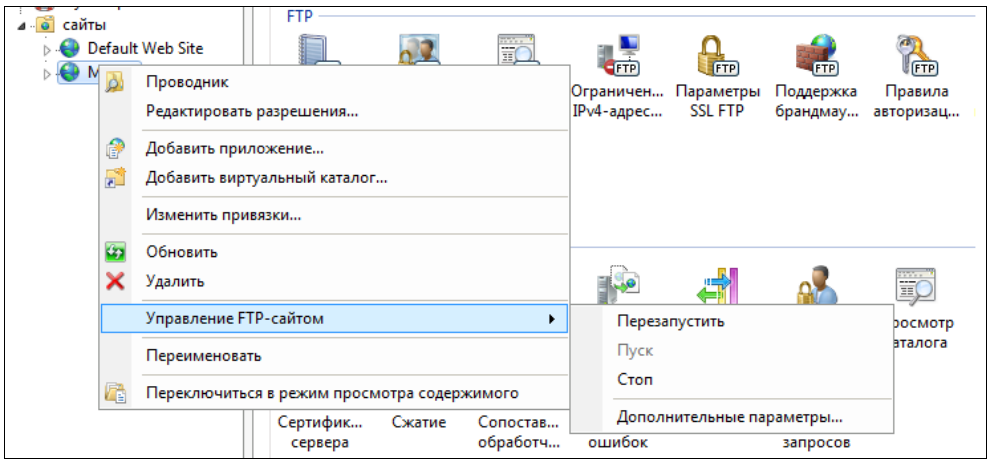

Рис. 8.14. Команды управления сайтами и опции изменения их параметров

колы, адреса и порты, по которым можно подключаться к сайту. Если для сайта указывается несколько привязок, то на значке глобуса рядом с именем сайта в окне диспетчера служб IIS (см. рис. 8.8) появляется вопросительный знак.

Перечисленных выше настроек вполне достаточно для создания простых веб- и FTP-узлов; дополнительные параметры можно искать и конфигурировать по мере усложнения задач. Многие команды по управлению и настройке сайтов имеются в контекстом меню выбранного веб- или FTP-сайта (рис. 8.14). Отсюда легко переключиться в режим просмотра содержимого сайта, остановить или перезапустить сервис, редактировать разрешения NTFS, создавать *виртуальные каталоги* (псевдонимы) и т. д.

ПРИЛОЖЕНИЕ 1

Быстрые клавиши Windows 7

В системах Windows существуют различные сочетания клавиш (keyboard shortcuts, или *быстрые клавиши* — hot keys), позволяющие эффективно управлять окнами, задачами, системными функциями и т. п. Немало сочетаний впервые появились в Windows 7, поскольку в этой системе реализовано много функций, отсутствующих ранее (в особенности это относится к управлению окнами и задачами). Некоторые клавиши просто необходимо знать для эффективной работы в системе, поэтому в данном приложении приведены важнейшие из них.

В табл. П1.1 и П1.2 перечислены основные клавиши, используемые для управления *новыми* функциями Windows 7. В табл. П1.3 включены клавиши, специфические для Windows 7 и общие для многих версий Windows (для большей полноты картины), а в табл. П1.4 указаны некоторые клавиши для управления проигрывателем Windows Media Player 12.0[1].

> ***ВНИМАНИЕ!***
>
> Быстрые клавиши можно назначить для запуска любого приложения, установленного в системе[2]. Для этого выберите значок приложения, откройте окно свойств и перейдите на вкладку **Ярлык** (Shortcut). Щелкните по полю **Быстрый вызов** (Shortcut key) и нажмите клавишу <Ctrl> — автоматически предлагается комбинация <Crtl>+<Alt>+ +<символ>. Третьим символом может быть любая клавиша (символьная, цифровая, функциональная...). Нажмите недостающую клавишу (иногда можно ограничиться и двумя клавишами, например <Ctrl>+<F7>). Нужно лишь быть уверенным в том, что выбранная комбинация не используется еще где-то.

---

[1] На самом деле этих клавиш почти в два раза больше, но редкие сочетания при необходимости несложно найти в Интернете.

[2] Например, при частом обращении к окну сетевых подключений крайне удобно назначить быстрые клавиши команде `ncpa.cpl`, открывающей данное окно. Аналогичную операцию можно проделать и для отдельных сетевых соединений.

Таблица П1.1. *Управление окнами*

Клавиши	Действие
<Win>+<Space>	Временно сделать все окна прозрачными и показать рабочий стол со значками и гаджетами (вызов функции Aero Peek)
<Win>+<Home>	Свернуть все окна, кроме активного (вызов функции Aero Shake)
<Win>+<Стрелка вверх>	Развернуть окно (Maximize)
<Win>+<Стрелка вниз>	Свернуть в окно (Restore/Minimize)
<Win>+<Shift>+ +<Стрелка вверх>	Развернуть окно до максимума по вертикали
<Win>+<Shift>+ +<Стрелка вниз>	Восстановить исходный размер по вертикали
<Win>+<Стрелка влево>	Развернуть окно и прикрепить к левому краю экрана (или восстановить прикрепленное к правому краю окно)
<Win>+<Стрелка вправо>	Развернуть окно и прикрепить к правому краю экрана (или восстановить прикрепленное к левому краю окно)
<Win>+<P>	Включение окна с параметрами презентаций (presentation settings), где можно выбрать режим отображения рабочего стола на дополнительном мониторе (включение/выключение, клонирование или расширение)

Таблица П1.2. *Управление задачами и рабочим столом*

Клавиши	Действие
<Win>+<G>	Вывести гаджеты на передний план (поверх всех окон)
<Win>+<+> и <Win>+<->	Включение экранной лупы и просмотр увеличенного изображения (используются клавиши "+" и "-" на цифровой клавиатуре)
<Ctrl>+<Колесико мыши>	Увеличение или уменьшение масштаба изображения (работает на рабочем столе, в окне Проводника, в браузере Internet Explorer, при просмотре изображений, во многих приложениях)
<Win>+<цифра (1–9)>	Запуск или открытие окна приложения, расположенного на панели задач под указанным номером (начиная слева)
<Средняя кнопка мыши> или <Shift>+<Левая кнопка мыши>	Запуск нового экземпляра приложения, представленного на панели задач
<Ctrl>+<Shift>+ +<Левая кнопка мыши>	Запуск нового экземпляра приложения, представленного на панели задач, *с административными правами*
<Alt>+<Tab> или <Alt>+<Shift>+<Tab>	Переключение окон в режиме 2D
<Win>+<Tab> или <Win>+<Shift>+<Tab>	Переключение окон в режиме 3D
<Win>+<M> или <Win>+<D>	Сворачивание всех окон

Таблица П1.3. *Общие задачи и функции систем Windows*

Клавиши	Действие
<Alt>+<P>	Включение *области (панели) предварительного просмотра* (preview pane) в окне программы Проводник[1] (Windows Explorer)
<Win>+<Pause/Break>	Открывает окно системы Windows
<Win>+<E>	Запуск Проводника (Windows Explorer); открывается узел **Компьютер** (Computer)
<F10>	Включение классического меню в активном окне приложения или системном окне (при его наличии)
<Alt>+<Enter>	Открывает в Проводнике окно свойств для выбранного элемента[2] (файла, папки и т. д.)
<Ctrl>+<Shift>+<N>	Создание новой папки в окне Проводника (при этом неважно, какой язык ввода выбран)
<Alt>+<Стрелка вверх>	В окне Проводника или в *стандартном* окне **Открыть**/**Сохранить** (Open/Save) переход к родительской папке (на один уровень вверх)
<Ctrl>+<Shift>+<Esc>	Запуск диспетчера задач
<Win>+<F>	Индексированный поиск в специальном окне поиска
<Win>+<L>	Блокировка окна (возможно переключение пользователей)
<Win>+<R>	Открывается окно **Выполнить** (Run) для ввода строковых команд

Таблица П1.4. *Управление проигрывателем Windows Media 12.0*

Клавиши	Действие
<Ctrl>+<1>	Переход в окно библиотеки
<Ctrl>+<2>	Работа в режиме обложки
<Ctrl>+<3>	Отображение окна текущего списка воспроизведения
<Ctrl>+<7>	В окне библиотеки: добавить к списку воспроизведения (Play)
<Ctrl>+<8>	В окне библиотеки: добавить к списку записи (Burn)
<Ctrl>+<9>	В окне библиотеки: добавить к списку синхронизации (Sync)
<Ctrl>+<P>	Воспроизведение/Пауза
<Ctrl>+<S>	Останов при воспроизведении
<Ctrl>+<W>	Останов при воспроизведении или паузе

[1] Эта комбинация не работает, если в окне Проводника включен русский язык.

[2] Думается, немногие пользователи знают об этой полезнейшей комбинации. При частой работе с разрешениями файлов, общими папками и т. п. данные клавиши становятся просто незаменимыми.

Таблица П1.4 *(окончание)*

Клавиши	**Действие**
<Ctrl>+<B>	Предыдущий трек или глава (chapter)
<Ctrl>+<F>	Следующий трек или глава (chapter)
<Ctrl>+<Shift>+<C>	Включение/Выключение субтитров, если они имеются (для видео или DVD)
<Ctrl>+<Shift>+<B>	Перемотка назад при просмотре DVD
<Ctrl>+<Shift>+<F>	Включение/Выключение перемотки вперед
<Ctrl>+<Shift>+<G>	Ускоренное воспроизведение
<Ctrl>+<Shift>+<N>	Воспроизведение с нормальной скоростью
<Ctrl>+<Shift>+<S>	Замедленное воспроизведение
<F7>	Выключение звука (mute)
<F8>	Уменьшение громкости
<F9>	Увеличение громкости
<F10>	Включение классического меню в окне библиотеки

ПРИЛОЖЕНИЕ 2

Полезные веб-сайты

Перечислим некоторые основные веб-сайты компании Microsoft, которые могут быть полезны для поиска дополнительной информации, решений и системных утилит или загружаемых компонентов. (Русскоязычные ресурсы отмечены буквами РУС.)

- *Домашняя страница Windows 7* (главная страница операционных систем Windows 7):

  http://windows.microsoft.com/ru-RU/Windows7/products/home (РУС)

  http://www.microsoft.com/windows/windows-7/

- *Microsoft TechNet* (домашняя страница веб-сайта "Microsoft TechNet", являющегося крупнейшей библиотекой статей для IT-специалистов по всем продуктам Microsoft. Содержит множество обзоров для знакомства с Windows 7 и изучения ее возможностей и технологий):

  http://technet.microsoft.com/ru-ru/ (РУС)

  http://technet.microsoft.com/en-us/

- *Центр загрузки Microsoft* (Microsoft Download Center) (главный портал для скачивания различных административных утилит и дополнительных программ, которые проще искать не по прямой ссылке, а по названию утилиты или имени дистрибутивного файла):

  http://www.microsoft.com/downloads/ru-ru/ (РУС)

  http://www.microsoft.com/downloads

- *Центр решений Windows 7* (Windows 7 Solution Center) (информационный портал, знакомящий с функциями и технологиями, реализованными в Windows 7, и предлагающий другую информацию, полезную при эксплуатации системы; имеются автоматизированные решения на английском языке, позволяющие диагностировать и устранить некоторые проблемы):

  http://support.microsoft.com/ph/14019#tab0

- *Windows Quality Online Services: Windows Logo'd Products List* (списки оборудования, совместимого с системами Windows 7; полезны для выбора оборудования, поддерживающего все заявленные в системе функции, например для поиска устройств воспроизведения мультимедийных потоков категории Digital Media Renderer):

  http://winqual.microsoft.com/hcl/

- *Технический центр Windows Client* (раздел, посвященный развертыванию Windows 7 и особенностям этой системы; ссылки на статьи сообществ, форумы и блоги):

  http://technet.microsoft.com/ru-ru/windows/dd361745.aspx (РУС)

- *Форум Windows 7* (русскоязычный форум TechNet, посвященный Windows 7):

  http://social.technet.microsoft.com/Forums/ru-RU/windows7ru (РУС)

- *Microsoft Malware Protection Center* (Центр средств защиты от нежелательных программ; здесь можно найти информацию о последних решениях Microsoft и обнаруженных опасностях в этой области, а также вручную скачать последние файлы описаний (definitions) для существующих программ — Windows Defender, Microsoft Security Essentials и т. д.):

  http://www.microsoft.com/security/portal/

  Прямая ссылка для скачивания Microsoft Security Essentials для ОС используемой разрядности (Windows XP, Windows Vista и Windows 7) и любого языка:

  http://www.microsoft.com/security_essentials/

- *Microsoft Windows Media — источник цифровых развлечений* (портал ссылок на мультимедийные программы Windows; здесь можно скачать пакет Windows Media Encoder 9 Series для кодирования и редактирования потоков мультимедиа):

  http://www.microsoft.com/windows/windowsmedia/ru/default.aspx (РУС)

- *The Green Button — Your Media Center Community* (Официальное сообщество пользователей Windows Media Center) (на этом англоязычном форуме можно найти практические советы по использованию возможностей Windows Media Center всех версий (включая Windows 7), а также ссылки на программы и утилиты, расширяющие эти возможности, например утилиты для работы с файлами телевизионных записей и т. п.):

  http://thegreenbutton.com/

Рекомендуемая литература

Для более глубокого знакомства с операционными системами Windows 7 предлагаем обратить внимание на следующие книги:

- Чекмарев А. Н. Microsoft Windows 7. Руководство администратора. — СПб.: БХВ-Петербург, 2010. — 896 с.: ил. (наиболее полное руководство по данной теме, охватывающее все системные компоненты и службы)
- Чекмарев А. Н. Microsoft Windows 7 для пользователей. — СПб.: БХВ-Петербург, 2010. — 560 с.: ил. + Видеокурс (на CD-ROM) (руководство, ориентированное на домашних пользователей)
- Чекмарев А. Н. Переход на Windows 7 с предыдущих версий. — СПб.: БХВ-Петербург, 2010. — 352 с.: ил. (руководство для уверенных в своих силах пользователей Windows XP и Windows Vista, помогающее им мигрировать на Windows 7 и быстро освоить новые способы решения привычных задач)

Следующие книги позволят более глубоко разобраться с принципами построения компьютерных сетей и используемыми технологиями[1]:

- Колисниченко Д. Н. Беспроводная сеть дома и в офисе. — СПб.: БХВ-Петербург, 2009. — 480 с.: ил.
- Поляк-Брагинский А. В. Локальная сеть. Самое необходимое. — СПб.: БХВ-Петербург, 2009. — 592 с.: ил.
- Поляк-Брагинский А. В. Локальные сети. Модернизация и поиск неисправностей. — СПб.: БХВ-Петербург, 2009. — 832 с.: ил.
- Поляк-Брагинский А. В. Сеть своими руками. — 3-е изд. перераб. и доп. — СПб.: БХВ-Петербург, 2008. — 640 с.: ил.
- Мак-Федрис Пол. Развертывание безопасных сетей в Windows Vista. — М.: Вильямс, 2009. — 528 с.: ил.

---

[1] Если требуется не академический подход, а практический взгляд на эти вопросы. Предложенный список книг, разумеется, не исчерпывающий, но нужно заметить, что книг по сетям Windows относительно немного; чуть ли не единственная книга посвящена сетевым решениям в Windows Vista, а по Windows 7 вообще нет специализированных книг, рассматривающих сетевые возможности этой версии.

Предметный указатель

I

J

L

M

N

P

R

S

T

U

V

W

X

А

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ч

Ш