Верх упорства — набирать неверный пароль,
пока компьютер не согласится...

Глава 11

Локальная сеть

Как устроена локальная сеть и по каким принципам она работает?

Адресация

Сеть — «сущность», разработанная для передачи данных между двумя объектами посредством канала связи. В каждой сети должны быть определены правила, в соответствии с которыми к ресурсам каждого объекта будет осуществляться доступ (в качестве аналогии — ситуация с соседом по комнате, который знает кому и какие продукты разрешено брать из общего холодильника). Набор таких правил называется Media Access Control (в вольном переводе — «контроль доступа к медиа»), или, сокращенно, MAC.

Все сетевые устройства должны иметь уникальный идентификатор для обеспечения четкой адресации. Таким образом, посылаемые по сети данные должны содержать в себе информацию об идентификаторе (адресе) получателя и отправителя (чтобы знать, куда надо посылать ответ). Формат такого адреса зависит от типа используемого протокола. Чаще всего в локальных сетях используется стандарт Ethernet, который предполагает, что в качестве адреса берется число вида 11–A0–17–3D–BC–01 (занимает 6 байт), которое абсолютно уникально для любого устройства на планете. Это число обычно называют MAC-адресом или физическим адресом устройства.

ПРИМЕЧАНИЕ

В идеале предполагалось, что MAC-адрес будет жестко связан с сетевым устройством и менять его пользователи не смогут (с целью добиться уникальности). Однако некоторые производители начали выпускать устройства, допускающие изменение MAC-адреса на свое усмотрение. Это иногда может привести к путанице и сбоям в работе сети.

MAC-адрес не единственный идентификатор компьютера. Обычно каждому компьютеру, работающему в сети, присваивается еще и IP-адрес.

IP-адрес имеет вид 192.168.1.1 (занимает 4 байта) и назначается администратором во время настройки компьютера для работы в сети.

MAC-адрес используется только в пределах локальной сети при обмене данными между коммутатором (устройством, соединяющим несколько подсетей) и компьютером данной подсети. Например, есть **компьютер 1**, входящий в **подсеть 1**, которому надо передать данные на **компьютер 2** из **подсети 2**. Коммутатор, иногда его также называют свитчем (от англ. switch), связывает **подсеть 1** и **подсеть 2**. Коммутатор, получив пакет для **компьютера 2**, должен

узнать его MAC-адрес, поскольку в пришедшем запросе с **компьютера 1** этот адрес не указан (**компьютер 1** обладает данными только об IP-адресе **компьютера 2**). Поэтому перед коммутатором встает задача поиска MAC-адреса по известному IP-адресу, который указан в запросе **компьютера 1** в качестве адреса назначения.

Стоит остановиться подробнее на том, как происходит маршрутизация пакетов данных при работе в локальной сети. Итак, процесс маршрутизации начинается с определения IP-адреса компьютера-отправителя. Каждый пакет содержит такой адрес. Кроме того, в заголовке пакета записан IP-адрес его места назначения. Если отправляющий компьютер определяет, что адрес доставки находится не в его подсети, пакет направляется коммутатору (который выполняет и функции маршрутизатора). Этот коммутатор определяет IP-адрес пакета и проверяет по своей таблице, не расположен ли компьютер-получатель в локальной физически подключенной к нему подсети. Если выясняется, что IP-адрес получателя принадлежит данной подсети, коммутатор начинает поиск в так называемом ARP-кэше (внутреннем хранилище IP- и MAC-адресов локальных устройств), позволяющем сопоставить IP- и MAC-адреса.

При обнаружении нужного MAC-адреса коммутатор помещает его в заголовок пакета (удаляя собственный MAC-адрес, который больше не нужен) и направляет пакет по месту назначения. Если MAC-адрес получателя не найден в ARP-кэше, коммутатор посылает ARP-запрос в подсеть, соответствующую IP-адресу получателя. Здесь разыскиваемый компьютер передает ответ на запрос и указывает свой MAC-адрес. Затем коммутатор обновляет содержимое ARP-кэша, устанавливает полученный MAC-адрес в заголовке пакета и отправляет его. Если пакет не предназначен для физически подключенной к нему подсети, он направляет его на коммутатор следующего сегмента.

Процесс построения и обновления таблиц маршрутизации практически непрерывен. Он осуществляется средствами, использующими интеллектуальные протоколы обнаружения (RIP или OSPF). В таблице каждого коммутатора указан оптимальный маршрут до адреса назначения или до коммутатора следующего сегмента (если адрес не принадлежит локальной подсети). Последовательно просматривая собственные таблицы маршрутизации, соответствующие устройства передают пакет по цепочке. Этот процесс продолжается до тех пор, пока пакет не достигнет пункта назначения.

При пересылке пакета через множество подсетей существует опасность образования «петель» — неправильно настроенный коммутатор постоянно возвращает

пакет тому коммутатору, через который данный пакет уже проходил. Для исключения этого предусмотрена TTL-функция (Time To Live), позволяющая задать предел времени поиска получателя пакета в сети. Значение TTL устанавливается заранее и уменьшается на единицу при каждом прохождении через любой коммутатор. Если величина TTL становится равной нулю, пакет удаляется, а коммутатор отсылает отправителю специальное сообщение.

Для определения MAC-адреса по IP-адресу используется протокол разрешения адреса ARP (Address Resolution Protocol). Принцип его работы следующий. Узел, которому нужно определить MAC-адрес (в данном случае это коммутатор), формирует специальный запрос, указывая в нем известный IP-адрес, и рассылает широковещательный запрос (на все компьютеры подсети). Компьютеры, получившие данный запрос, сравнивают указанный в нем IP-адрес с собственным. В случае совпадения компьютер формирует ответ, в котором указывает свой IP-адрес и свой MAC-адрес.

Основы двоичной системы счисления

Чтобы разобраться с тонкостями IP-адресации, масками подсети, сначала придется освоить азы двоичной системы счисления. В обыденной жизни мы привыкли иметь дело с так называемой десятичной системой счисления, когда числа представляются цифрами от 0 до 9. Компьютерная же логика основана на двоичной системе, когда для представления чисел используются только две цифры — 0 и 1. Эти цифры называются битами. Набор из восьми битов называется байтом. Обычно информация передается байтами — нельзя отдельно передать 3 или 9 бит данных, можно только 1 или 2 байта соответственно. Поэтому в двоичном виде принято записывать числа с предваряющими нулями, чтобы добиться кратности восьмерке. Например, число 1 будет представлено как 00000001, число 3 — как 00000011, а число 64 — как 01000000. Благодаря информации, представленной на рис. 11.1, вы без труда научитесь переводить любое десятичное число в двоичную форму. На рисунке условно изображен один байт и показано, какой бит какое число кодирует. Дело в том, что у каждого бита есть свой «вес», который зависит от его позиции в байте, вес увеличивается справа налево путем умножения на двойку. Комбинируя веса битов, можно закодировать любое число от 0 до 255. Для б**о**льших значений потребуется использовать большее количество байт.

Рис. 11.1. Распределение весов в одном байте

Маска подсети

IP-адрес и маска подсети — две составляющие, которые однозначно идентифицируют компьютер в сети. Чтобы задать их вручную, откройте меню **Пуск ▸ Настройка ▸ Панель управления ▸ Сетевые подключения** и здесь в свойствах сетевого подключения на вкладке **Общие** щелкните два раза кнопкой мыши на пункте **Internet Protocol (TCP/IP)**. Откроется окно, изображенное на рис. 11.2.

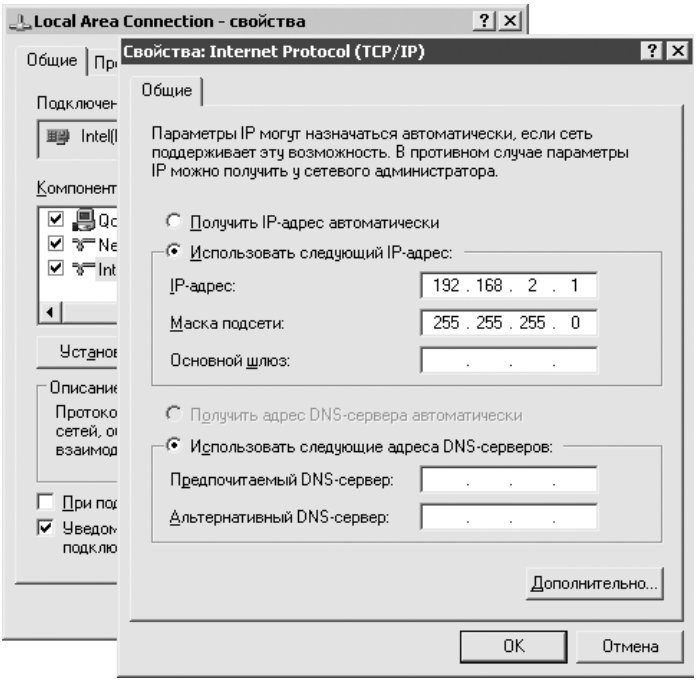


Рис. 11.2. Маска подсети задается здесь

В оригинале IP-адрес и маска представлены в двоичном виде. Например, число 192 в двоичном представлении выглядит как 11000000. Это немного непривычно, но, на самом деле, разбираться с адресацией гораздо проще именно в таком виде. Кстати, каждое число в адресе, отделенное точкой, называется октетом. Таким образом, адрес 192.168.2.1 состоит из четырех октетов. В двоичном виде каждый октет содержит 8 бит.

О чем говорят цифры на рис. 11.2? О том, что адрес вашей подсети (да, у нее тоже есть адрес) 192.168.2.0, а адрес компьютера в ней фактически 0.0.0.1. Как видите, IP-адрес просто раскладывается на составляющие. Почему именно так? Потому что разложение основывается на маске подсети. Три первых октета маски равны 255 — это говорит о том, что в IP-адресе первые три октета

относятся к адресу подсети. Если бы маска была 255.255.0.0, то адрес подсети был бы 192.168.0.0, а адрес компьютера в этой подсети — 0.0.2.1.

Теперь возвратимся к нашей прежней маске — 255.255.255.0. Всегда следует иметь ввиду, что в каждой подсети имеется два зарезервированных адреса, которые нельзя назначать компьютерам. С одним — в данном случае 192.168.2.0 — вы уже знакомы (он не может быть адресом компьютера, поскольку является адресом подсети). И второй — 192.168.2.255, который является широковещательным запросом на всю подсеть, имеющую адрес 192.168.2.0.

К слову, вы можете поэкспериментировать с адресами в своей домашней сети. Например, у меня дома адрес подсети 192.168.2.0, и если я посылаю сообщение по адресу 192.168.2.255, то оно приходит на все компьютеры (в том числе и на мой собственный). Попробовать сделать то же вы можете, выполнив в консоли команду типа `net send 192.168.2.255 привет всем`.

Теперь попробую доказать, что двоичное представление адресов и масок только упрощает жизнь. К примеру, в университете имеется сеть из нескольких десятков компьютеров. Логично было бы разделить ее на две подсети: студенческую и сеть сотрудников. Поскольку из-за плохого финансирования роста количества компьютеров не предвидится, то нет смысла резервировать большой диапазон IP-адресов. Посему сеть с маской 255.255.255.0 будет слишком большой, и весь диапазон будет разделен на две части. Чтобы этого добиться, будет использоваться маска подсети 255.255.255.128. Ее двоичный эквивалент — 11111111.11111111.11111111.10000000.

Как видите, в четвертом октете старший бит равен 1, а не 0. Итак, в данном случае для адреса подсети будет выделено три октета и один бит. Чтобы пояснить, представьте показательный IP-адрес 192.168.2.1 в двоичном виде. Получится: **11000000.10101000.00000010.0**0000001.

Часть адреса, выделенная жирным шрифтом, является адресом подсети. Если бы маска была 255.255.255.0, то адрес подсети и показательный выглядели бы так: **11000000.10101000.00000010**.00000001. Как видите, разница всего в одном бите.

Что же меняется от одного бита? В итоге образуются две подсети с диапазоном адресов 192.168.2.1–192.168.2.126 (для студенческой) и 192.168.2.1–192.168.2.254 (для сотрудников). Таким образом, студенты смогут видеть только себя, а преподаватели (IP-адреса им надо раздавать начиная с 192.168.2.128) — и себя, и студентов.

Для полной ясности осталось только разобраться, почему у первой подсети последним является адрес 192.168.2.126, а не 192.168.2.127. Дело в том, что для

данной подсети этот адрес является широковещательным. Что же общего у адресов 192.168.2.127 (маска 255.255.255.128) и 192.168.2.255 (маска 255.255.255.0)? То, что в обоих случаях в двоичном обозначении адрес компьютера, отделенный от адреса подсети, состоит из единиц (это и является признаком широковещательного запроса). Смотрите сами. В первом случае адрес выглядит как 11000000.10101000.00000000.01111111 (маска 255.255.255.128), во втором случае — как 11000000.10101000.00000000.11111111 (маска 255.255.255.0).

Лучше освоить работу с масками подсети и переводом IP-адресов в двоичный вид поможет утилита LanCalculator (есть на прилагаемом компакт-диске и на сайте **www.lantricks.com**). Кроме того, она поможет автоматизировать расчет широковещательного IP-адреса, IP-адреса сети и количества IP-адресов в подсети.

Теперь вам наверняка будет понятен анекдот: «Сегодня на маскарад все пришли в масках: Серж в маске льва; Константин в маске волка; Наталья в маске лисы; Администратор Леша в 255.255.255.0».

Протоколы

О существовании протокола TCP/IP вам уже наверняка доводилось слышать. Это главный протокол, используемый в локальных сетях и Интернете. Его основу составляет протокол межсетевого взаимодействия IP (Internet Protocol). К основным функциям протокола IP относятся:

- передача между сетями различных типов адресной информации в унифицированной форме;
- сборка и разбиение пакетов на части при передаче их между сетями с различными максимальными значениями длины пакета.

Протокол UDP является более простым по сравнению с TCP, поскольку не требует подтверждения доставки и не осуществляет контроль ошибок. За счет этого обмен данными посредством данного протокола может осуществляться быстрее, однако это справедливо лишь для сетей с качественной связью. Если связь не очень качественная, то пакеты могут теряться, дублироваться или приходить в неверном порядке.

Более надежным и более распространенным протоколом является протокол TCP, который осуществляет контроль ошибок и запрашивает подтверждение доставки. Как и в протоколе UDP, для работы с приложениями используются порты.

ПРИМЕЧАНИЕ

Что такое порт? Любое запущенное сетевое приложение на компьютере использует определенный порт. Обычно один порт использует только одно приложение, поэтому IP-адрес компьютера и номер порта могут однозначно указывать на тот или иной сетевой процесс.

Назначение номеров портам, как правило, осуществляется операционной системой. Для наиболее распространенных сервисов используются стандартные номера портов (FTP — 21, HTTP — 80 и т. д).

Протокол обмена управляющими сообщениями ICMP (Internet Control Message Protocol) позволяет коммутатору сообщать компьютеру об ошибках, которые возникли при передаче данных. ICMP — это протокол сообщения об ошибках, однако, кроме того, он предоставляет сетевым администраторам средства для тестирования доступности компьютеров в сети. Эти средства представляют собой так называемый эхо-протокол, включающий обмен двумя типами сообщений — эхо-запросами и эхо-ответами. Администратор посылает по сети эхо-запрос, содержащий IP-адрес компьютера, доступность которого нужно проверить. Компьютер, который получает эхо-запрос, формирует и отправляет эхо-ответ.

В Windows используется команда `ping`, которая предназначена для тестирования доступности узлов. Она обычно посылает серию эхо-запросов к тестируемому компьютеру и затем предоставляет статистику об эхо-ответах и среднем времени реакции сети на запросы.

Как организовать домашнюю сеть?

Далее мы рассмотрим общие моменты построения локальной сети, подробно останавливаясь лишь на наиболее важных или сложных деталях. Но прежде чем начать, нужно ответить на вопрос, который многие уже склонны считать риторическим: в чем выгода от подключения? Во многом. Грубо говоря, вы увеличиваете размер своего жесткого диска в несколько раз за счет других пользователей. В дополнение к этому получаете возможность обмениваться данными и, в конце концов, просто общаться с новыми людьми, о существовании которых раньше и не подозревали. Все это лишь прелюдия к дальнейшим перспективам, предоставляемым локальной сетью, о которых будет сказано чуть позже. А пока начнем плавно переходить к реализации задуманного.

Проблема выбора

Пока окончательно не наступит время беспроводных соединений, клубок проводов возле компьютера останется неизбежным. К вопросу выбора кабеля

придется подходить серьезно, поскольку неудачно выбранный коммутатор еще можно заменить, а вот уже проложенный кабель — вряд ли.

Изначально для соединения компьютеров между собой применялся коаксиальный кабель, максимальная пропускная способность которого была 10 Мбит/с. Сейчас в широком обиходе так называемая «витая пара» (разрежьте кабель и поймете, откуда название) с максимальной скоростью передачи информации 100 Мбит/с. Витая пара бывает двух типов: экранированной и неэкранированной. Последняя наиболее распространена, поскольку стоит меньше. Если позволяют средства, лучше выбрать экранированный кабель: во-первых, он просто физически прочнее, а во-вторых, помех в нем гораздо меньше, вследствие чего увеличивается скорость передачи данных (в некоторых образцах больше 100 Мбит/с).

Кроме того, среди бывалых сетевых пользователей ходят слухи о некой военной витой паре, которая прекрасно подходит для создания «воздушек» (соединений между соседними домами, образованных с помощью перекинутого через крыши кабеля), поскольку менее подвержена воздействию окружающей среды и к тому же настолько прочна, что не требует несущей опоры. Раздобыть данный экземпляр можно, если обратиться за помощью на специализированные форумы.

После того как вы определились с типом используемого кабеля, самое время продумать маршрут, по которому будет проложен кабель.

Прокладываем провода

В обыкновенных домах советской застройки есть всего два пути связи между подъездами.

Первый путь — прокладывать кабель через чердак дома, пуская его вместе с линиями кабельного телевидения и радио вниз через щитки на площадках.

Второй путь — тянуть через подвал. В данном случае могут возникнуть трудности, поскольку между подъездами обычно стоят металлические двери, к тому же вечная сырость — известный враг всего электрического. В общем, наиболее оптимальным путем остается путь под номером один. Он и будет рассмотрен далее.

Как уже говорилось, лезть придется на чердак дома, а там обычно живут голуби. Много голубей. Поэтому вариант с домашними тапочками сразу отпадает — лучше всего подойдут старые кроссовки или сапоги. Не помешают кепка на голову и мощный фонарик. Вход на чердак есть не во всех подъездах дома, и обычно его преграждает дверь, ключи от которой придется попросить у работников коммунальных служб или пожарных.

Самая трудная задача — найти место, через которое можно проталкивать кабель, поэтому идеальный вариант, когда с вами есть специалист (почти во всех крупных городах есть люди, которые прокладывают сеть за деньги). За советом можно обратиться и к тем, кто монтировал в вашем доме кабельное телевидение или кодовую дверь. Если такой возможности нет, придется все делать самостоятельно на свой страх и риск. В последнем случае нужно сориентироваться на чердаке по вентиляционным шахтам, так чтобы оказаться над щитком нужного подъезда. Где-то в этой области из пола должна торчать высокая металлическая трубка — в нее, как правило, входит один провод (предположительно это радио) — в эту трубку и опускают кабель для локальной сети. Обычно кабель приклеивают скотчем к тонкой стальной проволоке для большей жесткости и, соответственно, лучшей проходимости и стараются протолкнуть вниз. Если все прошло удачно, свободный конец кабеля появится из пластмассового желоба в щитке на площадке верхнего этажа. Чтобы добраться до нижних этажей, кабель следует опускать в такой же желоб в щитке, но идущий вниз. В целях вашей безопасности рекомендуется поручить этот процесс специалистам.

Дело техники

В ходе монтажных работ вам наверняка понадобятся следующие компоненты и инструменты.

- Кабель:
  - UTP (Unshielded Twisted Pair) — неэкранированная витая пара;
  - STP (Shielded Twisted Pair) — экранированная витая пара.
- Вилки RJ-45 (в народе «коннекторы»).
- Щипцы обжимные.
- Скобы для крепления электрокабеля.
- Молоток.

Когда необходимая инфраструктура создана, остальное — дело техники. Чаще всего на верхних этажах размещают коммутатор, к которому подключают кабель, идущий с чердака. Таким образом, происходит разветвление канала на необходимое количество ветвей. Как правило, в домашних сетях предпочитают использовать коммутаторы товарных марок Surecom или Acorp из-за их доступной цены. Стоит отметить, что продукция Surecom характерна тем, что в ней быстро перегорают порты, поэтому лучше покупать с запасом (к примеру, вместо 5-портового коммутатора брать 8-портовый). Про Acorp же известно, что это оборудование крайне плохо работает с «воздушками» и чувствительно к перепадам напряжения.

Если вы можете позволить себе более высокие затраты на покупку коммутаторов, то обратите внимание на продукцию таких производителей, как 3Com, Zyxel, D-Link или Planet. Они предлагают продукцию, пожалуй, наиболее приемлемого соотношения цены и качества. Также учтите, что идеальным вариантом будет, если сетевые карты и коммутаторы в вашей сети одной марки. Разобравшись с оборудованием, останется только обжать кабель.

Известны два варианта обжатия витой пары, они изображены на рис. 11.3 и рис. 11.4. Если вы подключаете компьютер к коммутатору, на обоих концах следует обжимать кабель согласно одной из предложенных схем. Если же на каждом конце обжимать по-разному, то получится так называемый «перевертыш» — кабель, которым можно напрямую соединять два компьютера.

Последовательность действий при обжиме кабеля следующая.

Обрежьте конец кабеля. При этом лучше всего воспользоваться резаком, встроенным в обжимной инструмент, или острыми кусачками.

Расплетите и выровняйте провода, уложив их в один ряд в соответствии с выбранным вариантом обжима.

Обрежьте провода так, чтобы их длина была около 10 мм.

Вставьте провода в пазы разъема вилки RJ-45 в соответствии с выбранным вариантом обжима.

Аккуратно поместите разъем в обжимной инструмент, держась за кабель, и затем аккуратно произведите обжим. Вы должны услышать легкий щелчок пластмассовой перегородки.

После того как вы вставите один конец обжатого кабеля в порт коммутатора, а другой — в разъем сетевой карты, на ней должна загореться зеленая лампочка. Это значит, что кабель физически не поврежден, и вы почти у цели.

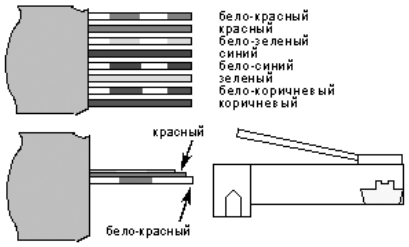


Рис. 11.3. Первый вариант обжима кабеля

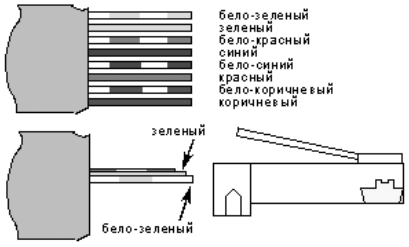


Рис. 11.4. Второй вариант обжима кабеля

Финишная прямая

В Windows 9x сложностей с сетевыми настройками обычно не возникает — доста-

точно лишь согласованно выставить IP-адреса и маски подсети. Поэтому нет смысла уделять системам 9x свое время, тем более что их время уже давно прошло. А вот настройкой Windows XP стоит заняться вплотную из-за некоторых особенностей.

По-умолчанию обладатели Windows XP Professional закрыты для доступа извне настройками политик безопасности. Чтобы разрешить другим пользователям доступ к этому компьютеру по сети, придется эти политики откорректировать.

Первым делом откройте меню **Пуск ▸ Выполнить** и запустите оснастку **Групповая политика** командой `gpedit.msc`. Далее, воспользовавшись деревом компонентов в левой части окна, перейдите по адресу **Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Назначение прав пользователя**. Здесь два раза щелкните кнопкой мыши на названии политики **Доступ к компьютеру из сети** и в открывшемся окне добавьте пользователя **Гость**, а из политики **Отказать в доступе к компьютеру из сети** пользователя **Гость** удалите (рис. 11.5).

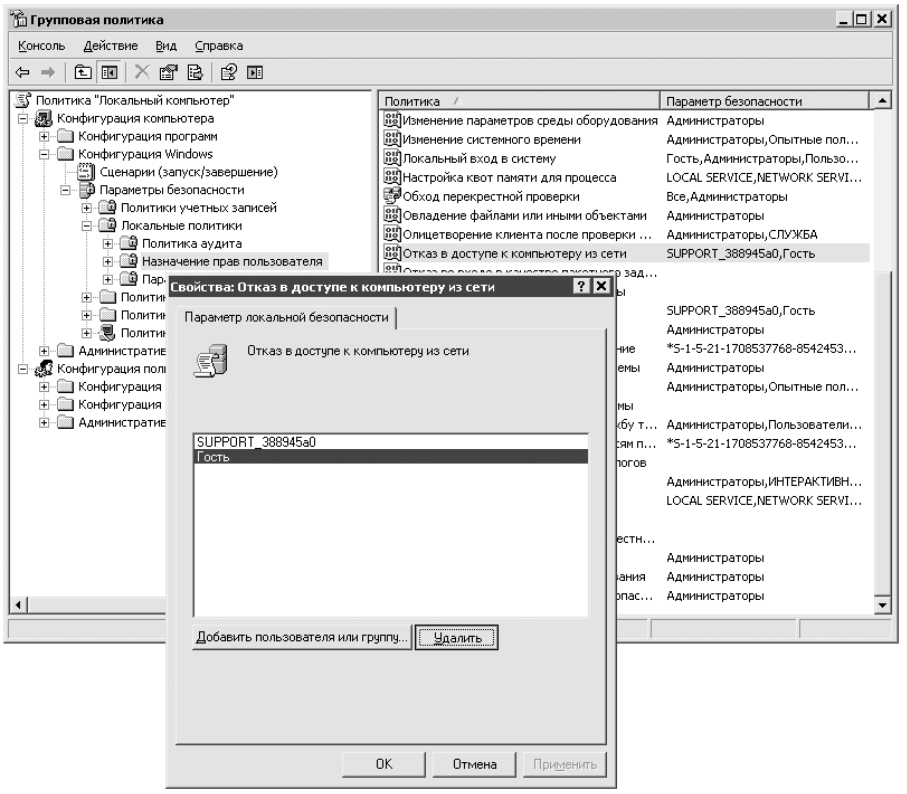


Рис. 11.5. Удаление пользователя из настроек политики

Затем выполните в меню **Пуск ▸ Выполнить** команду `compmgmt.msc`, перейдите к пункту **Локальные пользователи и группы ▸ Пользователи**, щелкните два раза кнопкой мыши на имени пользователя **Гость** и в открывшемся окне снимите флажок **Отключить учетную запись** (рис. 11.6).

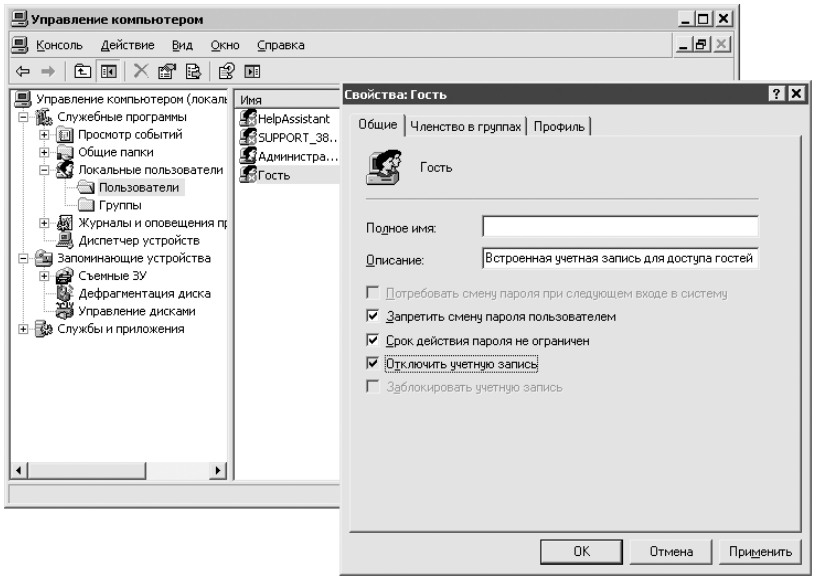


Рис. 11.6. Включаем учетную запись Гость

Обладателям Windows XP SP1 придется в свойствах подключения по локальной сети на вкладке **Дополнительно** также выключить брандмауэр, иначе остальные пользователи вас просто не увидят.

ПРИМЕЧАНИЕ

Домашняя сеть иногда заставляет решать неожиданные задачи. К примеру, входил компьютер в сеть, а потом вдруг перестал в ней появляться. Самое обидное, что его никто не видит, а он видит всех. Прямо мистика какая-то... Тайна такого загадочного поведения заключается в параметрах безопасности Windows XP SP1. Как известно, в этой системе имеется встроенный брандмауэр, и если его активировать для соединения с локальной сетью, то компьютер становится «невидимым», так как брандмауэр предупреждает все попытки подключения к компьютеру. Если у вас такая же проблема, откройте Свойства соединения по локальной сети и отключите брандмауэр. В Windows XP SP2 данная проблема решена.

Глобальные перспективы локальной сети

Как только ваша локальная сеть переступит рубеж хотя бы в десять пользователей, уже имеет смысл вести переговоры с провайдером о предоставлении вам

доступа к Интернету по технологии ADSL (об этом далее в разделе). Как правило, провайдер бесплатно предоставляет вам свой модем, и дальше вы платите только за объем используемого трафика.

С помощью какой команды можно посмотреть, какие процессы запущены у пользователя на другом компьютере, и завершить тот или иной?

Узнать список запущенных на удаленном компьютере процессов может помочь команда консоли `tasklist`. В результате ее выполнения вы получите список всех процессов и их PID (уникальный идентификатор процесса) — рис. 11.7. Для получения более детальной информации добавьте к данной команде ключ `/v`.

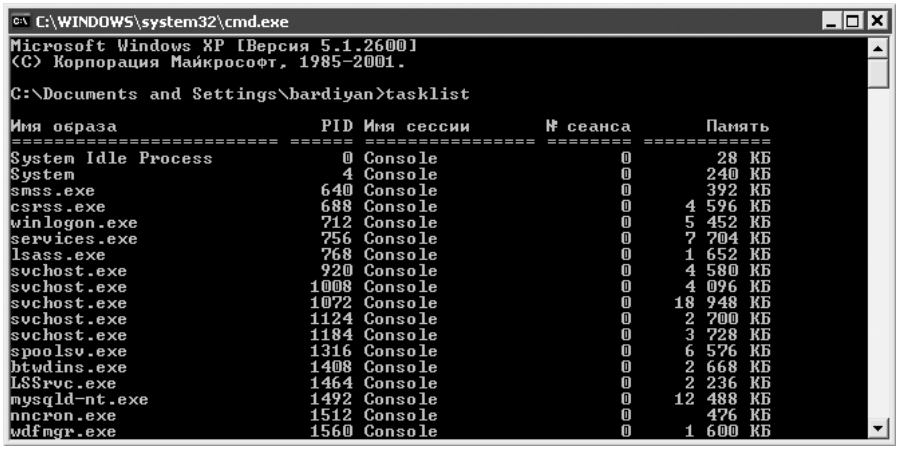


Рис. 11.7. Результат выполнения команды tasklist

Чтобы удаленно завершить процесс на компьютере пользователя, используется команда `taskkill`. Например, `taskkill /s \\notebook114 /u administrator /p 111111 /pid 1008`, где `1008` — это PID процесса, который вы узнали в результате выполнения команды `tasklist`.

Также может помочь утилита Remote Task Manager (есть на прилагаемом компакт-диске и на сайте **www.protect-me.com/rtm**). Она предназначена для управления процессами, запущенными на удаленном компьютере, но на самом деле способна совершать гораздо больше действий. Предлагаем вашему вниманию краткий перечень ее возможностей:

- просматривать текущие сетевые подключения (процесс, протокол, адрес, порт, состояние) и закрывать ненужные;

- наблюдать за сетевой активностью компьютера (подключения, свойства, трафик);
- добавлять или удалять общие сетевые ресурсы;
- следить за производительностью системы (вкладка **Perfomance**, которая аналогична используемой в **Диспетчере задач Windows**);
- просматривать и удалять записи из журнала системных событий;
- управлять работой драйверов удаленной машины;
- управлять системными службами (запускать, останавливать, редактировать, создавать, удалять);
- контролировать запущенные процессы и приложения.

Интересной является возможность устанавливать права доступа и сменять владельца системных служб, драйверов. Как сделать это стандартными средствами Windows, мне неизвестно.

Remote Task Manager (рис. 11.8) способен перезагружать и выключать удаленный компьютер; блокировать его и затем снимать блокировку; а также запус-

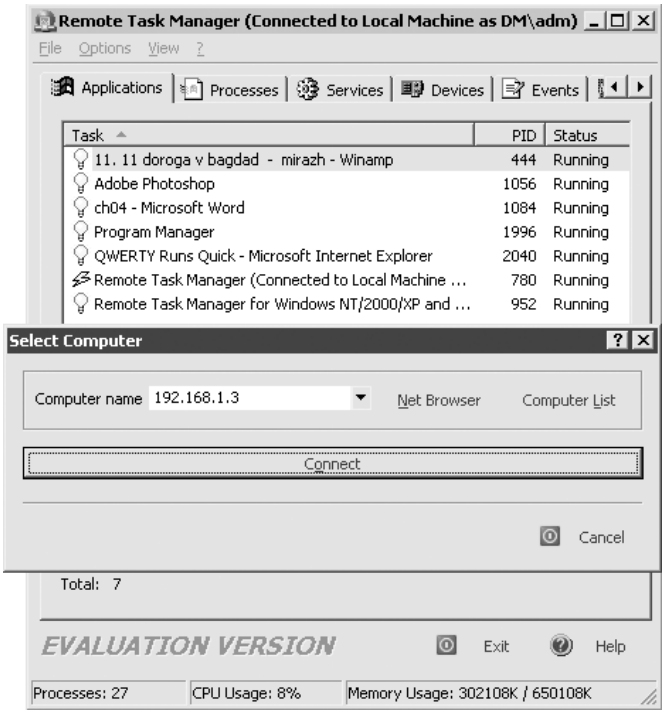


Рис. 11.8. Окно приложения Remote Task Manager

кать на нем произвольную программу. Установка Remote Task Manager на удаленном компьютере не требует физического присутствия администратора. Достаточно только нажать клавишу **F3**, указать имя компьютера и дать согласие на установку на нее сервиса Remote Task Manager. От вас требуется только указать адрес файла `rtmservice.exe` (находится в папке установки программы), и, само собой, вы должны обладать правами администратора.

Кроме того, можно воспользоваться утилитой PCViewer (**www.microsoft.com**).

При обращении к ресурсам в локальной сети система создает ярлыки к ним. Как сделать, чтобы этого не происходило?

Это делается в два этапа.

Для начала запустите **Проводник**, откройте меню **Сервис ▸ Свойства папки** и на вкладке **Вид** и снимите флажок **Автоматический поиск сетевых папок и принтеров** (рис. 11.9), чтобы в папке **Сетевое окружение** не создавались ярлыки на сетевые ресурсы, которые вы посещали.

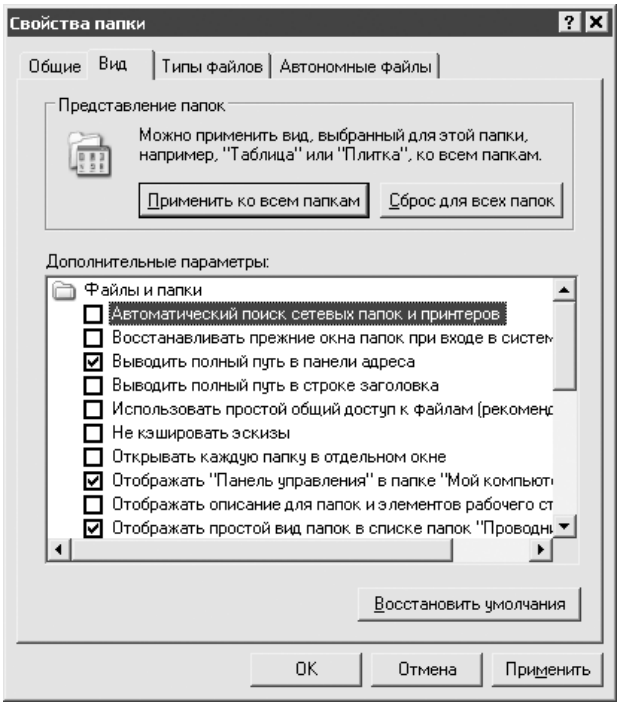


Рис. 11.9. Отключение автоматического поиска сетевых папок

Далее запустите оснастку **Групповая политика** (команда `gpedit.msc` меню **Пуск ▸ Выполнить**), перейдите по адресу **Конфигурация пользователя ▸ Административные шаблоны ▸ Рабочий стол** и включите политику **Не добавлять общие папки, из которых открыты документы**.

Как ускорить доступ к наиболее часто используемым папкам другого компьютера?

Обычно если нужно что-то найти на компьютере другого пользователя, приходится открывать **Сетевое окружение**, выбирать нужную машину из списка доступных компьютеров и просматривать доступные диски и папки. Но есть способ более быстрый. Можно подключить часто используемую папку другого компьютера в качестве сетевого диска либо создать для нее ярлык, избавив себя от путешествия (порой оно оказывается чересчур долгим) по списку машин в **Сетевом окружении**.

Сетевой диск

В гл. 5 уже рассказывалось о подключении сетевого диска, однако в тот раз это делалось только средствами **Проводника**. Сейчас же будет рассмотрен способ подключения сетевого диска с помощью командной строки — в некоторых случаях это может оказаться удобнее. Например, нужно подключить папку **mp3**, расположенную на компьютере **Olia**. В таком случае в консоли выполните команду `net use x: \\Olia\pict`, где `x` — это буква подключаемого диска, под которой он будет виден в вашей системе; `\\Olia\pict` — путь к искомой папке. После успешного выполнения команды вы увидите у себя новый диск (рис. 11.10).

В консоли увидеть список подключенных в данный момент дисков можно с помощью команды `net use`. Для удаления диска **X** выполните в консоли команду `net use x: /delete`. Чтобы сетевой диск автоматически подключался после перезагрузки, воспользуйтесь ключом `/persistent:yes`, то есть `net use x: \\Olia\pict/persistent:yes`.

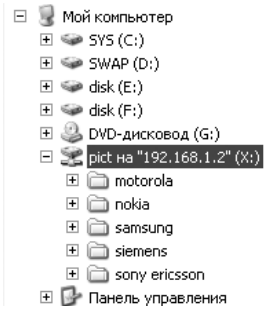


Рис. 11.10. Так выглядит сетевой диск в Проводнике

Есть еще один способ подключения сетевого диска. Откройте **Сетевое окружение**, найдите нужную папку и щелкните на ней правой кнопкой мыши. В открывшемся меню выберите команду **Подключить сетевой диск**.

Ярлык

У сетевых дисков есть недостаток — они подключаются при загрузке, отнимая время, поэтому в некоторых случаях достаточно ограничиться ярлыком для нужной папки. Откройте **Сетевое окружение**, найдите нужную папку и щелкните на ней правой кнопкой мыши. В открывшемся меню выберите команду **Создать ярлык**.

Время от времени компьютер начинает «тормозить», это как-то связано с локальной сетью. В чем может быть дело?

Нередко желание поделиться всем, что есть на диске, с остальными пользователями приводит к пагубным последствиям — компьютер начинает «тормозить», работать с ним становится практически невозможно. Такое происходит из-за большого количества обращений к машине через сеть (в гл. 5 уже говорилось о том, как узнать, кто в данный момент использует сетевые папки). Например, один человек решил скопировать себе парочку фильмов, а другой — послушать вашу музыку или посмотреть фотографии. Этого вполне достаточно, чтобы производительность вашего компьютера значительно снизилась. Бороться с таким явлением можно двумя способами. Самый предпочтительный — на вкладке **Доступ** (рис. 11.11) окна свойств папки указать с помощью

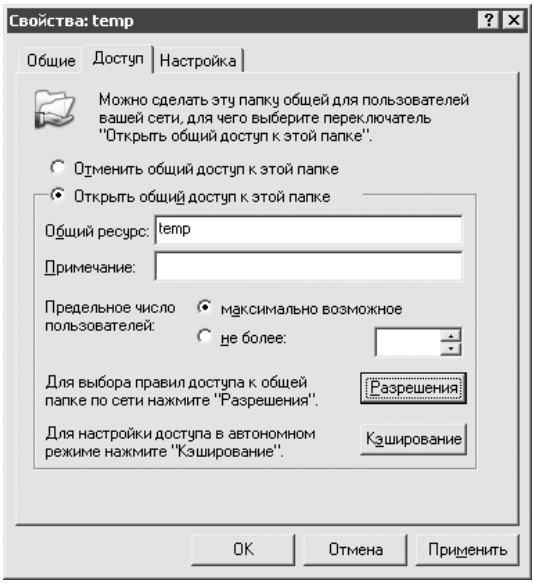


Рис. 11.11. Здесь можно ограничить количество сетевых пользователей папки

переключателя **Предельное число пользователей** количество одновременных подключений не более одного или двух, особенно если в этой папке содержатся большие файлы: музыка или фильмы.

Кроме того, в оснастке **Управление компьютером** можно видеть, какие удаленные пользователи работают с вашими файлами, а также их отключать. Для этого откройте **Панель управления ▸ Администрирование ▸ Управление компьютером** (либо выполните команду `compmgmt.msc` в меню **Пуск ▸ Выполнить**). В открывшемся окне перейдите по адресу **Общие паки ▸ Сеансы**.

Как закрыть сразу все сетевые сессии?

Сделать это можно либо с помощью оснастки **Общие папки** (команда `fsmgmt.msc`), либо с помощью команды, закрывающей все сетевые сессии и отключающей всех пользователей, которые открыли папки или файлы на вашей машине: `net session /delete`.

Как скрыть свой компьютер в локальной сети, чтобы никто не мог обнаружить, включен он или нет, но я работать мог?

Локальная сеть — это хорошо. Но иногда даже хорошего бывает много: приходит усталость и хочется отдохнуть, побыть наедине с компьютером, а надоедливые пользователи из локальной сети все скачивают музыку, фильмы, «стучатся» в чат... Можно, конечно, выдернуть кабель из сетевой карты, но делать это истинным (а значит, ленивым) компьютерным пользователям слишком сложно. Гораздо проще набрать в консоли команду `net config server /hidden:yes`. Чтобы вновь «появиться» в сети, выполните команду `net config server /hidden:no`. Есть и другой вариант: выполните команду `services.msc` в меню **Пуск ▸ Выполнить**. В списке служб выберите службу **Сервер** и остановите ее. Чтобы эффект «невидимости» сохранился после перезагрузки, выберите в раскрывающемся списке **Тип запуска** окна свойств службы пункт **Отключено**.

Еще один способ — включить брандмауэр Windows и запретить использование исключений: откройте **Панель управления ▸ Сетевые подключения**. Правой кнопкой мыши щелкните на значке подключения и в открывшемся меню выберите команду **Свойства**. Перейдите на вкладку **Дополнительно**, в области настроек **Брандмауэр Windows** нажмите кнопку **Параметры** и в следующем окне установите флажки: **Включить** и **Не разрешать исключения** (рис. 11.12).

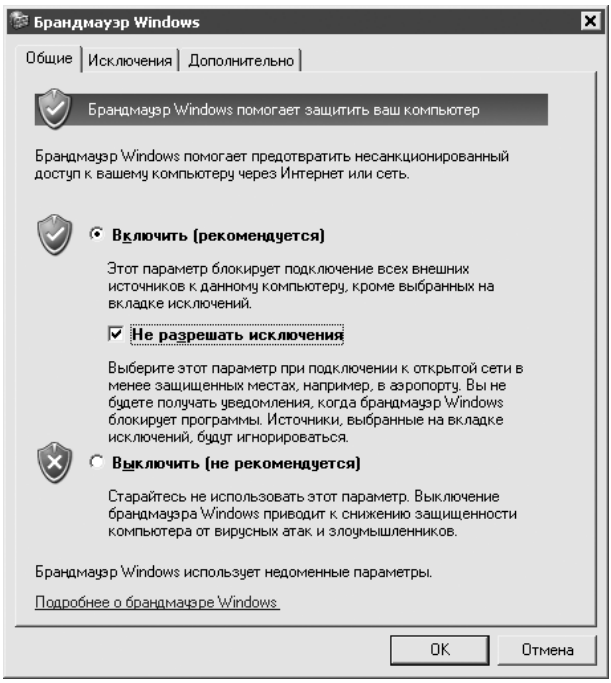


Рис. 11.12. Включение брандмауэра Windows

Как можно скрыть сетевую папку?

Если вы хотите скрыть свои сетевые папки от обычных пользователей, которые не знают «секрета», то в свойствах скрываемой папки перейдите на вкладку **Доступ**, затем нажмите кнопку **Новый общий ресурс** и перед новым названием ресурса поставьте символ `$`, например `$Новая папка`.

Как использовать несколько IP-адресов?

Чтобы изменить свой IP-адрес, откройте меню **Пуск ▸ Настройка ▸ Панель управления ▸ Сетевые подключения**, щелкните правой кнопкой мыши на значке активного сейчас подключения и в открывшемся меню выберите команду **Свойства**. На вкладке **Общие** в разделе **Компоненты, используемые этим подключением** выберите пункт **Internet Protocol (TCP/IP)** и нажмите кнопку **Свойства**. В открывшемся окне установите переключатель в положение **Использовать следующий IP-адрес** и в соответствующем поле укажите новое значение IP-адреса.

Чтобы назначить данной сетевой карте еще несколько IP-адресов (если часто приходится подключаться к разным сетям), нажмите кнопку **Дополнительно**,

в области **IP-адреса** нажмите кнопку **Добавить** и в следующем открывшемся небольшом окне укажите дополнительный IP-адрес и новую маску подсети (рис 11.13).

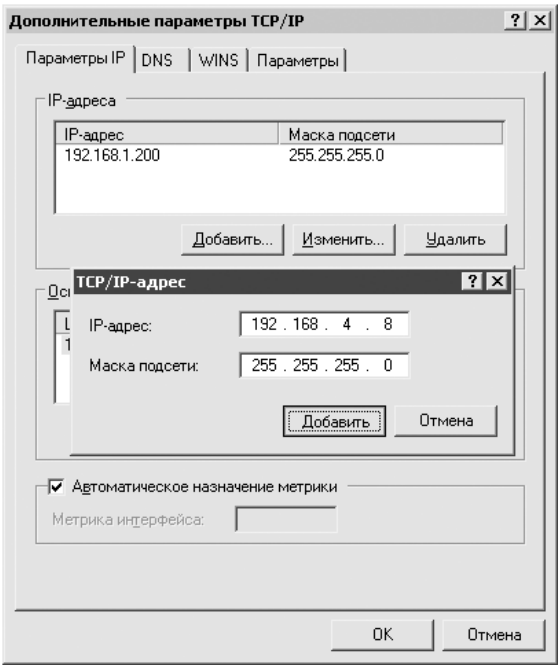


Рис. 11.13. Добавление второго IP-адреса

Как можно проверить качество соединения между компьютерами?

Команда ping

Данная команда является просто незаменимым инструментом, `ping` — своего рода «глаза» администратора. С помощью этой команды очень удобно определять доступность компьютера в сети — достаточно отправить ему запрос, к примеру `ping dima` (вместо имени можно использовать и IP-адрес). Полученный результат будет иметь такую форму: `Reply from dima: bytes=32 time<10ms TTL=252`. Из полученной информации видно, что 32 байта информации посылалось компьютеру **dima**, и полученное время ответа составило менее 10 мс, что говорит о хорошей связи.

Команда `ping` может посылать запросы в бесконечном цикле (ключ `-t`). Эту возможность используют как для осуществления контроля над каналом связи,

так и при ожидании ответа сервера. Представьте ситуацию, когда нужно срочно забрать письмо с почтового сервера, а он в данный момент не работает. Ожидая подходящего момента, просто запустите в консоли `ping mail.server.ru -t`. Как только сервер заработает, вы сразу же узнаете об этом по изменившимся результатам команды. Прервать ее выполнение можно, нажав сочетание клавиш **Ctrl+C**.

Монитор производительности

В Windows встроено мощное средство осуществления контроля над производительностью компонентов системы: процессора, сетевого адаптера, локальных дисков, файла подкачки и многого другого. Вы даже можете строить график использования процессора тем или иным приложением.

За счет своей функциональности монитор производительности может произвести впечатление слишком сложного в использовании инструмента, но это не так. Первое впечатление, как это часто бывает, обманчиво.

Чтобы запустить монитор производительности, откройте меню **Пуск ▸ Настройка ▸ Панель управления ▸ Администрирование ▸ Производительность** либо выполните в меню **Пуск ▸ Выполнить** команду `perfmon.msc`. И тот и другой способы приводят к запуску оснастки **Производительность** (в мультиязычных версиях Windows она называется **Perfomance**). В меню оснастки есть два пункта, которые наиболее интересны. Первый — **Системный монитор**. Активировав его, в правом окне вы увидите графики, отражающие уровень производительности компонентов, над которыми осуществляется мониторинг. По умолчанию здесь осуществляется отслеживание работы процессора и памяти (список счетчиков расположен под графиком). Поскольку в данном случае необходимо узнать производительность сети, на ней и сосредоточимся. Счетчики других системных компонентов лучше удалить (сделать это можно с помощью клавиши **Delete**). Чтобы добавить счетчик, нажмите кнопку с изображением плюса, расположенную над графиком, либо сочетание клавиш **Ctrl+I**.

В открывшемся окне **Добавить счетчики** в списке **Объект** выберите пункт **Сетевой интерфейс**, тут же в нижней левой области появится список соответствующих этому объекту счетчиков, а в нижней правой — список имеющихся на вашем компьютере сетевых интерфейсов. Сейчас главное — не запутаться. Для проверки скорости локальной сети выберите тот интерфейс, название которого соответствует названию вашей сетевой карты, например **Intel(R) PRO_100+MiniPCI**. Что касается счетчиков, то из всего многообразия интересны только счетчики **Получено байт/сек** и **Отправлено байт/сек**. Выберите эти счетчики, нужный сетевой интерфейс и нажмите кнопку **Добавить**. Далее в главном окне оснастки щелкните

правой кнопкой мыши на графике или любом из счетчиков, выберите в появившемся меню команду **Свойства** и открывшемся окне на вкладке **График** измените значения в области **Диапазон значений вертикальной шкалы**. В поле **Максимум** рекомендуется записать `1000`.

Для получения конкретной информации о скорости передачи данных в локальной сети скопируйте большие объемы данных поочередно на несколько машин. Показания счетчиков отразят ситуацию (рис. 11.14).

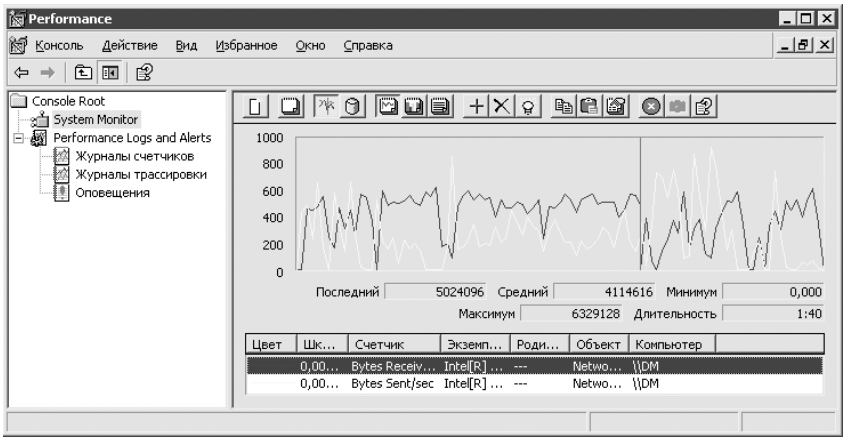


Рис. 11.14. Монитор производительности

Второй пункт оснастки **Производительность**, о котором хотелось бы сказать пару слов, — **Журналы счетчиков**. Данный элемент используется для создания более полного представления о производительности компонентов компьютера. Он позволяет записывать показания счетчиков в файл для осуществления последующего анализа данных за долгий период времени и как следствие — получения более точных результатов.

Перейдите в левой части оснастки **Производительность** по древовидному меню к пункту **Журналы счетчиков**. В правой части окна щелкните правой кнопкой мыши, в появившемся меню выберите команду **Новые параметры журнала** и в открывшемся окне укажите имя (например, `Localnet`). В следующем окне нажмите кнопку **Добавить счетчики** (процесс выбора счетчиков был описан чуть выше). После перейдите на вкладку **Файлы журнала** и укажите тип файла журнала **Текстовый файл (разделитель — запятая)**. Чтобы указать место размещения файла на диске, нажмите кнопку **Настроить**.

Когда настройки будут завершены, в оснастке **Производительность** щелкните на только что созданном журнале счетчиков правой кнопкой мыши и в откры-

вшемся меню выберите команду **Запуск** — этим вы начнете сбор данных с выбранных счетчиков.

Я слышал, что с помощью MAC-адреса можно ускорить обращение к другому компьютеру. Как это реализовать?

В начале этой главы уже затрагивалась тема MAC-адресов. Знание MAC-адреса позволяет напрямую обращаться к компьютеру в локальной сети, минуя коммутатор. В Windows предусмотрена возможность запоминать MAC-адреса компьютеров, с которыми производилось соединение. Эта информация хранится в ARP-кэше в виде таблицы IP-адресов и соответствующих им MAC-адресов. Чтобы избежать конфликтов, по умолчанию записи в ARP-кэше хранятся две минуты. Данная мера позволяет избежать неприятностей, если компьютер (запись о котором хранится в ARP-кэше) меняет свой IP-адрес или сетевую карту (в этом случае меняется MAC-адрес). Но если в вашей сети такие изменения не происходят, то можно увеличить время хранения записей в ARP-кэше, обеспечив тем самым себе более высокую скорость доступа к другим компьютерам. Чтобы сделать это, выполните следующие действия.

Откройте **Редактор реестра** (выполните команду `regedit.exe` в меню **Пуск ▸ Выполнить**).

Перейдите в раздел `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameter`.

Создайте здесь новый параметр типа `DWORD` с именем `ArpCacheLife`.

Дважды щелкните кнопкой мыши на этом параметре и установите время в секундах, в течение которого будут храниться записи.

После перезагрузки изменения вступят в силу.

ПРИМЕЧАНИЕ

Просмотреть, какие записи в данный момент находятся в ARP-кэше, можно с помощью консольной команды arp -a, а чтобы записать эти данные в файл, выполните команду arp –a › c:\arp.txt.

Есть еще один более гибкий способ, который позволяет добавлять статические ассоциации между выбранным IP-адресом и MAC-адресом. Например, компьютер с IP-адресом 192.168.1.2 имеет MAC-адрес 00-14-85-86-cb-8a, и этот адрес требуется запомнить, чтобы в дальнейшем была возможность обращаться

к этому компьютеру напрямую по MAC-адресу. Для этого откройте командную строку (команда `cmd` меню **Пуск ▸ Выполнить**) и выполните в ней команду `arp -s 192.168.1.2 00-14-85-86-cb-8a`.

ПРИМЕЧАНИЕ

Жесткое привязывание к MAC-адресу в некоторых случаях позволяет увеличить безопасность, затруднив атаки взломщиков, которые основываются на подмене доверенных серверов или устройств. Например, вполне логичным с точки зрения безопасности было бы жестко связать IP-адрес DNS-сервера и контроллера домена с их MAC-адресами.

Как уменьшить время поиска компьютера в сети?

Если при обращении к компьютеру локальной сети используется его имя вместо IP-адреса, на то, чтобы провести преобразование этого имени в IP-адрес, тратится некоторое время, в больших сетях довольно значительное. Чтобы сэкономить драгоценные секунды, можно использовать заранее известные IP-адреса компьютеров. Узнать IP-адрес — например, компьютера **Dima** — можно с помощью команды `ping dima` в меню **Пуск ▸ Выполнить**.

IP-адреса наиболее посещаемых вами компьютеров рекомендуется заносить в специальный файл `hosts` (без расширения), который находится в папке `windows\system32\etc`. Этот файл содержит таблицу соответствия IP-адресов и имен компьютеров. Каждый элемент должен располагаться в отдельной строке — напротив IP-адреса должно находиться имя соответствующего ему компьютера. Строка в файле `hosts` должна выглядеть примерно так: `192.168.1.7 dima`.

Можно ли настроить систему так, чтобы обращаться к ней только по IP-адресу?

Немного ускорить работу сети и избавиться от нежелательных гостей на своем компьютере поможет отключение NetBIOS. В результате нельзя будет по сети зайти на ваш компьютер, просто зная его сетевое имя, например `\\Dima`. Потребуется использовать его IP-адрес. Правда, вам тоже придется забыть про сетевые имена других компьютеров и использовать их IP-адреса для доступа.

ПРИМЕЧАНИЕ

NetBIOS (Network Basic Input/Output System) был разработан в 1983 году по заказу корпорации IBM в качестве прикладного программного интерфейса, с помощью которого клиентское программное обеспечение могло бы обращаться к ресурсам локальной сети. NetBIOS обладает собственной службой имен.

Казалось бы, крайне неудобное решение, однако оно обладает своими достоинствами:

- посторонним пользователям и сетевым вирусам будет труднее проникнуть на ваш компьютер, не зная его IP-адреса;
- сеть будет работать быстрее и стабильнее.

Пускай вас не пугает, что к другим компьютерам придется обращаться по их IP-адресам, — вам не придется запоминать хитрые комбинации из цифр вида 192.168.1.7, ведь для перехода можно создать ярлык. Вот как это делается. Создайте копию любого ярлыка на **Рабочем столе**. Затем щелкните на этой копии правой кнопкой мыши и выберите в открывшемся меню команду **Свойства**. В открывшемся окне в поле **Объект** наберите примерно следующее: `\\192.168.1.7`. Нажмите кнопку **Применить**. Теперь при щелчке кнопкой мыши на этом ярлыке будет открываться список сетевых папок компьютера, имеющего IP-адрес192.168.1.7.

Как получить список активных сетевых сервисов?

Чтобы получить список активных в данный момент сетевых сервисов, откройте командную строку (выполните команду `cmd` в меню **Пуск ▸ Выполнить**) и выполните команду `netstat`. Отобразится список всех активных подключений. Чтобы как-то детализировать выдаваемую командой `netstat` информацию, придется использовать ключи. Ниже перечислены наиболее полезные из них.

- `-a` — отображение всех подключений и ожидающих портов.
- `-b` — отображение исполняемого файла, участвующего в создании каждого подключения, или ожидающего порта. Иногда исполняемые файлы содержат множественные независимые компоненты. Тогда отображается последовательность компонентов, участвующих в создании подключения, либо ожидающий порт.
- `-n` — отображение адресов и номеров портов в числовом формате.
- `-o` — отображение кода (ID) процесса каждого подключения.
- `-p протокол` — отображение подключений для протокола, задаваемых этим параметром. Допустимые значения: TCP, UDP, TCPv6 или UDPv6.
- `интервал` — повторный вывод статистических данных (через указанный промежуток времени в секундах). Для прекращения вывода данных нажмите сочетание клавиш **Ctrl+C**. Если параметр не задан, сведения о текущей конфигурации выводятся только один раз.

Можно ли сделать резервную копию настроек соединения?

Если вы хотите сохранить настройки модемного соединения (название, имя пользователя, телефон), к примеру, чтобы воспользоваться ими после переустановки Windows, сделайте следующее.

Запустите **Редактор реестра** (откройте меню **Пуск ▸ Выполнить** и в открывшемся окне выполните команду `regedit`).

Перейдите в раздел `HKEY_CURRENT_USER\RemoteAccess\Profile` и выделите здесь соединение, настройки которого хотите сохранить.

В меню **Файл ▸ Экспорт** укажите название файла (к примеру, `isp.reg`), в котором будут сохранены настройки.

Чтобы восстановить настройки, просто запустите файл `isp.reg`, дважды щелкнув на нем кнопкой мыши.

Можно ли узнать имя пользователя, работающего за соседним компьютером?

Самый легкий способ получить подобную информацию — воспользоваться командой `nbtstat`. Существует два варианта ее использования (зависит от того, знаете ли вы имя машины или только ее IP-адрес).

Первый вариант: `nbtstat -a имя_компьютера`. Например, `nbtstat -a olia`.

Если известен только IP-адрес, воспользуйтесь командой `nbtstat -A IP-адрес`. Например, `nbtstat -A 192.168.1.7`.

Как управлять другим компьютером через сеть?

Стандартные средства Windows

В Windows XP появился инструмент **Удаленный рабочий стол**, который предназначен для управления удаленными компьютерами. По своей сути **Удаленный рабочий стол** является доработанным до нужд пользователей сервисом терминалов, который раньше был доступен только в серверных операционных системах.

Сейчас же требования к версии операционной системы следующие: компьютер, к которому производится подключение, должен находиться под управлением операционной системы Windows XP Professional (Home Edition не годится)

или выше; на остальных машинах может быть любая Windows — нужно только установить соответствующую клиентскую часть. Для установки компонента воспользуйтесь компакт-диском Windows XP. На странице приветствия выберите сначала пункт **Выполнение иных задач**, а затем **Установка удаленного управления рабочим столом**.

На компьютере, к которому вы собираетесь подключиться, выполните следующее. Откройте **Панель управления ▸ Система** (или нажмите сочетание клавиш **Windows+Pause Break**), на вкладке **Удаленные сеансы** установите флажок **Разрешить удаленный доступ к этому компьютеру**. Затем нажмите кнопку **Выбрать удаленных пользователей** и укажите те учетные записи, используя которые можно будет подключаться к данному компьютеру (рис. 11.15). Только имейте в виду, что пароли у выбираемых учетных записей не должны отсутствовать или быть пустыми.

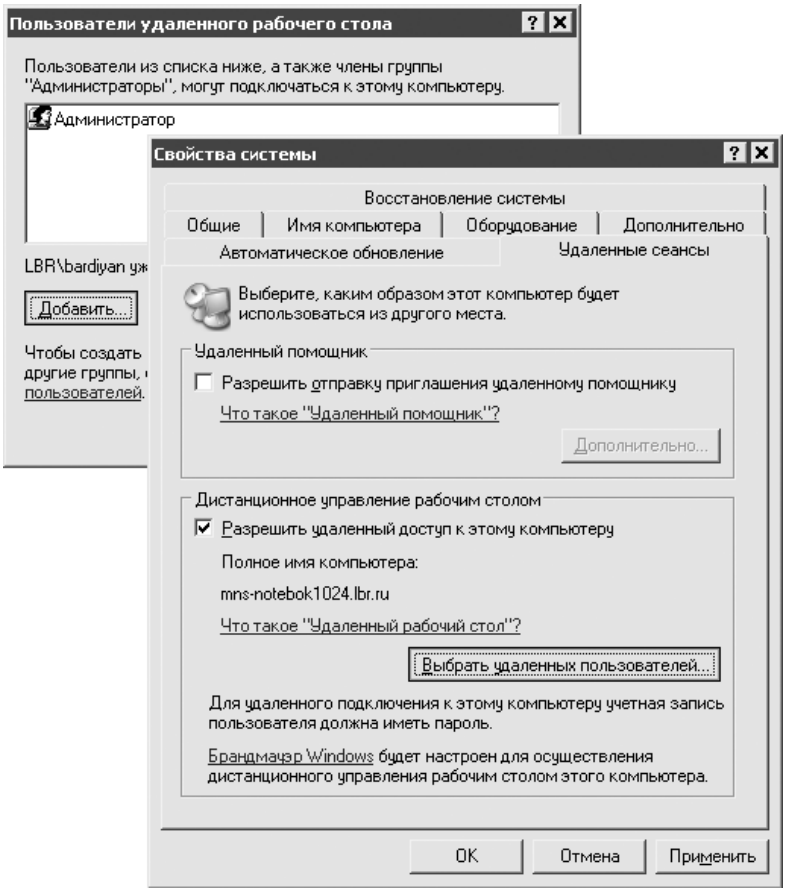


Рис. 11.15. Выбор удаленных пользователей

Теперь на своем компьютере (обязательно с установленной операционной системой Windows XP) запустите клиент: откройте меню **Пуск ▸ Программы ▸ Стандартные ▸ Связь ▸ Подключение к удаленному рабочему столу** (либо выполните команду `mstsc` в меню **Пуск ▸ Выполнить**). Останется только указать имя компьютера или его IP-адрес и произвести настройки с помощью кнопки **Параметры** (рис. 11.16).

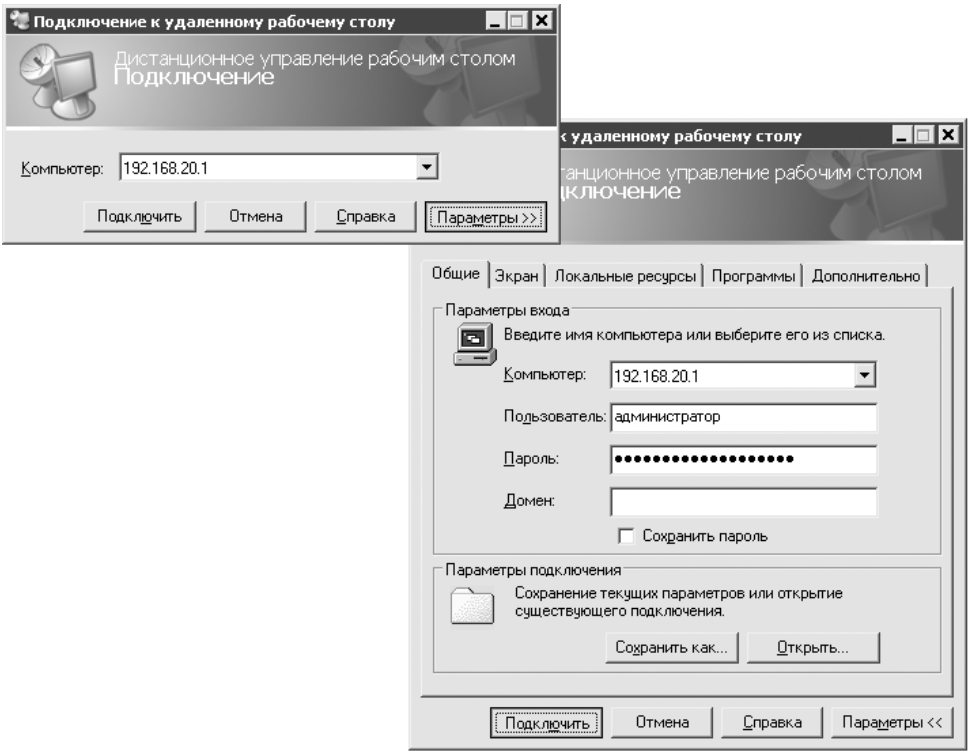


Рис. 11.16. Сокращенный и расширенный режимы службы подключения к удаленному Рабочему столу

На вкладке **Общие** укажите имя или IP-адрес компьютера, к которому собираетесь подключиться, и пароль.

На вкладке **Экран** задайте разрешение экрана удаленного **Рабочего стола** и выберите цветовую палитру. Чем меньше указанные значения, тем быстрее будет осуществляться передача данных и, соответственно, работа с компонентом **Удаленный рабочий стол**.

На вкладке **Локальные ресурсы** можно указать, следует ли воспроизводить звук удаленного компьютера на вашем и в каких случаях будет использоваться сочетание клавиш **Alt+Tab**. Обратите внимание на область настроек

Устройства. Здесь вы можете настроить некоторые интересные параметры. Если желаете, чтобы ваши локальные диски отображались в **Проводнике** удаленного компьютера (в таком случае удобнее копировать файлы), то установите флажок **дисковые устройства**. Чтобы можно было печатать на своем локальном принтере прямо с удаленного компьютера, установите флажок **принтеры**.

На вкладке **Программы** можно указать, если в этом есть необходимость, какую программу следует запускать на удаленном компьютере при подключении к нему.

Чем выше пропускная способность вашей сети, тем комфортнее можно будет выполнять задачи на удаленном компьютере. Например, при скорости подключения 100 Мбит/с через удаленный **Рабочий стол** вполне можно слушать музыку (но этим все же лучше не увлекаться, поскольку данный инструмент предназначен для других целей). Если же вы вынуждены работать при более низких скоростях подключения (модем, 10-мегабитная сеть или Wi-Fi), то придется позаботиться об оптимизации настроек. Поможет в этом вкладка **Экран**, о которой уже было сказано, а также вкладка **Дополнительно**, на которой можно отказаться от некоторых эффектов (анимации, использования тем оформления, фонового рисунка), что тоже уменьшит нагрузку на сеть.

Чтобы не приходилось каждый раз в случае возникновения необходимости настраивать параметры подключения, нажмите кнопку **Сохранить как** на вкладке **Общие** и сохраните файл `Default.rdp` в папке **Мои документы**.

Кстати, при двойном щелчке кнопкой мыши на файле с расширением RDP автоматически будет запускаться **Подключение к удаленному рабочему столу** с параметрами, записанными в открываемом файле. Пользоваться этим удобно, если часто возникает необходимость подключаться к нескольким компьютерам. В таком случае создайте для каждого подключения свой RDP-файл (редактировать их можно не только инструментом **Подключение к удаленному рабочему столу**, но и в текстовом виде **Блокнотом**). Разместив RDP-файлы в одной папке и дав им соответствующие имена, можно вынести данную папку на **Панель задач** (рис. 11.17).

При осуществлении соединения у вас создается полное ощущение входа в Windows — даже проигрывается характерная мелодия. Пользователь, работавший в это время за компьютером, остается не у дел — его сессия принудительно завершается и компьютер блокируется. Теперь вы хозяин. Дальнейшая работа почти ничем не отличается от той, если бы вы сидели непосредственно перед компьютером.

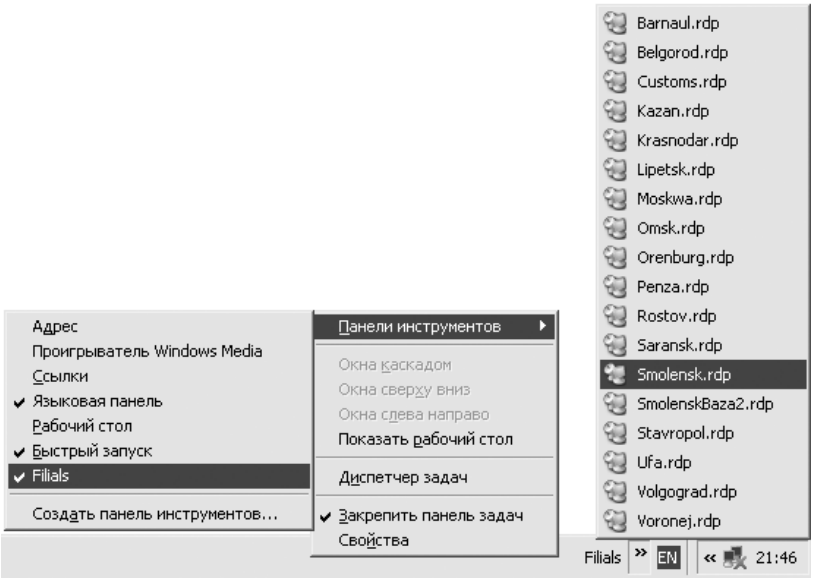


Рис. 11.17. Использование нескольких RDP-файлов

На этом краткое знакомство с **Удаленным рабочим столом** можно считать законченным — инструмент простой и, чтобы им пользоваться, особых навыков не требует.

Более мощное управление

Администраторы для работы с компьютерами пользователей предпочитают применять более мощный коммерческий инструмент под названием DameWare NT Utilites (**www.dameware.com**). Описание его возможностей выходит за рамки данной книги. Чтобы почувствовать функциональные преимущества этой программы перед **Удаленным рабочим столом**, просто взгляните на рис. 11.18.

Как выключать и перезагружать компьютер через сеть?

Чтобы перезагрузить компьютер, подходить к нему совсем не обязательно, достаточно просто выполнить в консоли команду `shutdown -s -m \\имя_удаленного_компьютера`. Если на удаленном компьютере установлена система Windows 2000/XP, то результатом будет выключение (ключ `-s`). Чтобы перезагрузить компьютер, воспользуйтесь ключом `-r`. Кроме того, можно установить таймер (`-t`) и ввести сообщение (`-c`). Например, команда `shutdown -r -m \\компьютер -t 60 -c "кто не сохранился, я не виноват"` от-

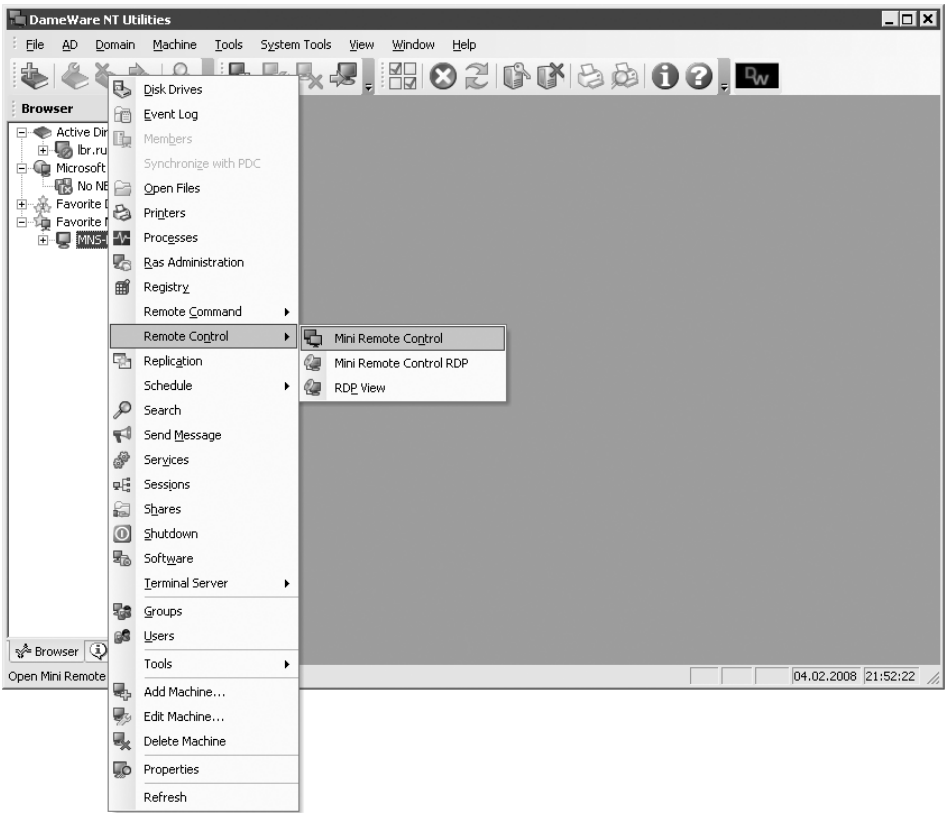


Рис. 11.18. Главное окно программы DameWare NT Utilites

кроет у пользователя на компьютере окно с соответствующим сообщением (рис. 11.19) и перезагрузит удаленный компьютер через 60 секунд. Кстати, открывающееся при этом окно идентично тому, которое создавал знаменитый вирус MSBlaster.

Команда `shutdown -i` сопровождает завершение работы графическим интерфейсом.

Чтобы разрешить обычным пользователям применять все возможности команды `shutdown`, запустите оснастку **Локальная политика безопасности** (откройте меню **Пуск ▸ Настройка ▸ Панель управления ▸ Администрирование ▸ Локальная политика безопасности** или в меню **Пуск ▸ Выполнить** выполните команду `secpol.msc`) и в разделе **Локальные политики ▸ Назначение прав пользователя ▸ Принудительное удаленное завершение** добавьте пользователя, которому хотите разрешить удаленно завершать работу этого компьютера.

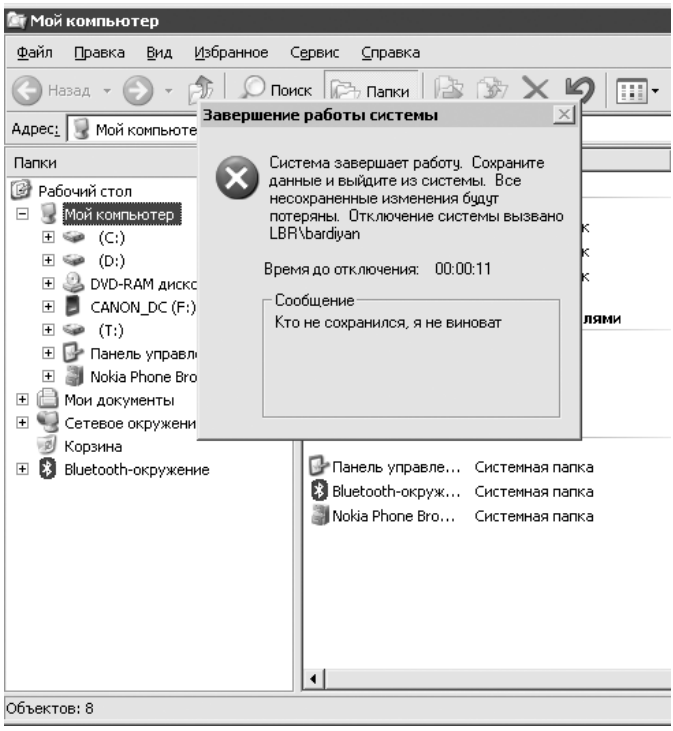


Рис. 11.19. Так выглядит экран у компьютера, который удаленно выключают

Как создать собственное радио в локальной сети?

Для сетевой карты, 100-мегабитного кабеля и коммутатора нет абсолютно никакой разницы, какую информацию передавать: изображения, текстовые файлы или потоковое аудио. Поэтому для организации вещания в локальной сети понадобятся лишь пара программ и микрофон. На компьютере, с которого будет производиться вещание (сервере), голос будет оцифровываться, сжиматься и передаваться по сети. С музыкой еще проще — изначальный цифровой аудиопоток лишь подвергнется дополнительному сжатию. «Слушателям» понадобится только запустить на своих компьютерах Winamp и настроиться на нужную «волну». То есть все необходимое программное обеспечение и его настройка производятся на сервере. Вот список того программного обеспечения, с которым придется иметь дело.

- SHOUTcast Server (есть на прилагаемом компакт-диске и на сайте **www.shoutcast.com**) или, в качестве альтернативы, IceCast (**www.icecast.org**) — программа-сервер, к которой будут осуществлять подключение пользователи, желающие послушать ваше радио.

- Проигрыватель Winamp (**www.winamp.com**) и SHOUTcast DSP Plug-in for WinAMP (**www.shoutcast.com**) — дополнения, которые будет передавать серверу потоковые данные от проигрывателя, а он, в свою очередь, перенаправлять их клиентам-слушателям. Надо отметить, что разыс-кать SHOUTcast DSP Plug-in for WinAMP на сайте производителя оказалось сложнее, чем можно было предположить. Поэтому он размещен на прилагаемом к книге компакт-диске.
- SAM Broadcaster (**www.spacialaudio.com**) — полноценная DJ-станция, которая обладает возможностями управления воспроизведением музыкальных дорожек и способна применять различные эффекты к ним. Либо как вариант — DJ Traktor (**www.native-instruments.com**).

Как уже отмечалось, от слушателей требуется только наличие проигрывателя Winamp.

Первым делом установите и запустите SHOUTcast Server, который и будет осуществлять непосредственно передачу медиаинформации с вашего компьютера в локальную сеть. Процесс его установки не представляет сложностей, поэтому он будет опущен.

Все настройки SHOUTcast Server производятся в файле конфигурации. Чтобы приступить к его изменению, в главном окне программы откройте меню **Edit config** (рис. 11.20).

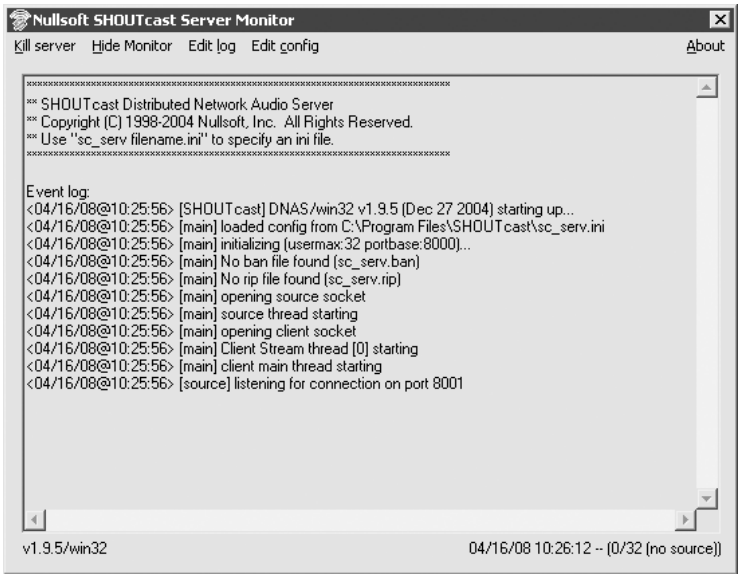


Рис. 11.20. Окно программы SHOUTcast Server

В текстовом редакторе **Блокнот** откроется файл `sc_serv.ini` (файл можно самостоятельно найти на диске и открыть с помощью того же файлового менеджера Far). У вас появится возможность изменить множество параметров, наиболее важные из них перечислены ниже.

- **MaxUser** — определяет максимальное количество подключений, то есть слушателей.
- **Password** — здесь указывается пароль для администрирования (локального и удаленного) через браузер. Кроме того, этот же пароль необходимо задать в настройках SHOUTcast DSP Plug-in для подключения к серверу. Крайне рекомендуется использовать надежный пароль длиной не менее девяти символов — хакеры не дремлют.
- **Port Base** — определяет порт вашего компьютера, к которому будут подключаться другие пользователи. По умолчанию он имеет значение `8000`, и лучше всего это значение не менять, так как можно ошибочно указать уже задействованный другой программой порт.

Чтобы сделанные настройки вступили в силу, перезапустите SHOUTcast Server.

ПРИМЕЧАНИЕ

Рассмотренный выше способ реализации потокового вещания в сети отнюдь не единственно возможный. Сделать свое «радио» в сети можно и с помощью Windows Media Encoder либо сервера jetCast (www.jetaudio.com), входящего в комплект проигрывателя JetAudio. Однако данные реализации не являются настолько распространенными на русскоязычной территории, как вещание на основе SHOUTcast Server.

Единственным программным продуктом, который может претендовать на звание достойного конкурента, можно назвать приложение IceCast (www.icecast.org). В чем его особенности? SHOUTcast Server поддерживает только вещание в формате MP3, в то время как IceCast способен работать со множеством форматов, в том числе и OGG. Помимо этого, в IceCast реализована поддержка неограниченного количества вещающих каналов (у SHOUTcast только один). Очень важное отличие IceCast — открытый код. Если вам не хватает каких-либо функций или вы нашли ошибку, то вправе самостоятельно изменить исходные коды по своему вкусу. В ShoutCast это невозможно. Тем не менее IceCast гораздо менее распространен у провайдеров, и для вещания в Глобальной сети приходится обзаводиться собственным сервером. Решение это достаточно дорогое, и, кроме того, для его реализации требуется помощь опытного системного администратора, способного выполнить настройку. IceCast обратно совместим с SHOUTcast и может использоваться в описанной выше связке без внесения изменений в другие программы.

Установка SHOUTcast DSP Plug-in тоже не представляет никаких сложностей — она производится автоматически в папку Winamp. Для настройки приложения

запустите Winamp, нажмите сочетание клавиш **Ctrl+P** или щелкните кнопкой мыши на левом верхнем углу проигрывателя и далее в открывшемся меню выберите пункт **Preferences**. В открывшемся окне **Winamp Preferences**, используя древовидное меню, перейдите по адресу **Plug-ins ▸ DSP Effect** и в правой части окна два раза щелкните на названии **Nullsoft SHOUTcast Source DSP** (рис. 11.21).

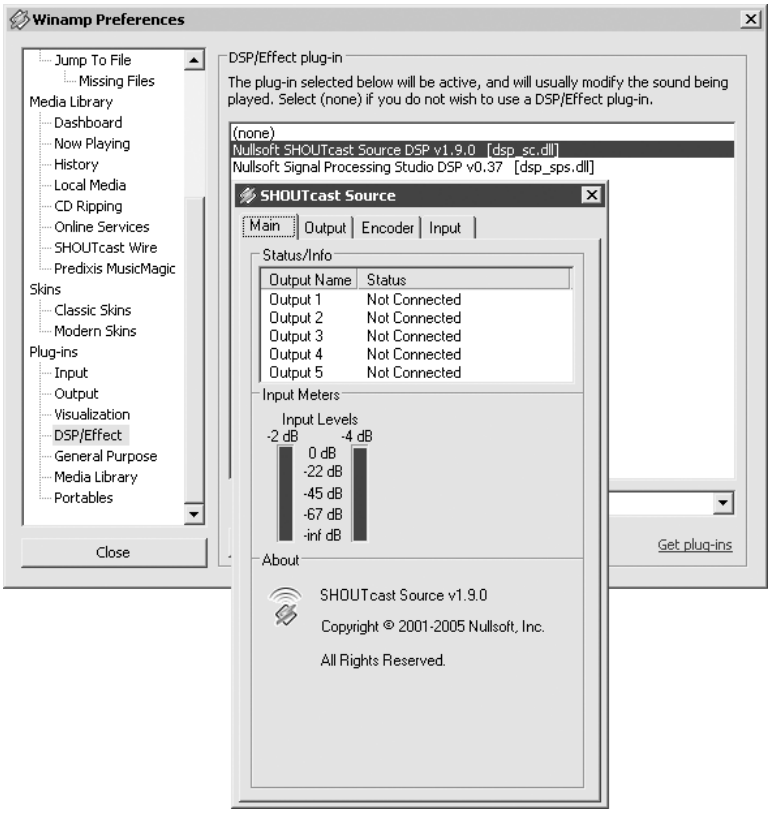


Рис. 11.21. Главные настройки SHOUTcast DSP Plug-in

В окне SHOUTcast Source на вкладке **Main** будет отображаться количество ваших слушателей — здесь ничего не трогайте и переходите на вкладку **Output** (рис. 11.22). В поле **Password** укажите тот же пароль, который вы указывали в соответствующем параметре при настройке SHOUTcast Server. То же самое сделайте и с полем **Port**.

В строке **Address** можно указать IP-адрес компьютера, на котором установлен SHOUTcast Server. Поскольку в данном случае SHOUTcast Server и SHOUTcast DSP Plug-in установлены на одном компьютере, редактировать это поле нет необходимости, оставьте как есть — `localhost`.

Вкратце об остальном. Установив флажок **Automatic Reconnection on Connection Failure**, вы укажете на необходимость автоматически восстанавливать связь после разрыва соединения. В поле **Reconnection TimeOut** можно указать величину временной задержки перед следующей попыткой связи с сервером. Лучше оставить как есть.

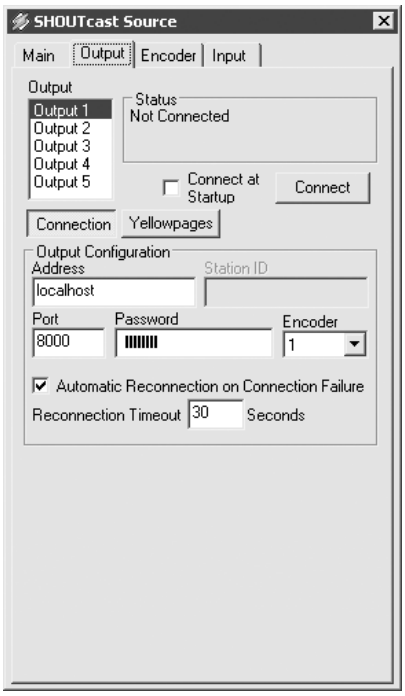


Рис. 11.22. Настройка SHOUTcast DSP Plug-in

Теперь нажмите кнопку **Yellowpages**. Самое время задумчиво почесать затылок, стимулируя воображение. Дело в том, что здесь предлагается вписать различную информацию о станции, а именно: ее название (поле **Description**); адрес станции (**URL**); жанр, в котором идет вещание (**Genre**), и ICQ-номер диджея (в данном случае ваш). В нижней части окна вы можете активировать функцию отображения информации о композиции, содержащейся в тегах файла, установив флажок **Enable Title Updates**, а также указать на необходимость опубликования информации о вашей радиостанции в Интернете. С этим на начальной стадии не стоит торопиться, поскольку счет за исходящий трафик от провайдера не обрадует. В самом начале рекомендуется ограничить свои амбиции локальной сетью.

В окне конфигурации перейдите на вкладку **Encoder**. Здесь можно указать битрейт, который будет использоваться при вещании, а также режим: моно или стерео. Можно заранее задать до пяти различных условий трансляции, после чего переключаться между ними в зависимости от числа пользователей и скорости соединения.

На вкладке **Input** предлагается выбрать источник вещания (**Input Device**). Если, кроме музыки, размещать в эфире ничего не планируется, оставьте значение **Winamp (Reccomended)**. Если же вы собираетесь работать в эфире с микрофоном или транслировать звук из других источников, то выберите пункт **Soundcard Input**. Внизу появится список параметров, которые стоит рассмотреть подробнее. Нажав кнопку **Open Mixer**, вы откроете окно стандартного системного микшера. Кнопка **Push to Talk** необходима, для того чтобы, не прерывая звучания музыкальной композиции, использовать в эфире микрофон.

Кнопка **Lock** включает залипание клавиши **Push to talk**. Регулятор **Music Level** определяет уровень громкости воспроизведения основной фонограммы, регулятор **BG Music Level** — уровень громкости фоновой музыки при речевом эфире, регулятор **Mic Level** — уровень громкости микрофона, а регулятор **Fade Time** — скорость снижения или нарастания уровня громкости во время перехода из одного режима в другой.

На деле все происходит следующим образом: во время звучания музыкальной композиции нажмите кнопку **Push to talk**. Громкость звучащей музыки понизится до установленного с помощью параметра **BG Music Level** уровня с одновременным повышением уровня громкости микрофона (параметр **Mic Level**). После завершения речевого сообщения отпустите кнопку **Push to talk**.

На этом настройку SHOUTcast DSP Plug-in можно считать законченной. Возвратитесь на вкладку **Output** и нажмите кнопку **Connect** (программа SHOUTcast Server должна быть запущена). Вещание начнется.

Как вы могли понять, SHOUTcast Server позволяет осуществлять удаленное администрирование. Введите в браузере адрес `IP-адрес_сервера:порт` (например, `192.168.1.100:8000`) и щелкните на ссылке **Admin**. Вы попадете в меню администратора, если, правда, предварительно правильно укажете имя пользователя и пароль (тот, который указали в файле конфигурации сервера). Здесь вы сможете отключать пользователей, просматривать LOG-файл сервера, а также бронировать места на сервере для определенного IP-адреса.

Инструкцию по установке SHOUTcast Server на Linux вы найдете по адресу **www.nixp.ru/articles/shoutcast_linux**.

В принципе, описанного выше достаточно для начала «радиотрансляции»: в эфире будет играть музыка и разговаривать диджей. Однако на настоящем радио в студии работает еще и звукорежиссер, который выполняет сведение треков, добавляет различные эффекты (например, аплодисменты, смех), регулирует окраску звучания голоса ведущего и т. п.

Раз уж вы собрались делать свое радио, то и вам без всего этого никак нельзя. В роли громоздкого и очень дорогого звукорежиссерского пульта может выступать программа SAM Broadcaster (**www.spacialaudio.com**), а функции звукорежиссера вполне может выполнять и диджей.

Приложение SAM Broadcaster (рис. 11.23) считается самым прогрессивным по своим возможностям. Это целый аудиокомплекс, который может работать как в ручном, так и в автоматическом режиме, с поддержкой возможности удаленного заказа композиций слушателями через веб-интерфейс.

Рис. 11.23. Окно программы SAM Broadcaster

Для работы программы требуется наличие установленной на компьютере одной из следующих баз данных: FireBird, PostgreSQL, MS SQL или MySQL. По причине бесплатности и наибольшей распространенности среди домашних пользователей последней процесс установки будет рассмотрен на ее примере.

Сначала вам потребуется скачать с сайта **www.mysql.com** пакет MySQL Server Full (около 38 Мбайт). Затем с сайта **www.spacialaudio.com** — полную версию (не перепутайте с «патчем») SAM Broadcaster MySQL (еще около 58 Мбайт).

Имейте в виду, что если вам нужен веб-интерфейс, то для его реализации потребуется установка связки MySQL, Apache и PHP. Но этот вариант рассматриваться не будет.

Итак, первым делом установите MySQL Server, затем SAM Broadcaster, который создаст базу с названием SAMDB.

Обратите внимание, что SAM Broadcaster выступает заменителем SHOUTcast DSP Plug-in вместе с Winamp и самостоятельно подключается к серверу вещания, будь то SHOUTcast Server, ICEcast или Windows Media Encoder.

Таким образом, на качественном сервере радиовещания потребуются только SAM Broadcaster и SHOUTcast Server.

От слов к делу. Сначала необходимо запустить SHOUTcast Server (процесс его настройки был рассмотрен чуть выше), и только после этого можно запускать SAM Broadcaster.

После запуска программы от обилия функций кружится голова и минут десять уходит на то, чтобы просто все просмотреть, попытаться свести несколько песен, прослушать FX-эффекты и беспорядочно понажимать различные кнопки. Только утолив жажду эмпирического познания, можно спокойно приступить к конфигурированию.

Настроек у программы огромное количество, но рассмотрены будут лишь самые необходимые.

Первым делом откройте меню **Window ▸ Encoders**. В открывшемся окне нажмите кнопку с изображением крестика и выберите кодек (в данном случае это будет MP3). Далее откроется окно, в котором на вкладке **Converter** вы можете указать настройки кодека: выбрать битрейт и определить режим вещания (моно или стерео).

Кроме того, для настройки предлагается использовать предустановленные значения из раскрывающегося списка: **CD Quality**, **Radio Quality**, **Telephone Quality**.

На вкладке **Server Details** вы можете выбрать тип используемого сервера вещания (в рассматриваемом случае это SHOUTcast). Далее идут поля, необходимые для указания параметров подключения к нему.

- **Server IP** — здесь указывается адрес компьютера, на котором установлен и работает вещающий сервер. Если он находится на одном компьютере с программой SAM Broadcaster (как в данном случае), то используйте значение `localhost`.
- **Server Port** — здесь нужно указать порт, через который производится трансляция вещания (в данном случае `8000`, если вы не меняли это значение в настройках SHOUTcast Server).
- **Password** — используется для указания административного пароля для доступа к SHOUTcast Server.

Раздел **Station Details** содержит в себе информацию о вашей станции, которая частично будет отображаться проигрывателями слушателей и на веб-интерфейсе.

ПРИМЕЧАНИЕ

На одном MP3-формате мир не держится. Есть и другие, открытые, форматы, например OGG Vorbis. Формат OGG разрабатывался исходя из уже известных достоинств и недостатков MP3. В данном формате корректно работает вещание в режиме VBR (с переменным битрейтом), кроме того, в OGG изначально в качестве основной кодировки тегов использовался unicode, а не latin-1, что позволяет забыть о головной боли, вызываемой кодировками в тегах песен.
Однако, пожалуй, главным достоинством формата OGG является качество воспроизведения на минимальных битрейтах. Например, со значениями битрейта 24 или 32 Кбит/с OGG звучит почти как 96-кбитный MP3. Использование OGG на низких битрейтах — идеальное решение для тех пользователей, которые вынуждены работать с низкими скоростями подключения.

Закончив настраивать кодек, обратите внимание на главное окно программы SAM Broadcaster. На панели инструментов выберите любой из столов диджея (**Desktop A**, **Desktop B** или **Desktop C**) — каждый из них имеет свои преимущества.

В окне **Playlist** нажмите кнопку с изображением знака «плюс» и добавьте новые файлы в список воспроизведения. Этот список хранится в MySQL-базе. Чтобы его воспроизвести, композиции нужно поставить в очередь на воспроизведение в окно **Queue**. Сделать это можно путем перетягивания композиции из списка воспроизведения в окно очереди либо просто с помощью клавиши **Enter**, предварительно выделив название композиции. Чтобы выделить все композиции сразу, нажмите сочетание клавиш **Ctrl+A**.

Добавив файлы, нажмите на панели **Deck A** или **Deck B** кнопку воспроизведения, чтобы начать вещание, при этом вы сами будете слышать то, что вещаете. Теперь любой подключившийся к вашему серверу будет принимать трансляцию.

Ниже рассмотрены некоторые наиболее полезные звуковые эффекты, которые позволяет создать SAM Broadcaster:

- **Fading** — добавляет настраиваемое плавное снижение громкости в конце воспроизводимого трека и плавное ее нарастание в начале следующего музыкального фрагмента, сопровождающееся наложением этих участков друг на друга в заданном интервале времени;
- **Gap Killer** — автоматический пропуск пауз в записи при воспроизведении.

Чтобы ознакомиться с остальными настройками программы, откройте меню **File ▸ Config**. Здесь вы сможете настроить работу перечисленных только что звуковых эффектов (пункты **Crossfading** и **Gap killer**), установить правила повторения музыкальных композиций (**Playlist rotation rules**): какое время не проигрывать композиции одного исполнителя и минимальный интервал, через который может повториться песня. Опытным пользователям подобных программ наверняка пригодится пункт **Audio mixer pipeline**, воспользовавшись

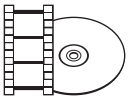
которым можно настроить работу аудиомикшера. Должен признаться, что для человека, не посвященного в звукорежиссуру, это настоящие дебри.

Чтобы подключиться к вашей радиостанции, пользователям потребуется совсем немного усилий:

- запустить Winamp;
- нажать кнопку **Add** и выбрать в открывшемся меню команду **Add URL**;
- в открывшемся окне указать IP-адрес сервера и через двоеточие порт, например `192.168.1.100:8000`.

Есть и более простой способ: разошлите потенциальным слушателям ссылку вида **IP-адрес_сервера:порт/listen.pls**. При щелчке кнопкой мыши на ней автоматически будет запускаться Winamp.

Если прослушать радио не получается, проверьте работоспособность радиосервера. Для этого достаточно набрать в стоке адреса браузера IP-адрес компьютера, на котором установлен этот сервер, и порт. На открывшейся странице вы увидите информацию, которая была занесена в настройки SHOUTcast DSP Plug-in.



ВИДЕОКУРС

На компакт-диске, прилагаемом к книге, вы найдете видеоурок «Урок 18. Создание радио в локальной сети», демонстрирующий возможности описанных в разделе программ для создания собственного радио.

Сетевые радиостанции скажут свое веское слово уже в ближайшие годы. В связи с повсеместным распространением беспроводных сетей Интернет может стать доступным всюду — дома, в автомобиле, на даче, а вместе с Интернетом станут доступны и сетевые радиостанции. Тогда FM-станциям придется серьезно потесниться, чтобы освободить место под солнцем для выросших в условиях домашних локальных сетей коллег.

ПРИМЕЧАНИЕ

Для сетевого вещания обычно используются битрейты 192, 128, 96, 64, 32 и 24 Кбит/с. Самый популярный формат вещания — MP3. Следует отметить, что на битрейтах ниже 64 Кбит/с MP3 звучит далеко не лучшим образом. Посему если приходится вещать со скоростью 32 или 24 Кбит/с, используется вещание в режиме моно, что позволяет экономить половину пропускной способности для небольшого повышения качества. Что же насчет трафика? В среднем при работе станции с пропускной способностью потока 128 Кбит/с фактически каждый компьютер слушателя непрерывно скачивает с сервера файл со скоростью 16 Кбайт/с, или 960 Кбайт/мин, или 56 Мбайт/ч. То есть за один час прослушивания вы расходуете примерно 56 Мбайт сетевого трафика. При использовании более низких битрейтов суммарный трафик пропорционально уменьшится: 28 Мбайт для скорости 64 Кбит/с и 14 Мбайт для скорости 32 Кбит/с.

Не работает сеть, что делать?

Проверка настроек

В компоненте **Панель управления ▸ Система** на вкладке **Имя компьютера** обратите внимание на имя компьютера и название рабочей группы: у каждого компьютера в домашней сети должно быть уникальное имя, а название рабочей группы (если не используется домен) должно совпадать. При написании имени компьютера и названия рабочей группы лучше использовать заглавные латинские буквы — это поможет избежать целого ряда проблем. Не используйте имена длиной более 15 знаков (это относится и к общим папкам), также не включайте в них пробелы и другие спецсимволы.

Проверить настройки сетевого соединения можно с помощью компонента **Сетевые подключения Панели управления**. Здесь щелкните правой кнопкой мыши на значке активного соединения и в открывшемся меню выберите команду **Свойства**. В открывшемся окне на вкладке **Общие** проверьте, чтобы здесь были установлены следующие сетевые компоненты.

- **Клиент для сетей Майкрософт**. Если его нет, нажмите кнопку **Установить** и добавьте его.
- **Служба доступа к файлам и принтерам сетей Майкрософт**. Эта служба обеспечивает сетевой доступ к файлам и принтерам данного компьютера.
- **Протокол TCP/IP**. Если данный пункт отсутствует, нажмите кнопку **Установить** и добавьте его.

Если вы нашли компонент, отсутствующий в этом списке, лучше его отключите. Чтобы было удобнее контролировать поведение сети, установите флажки **При подключении вывести значок в область уведомлений** и **Уведомлять при отсутствующем или ограниченном подключении**.

Теперь нужно проверить настройки непосредственно протокола TCP/IP. В соответствии с конфигурацией вашей сети либо задайте явным образом в его настройках IP-адрес и маску подсети, либо используйте функцию автоматического присвоения (если у вас доменная организация сети). Удостоверьтесь, чтобы маски подсети на всех компьютерах вашей сети совпадали, а IP-адрес у каждого был уникальным. Нажмите кнопку **Дополнительно**, в открывшемся окне перейдите на вкладку **WINS** и, если вам необходимо обращаться к другим машинам сети по имени, установите переключатель **Параметры NetBIOS** в положение **Включить NetBIOS через TCP/IP**. Это несколько снизит скорость работы сети и ослабит безопасность, но для начинающих пользователей лучше оставить этот пункт активным.

Вернитесь к окну свойств сетевого подключения. Справа от названия вашей сетевой карты должна быть кнопка **Настроить**. Нажмите ее — откроется окно свойств сетевой карты. Перейдите на вкладку **Дополнительно**, в списке **Свойство** выберите параметр **Link Speed & Duplex** и попробуйте поэкспериментировать с его значениями — возможно, поможет принудительная установка режима **100 Mbps/Full Duplex** или **100 Mbps/Half Duplex** вместо режима автоматического определения скорости. Либо попробуйте понизить скорость, установив, например, значение **10 Mbps/Full Duplex** или **10 Mbps/Half Duplex**.

Решение проблем

В Windows XP/2003 стек протоколов TCP/IP считается компонентом ядра операционной системы и для его переустановки используется консольная команда `netshell`. В случае появления необъяснимых проблем с сетью можно воспользоваться командой `netsh int ip reset c:\reslog.txt`. Ее выполнение обеспечит возвращение стека в состояние, в котором он был сразу после установки системы, а файл журнала `reslog.txt` покажет, какие изменения при этом произошли.

Повреждения или удаления системных файлов могут вызвать множество сбоев, начиная с отключения вкладки **Доступ** в свойствах папок и заканчивая появлением сообщений об ошибках. Для проверки файлов необходимо выполнить команду `sfc /scannow`.

Правой кнопкой мыши щелкните на значке активного сетевого соединения и в открывшемся меню выберите команду **Исправить**.

Один из основных инструментов, используемых для выяснения причин сбоев, — команда `ping`. Она позволяет получить информацию о работоспособности сети, а также убедиться в том, что нет разрывов кабеля и работает стек TCP/IP. Для ее выполнения введите в командной строке команду вида `ping 192.168.1.5` — после ее выполнения вы узнаете, за какое время был получен отклик от машины с IP-адресом 192.168.1.5. Если время отклика велико, то, скорее всего, вы имеете дело с аппаратными проблемами: некачественный или слишком длинный кабель, перегибы и т. д. Проверьте подобным образом связь со всеми IP-адресами, чтобы выявить проблемные участки. Если же не работает команда `ping 127.0.0.1`, то проблема в вашей системе и стеке протоколов TCP/IP. Попробуйте его переустановить с помощью команды `netshell`.

Если другие пользователи не могут получить доступ к вашему компьютеру по сети, в меню **Пуск ▸ Настройка ▸ Панель управления ▸ Администрирование** запустите оснастку **Локальная политика безопасности**. Далее перейдите по дереву

настроек в раздел **Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Назначение прав пользователя**. Здесь два раза щелкните кнопкой мыши на названии политики **Доступ к компьютеру из сети** и в открывшемся окне добавьте пользователя **Гость**, а из политики **Отказать в доступе к компьютеру из сети** пользователя **Гость** удалите. Затем выполните в меню **Пуск ▸ Выполнить** команду `compmgmt.msc`, перейдите в раздел **Локальные пользователи и группы ▸ Пользователи**, щелкните два раза кнопкой мыши на имени пользователя **Гость** и в открывшемся окне снимите флажок **Отключить учетную запись**.

Встречаются ситуации, когда в Windows XP папка **Сетевые подключения** вдруг оказывается пуста или не удается создать новое сетевое соединение. Решить проблемы можно одним из следующих способов: установив в систему обновления Q329441; запустив вручную службы **Telephony** и **Remote Access Connection Manager** и выставив для них режимы автоматического запуска; войдя в систему с правами администратора; или перерегистрировав несколько системных библиотек командами `regsvr32 netshell.dll`, `regsvr32 netcfgx.dll`, `regsvr32 netman.dll` и `regsvr32 ole32.dll`.

Что выбрать: домен или рабочую группу?

В контексте локальной сети домен служит для централизованного хранения учетных записей пользователей и политик безопасности. Используя доменную систему, удобнее управлять компьютерами пользователей и доступом к ресурсам, поскольку в этом случае изначально реализована возможность централизованного администрирования.

Организация сети как рабочей группы заставляет администратора побегать, чтобы определить одинаковые настройки для каждого члена сети: несколько раз отредактировать политики безопасности, внести изменения в реестр. Такой подход крайне неэффективен. Единственным его достоинством является дополнительная физическая нагрузка во время такой беготни, позволяющая сэкономить на тренажерном зале. Но лучше не экономить, а делать все как следует: настроить контроллер домена и затем со спокойной совестью заниматься своими делами. В таком случае толку будет больше, да и чувство морального удовлетворения посетит наверняка. К тому же доменная организация выводит сеть на качественно новый уровень — делает ее более гибкой и настраиваемой.

Чем больше компьютеров в сети, тем более оправдан будет доменный способ организации сети. Возможно, для организации сети из 5–6 компьютеров нет

смысла проводить бессонные ночи за настройкой сервера, поэтому рабочая группа будет наиболее оптимальным решением по соотношению трудозатраты/эффективность. Но когда количество компьютеров в сети превысит два десятка, тут уже самое время задуматься о домене.

Как настроить прокси-сервер?

Процесс настройки будет проиллюстрирован на примере прокси-сервера Squid, пришедшего из урожайного на хорошие программы мира Unix-систем. Бесплатный, нетребовательный к ресурсам, но, несмотря на это, функциональный Squid представляет собой мощный программный продукт, на основе которого вы сможете создать настоящий сервер. Основные возможности, предоставляемые Squid:

- кэширование страниц;
- распределение канала по приоритетам;
- авторизация по IP- и MAC-адресам;
- блокирование доступа к нежелательным ресурсам по IP-адресам, фразам в адресе страницы, заголовке;
- подключаемые модули удаления баннеров, подсчета статистики переданных/полученных данных.

Поначалу всякому пользователю, который привык к тому, что в операционных системах Windows большинство программ работает с использованием графического интерфейса, будет сложно, потому что, следуя традициям Unix-систем, работа с прокси-сервером Squid осуществляется посредством командной строки и все его настройки задаются в специальном конфигурационном файле — `squid.conf`. Честно говоря, вначале мне тоже было некомфортно работать с программой только через командную строку и конфигурационный файл. Но с течением времени я прочувствовал, насколько это удобно.

Процесс установки Squid незамысловат и прозрачен.

Распакуйте содержимое архива в папку с коротким именем, располагающуюся в корне диска. Рекомендуется использовать папку `c:\squid`.

Из папки `c:\squid\bin` выполните команду `squid.exe -i -n squid_nt`. Ключ `-i` обозначает, что будет проведена установка Squid в качестве службы Windows, а ключ `-n` присваивает ей название, которое будет отображаться в оснастке **Службы**. После выполнения этой команды служба будет сконфигурирована как автоматически загружаемая.

Теперь нужно указать настройки кэша в файле `squid.conf`. В папке `c:\squid\etc` находится файл `squid.conf.default` — удалите его расширение `default`, так чтобы получилось `squid.conf`. То же сделайте и с файлом `mime.conf.default`. Затем откройте файл `squid.conf` в текстовом редакторе, найдите в нем строку `cache_dir ufs c:/squid/var/cache 100 16 256` и уберите знак `#` (раскомментируйте ее). Теперь найдите строку `TAG: visible_hostname` и под ней напишите `visible_hostname myserver`.

Запустите службу `squid_nt` либо из оснастки **Службы** либо из консоли с помощью команды `net start squid_nt`.

ПРИМЕЧАНИЕ

Для отладки программы при возникновении ошибок запустите файл squid.exe с ключом –X либо проверьте содержимое файла squid.exe.log из папки sbin.

Минимальная настройка Squid тоже не отнимает много времени и не требует от головного мозга особых усилий. Все настройки указываются в файле `squid.conf`.

Для начала определите, какой порт будет «прослушивать» Squid на предмет поступления запросов от других компьютеров, и затем в файле `squid.conf` раскомментируйте строку `http_port`, указав в ней значение предпочитаемого порта, — это значит, что Squid будет работать на этом порту (значение можно изменить по своему усмотрению).

Одним из важнейших понятий в Squid является список контроля доступа (ACL или Access Control List). Его записи имеют следующий вид: `acl Olia src 192.168.1.4`. В результате добавления такой строки в файл `squid.conf` вы ассоциируете с именем `Olia` IP-адрес `192.168.1.4`. Теперь, чтобы разрешить доступ в Интернет компьютеру с этим IP-адресом, ниже допишите строку `http_access allow Olia`, а чтобы, наоборот, запретить — строку `http_access deny Olia`. Как правило, стандартной является ситуация, когда имеется группа компьютеров, которым нужно разрешить доступ в Интернет, а остальным — отказать в доступе. Решается данная задача добавлением в файл следующих строк (листинг 11.1).

Листинг 11.1. Разграничение прав доступа к Интернету

```
acl Privilege src 192.168.1.1-192.168.1.9
acl Oleg src 192.168.1.20
http_access allow Privilege
http_access allow Oleg
http_access deny all
```

Если описать это «человеческим» языком, то получится, что группа компьютеров с IP-адресами из диапазона от 192.168.1.1 до 192.168.1.9, а также машина с IP-адресом 192.168.1.20 получат доступ в Интернет. Остальным же в доступе будет отказано. В целях обеспечения безопасности рекомендуется, чтобы в конце всех инструкций `http_access allow` шла запретительная запись `http_access deny all`. Это значит, что для всех объектов, для которых не было указано разрешительной инструкции `http_access allow`, доступ нужно запретить.

Чтобы запретить пользователям доступ к определенным сайтам, потребуется сначала создать список доступа по доменному имени (команда `acl BlockSite dstdomain .anekdot.ru`) или IP-адресу сайта (команда `acl BlockSite dst 194.67.0.94`), а потом запретить этому списку доступ `http_access deny BlockSite`.

Как найти все сетевые папки в локальной сети?

Поможет в этом приложение LanScope (есть на прилагаемом компакт-диске и на сайте **www.lantricks.com**) — многопотоковый сканер сети (рис. 11.24). Программа

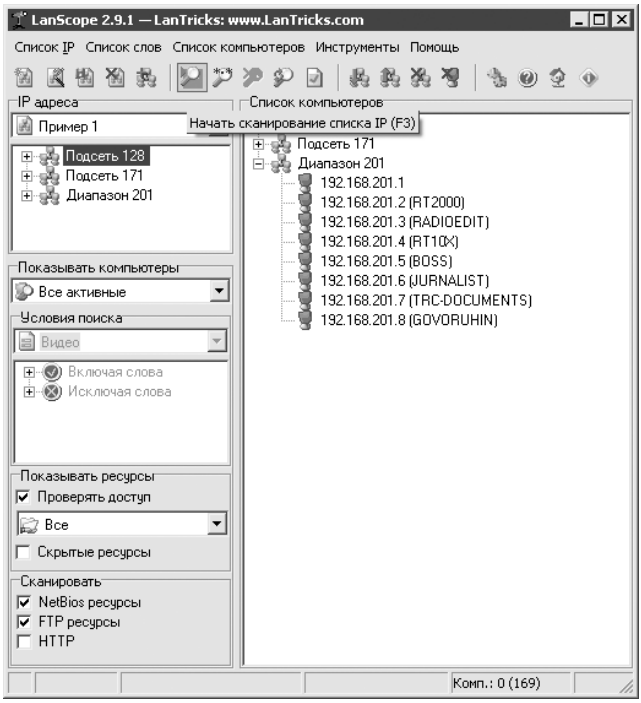


Рис. 11.24. Главное окно программы LanScope

позволяет осуществлять мониторинг сети на наличие доступных ресурсов NetBios (Samba), FTP и HTTP, сканируя заданные диапазоны IP-адресов, а также сообщает об установленных правах доступа к ресурсам: чтение или запись.

Сканер ресурсов может выполнять поиск и по заданному имени ресурса, например **music**, **video** и т. п.

Кроме того, может показаться интересной утилита LanSpy (**www.lantricks.com**) — это сканер безопасности, предназначенный для исследования сети. Он осуществляет сбор информации (рис. 11.25) о компьютере: позволяет узнать доменное и NetBios-имена ресурса, его MAC-адрес, тип используемых сетевых адаптеров, имена пользователей, настройки безопасности, определить наличие разделяемых ресурсов, сервисов, получить информацию из реестра и журнала событий.

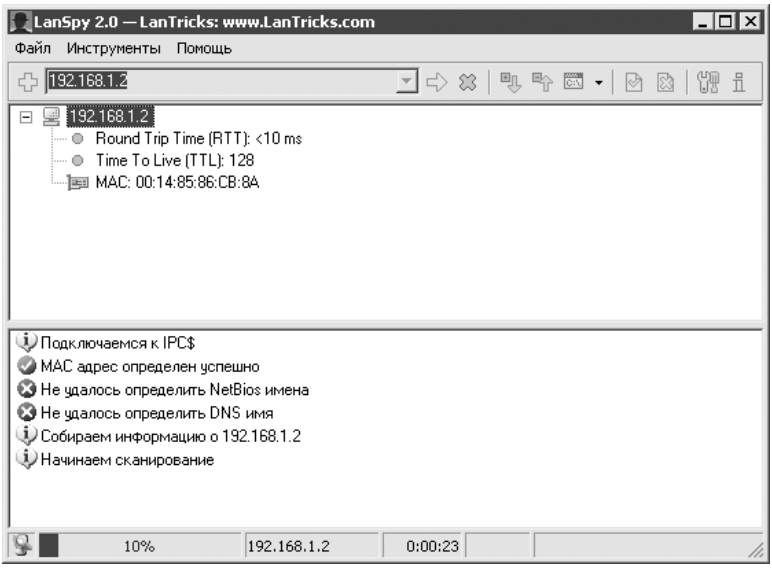


Рис. 11.25. LanSpy собирает информацию об удаленном компьютере

В программу также включен сканер, который определяет используемые сервисы на удаленном компьютере для открытых портов и собирает отклики для каждого сервиса.

Как ускорить копирование файлов через локальную сеть?

При копировании файлов большого размера в пределах локальной сети любой сбой может вызвать ошибку. В этом случае вам придется пережить несколько

неприятных минут и начать операцию сначала. Чтобы такого не произошло, можно попробовать воспользоваться программой KillCopy (есть на прилагаемом к книге компакт-диске и на сайте **www.killprog.com**), которая без проблем позволит исключить потерю копируемых данных в случае внезапного отключения связи и при ее восстановлении продолжит загрузку. Особенно полезной эта программа может оказаться при использовании в старых, не очень быстрых сетях.

Если выбрать в контекстном меню **Проводника** команду **KillCopy to** (рис. 11.26), откроется окно, в котором вам будет предложено указать целевой каталог копирования.

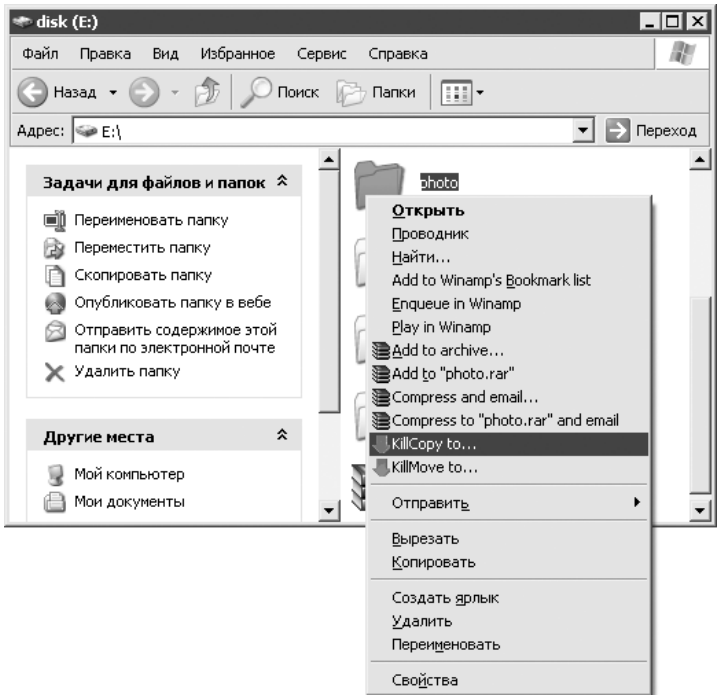


Рис. 11.26. KillCopy в контекстном меню Проводника

Сюда можно добавить несколько предпочитаемых адресов, куда вы обычно копируете файлы, для чего нужно лишь создать в папке `KillCopy\Favorites` текстовые файлы с расширением `lst`, содержащие пути копирования файлов. При следующем открытии окна эти файлы будут доступны как целевые папки, причем начать копирование можно, дважды щелкнув кнопкой мыши на целевом объекте.

Все хорошо, что хорошо качается...

Глава 12

Интернет

Как получить доступ к компьютеру друга и его папкам через Интернет?

Чтобы подключиться к удаленному компьютеру, необходимо, чтобы у него имелся реальный (обратите внимание!) IP-адрес и был открыт, например, порт 3389 (порт удаленного **Рабочего стола**). Если все это есть, на своем компьютере выполните из меню **Пуск** команду `mstsc`. Далее в открывшемся окне укажите IP-адрес компьютера друга, нажмите кнопку **Параметры** и на вкладке **Локальные ресурсы** установите флажок **дисковые устройства** (рис. 12.1) — это позволит копировать файлы удаленного компьютера через **Проводник** на свои диски. Обратите внимание, что вам также потребуется знать пароль администратора, который используется на компьютере друга.

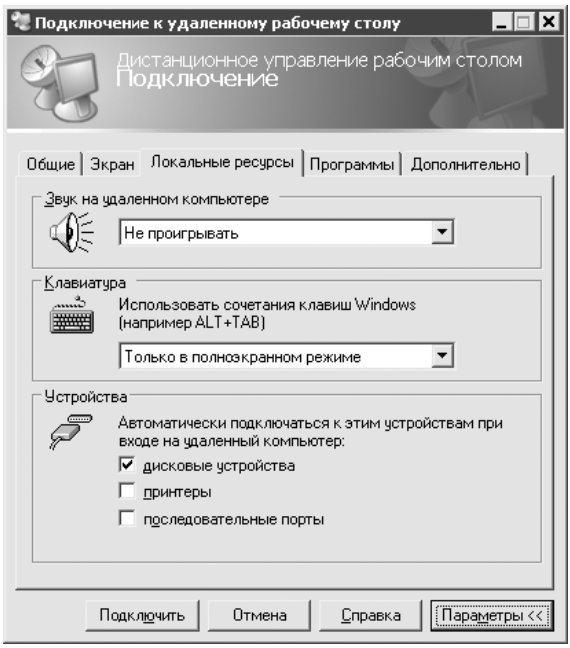


Рис. 12.1. Настройка удаленного Рабочего стола для обмена файлами

Есть и другой способ обмена файлами с другом, при котором вам не потребуется знать его пароль. Для этого достаточно лишь установить на компьютере друга веб-сервер (например, IIS или Apache) или FTP-сервер (например, FileZilla), а дальше вам просто нужно будет набрать в строке браузера IP-адрес товарища, у которого установлен один из предложенных серверов, и получить доступ к опубликованным веб-каталогам. Далее на примере веб-сервера IIS, поскольку он входит в состав пакета установки Windows (то есть

всегда под рукой) и наиболее прост в настройке, будет кратко проиллюстрирована работа по данной схеме.

Устанавливать IIS нужно на компьютере друга, и, соответственно, все настройки выполнять нужно на нем же. Прежде всего установите IIS в систему. Для этого откройте **Панель управления ▸ Установка и удаление программ** (или выполните команду `appwiz.cpl` в меню **Пуск ▸ Выполнить**). В открывшемся окне нажмите кнопку **Установка компонентов Windows**, которая расположена слева. В окне **Мастер компонентов Windows** установите флажок **Internet Information Services (IIS)** и нажмите кнопку **Далее** (рис. 12.2).

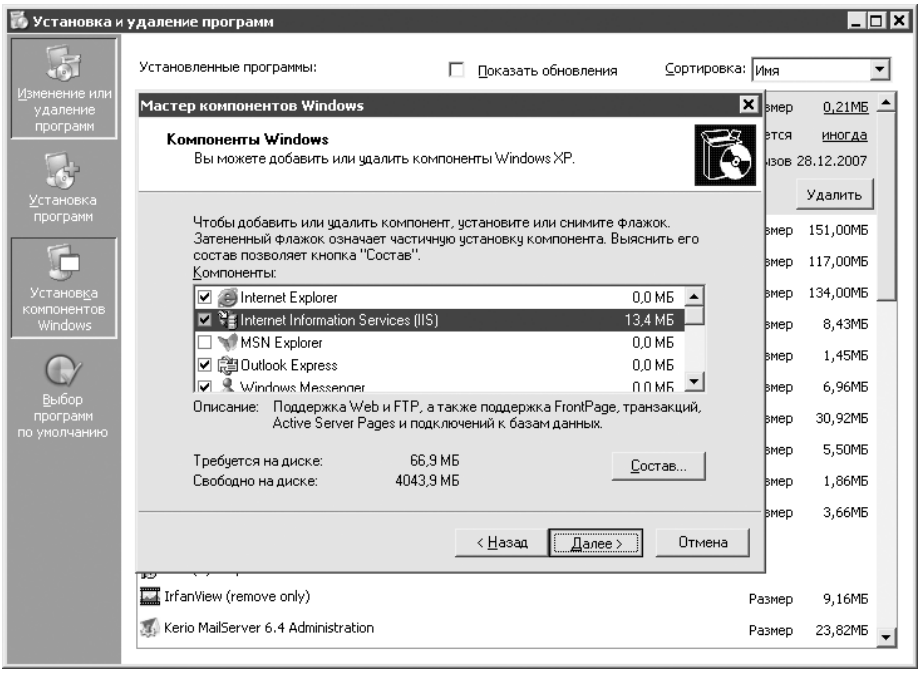


Рис. 12.2. Установка IIS

Установив IIS, откройте **Панель управления ▸ Администрирование ▸ Internet Information Services**. В левой части в древовидном меню выберите пункт **Веб-узел по умолчанию** и щелкните на нем правой кнопкой мыши. В открывшемся меню выполните команду **Создать ▸ Виртуальный каталог** (рис. 12.3). Запустится мастер, с помощью которого вы сможете сопоставить с выбранным вами псевдонимом любую папку на данном компьютере. Обратите внимание, что на последнем этапе при настройке прав доступа к папке следует установить флажок **обзор**. Например, если выбран псевдоним `download`, чтобы обратиться к нужной вам папке с удаленного компьютера, в браузере набери-

те `http://213.184.96.72/download`, где `213.184.96.72` — IP-адрес компьютера, на котором расположена папка.

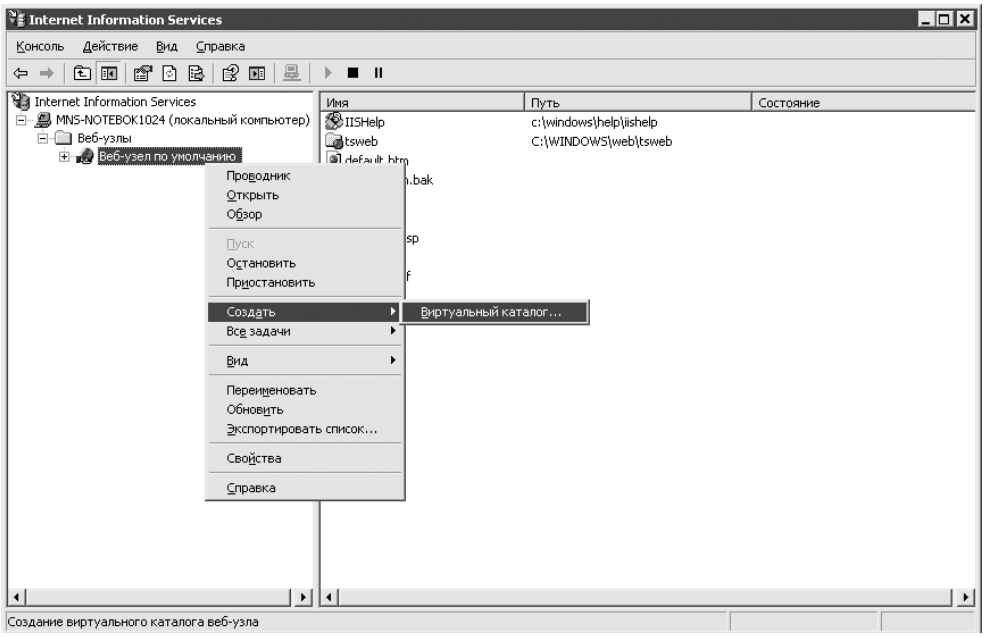


Рис. 12.3. Создание виртуального каталога в IIS

Произошла ошибка Internet Explorer с предупреждением, что приложение будет закрыто. Что делать, чтобы такая ошибка больше не возникала?

Такое сообщение иногда появляется при просмотре веб-страницы, содержащей ActiveX-компоненты. Решений может быть несколько.

- Для решения проблемы «на скорую руку» запустите Internet Explorer, откройте меню **Сервис ▸ Свойства обозревателя** и в открывшемся окне перейдите на вкладку **Безопасность**. Выберите зону **Интернет** и нажмите кнопку **Другой**. В списке параметров безопасности в группе **Элементы ActiveX и модули подключения** все переключатели установите в положение **Отключить** (рис. 12.4).
- Для решения данной проблемы, по заверениям Microsoft (**support.microsoft.com/kb/899812/**), также достаточно установить обновление 890923 либо Service Pack 2 для Windows XP.

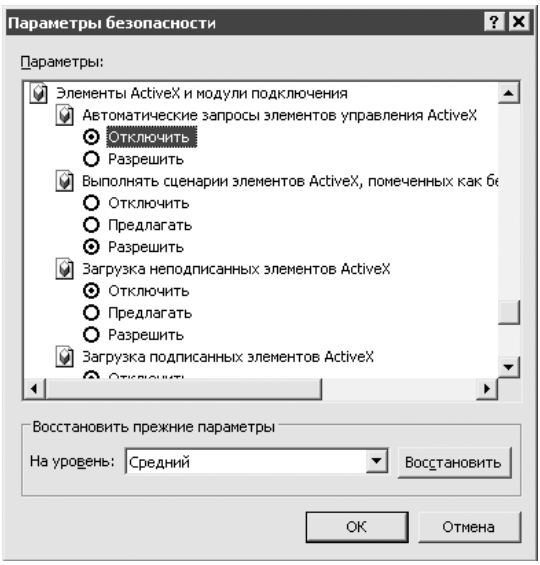


Рис. 12.4. Настройка параметров безопасности Internet Explorer

Internet Explorer сообщает об ошибке Не удается открыть страницу поиска. Если ввести IP-адрес сайта, то он открывается. В чем может быть причина?

Очень похоже, что проблема с настройками DNS-сервера. Убедитесь, что в настройках интернет-подключения у вас верно указан адрес DNS-сервера провайдера. Убедитесь также, что он отвечает (выполните команду `ping`). Нелишне будет и сбросить DNS-кэш командой `ipconfig /flushdns` в меню **Пуск ▸ Выполнить**.

При запуске Internet Explorer автоматически открывается какой-то сайт. Удаляю, а он появляется снова. Как избавиться от этого?

Некоторые разработчики сайтов пишут коды, которые записываются в реестр Windows и изменяют настройки Internet Explorer. В частности, при вводе в строку браузера адреса сайта вы можете обнаружить, что к нему добавляется дополнительный префикс (например, `http://www.gravedigger.com/redirect.php?`). Это значит, что все ваши обращения в Сеть проходят через сайт **www.gravedigger.com**, который таким образом повышает свою посеща-

емость либо собирает статистику и ваши пароли. Загрузка страниц в таком случае будет осуществляться медленнее, и вдобавок ко всему может еще и появиться какой-нибудь баннер. В общем, неприятно. Избавиться от такого явления можно, открыв реестр и перейдя в нем по адресу: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL`. Здесь внимательно просмотрите содержимое разделов `DefaultPrefix` и `Prefixes`. Если найдете адрес сайта **www.gravedigger.com**, тут же его удаляйте. Если в указанной ветви найти адрес не удалось, то попробуйте осуществить поиск по всему реестру (рис. 12.5).

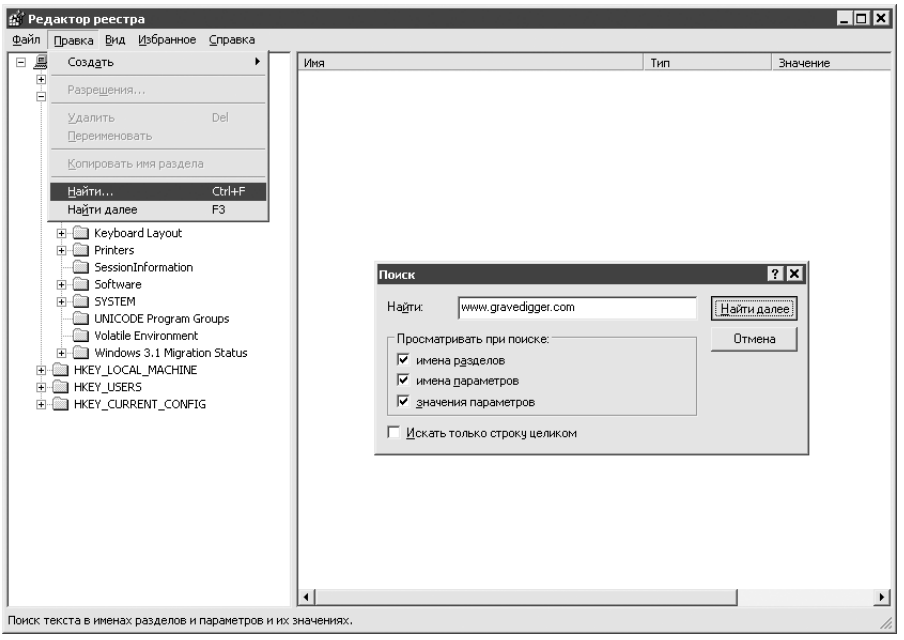


Рис. 12.5. Поиск адреса сайта в реестре

Попробуйте еще открыть меню Internet Explorer **Сервис ▸ Свойства обозревателя**, в открывшемся окне на вкладке **Общие** в области настроек **Временные файлы Интернета** нажмите кнопку **Удалить файлы**. Возможно, там и скрыт вредоносный код, запускающий страницу через некоторый интервал времени.

Есть еще один вариант решения проблемы — переустановка браузера Internet Explorer. Для этого в окне **Запуск программы** выполните команду `Rundll32.exe setupapi, InstallHinfSection DefaultInstall 132 %windir%\inf\ie.inf`. При этом не забудьте поместить компакт-диск с пакетом установки Windows XP/2000 в CD-привод. Если установочные файлы Windows находятся на жестком диске, путь к ним вы сможете указать, используя специальное окно, которое откроется в процессе установки.

Нелишне будет также просмотреть программы, которые указаны в списке автозагрузки (выполните команду `msconfig` в меню **Пуск ▸ Выполнить**), и удалить из него подозрительные. Только делайте это очень осторожно — можно удалить по незнанию что-то важное. Поэтому, прежде чем что-либо удалять, осуществите поиск по названию программы в Google — «мировой разум» подскажет, как следует поступить с сомнительной программой и за что она отвечает.

Как узнать при работе в Интернете свой IP-адрес или IP-адрес какого-нибудь сайта?

Узнать свой IP-адрес вы можете с помощью сайтов **www.2ip.ru** и **yoip.ru**. Узнать IP-адрес сайта (вернее, сервера, на котором он размещен) — с помощью команды `ping`. Если, к примеру, вас интересует адрес сайта **yandex.ru**, в консоли выполните команду `ping yandex.ru`.

Правда ли, что можно определять местоположение по IP-адресу?

Никого уже не удивляет, если пользователи из Москвы и Нью-Йорка на один и тот же поисковый запрос получают разные результаты. Давно известны факты, когда некоторые платежные системы отказывались работать с клиентами из стран СНГ. Это происходит без явного указания своего местоположения пользователем — все определяется автоматически, ведь зная IP-адрес, есть возможность обнаружить и географическое местоположение пользователя, а также определить имя его провайдера или работодателя. Кроме IP-адреса, существуют и другие средства; современные сервисы способны дополнительно отслеживать маршрут пакетов в Сети, чтобы уже по маршрутизаторам точно определить адрес (точность составляет 80 % для города и 99 % для страны). Большинство сервисов такого характера являются платными: **www.digitalenvoy.net**, **www.quova.com**, **www.akamai.com**, **www.ip2location.com**.

Просмотреть регистрационную информацию (о тех, кто купил пул IP-адресов, в который входит искомый) можно на сайте **www.ripe.net**. Данный ресурс бесплатен, однако следует иметь в виду, что регистрационная информация не всегда может соответствовать реальной ситуации. К примеру, провайдер, который в регистрационных данных указал свой московский офис, может предоставлять услуги интернет-доступа по всей России, и, если проверить IP-адрес пользователя из Владивостока, который обслуживается данным провайдером, на сайте **www.ripe.net**, можно будет подумать, что этот человек из Москвы, хотя это не так.

Страну определить можно в большинстве случаев точно, с вероятностью 99 %, за исключением случаев, когда речь идет о выделенных корпорациям вроде Intel, IBM, Microsoft и т. д. IP-адресах, филиалы которых находятся во всех странах мира.

Помочь в определении местоположения по IP-адресу также может программа VisualRoute (есть на прилагаемом к книге компакт-диске) (рис. 12.6).

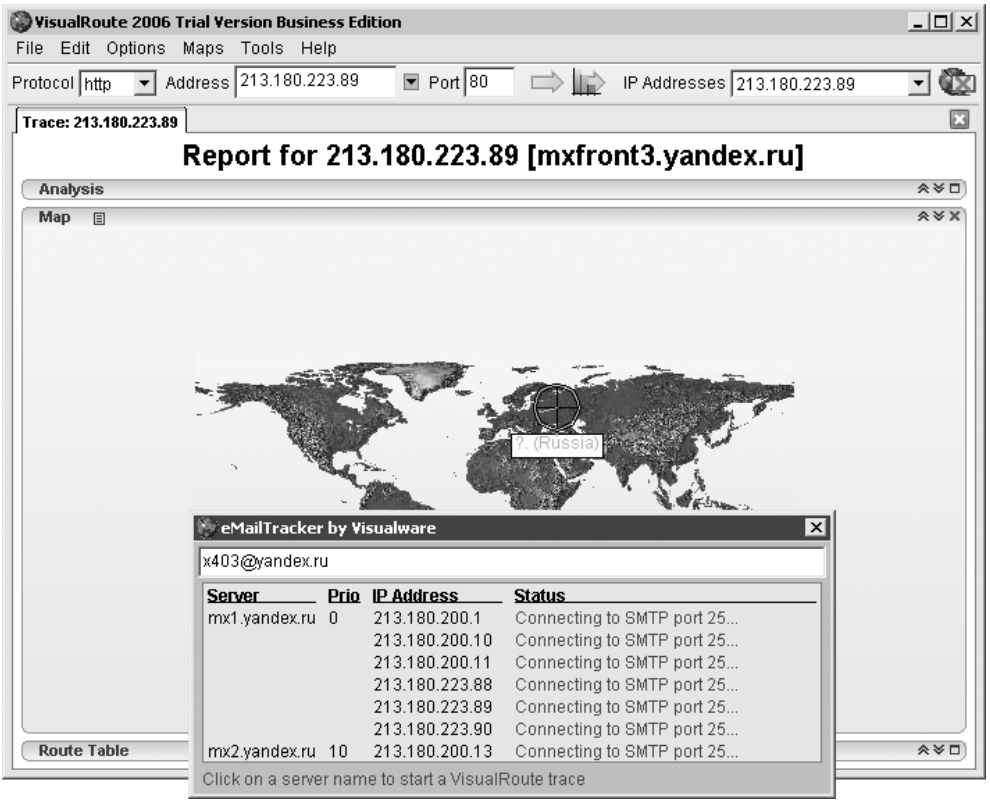


Рис. 12.6. VisualRoute позволяет определить местоположение и по почте

Можно ли по IP-адресу определить номер телефона, с которого производится подключение?

Теоретически можно. По IP-адресу можно узнать, через какого провайдера компьютер подключен к Интернету (например, с помощью сервиса Whois), поскольку все IP-адреса закреплены за конкретными провайдерами. Для обычных людей на этом все заканчивается, но спецслужбы или те, кто взломал базу данных вашего провайдера, могут пойти дальше.

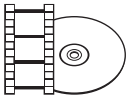
У каждого провайдера есть база данных своих клиентов с их адресами и номерами телефонов. У каждого клиента есть свой идентификатор. Все провайдеры ведут журналы подключений: в какое время и под каким IP-адресом (если тот динамический) их клиенты подключались. Если IP-адрес статический, то все гораздо проще. Зная, что компьютер с IP-адресом, например, 82.115.114.253 был в Интернете в 12 часов дня 31 мая, можно выяснить:

- кто его провайдер;
- какому клиенту данного провайдера 31 мая в 12 часов дня был присвоен IP-адрес 82.115.114.253.

Как сохранять записи, загружаемые с сайта www.YouTube.com?

На пресловутом сайте **youTube.com** часто встречаются интересные записи, но, к сожалению, разработчики сервиса позаботились о том, чтобы сделать возможность скачивания файлов очень уж неявной. Поставленную задачу можно решить с помощью специализированного ресурса **www.skachivai.ru**. Введите в специальной строке данного сайта ссылку на ролик, который хотите скачать с YouTube, затем нажмите кнопку **Сохранить видео** и укажите адрес, куда нужно сохранить файл на жестком диске. Дождитесь завершения закачки и переименуйте искомый файл, добавив ему расширение FLV. После этого файл можно просмотреть любым проигрывателем, поддерживающим работу с FLV-файлами, например Media Player Classic (**mpc.darkhost.ru**). Можно также воспользоваться сайтом **www.videosaver.ru**.

Кроме того, для этих целей можно использовать бесплатную утилиту save2pc Lite (есть на прилагаемом компакт-диске и на сайте **www.save2pc.com**).



ВИДЕОКУРС

Чтобы лучше представлять работу описанной программы, просмотрите урок «Урок 19. Приложение save2pc Lite».

По какому принципу работает Google?

Указывая в форме поиска любой запрос, будь то «бивни мамонта» или «веб-дизайн», каждый надеется, что ссылка на документ с нужной информацией окажется самой первой среди результатов поиска. Это, конечно, пока только мечты, но разработчики поисковых систем на сегодняшний день прилагают немало усилий, чтобы приблизить их к реальности.

В специальной терминологии существует понятие релевантности ответа. Говоря развернуто, релевантность — это степень соответствия найденных документов тому, что в действительности искал пользователь. Чем выше уровень релевантности ответа, тем «выше» такие документы в списке результатов поиска.

Во многом популярность поисковой системы Google обязана тому, что ее создатели (сотрудники Стенфордского университета Сергей Брин (Sergey Brin) и Лоуренс Пейдж (Lawrence Page)) путем внедрения ряда новшеств сумели добиться более высокой степени релевантности ответа, чем у существовавших на то время крупных поисковых систем Altavista и Inktomi. В результате за несколько лет Google стал всемирно известен, и сегодня бóльшая часть всех создаваемый в Сети поисковых запросов приходится на его долю.

Ниже на основе опубликованных разработчиками Google ноу-хау будут рассмотрены особенности работы данной поисковой системы.

Качество содержимого

Документы, полученные в результате поиска, сортируются в соответствии с их «качеством». Оценка качества содержимого документов в Google имеет название PageRank (PR). Документы, имеющие больший PR, всегда будут находиться на более высоких позициях в результатах поиска. При расчете PR принимаются во внимание количество ссылок с других сайтов на эту страницу и авторитетность (популярность) ссылающихся на нее страниц. Согласно этим правилам ссылка, например, с **ntv.ru** увеличит PR на большее значение, чем та же ссылка со страницы **vasya.narod.ru**, на которую заходит один человек в сутки, да и то сам владелец.

В основу принципа расчета PR заложена аксиома, что на важную информацию ссылаются чаще, нежели на бесполезную.

Описания ссылок и размер шрифта

Google не оставляет без внимания и описания ссылок на индексированные документы, подразумевая, что если уж вы разместили на своем сайте ссылку на другой ресурс, то перед этим его обстоятельно изучили и попытались в тексте ссылки отразить содержание сайта. Это решение позволило более адекватно проводить поиск в накопленной базе данных и одновременно стимулировать повышение полезности сайтов. Теперь даже у незадачливых дизайнеров появилась мотивация отказаться от ссылок со словами «здесь» и «сюда».

Не обделено вниманием и содержимое, заключенное в тегах <title></title>, — ему тоже придается большое значение. В идеальном случае ключевые слова сайта должны употребляться в названии страницы.

Кроме всего прочего, Google хранит сведения о размере шрифта и смещении каждого слова относительно начала документа. Это означает, что, например, по запросу «рояль» в первую очередь будут отображены документы, в которых искомое слово выделено более крупным шрифтом или находится ближе к началу документа.

Взаимное расположение слов

В Google учитывается не только близость слов к началу документа, но и взаимное расположение слов, указанных в поисковом запросе, то есть по фразе «карманный компьютер» — если такое словосочетание нигде не встречается — первым будет отображен документ, в котором слово «карманный» находится от слова «компьютер» на наименьшем расстоянии. Эта технология называется Proximity search (поиск по наиболее близкому расположению слов друг относительно друга).

Схема работы Google

Чтобы было где осуществлять поиск, нужно сначала создать базу данных, то есть собрать информацию. Всю основную работу по ее сбору выполняют интернет-роботы, которые, путешествуя по адресам Сети, из базы данных специального URL-сервера скачивают и передают содержимое страниц на сервер хранения документов, где за дело принимается другая программа — индексатор. Она занимается тем, что разбивает текст документа на составляющие его слова, запоминая при этом их местонахождение, шрифт; определяет, является ли слово названием документа, URL или текстом ссылки. Вся эта информация складывается в набор своеобразных контейнеров. Затем создается гигантский словарь, в котором каждому слову соответствует набор документов, где это слово встречается.

При осуществлении поиска в словаре будет найдено искомое слово; исходя из этого будет получен набор документов, в которых это слово встречается. Далее, на основании PageRank, размера шрифта и множества других параметров будут распределены порядковые номера документам, и пользователю будет выдан список найденных источников информации.

Добавление страниц в базу

Если интернет-роботу Google встретился URL, которого еще нет в базе данных, то этот адрес будет занесен в базу данных, и в дальнейшем документ, на который

указывает эта ссылка, будет проиндексирован. Таким образом, система поиска новых документов, при условии, что на них ссылается хоть какой-нибудь сайт, становится самодостаточной.

Владельцы совсем новых ресурсов, на которые еще никто не ссылается, могут зарегистрировать сайт вручную, воспользовавшись специальной формой. Введенные в нее адреса после проверки на корректность также попадут в базу данных.

Я слышал, что при поиске в Google можно использовать специальные команды. Как это делать?

При переизбытке информации наиболее важным является умение находить требуемые данные, отсеивая мусор. Теперь, чтобы найти что-либо в Сети, недостаточно просто ввести слово в форму поиска (слишком уж много разнообразной информации будет найдено), придется подумать о том, как конкретизировать свой запрос. В современном Интернете уже предусмотрено несколько вариантов того, как это сделать. Что будет происходить в Сети, когда к ней будут подключены домашние холодильники и у каждого будет свой сайт, даже представить сложно.

Во многих технических вузах преподают предмет «Теория информации». В данной теории есть одна аксиома, которая здесь будет весьма к месту: «избыток информации — то же, что ее отсутствие». Это как со звуком — если он слишком громкий, то можно оглохнуть и ничего больше не услышать.

Чтобы не «оглохнуть», в грядущую информационную эпоху придется идти впереди толпы обывателей. Когда большинство, не задумываясь, примитивно набирает запрос в строке Google, вы можете продвинуться дальше и использовать эту поисковую машину на полную мощь.

Логика по умолчанию

Всякий раз при использовании нескольких слов в запросе имеет значение — будет производиться поиск по каждому из слов в отдельности или по всему запросу в целом. Ответ на этот вопрос зависит от того, какой логический оператор используется по умолчанию при обработке запроса. Это может быть один из двух операторов: `AND` (поиск по всем словам) либо `OR` (по каждому в отдельности).

Google по умолчанию использует оператор `AND`, то есть если вы укажете в запросе `карманный компьютер`, то Google будет искать словосочетание целиком.

Если же вы напишете `карманный OR компьютер`, дополнительно будут найдены страницы, где встречается только одно из этих двух слов (например, `карманный словарь` или `персональный компьютер`).

Теперь пример посложнее. Вашему вниманию предлагается следующая конструкция: `связь (3G OR G3)`. Столкнувшись с таким запросом, Google отыщет для вас страницы, на которых встречается упоминание слова «связь» в контексте мобильных сетей третьего поколения (нет строгого правила, как их называть — G3 или 3G).

Согласитесь, поиск начинает немного походить на программирование. По аналогии с языком C, вы можете использовать вместо оператора `OR` символ `|`. В таком случае записанная в терминах Google знаменитая дилемма «быть или не быть» в строке поискового запроса будет выглядеть как `быть | не быть`. Неплохое название для романа в стиле киберпанк.

Скажу несколько слов об использовании минусов. Например, вас интересует все, что связано с именем Билл, но совершенно не интересует Билл Гейтс. Что в этом случае вы делаете? Все очень просто — используете «минус»: `Билл -Гейтс`. Приведенная конструкция однозначно даст понять Google, что вас интересуют все страницы, в которых упоминается слово «Билл», за исключением тех, где упоминается слово «Гейтс».

Если вам требуется найти некую фразу целиком, то воспользуйтесь для этих целей кавычками: `"Молекулярная физика"`. По вашему запросу будут найдены страницы, на которых присутствует данное словосочетание.

Команды особого назначения

Дополнительные команды Google позволяют добиться лучших результатов и сузить область поиска. С их помощью вы можете указать Google, что не нужно просматривать все страницы из кэша, потому что вас интересуют, к примеру, только сайты с доменной зоны **com** или **ru.** Вы можете управлять и поиском по самой странице, указывая, в какой ее части следует искать, и т. д. Ниже приведены дополнительные команды Google.

- `intitle:` — ограничивает поиск только заголовком страницы. Говоря техническим языком — содержимым тега `<title>`. Например, демонстрационный запрос `intitle:первая полоса` (пробелов между командой и параметром быть не должно) приведет к тому, что Google выдаст ссылки на первую полосу русскоязычных интернет-газет.
- `inurl:` — по этой команде поиск будет проводиться только в URL. Обычно эту инструкцию используют не поодиночке, а вместе с другими, когда хотят отыскать страницу поиска. Например, команда `inurl:search` вы-

ведет список страниц, у которых в адресе встречается слово search, как в этих случаях: **search.aol.com** или **home.netscape.com/home/internet-search.html**. Эту команду часто используют хакеры, чтобы находить сценарии проверки пароля, на которые нет ссылок с главной страницы сайта. Google не так уж и редко используется злоумышленниками для поиска уязвимых мест.

- `intext:` — при поиске не учитываются заголовки страниц и ссылки, просматривается только текст тела страницы (который заключен в теге `<body>`). Это полезно при поиске фрагмента текста, и вам, по большому счету, безразлично, какой у страницы заголовок и какие ссылки.

- `site:` — одна из самых полезных и наиболее употребительных команд. Позволяет ограничить поиск поддоменами указанного домена. Звучит запутанно, но на практике все гораздо проще. Предположим, вас интересуют статьи, которые публиковала **gazeta.ru** о выборах в Беларуси. В строке запроса пишем: `выборы в Беларуси site:gazeta.ru`.

  Можно не ограничиваться конкретным сайтом, а задать, к примеру, область. Выглядеть это будет следующим образом: `программирование site:narod.ru`. Тогда Google будет осуществлять поиск во всех поддоменах **narod.ru.**

- `link:` — возвращает список страниц, которые ссылаются на заданный сайт. Для наглядности введите `link:qwerty.by` и получите список страниц, ссылающихся на ресурс **qwerty.by**. Это просто незаменимый инструмент мониторинга для тех, кто занимается «раскруткой» сайтов. Простым обладателям домашней странички тоже будет любопытно.

- `cache:` — находит копию страницы, проиндексированной Google, даже если эта страница уже недоступна по адресу в Интернете или изменила свое содержание. Иными словами — поиск в кэше Google. Пригодится для просмотра страниц, контент которых часто меняется. Выглядит так: `cache: www.news.com`.

- `filetype:` — еще одна чрезвычайно полезная команда. Позволяет искать в Интернете файлы с заданным расширением. Однако будьте внимательны: параметры команды понимаются Google слишком буквально, и если вы сначала наберете `filetype:htm`, а потом `filetype:html`, то результаты поиска в обоих случаях будут разными. Google поддерживает некоторые наиболее популярные форматы от Microsoft: PPT, XLS и DOC. Кроме того, вы можете искать даже сценарии, созданные для динамического генерирования контента, такие как ASP, PHP, CGI и т. д.

  Инструкция `filetype:` также используется хакерами в неблаговидных целях. Например, запись `authorisation filetype:php` может помочь злоумышленнику найти сценарий проверки пароля. И если написавший

его программист был не очень грамотным специалистом, то последствия этого будут плачевными.

- `related:` — эта команда приказывает Google выводить список страниц, принадлежащих одной категории со страницей, указанной в параметрах. Например, команда `related:google.com` возвратит ряд ссылок на другие поисковые машины. `related:`—удобное средство, если вы хотите узнать, к какой категории относит ваш сайт Google, или если вы хотите найти авторитетные информационные сайты. Google при выводе результатов сортирует сайты в порядке значимости, и если вы введете, например, `related:cnn.com`, то первые позиции среди результатов будут занимать наиболее весомые издания схожей тематики: The New York Times, Washingtonpost и т. д.

Смешивать осторожно

Это как у бармена: если намешаешь несовместимых компонентов в коктейль, то клиенту станет плохо прямо за барной стойкой или он вообще откажется пить. Примерно то же происходит и с Google во время поиска, потому что не все команды совместимы между собой.

Есть команды-одиночки, которые не желают работать в паре с другими. Одной из таких является `link:`, она отображает все страницы, которые ссылаются на указанный в параметрах URL. Казалось, удобным было бы использовать данную команду совместно с `site:`, чтобы задавать еще и ограничения на домены. Например, вам интересно узнать, из какой доменной зоны ссылаются чаще на ваш сайт — из **ru** или из **net**. Однако запрос вида `link:mysite.com site:ru` не произведет на Google должного эффекта, поскольку `link:` работает только поодиночке. Обходные пути, естественно, найдутся (недаром ведь в разработке Google принимали участие русские). Для интереса можно поэкспериментировать с такой комбинацией команд: `inanchor:mysite.com -inurl:mysite.com site:ru`. В данном случае логика такова: сначала находят сайты, у которых в описании ссылки встречается адрес нужного сайта. Далее исключают из результата поиска сам **mysite.com** и его поддомены (если таковые имеются), а затем отбирают только страницы, принадлежащие к доменной зоне **ru**. Этот вариант небезупречен, но главное — идея, доработать этот запрос до конкретных нужд вы сможете самостоятельно.

Несколько слов о комбинациях, которые не должны встречаться в ваших поисковых запросах. Не рекомендуется озадачивать Google взаимоисключающими запросами типа `site:linux.by -inurl:by` либо `happy (site:ru OR site:by`.

Теперь о разрешенных комбинациях. После ряда испытаний хорошо себя проявили в совместной работе следующие команды: `intitle:`, `site:`, `inurl:`, `filetype:`. Например, вас интересуют архивы электронных книг на английском языке. Составляете такой запрос: `books intitle:"index of" inurl:ftp`. В результате получаете ссылки на весьма приличные FTP-архивы. Запрос можно перевести на «человеческий» язык так: вас интересуют страницы, где встречается слово «book», заголовок страницы должен содержать фразу «index of» (характерную для списка в FTP-архиве), а для верности, что вы имеете дело с FTP, URL должен содержать слово «FTP». Возможны различные вариации на эту тему.

Например, можно взять следующий адрес URL, который формирует Google во время поиска: **http://www.google.com/search?num=55&hl=en&q=piter**.

Нужно рассмотреть по порядку, что все это значит:

- **num=55** — количество результатов на одной странице (может быть от 1 до 100), по умолчанию 10, в случае примера 55;
- **hl=en** — задает язык интерфейса Google, в данном случае это английский, но если измените на **hl=ru**, то все надписи в Google будут появляться на русском;
- **q=piter** — это и есть сам запрос (к сожалению, ввести русский запрос в адресной строке нормальный человек не в состоянии — вот так, например, выглядит слово кактус: **q=%D0%BA%D0%B0%D0%BA%D1%82%D1%83%D1%81**).

Кроме того, вы смело можете добавить к URL еще несколько параметров:

- **as_qdr=m1** — указывает максимальный «возраст» найденной информации в месяцах. Значения могут быть от 1 до 12;
- **safe=on** — включает так называемый **safe search** (систему фильтров, которая блокирует по большей части информацию явного сексуального характера).

Важно уяснить одно: пространства для вашей фантазии, даже в рамках приведенных четырех команд, вполне достаточно.

На некоторых сайтах используется поиск средствами Google. Как это реализовано?

В листинге 12.1 приведена форма, которая заставит Google искать на вашем сайте. Чтобы все заработало, разместите этот HTML-код на странице и укажите свой

адрес вместо **mysite.com**, а посетители будут искать интересующую их информацию на сайте средствами Google.

Листинг 12.1. Поисковая форма своими руками

```
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<form method="get" action="http://www.google.com/search">
<input type="text" name="q" size=32 maxlength=110 value="">
<input type="submit" name="sa" value="Google!">
<input type="hidden" name="as_sitesearch" value="mysite.com">
<input type="hidden" name=hl value="ru">
</form>
```

Кроме того, вы можете модифицировать форму по своему усмотрению, добавляя новые параметры. Например, строка `<input type="hidden" name="as_filetype" value="txt">` заставит Google искать только текстовые документы.

Ограничение на «свежесть» результата выставляется следующим образом. Добавьте строку `<input type="hidden" name="as_qdr" value="m3">` — это будет соответствовать результатам трехмесячной давности. Если хотите найти данные шестимесячной давности, вместо `m3` используйте `m6`, если ищете информацию за год, то замените `m3` латинским `y`.

Количество результатов на странице контролируется параметром `<input type="hidden" name="num" value="50">`.

Можно ли сделать поиск в «Яндексе» более эффективным?

По поводу рекламного слогана «найдется все», который использует «Яндекс», есть хорошая шутка: «Не наврали, проверил — "все" нашлось 316 950 768 раз».

На поле англоязычного поиска Google сумел потеснить «товарищей по команде» и на сегодняшний день является крупнейшим игроком. В русскоязычном Интернете таких кардинальных изменений не произошло, в лидерах по-прежнему остается «Яндекс».

Несомненным плюсом является то, что «Яндекс» учитывает морфологию русского языка во время поиска, то есть рассматриваются все формы искомого слова. Задайте запрос `смотреть`, и в результате поиска будут найдены ссылки на документы, содержащие, кроме «смотреть», слова «смотри», «смотрите», «смотрел» и т. д. Это очень удобно. У вас есть также возможность обуздать фантазию поисковой системы и заставить ее искать строго по указанному вами слову.

Добиться этого вы сможете, поставив восклицательный знак перед искомым словом (без пробела). Вот так: `!смотреть`.

В отличие от Google, «Яндекс» делает различие между заглавными и строчными буквами. Действует следующее правило: если в окне поиска вы набрали слово с заглавной буквы, то найдены будут только страницы, на которых это слово начинается с заглавной. Если слово написано со строчной буквы, то отыщутся все варианты написания: как со строчной, так и с заглавной. Например, в ответ на запрос `Пианист` найдутся ссылки на известный фильм Р. Поланского. А вот по запросу `пианист` будет найдено большее число страниц, среди которых упоминания о данной профессии.

Показать «Яндексу», что слово обязательно должно быть найдено, можно, поставив перед ним знак +. В противоположность этому запишите его со знаком –, если вы не желаете, чтобы какое-либо слово встречалось в результатах поиска.

По умолчанию при обработке запроса «Яндекс», как и Google, использует логический оператор `и`. Это значит, что каждое слово, входящее в запрос, должно быть найдено. Переопределять данное умолчание удобно при поиске слов, близких по значению, — синонимов. Предположим, вам захотелось сегодня повеселиться, и вы входите в Интернет, чтобы почитать что-нибудь смешное. Вам все равно, что это будет: анекдоты, приколы или юмористические рассказы. В такой ситуации можно озадачить «Яндекс» запросом вроде: `юмор | шутка | анекдот | прикол`. В результате на первых страницах вы получите ссылки на наиболее рейтинговые ресурсы по этой тематике. Знак `|` означает, что вместо логического оператора `и` во время поиска будет использоваться оператор `или`. Следовательно, «Яндекс» будет требовать, чтобы на сайте содержалось хотя бы одно из перечисленных слов. Между прочим, если вы хотите использовать указанную конструкцию вместе с другими словами, то заключите ее в скобки. Вот так: `компьютерные (юмор | шутка | анекдот | прикол)`.

Поиск с расстоянием

Первым делом представьте, что все слова в вашем запросе пронумерованы начиная с единицы. У «Яндекса» существует такое понятие, как расстояние между словами, и прелесть в том, что вы можете этим пользоваться. Расстояние между первым и вторым словом равно 1, между первым и третьим — 2. Расстояние между соседними словами, стоящими не в том порядке, будет отрицательным: –1.

Теперь о том, как с этим работать. Если между двумя словами находится знак / и число, необходимо, чтобы расстояние между словами не превышало это число.

К примеру, запрос `курсы /2 массажа` означает, что вы требуете документы, в которых между словами `курсы` и `массажа` может находиться только одно слово. Иными словами, подходят фразы: `курсы лечебного массажа`, `курсы точечного массажа` и просто `курсы массажа`.

В предыдущем случае расстояние может варьировать от 1 до 2. Можно задать значение жестко: введите запрос `курсы /+2 массажа`, и тем самым вы зафиксируете положение слова `массажа` относительно `курсы`. Среди результатов уже не будет встречаться фраза `курсы массажа`, только через слово.

Со знаком / можно комбинировать и другие знаки. Например, если вы ищете серьезный заработок, то может пригодиться следующее решение: `работа ~ /2 студентов`. Этот способ исключает такие варианты, как «работа для студентов», «работа студентам» и т. д.

Как отправить «Яндекс» в конкретное место

Аналогично Google «Яндекс» тоже умеет искать информацию не по всей странице, а только в определенных ее элементах. Возможные запросы:

- `$title Питер` — ищет в заголовках страниц название города и издательского дома;
- `$anchor яндекс` — находит ссылки, в которых есть слово «яндекс»;
- `#link="www.uinc.ru*"` — покажет все документы, которые ссылаются на сайт **www.uinc.ru**;

`#image="nokia"` — выбирает ссылки на сайты, на которых есть картинки с названием «nokia».

У каждого поисковика найдется пара недостатков, не исключение и «Яндекс».

Использование конструкции `#url="имя_сайта"`, которая, по заверениям «Яндекса», ограничивает поиск информации одним сервером, вызывает некоторые сомнения. На практике толку от ее использования мало.

Иногда возникает ощущение, что некоторые команды немного сыроваты, зато можно с уверенностью сказать, что поиск в «Яндексе» более интеллектуальный: чего стоят хотя бы использование расстояния между словами, двойные операторы и возможность все это комбинировать.

Оградите детей от неприятностей

Интернет наводнен нецензурной и порнографической информацией — это ни для кого не секрет. Желание оградить неподготовленное младшее поколение

от всего этого непотребства возникало не у одного родителя. Решений дается немало, не остался в стороне и «Яндекс». Вам предлагается нечто вроде безопасного поиска. Отправившись на «Семейный Яндекс» (**family.yandex.ru**), вы вряд ли найдете что-то неприличное. Например, по запросу `порно` было выдано ноль результатов, на грубые ругательства реакция такая же. Будто и нет такого в Сети вовсе. Создается впечатление, что Интернет стал чище.

Если вашим компьютером пользуются дети, то можно сделать стартовой страницей **family.yandex.ru**, и вероятность того, что малыши наткнутся в Сети на что-нибудь непристойное, резко уменьшится.

Правда ли, что через Интернет можно следить за полетом спутников и пассажирских самолетов?

Если ваши близкие частенько летают на самолетах, пока вы сидите дома и мнете от волнения платочек, то этот совет для вас. Чем пребывать в неведении до прихода SMS вроде «прилетел, все ок», отправляйтесь по адресу **earth.google.com** и установите программу Google Earth, которая позволяет просматривать информацию о полетах самолетов. Затем — по адресу **www.fboweb.com/antest/ge/intro.aspx?old=1**, где следует выбрать интересующую вас авиакомпанию и указать номер рейса. Нажмите кнопку **Track it!** для загрузки файла формата KML. Двойным щелчком кнопкой мыши нужно открыть скачанный файл в программе Google Earth и приступить к наблюдению за полетами самолетов. Все данные об их перемещении отображаются с пятиминутной задержкой.

По тянущемуся за каждым самолетом шлейфу можно определить траекторию полета и узнать направление движения лайнера. Если шлейф красный, значит, самолет вылетел из указанного на втором шаге аэропорта, если синий, то его путь следования лежит в родную воздушную гавань. Наконец, если в окне программы щелкнуть кнопкой мыши на изображении самолета, то высветится окошко с информацией о рейсе, маршруте следования, скорости воздушного судна в узлах и высоте полетах в футах.

Можно наблюдать и за разными спутниками. Помогут в этом программы Satellite Antenna Alignment (**www.al-soft.com/saa/satinfo.shtml**), Orbitron (**www.stoff.pl**) и HeavenSat (**www.heavensat.ru**) с русским интерфейсом.

На ресурсе **www.celestrak.com/NORAD/elements** вы найдете огромную базу (в формате TLE) с постоянно обновляемой информацией об орбитах многих тысяч спутников.

У меня не работает импульсный набор. Почему?

Не нужно быть очень наблюдательным, чтобы заметить, что Windows 2000/XP упорно не хочет пользоваться импульсным набором при подключении к Интернету (порой игнорируется даже соответствующий флажок в настройках). Заставить систему сделать это можно, указав перед телефонным номером латинскую букву `P` (это переводит модем в режим импульсного набора). Иными словами, в свойствах соединения вместо номера `600100385` надо указывать `p600100385`.

Как заставить модем выдерживать паузу при наборе номера?

Обучить свой модем терпению и заставить его ждать гудка несложно. Для этого достаточно поставить латинскую букву **W** после нужной цифры в номере. Например, комбинация `8w600100` заставит модем дожидаться длинного гудка после набора восьмерки. Можно использовать запятую, если требуется обычная пауза. При расчете времени следует ориентироваться на то, что одна запятая соответствует задержке в полсекунды.

Как можно аварийно отключить телефонное соединение?

У каждого пользователя хоть раз пропадали значки в **Панели задач** (сами по себе или после перезагрузки **Проводника**). Бывают ситуации, когда значок установленного интернет-соединения бесследно исчезает, после чего разорвать соединение можно, только дернув «рубильник» на модеме. Казалось бы, и способ неплохой, но все же хочется чего-то более изящного.

К счастью, в состав Windows входит полезная утилита `rasdial.exe`, которую можно найти в директории `windows\system32`. Она используется для управления телефонными соединениями через командную строку, с ее помощью можно как установить соединение, так и разорвать его. Создайте BAT-файл, в котором пропишите следующее: `%windir%\system32\rasdial.exe /disconnect`. Желающие могут сделать ярлык и разрывать соединение при помощи горячих клавиш.

Есть еще один способ, который рекомендуется для тех, кто сталкивается с описанной проблемой не так часто. Завершить телефонное соединение можно, проследовав в меню **Пуск ▸ Настройка ▸ Сеть и удаленный доступ к сети**, здесь

выбрать активное в данный момент подключение и щелкнуть на нем правой кнопкой мыши. В открывшемся списке укажите **Отключить**.

Как сделать, чтобы при попытке подключения к Интернету запрашивался пароль?

При запуске соединения с Интернетом у вас должны запрашиваться логин и пароль, если так не происходит, причиной этому, скорее всего, служит установленный флажок **Сохранять имя пользователя и пароль**. Щелкните два раза кнопкой мыши на значке подключения и в появившемся окне снимите флажок. В случае если после щелчка кнопкой мыши сразу начинает устанавливаться подключение, не запрашивая пароль, нужно сделать следующее: зайдите в **Панель управления ▸ Сетевые подключения** и щелкните правой кнопкой мыши на значке подключения, в ниспадающем меню выберите **Свойства**. В появившемся окне перейдите во вкладку **Параметры**. Установите флажки:

- **отображать ход подключения**;
- **запрашивать имя, пароль, сертификат и т. д.**;
- **запрашивать номер телефона**.

Нажмите **ОК**. И снова попытайтесь снять флажок **Сохранять имя пользователя и пароль**.

Теперь пароль потребуется вводить при каждом соединении. Может случиться так, что вы сами не будете знать пароль, введенный в сетевом подключении. В таком случае уточните его у своего провайдера интернет-услуг (возможно, он записан в договоре).

При попытке соединиться с Сетью модем издает звуки, обычные для этого процесса, а потом пишет ошибку 678. Модем тестировался на другом компьютере — отлично работает. Что делать?

Дело не в модеме. Причин может быть несколько.

- Если устанавливается подключение удаленного доступа, убедитесь, что набирается правильный номер. Попробуйте набрать этот номер на телефоне.
- Когда устанавливается подключение к виртуальной частной сети (VPN), проверьте правильность имени узла или IP-адреса конечного сервера и повторите попытку подключения.

- Если после настройки модем также выдает ошибку 678, то, возможно, в вашем компьютере стоят блокирующие программы (антивирусы или брандмауэры), которые некорректно настроены и мешают установлению связи, — попробуйте их отключить и попытайтесь установить соединение.

Откройте **Панель управления ▸ Сетевые подключения**. Щелкните на подключении правой кнопкой мыши и выберите пункт **Свойства**. В открывшемся окне перейдите во вкладку **Безопасность**. Здесь следует установить настройки, которые требует ваш оператор связи. Попробуйте выбрать параметры безопасности **Обычные** (при проверке используется небезопасный пароль). Загляните на вкладку **Сеть**, — здесь обязательно должен быть установлен флажок **Протокол Интернета TCP/IP**.

Видел однажды, что при запуске браузера в нем появляется список всех ссылок из Избранного. Как это сделать?

Куда пойти, куда податься — этим вопросом наверняка задавались и вы, глядя грустными глазами в пустое окно Internet Explorer. А ведь можно несколько смягчить проблему, если выводить каждый раз при старте браузера страницу со своими закладками. Все интересное будет прямо перед вами. В этом случае имеется еще один плюс: наверняка много старых добрых сайтов затерялось в **Избранном** лишь потому, что вам лень их искать в многочисленных вложенных папках. Теперь все будет иначе: нужно закладки папки **Избранное** превратить в гиперссылки и создать из них HTML-файл. Для этого следуйте по маршруту **Файл ▸ Импорт и экспорт**, в открывшемся окне мастера выберите строчку **Импорт избранного** и поместите где-нибудь файл `bookmark.htm`, содержащий ваши закладки. Затем потребуется сделать его стартовой страницей в браузере (**Сервис ▸ Свойства обозревателя**, раздел **Домашняя страница**), и проблема выбора решена.

Как вызвать адрес из Избранного в браузере одним нажатием кнопки?

Эта возможность есть в браузерах Internet Explorer, Firefox и Opera. Любой сайт можно вызывать одним нажатием кнопки. Приведем примеры реализации для двух первых браузеров.

- Internet Explorer. Зайдите в меню **Избранное**, щелкните на нужной ссылке правой кнопкой мыши и в раскрывающемся меню выберите пункт **Свойства**. В появившемся окне обратите внимание на строку **Быстрый вызов**. Здесь

можно задать сочетание клавиш (обязательно использовать клавиши **Ctrl** и **Alt**).

- Firefox. Зайдите в меню **Закладки**, щелкните на нужной ссылке правой кнопкой мыши и в контекстном меню выберите пункт **Свойства**. В появившемся окне обратите внимание на строку **Краткое имя**. В отличие от Internet Explorer, здесь достаточно написать лишь одну сигнальную букву или цифру (например, `1`). Теперь, если в адресной строке вы напишете `1` и нажмете **Enter**, браузер загрузит указанный сайт.

Я слышал, что Избранное можно хранить в Интернете, благодаря чему оно никогда не потеряется. Как это сделать?

Нетрудно догадаться, что онлайновые сервисы служат резервными хранилищами ваших данных: ценные ссылки не пропадут при переустановке Windows или с безвременно ушедшим винчестером.

Поэтому понятна популярность интернет-ресурсов для хранения ценных ссылок — избранных закладок.

- Ценителям приватности имеет смысл посетить адрес **connectedy.com**. Полное и окончательное торжество анонимности. При регистрации у вас не спрашивают никакой личной информации. Файлы закладок импортируются из браузеров Internet Explorer и Firefox. Ресурс «понимает» русский язык, и никаких затруднений с распознаванием кодировок не возникает. Интерфейс подчеркнуто строгий: на странице показываются только список существующих папок и закладки из открытого в данный момент каталога. Из дополнительного — строка поиска по закладкам, меню для сортировки и правки открытых записей.

  Ссылки распределяются по папкам (возможны вложенные). Каждому каталогу соответствует отдельная категория, служащая в том числе для поиска подходящих материалов у других пользователей.

- Есть другой онлайновый ресурс — «Яндекс» (**zakladki.yandex.ru**). Воспользоваться им можно, зарегистрировавшись на сайте ресурса и получив виртуальный паспорт. Если у вас уже есть электронная почта на «Яндексе», то больше ничего не потребуется. Менеджер умеет добавлять закладки из Internet Explorer и Firefox. Полезен импорт ссылок с любой указанной вами веб-страницы. Такой способ добавления закладок существенно экономит время, даже странно, что эта услуга не слишком широко распространена.

Можно импортировать закладки как в корневой каталог вашего частного хранилища на сервере, так и во вложенную папку (если папки нет, создайте ее непосредственно в ходе импорта).

Не секрет, что посещать сайт, чтобы найти нужную ссылку, неудобно. Работать с ресурсом «Яндекс» так же комфортно, как и с меню **Избранное** в браузере, можно, установив «Яндекс.Бар» (**bar.yandex.ru**). Это позволит вам быстро работать с почтой на «Яндексе» и быстро добавлять/удалять/редактировать закладки.

- Ресурс **del.icio.us** — один из пионеров в данной области. Именно его администрацией был предложен базовый набор функций, который стал неписаным стандартом для служб этой категории и вместе с тем объектом дискуссий.

  Отдельная тема — механизм совместной работы пользователей ресурса. Социализация оказалась радикальной: добавляемые в систему ссылки по умолчанию становятся публичными и доступными любому. Некоторым пользователям такой подход не по душе, однако плата за ваши ссылки справедливая — закладки всего сообщества **Del.icio.us**. К тому же вы получаете возможность видеть, у каких пользователей в закладки добавлен тот же сайт, что и у вас. Обнаружив пользователя, который добавляет в закладки такие же сайты, можно предположить, что интересы у вас схожие. Поэтому, зайдя в его профиль и просмотрев полностью его список закладок, вы наверняка найдете что-то любопытное для себя. Гениально и просто.

Забыл пароль к ICQ и не могу войти со смартфона. С компьютера ICQ запускается автоматически. Можно найти пароль к ICQ в Windows?

Узнать сохраненный пароль к ICQ и другим программам поможет утилита PassView (**www.nht-team.org**). Довольно приличную коллекцию подобных программ вы сможете найти на сайте **www.nirsoft.net**.

Я слышал, что можно «лазить» по сайтам в Интернете, используя электронную почту. Каким образом?

Нередко начальство ограничивает своих подчиненных в пользовании Интернетом, разрешая только работу с электронной почтой. Делается это для того, чтобы сотрудники не «висели» в Интернете, а тратили время на выполнение

своих обязанностей. Но иногда ведь так хочется зайти на любимый сайт... Здесь приходит на помощь сервис под названием web-to-e-mail.

Суть его в том, что, отправив на специальный адрес письмо в определенном формате с указанием адреса страницы, можно получить ее на свой почтовый ящик.

Сейчас сервисы web-to-e-mail отходят в прошлое, но некоторые все еще функционируют, как, например, Webgate. Воспользоваться его услугами можно, отправив письмо на адрес **webgate@vancouver-webpages.com**. Для заказа страницы в теме письма (а не в теле) следует указать команду: `get адрес_страницы`, например `get http://www.qwerty.by/`. Обратите внимание, что в команде `get` следует указывать полный адрес желаемой страницы. Если все сделано правильно, результат не заставит себя долго ждать (рис. 12.7).

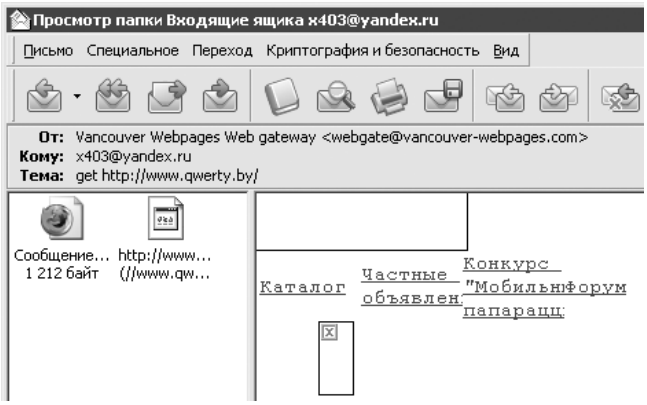


Рис. 12.7. Веб-серфинг через электронную почту

Как управлять удаленным компьютером через электронную почту?

Командовать компьютером, находясь в командировке за тысячи километров; следить за пользователями, которые работают на нем в ваше отсутствие... Ситуации, в которых может понадобиться удаленное управление через электронную почту, вам подскажет сама жизнь.

Всем забывчивым, предусмотрительным и просто любопытствующим хоть раз, но стоит это попробовать.

Представьте, что на вашем компьютере установлена специальная программа, которая периодически проверяет почту в поисках писем, адресованных ей лично.

Обнаружив нужное письмо, она выполняет переданные в нем команды. Само собой, о скорости получения результатов речи не идет, но это в данном случае не главное.

Наиболее проста в управлении программа **Autosend** (**www.filesharingbyemail.com**). Для работы с ней требуется установленная виртуальная JAVA-машина от SUN. Впрочем, с сайта производителя можно скачать дистрибутив с уже интегрированной JAVA-машиной, но размер его будет порядка 18 Мбайт.

Алгоритм работы Autosend таков: из любой точки мира отправляете письмо домой, в теме письма указываете нужные команды. К примеру, если вам потребовался файл, укажите полный путь к нему: `c:\boot.ini`. Autosend через определенные промежутки времени устанавливает соединение, проверяет почту и отключается. Через какое-то время заказанный файл будет вам выслан по почте. Если название файла вспоминается с трудом, поставьте в теме письма команду: `?find часть_имени_файла`. Autosend поищет его самостоятельно. Чтобы получить список всех файлов, укажите в теме: `?list` (если к этой команде добавить имя нужной папки, то программа выдаст листинг ее содержимого). Почти аналогично заказывается список каталогов: `?listf`.

Если заказанный вами файл слишком большой, то Autosend может разбить его на несколько частей. Более того, файлы можно не только заказывать, но и отправлять на домашний компьютер. Autosend поместит их в отдельный каталог.

На сайте разработчиков доступна версия Autosend для UNIX-систем, и это единственное преимущество Autosend перед RemoteByMail.

RemoteByMail (**www.runtime.org**) — более мощная программа для удаленного управления через электронную почту. RemoteByMail — весьма достойная разработка и заслуживает всяческих похвал. Главная ее отличительная особенность — умение запускать приложения, разработчики также позаботились о безопасности: в теме письма нужно указывать заранее определенный вами пароль. Команды RemoteByMail отдаются из тела письма.

С интерфейсом и настройками разобраться нетрудно. После запуска программы следуйте в **Tools ▸ Accounts** и создайте здесь учетную запись (их может быть несколько), которая будет ассоциирована с вашим электронным адресом.

В столбце **POP&SMTP settings** задайте те же настройки, что и в почтовом клиенте при работе с электронной почтой.

В столбце **Access** в разделе **Served clients** задаются почтовые домены (***@gmail.com**) или адрес элетронной почты (**dimoon@gmail.com**), с которых будут приниматься команды. С точки зрения безопасности лучше указывать конкретные адреса.

Внизу расположены список доступных команд и форма для ввода пароля. По умолчанию пароль **passw123** — обязательно его поменяйте!

Теперь по поводу команд. Есть команда отправки файлов — `send`, команда архивирования и отправки ZIP-архива — `zend`, а также команда просмотра содержимого каталога или диска — `dir`. Команда `hi` применяется для проверки работоспособности RemoteByMail.

К примеру, RemoteByMail контролирует адрес **x403@yandex.ru**, и вы хотите получить листинг диска **C:**. В таком случае потребуется с доверенного адреса выслать пароль и команду на **x403@yandex.ru** (рис. 12.8).

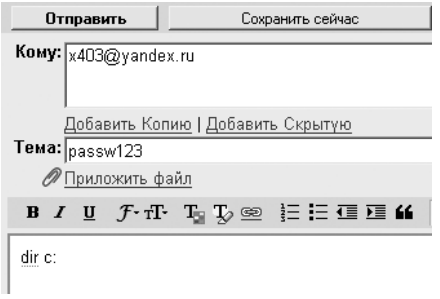


Рис. 12.8. Требование от RemoteByMail списка файлов и каталогов диска C:

Через некоторое время вам придет ответ с требуемой информацией (рис. 12.9).

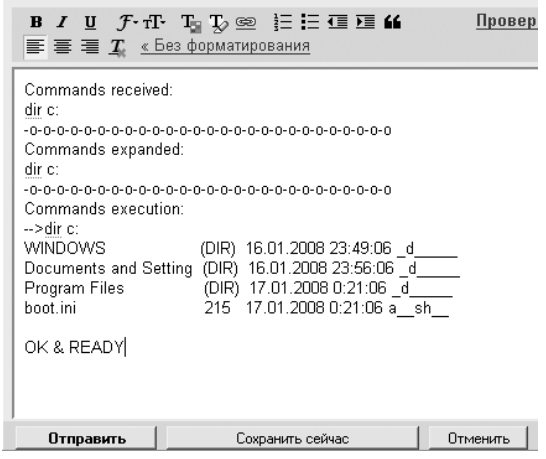


Рис. 12.9. RemoteByMail прислала список файлов и каталогов диска C:

Осталось познакомиться с еще одной командой — `execute`, которая позволяет запустить любое приложение или файл. Пользователям, хорошо владеющим

командной строкой Windows, эта команда предоставляет широкие возможности по манипулированию системой.

Между прочим, вы можете сами задавать новые команды для RemoteByMail, которые базируются на пяти встроенных. Это делается в меню **Tools ▸ Commands**.

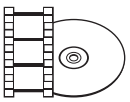
Какими программами можно рассылать письма в больших количествах?

Словосочетание «массовая рассылка» в последнее время приобрело крайне негативный оттенок и у большинства пользователей вызывает ассоциации с назойливыми рекламными письмами, которые каждое утро в умопомрачительных количествах обнаруживаются в электронной почте. Уставшим от спама в последнюю очередь приходит в голову, что в больших количествах можно рассылать не только рекламу, но и приглашения или анонсы подписчикам.

Хороших программ для массовой рассылки почты при всем обилии рынка не так уж и много, как и всего хорошего в жизни.

- G-Lock EasyMail (**www.glocksoft.com**) — классическая программа для массовой рассылки. Обладает понятным интерфейсом и мощным редактором сообщений (поддержка HTML, добавления картинок и файлов). Импортировать адреса можно из текстовых файлов, баз данных, HTML- и Excel-файлов. Процесс импорта занимает немного времени, при этом G-Lock EasyMail быстро определяет некорректные почтовые и повторяющиеся адреса.
- Advanced Mass Sender (**www.kbbsoftware.com**) — наиболее мощная программа, она уже давно получила отличную репутацию среди других решений для массовой рассылки писем. Если интерфейс Advanced Mass Sender показался вам слегка мудреным, не сомневайтесь — так оно и есть. Только проработав в программе какое-то время, вы оцените ее удобство. Поначалу же придется туго. В комплекте с приложениями идет несколько дополнительных утилит.
- Group Mail Free (**www.infacta.com**) производит впечатление программы, ориентированной на бизнес-применение в хорошем смысле этого слова. Если от предыдущих разработок слегка «попахивало» спамерскими штучками, то Group Mail Free в этом заподозрить никак нельзя. Интерфейс утилиты выполнен в стиле Office XP. Не только внешнее оформление роднит Group Mail Free со знаменитым офисным пакетом — программа использует словари Office для проверки орфографии. Текстовый редактор поддерживает макросы, но работа с HTML не предусмотрена.

Импортирование списков адресатов сделано добротно, электронное письмо удастся извлечь даже из самой запущенной базы.



ВИДЕОКУРС

В видеоуроке «Урок 20. Программы для рассылки писем» демонстрируется, как работать с описанными приложениями для отправки писем в больших количествах.

Как можно автоматизировать скачивание фотографий из различных фотогалерей, где показывается только по одной картинке?

Из корыстных целей владельцы фотогалерей не дают пользователям доступ ко всем фотографиям сразу, а предпочитают показывать по одной картинке (окруженной рекламными баннерами) на странице. Поэтому, чтобы скачивать интересующие подборки изображений с наименьшими затратами сил и времени, приходится прибегать к специальным программам.

- Обычно ссылки на серию картинок почти одинаковы (например: `pict1.jpg`, `pict2.jpg`), отличаются только порядковые номера. Программа Picture Pump (**zmey.com.ru**) умело этим пользуется. В простейшем случае практически единственное, что нужно сделать при работе с Picture Pump, — скопировать адрес файла картинки (например, `pict1.jpg`), вставить его в верхнее текстовое поле и заменить изменяющуюся часть названия подстановочным символом `@`, чтобы имя было не `pict1.jpg`, а `pict@.jpg`. Далее в раскрывающемся списке чуть ниже выберите пункт **URL сайта указывает на картинки**, установите начальное и конечное значения, а также шаг их увеличения. Если в названии файла картинки используются несколько цифр (например, `pict001.jpg`), то в поле **Шаблон** достаточно вписать столько символов `@`, сколько знаков в числе. После этого останется только указать папку для сохранения скачанных данных, и можно начать процесс нажатием кнопки **Старт**. Трудолюбивый Picture Pump (рис. 12.10) начнет закачивать файлы в несколько потоков и аккуратно складировать их на жесткий диск.

  Если в главном окне программы выбрать из раскрывающегося списка пункт **URL сайта указывает на страницы с картинками**, Picture Pump начнет анализировать указанные страницы и загружать те изображения, ссылки на которые есть в HTML-коде. Исключить из списка сохраняемых для вас картинок баннеры можно, проследовав в меню **Конфигурация проекта ▸ Ответ**, здесь задайте значение **Не скачивать файлы короче 20 — 30 Кбайт**.

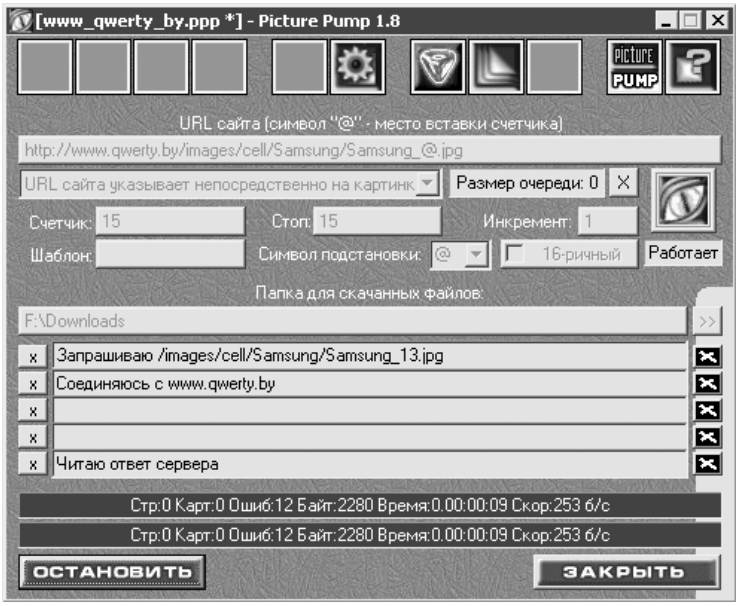


Рис. 12.10. Picture Pump в действии

Не забудьте в **Настройках пользователя** установить русский язык интерфейса.

- Обладатели неограниченного канала на доступ в Интернет могут не разменяться на мелочи, а просто натравить программу PicaLoader (**www.vowsoft.com**) на нужный сайт. Монстрообразный PicaLoader скачивает все графические файлы с заданного узла.
- Для массовой закачки фото также разработаны специальные плагины к Internet Explorer, такие как SavePicNoAsk (**www.unhsolutions.net/spna**). После установки плагина щелкните на любой ссылке правой кнопкой мыши, и, выбрав из контекстного меню **SavePicNoAsk-Save large pictures**, вы отправите адрес на «разбор» и скачивание картинок плагину SavePicNoAsk.

Как хранить свои файлы на серверах в Интернете?

Электронная почта в почтовой системе Gmail (**www.gmail.com**) всемирно известного Google — это больше чем просто «мыло», особенно после появления расширения для **Проводника** под названием GMail Drive (**www.viksoe.dk/code/gmail.htm**). Она позволяет использовать почтовый ящик на Google в качестве логического диска — после установки в вашем **Проводнике**, наряду с дисками **C:**, **D:**, будет еще и диск под названием **GMailDrive**. Копируя в него данные, вы фактически копируете их в свой почтовый ящик на Gmail. Теперь от себя

самого же вам начнут приходить письма, тема которых будет иметь примерно такой вид: **GMAILFS: /book/. [14;a;1]**. Не пугайтесь.

Штука действительно удобная, просто незаменимая для хранения резервных копий важных данных. Правда, копировать их придется вручную в **Проводнике**, поскольку обратиться к GMailDrive нельзя ни из консоли, ни из Total Commander, ни из других приложений.

Естественно, что работает все только при подключении к Интернету.

Функционирование GMail Drive не накладывает каких-либо ограничений на использование веб-интерфейса этого почтового сервиса. Все данные программа сохраняет в виде писем с вложенными файлами (именно по этой причине возникает лимит на размер одного файла — 10 Мбайт и отсутствие возможности их переименования).

Выгоды от использования ящика Gmail в качестве виртуального диска очевидны, например такой симбиоз можно с успехом использовать для синхронизации данных на разных территориально распределенных компьютерах. К тому же вся работа ведется по защищенному HTTPS-протоколу.

Нельзя не отметить сервис **docs.google.com**, который позволяет хранить, редактировать и создавать документы, совместимые с Word, прямо в Интернете. Если подключение к Сети вдруг пропадает, то можно продолжать работать над документом в браузере. Когда подключение к Интернету возобновится, изменения будут автоматически сохранены на сервере в Интернете. Очень удобно таким образом работать над документом из разных мест (дома, на работе). По большому счету, вам нужны лишьИнтернет и браузер.

Услуги по хранению файлов предоставляет сервис **www.box.net**, в отличие от **docs.google.com**, здесь можно хранить и ZIP-архивы. Для редактирования документов Microsoft Office можно использовать специальный плагин.

Как разместить сайт в Интернете?

Сейчас у многих появилась необходимость обзавестись своим представительством в Интернете, проще говоря — собственным сайтом. Неважно, какая цель вами движет, принцип размещения сайта в Сети от этого не зависит.

Регистрация доменного имени

Прежде всего требуется зарегистрировать доменное имя, которое в дальнейшем будет ассоциироваться с вашим сайтом. Проще говоря, доменное имя — это и есть адрес вашего сайта. Оно может быть доменом второго уровня, как,

например: **dima.ru**, **udaff.com**; или доменом третьего уровня: **dima.h1.ru**, **udaff.by.ru**; или даже четвертого уровня: **dima.at.tut.by**, **udaff.at.tut.by**.

Домен второго уровня проще запомнить, он выглядит привлекательнее, и потому регистрация таких адресов платная. В среднем их цена колеблется от 10 до 20 долларов в год, в зависимости от того, в какой доменной зоне вы будете регистрироваться: **ru**, **net**, **com**, **org** и т. д. Это не такие уж и большие деньги, к тому же если вы намерены всерьез заниматься сайтом, то это того стоит. В Интернете есть много сервисов по регистрации доменов, порой цены в них разнятся, поэтому не стоит выбирать только приведенные ниже сайты. Откройте страницу **www.ya.ru** и в строке поиска введите запрос: `регистрация домена`. Зарегистрировать домен второго уровня можно на сайтах: **www.webnames.ru**, **www.nic.ru**, **www.register.com**.

ПРИМЕЧАНИЕ

Доменное имя следует выбирать исходя из следующих критериев. Чем меньше символов в имени вашего домена, тем удобнее его набирать и проще запомнить. Если вы используете в качестве имени домена транслитерацию русского слова, то важно, чтобы его написание было однозначным. Например, слово «головой» можно написать по-разному: golovoi или golovoy.

Если же вы решили выбрать себе домен третьего или четвертого уровня, то знайте: они в большинстве своем предоставляются бесплатно, зарегистрироваться вы сможете на сайтах: **narod.ru**, **h1.ru**, **by.ru**. Однако не забывайте, что поскольку вы ничего не платите, то и не имеете почти никаких прав на свой сайт. В Интернете нередко случалось, когда хорошо раскрученный проект с большой посещаемостью, размещенный на бесплатном хостинге с бесплатным доменным именем, просто закрывался владельцами хостинга без каких-либо видимых на то причин и без последующего восстановления. Но этого не произойдет, если доменное имя будет принадлежать вам.

ПРИМЕЧАНИЕ

Киберсквоттинг — сравнительно новый бизнес, появившийся с ростом популярности Интернета. Киберсквоттер регистрирует доменные имена с целью их дальнейшей перепродажи, при этом цена на «хорошее» доменное имя может быть в несколько тысяч долларов. Поскольку доменное имя регистрируется на некоторый срок, то киберсквоттеры часто перерегистрируют на себя известные доменные имена, когда их владельцы забывают вовремя продлить регистрацию. Вернуть обратно доменное имя стоит немалых денег.

Разновидностью киберсквоттинга является тайпсквоттинг, когда регистрируется доменное имя, написанное с ошибкой. Например, существует очень популярный сайт www.download.com. Тайпсквоттеры регистрируют сайты с названиями: www.dawnload.com, www.donwload.com и www.downlaod.com, чтобы захватить себе часть посетителей, которые не очень внимательно смотрят на клавиатуру.

Хостинг

Хостинг — услуга по размещению файлов сайта на дисковом пространстве сервера хостинговой компании либо услуга размещения почтового или FTP-сервера на мощностях хостинговой компании.

Хостинг, как правило, разделяется на платный и бесплатный. Последний зачастую медленнее и не дает никаких гарантий клиенту. Ознакомиться с предложениями по предоставлению услуг хостинга можно, если зайти, к примеру, на **www.ya.ru** и набрать в строке поиска: `хостинг`. Наиболее крупной компанией на рынке данных услуг является **masterhost.ru**.

Как же связать купленный у одной компании хостинг и купленный у другой компании домен? После регистрации домена вам выдаются адреса для доступа к панели управления доменом, в этой панели следует указать адреса DNS-серверов, которые вы получите от компании, предоставляющей услуги хостинга.

Какой менеджер закачки выбрать?

По результатам опросов предпочтения пользователей менеджеров закачки разделяются следующим образом:

- Download Master;
- FlashGet;
- ReGet;
- GetRight.

Наибольший интерес представляет тройка лидеров.

Download Master

Download Master (**www.westbyte.com**) — наиболее функциональный менеджер закачек. Поэтому знакомство с ним имеет смысл начать с перечисления основных возможностей программы.

- Поддержка русскоязычного интерфейса; при проблемах с кодировкой, когда русские буквы не отображаются, можно использовать интерфейс на транслите.
- Поддержка списков закачек с широкими возможностями сортировки (по дате добавления, расширению, по приоритету).
- Плавающий индикатор скорости закачки, индикаторы активных закачек, управление активными закачками.

- **Активная Наглядная Корзина** — плавающее окно, позволяющее полноценно работать с программой без открытия главного окна со списком закачек. Плавающее окно включает в себя следующие объекты: индикатор скорости закачки, корзину добавления закачек, индикаторы активных закачек с возможностью управления ими, меню управления программой, краткий список закачек с возможностью их старта.
- Поддержка подключаемых модулей (плагинов) и обложек.
- Динамическая многопотоковая закачка.
- Докачка после обрыва связи с HTTP, HTTPS и FTP-серверами.
- Работа по расписанию, отключение компьютера после завершения закачки.
- Оптимальные настройки для работы с различными типами модемных соединений (ISDN, ADSL, LAN) и на различных скоростях.
- FTP-проводник.
- Поиск и добавление зеркал для закачки.
- Работа с ZIP-архивами: возможность просмотра содержимого ZIP-архивов перед закачкой, возможность закачивать только выбранные файлы из архива, проверять ZIP-архивы и восстанавливать поврежденные файлы, а также распаковывать архивы.
- Работа с RAR-архивами: возможность проверять RAR-архивы, возможность распаковывать архивы.
- Подробный файл журнала на каждую загрузку.
- История закачек.
- Менеджер сайтов для управления паролями и папками для сохранения (в некоторых случаях приходится вводить пароль для каждой закачки).
- Управление скоростью закачки, автоматический режим для комфортной работы с браузером.
- Возможность установки приоритетов для закачек.
- Программа дозвона для модемных соединений.
- Возможность синхронизации (автообновления) файлов на сервере и локальном компьютере.
- Проверка закачанных файлов на обновление.
- Возможность послушать музыкальные и просмотреть видеофайлы в процессе закачки; автоматическое получение информации о MP3-файлах при старте закачки.

- Возможность автоматически перезапускать закачку при понижении скорости, что позволяет избежать простоев.

Кроме этого, у Download Master развиты возможности интеграции: программа отслеживает содержимое буфера обмена, интегрируется в браузеры Microsoft Internet Explorer 4.0 и выше, Firefox, Mozilla, Opera 4.0 и выше, Netscape Communicator 6.0 и выше, а также с антивирусными программами.

Старт закачки. Способы скачивания информации при помощи Download Master.

- Щелкните кнопкой мыши на ссылке в браузере, и вместо стандартного окна **Сохранить как** появится окно добавления закачки Download Master. Если во время щелчка кнопкой мыши на ссылке будет нажата клавиша **Alt**, то закачка будет добавлена независимо от расширения файла.
- Щелкнув на ссылке правой кнопкой мыши, выберите из контекстного меню Internet Explorer или Opera пункт **Закачать при помощи Download Master** или **Закачать все при помощи Download Master**. При этом появится окно добавления закачки Download Master. Данный метод рекомендуется использовать, если Download Master по каким-то причинам не перехватывает закачку. Если вы выбираете **Закачать все при помощи Download Master**, то открывается окно добавления закачек, в котором вы можете указать выбранные для закачки файлы.

  Download Master автоматически отслеживает буфер обмена и при добавлении в него ссылки на файл или группу файлов с указанным в настройках программы расширением открывает окно добавления закачки Download Master.

ПРИМЕЧАНИЕ

Параметр URL мониторинг буфера обмена должен быть включен в настройках программы.

- Начать закачку можно нажатием кнопки **Добавить URL** на панели инструментов или щелчком правой кнопкой мыши на значке программы в **Панели задач**. В появившемся списке следует выбрать пункт **Добавить URL**. В появившемся окне добавления закачки вам необходимо вручную ввести интернет-адрес закачки.
- Стартовать закачку можно, перетащив ссылку (или выделенный текст) из браузера или почтовой программы в плавающее окошко.

Интеграция с браузером. Для упрощения процедуры добавления закачки Download Master интегрируется с браузером. После этого программа автоматически

перехватывает закачки и интегрируется в раскрывающееся меню **Закачать при помощи Download Master**.

Для настройки параметров интеграции перейдите в раздел **Настройки ▸ Общие**.

Если установлен флажок **Интеграция в Microsoft Internet Explorer**, то Download Master будет перехватывать закачки из Internet Explorer.

Если установлен флажок **Расширенная интеграция**, то Download Master будет перехватывать все закачки из Internet Explorer версии 6.0 и выше.

ПРИМЕЧАНИЕ

Если выбран данный параметр, то закачки будут перехватываться независимо от списка расширений, который указан в программе (только для Internet Explorer 6.0 и выше).

Если активизирован пункт **Использовать клавиши Alt и Ctrl при кликах на ссылках в браузере**, то при нажатой клавише **Alt** Download Master будет перехватывать все закачки из Internet Explorer и игнорировать их при нажатой клавише **Ctrl**.

Если установить флажок напротив пункта **Интеграция в Netscape, Mozilla**, то Download Master будет перехватывать закачки из Firefox, Mozilla и Netscape Communicator.

Если установлен флажок **Интеграция в Opera**, то Download Master будет перехватывать закачки из Opera.

ПРИМЕЧАНИЕ

Если у вас Opera ниже версии 7.10, то для вступления изменений в силу после установки флажка перезапустите браузер, откройте в нем File ▸ Preferences ▸ Multimedia и щелкните кнопкой мыши на Find plug-ins.

Возможности закачек. Download Master позволяет делать следующее.

- Автоматически сохранять закачки в различные папки в зависимости от расширения файлов.
- Систематизировать список закачек. Возможность создания неограниченного числа категорий и уровней вложенности позволит вам упорядочить список закачек в соответствии с пожеланиями. Вы можете свободно перетаскивать закачки из одной категории в другую, переносить папки из раздела в раздел и менять папки местами.
- Синхронизировать файлы на сервере и локальном компьютере. Данная категория может использоваться для синхронизации файлов, а также для старта

закачек в определенное время. Категория **Автообновление** содержит подкатегории с заданиями на синхронизацию. Вы можете редактировать текущие задания, а также добавлять неограниченное число новых заданий. При необходимости можно приостановить выполнение определенных заданий.

- Стартовать/останавливать/планировать все закачки из категорий можно простым перетаскиванием мышкой. Категория **Состояние** содержит подкатегории, соответствующие возможным состояниям закачек. Перетаскивая закачки из одной папки в другую, удобно управлять процессом закачки. Например, перетащив папку **Пауза** на папку **Закачивается**, можно стартовать все закачки, находящиеся в состоянии паузы; перетащив подпапку **Музыка** в подкатегорию **Запланировано**, можно запланировать все закачки, находящиеся в данной папке и всех подпапках.
- Восстанавливать удаленные закачки вы можете, перетащив их из категории **Удаленные** в любую другую папку. После выхода из программы или перезагрузки компьютера папка **Удаленные** очищается автоматически.

При добавлении закачки происходит распознавание типа файла. Название поля, по которому произошло распознавание, мерцает в течение 5 секунд.

Распознавание типа файлов происходит по их расширению (выполняется для тех расширений, которые прописаны для категорий), а также по регулярным выражениям для интернет-адреса. Нажав кнопку, вы можете:

- вызвать окно свойств для выбранной категории;
- добавить новую подкатегорию;
- установить флажок **Запоминать последнюю папку для категорий**.

ПРИМЕЧАНИЕ

В настройках программы должен быть установлен флажок Распознавать по категориям.

Использование регулярных выражений. Регулярные выражения должны заключаться в одинарные кавычки и отделяться пробелами. Вы можете указывать одновременно как расширения, так и регулярные выражения (приоритет имеют регулярные выражения в порядке их следования, то есть первое регулярное выражение имеет высший приоритет, а последнее из расширений — низший):

- например, благодаря выражению `'download.com'` в категорию будут помещаться все закачки, интернет-адрес которых содержит фразу **download.com**;

- `'(?i)metal{1,2}ica'` — в категорию будут помещаться все закачки, интернет-адрес закачки которых содержит слово **metallica** или **metalica**, независимо от регистра;
- `'(?i)metal{1,2}ica' '(?i)beatles' MP3 OGG` — в эту категорию будут помещаться все файлы, подходящие под регулярные выражения `'(?i)metal{1,2}ica'` и `'(?i)beatles'`, а также файлы с расширениями MP3 и OGG.

Менеджер сайтов. Менеджер сайтов удобно использовать в следующих случаях.

- Если для доступа к сайту или части сайта требуются имя пользователя и пароль.

  При этом вам будет достаточно один раз указать имя пользователя и пароль — в дальнейшем при доступе к этому сайту Download Master будет передавать эту информацию автоматически.
- Если для доступа к сайту требуется использование нестандартных настроек прокси-сервера.

  Вы можете выбрать прокси-сервер, необходимый для подключения к определенному сайту, или отключить использование прокси-сервера для доступа к этому сайту.
- Если файлы, закачиваемые с конкретного сайта, необходимо сохранять в определенную папку или категорию.

  После указания папки или категории для сохранения все файлы, закачиваемые с этого сайта или части сайта, будут сохраняться в указанной папке или категории. Если указаны и папка, и категория, то закачки будут добавляться в указанную категорию, а сохранятся в указанной папке.
- Если для определенных сайтов необходимо ограничивать максимальное число секций на закачку или закачек.

  После указания максимального количества секций на закачку или закачек для всех закачек, производимых с данного сайта или части сайта, число потоков или закачек не будет превышать введенное.

  Существующий список сайтов отображается в виде таблицы. Щелкнув кнопкой мыши на названии столбца, можно отсортировать список в соответствующем порядке, при этом порядок сортировки отобразится в виде стрелки. Со списком сайтов можно выполнять следующее.
- Добавить сайт в список сайтов, для чего используются такие настройки:
  - **Сайт** — адрес сайта или подраздела сайта, например **www.download.com/games**;
  - **Пользователь** — имя пользователя, если для загрузки файлов с сайта необходима авторизация;

  - **Пароль** — пароль для доступа к сайту, если для загрузки файлов с сайта необходима авторизация;
  - **Прокси-сервер** — прокси-сервер, который будет использован для всех закачек с данного сайта;
  - **Сохранять в указанной категории** — категория, в которую будут добавляться файлы, закачиваемые с данного сайта;
  - **Сохранять в указанной папке** — папка, в которой будут сохраняться файлы, закачанные с данного сайта;
  - **Ограничить количество секций на закачку** — максимальное количество секций на закачку для всех закачек, производимых с данного сайта или части сайта;
  - **Ограничить количество закачек** — максимальное количество одновременных закачек, производимых с данного сайта или части сайта.
- Изменить параметры для выбранного сайта. Выбрав сайт из списка и нажав кнопку **Изменить**, вы получите доступ к следующему окну, в котором сможете изменить ранее введенные параметры.
- Удалить указанный сайт из списка сайтов. Выбрав сайт из списка и нажав кнопку **Удалить**, вы удалите сайт.

Использование планировщика. Планировщик позволяет управлять работой Download Master в автоматическом режиме, его удобно использовать:

- когда необходимо или предпочтительно закачивать файлы в определенное время или дни недели;
- если нужно отключиться от Интернета или выключить компьютер в определенное время.

Для выбора файлов, которые будут закачиваться по расписанию, необходимо выбрать в раскрывающемся меню или меню **Файл** пункт **Запланировать**. После этого на значке состояния закачки появится значок, информирующий о том, что данный файл добавлен в список запланированных.

Выбрав пункт **Расписание** в меню **Закачки**, вы попадете в окно настроек планировщика.

Возможен один из трех режимов старта по расписанию:

- **единоразово** — планировщик запустится один раз в указанный день;
- **по дням недели** — планировщик будет запускаться в указанные дни недели;
- **ежедневно** — планировщик будет запускаться каждый день.

После выбора и настройки соответствующего режима вам необходимо указать время запуска планировщика.

Укажите время завершения работы планировщика и при необходимости установите флажок **Выполнять ежедневно**.

Установка действий, выполняемых при завершении работы планировщика — здесь вы можете указать, какие именно действия должны выполняться, когда планировщик завершает работу. Возможно выполнение следующих действий.

- **Выключить компьютер** — если установлен флажок, то Download Master будет выключать компьютер при завершении выполнения расписания.
- **Выход из программы** — если установлен флажок, то Download Master будет завершать работу при завершении выполнения расписания.
- **Отключиться от Сети Интернет** — если установлен флажок, то Download Master будет отключаться от Интернета при завершении выполнения расписания. Работает только при подключении по модемному соединению.
- **Очистить список запланированных задач** — если установлен флажок, то Download Master будет очищать список запланированных задач при завершении выполнения расписания.

Плавающее окошко. Оно имеет несколько функций.

- Информирование об общей скорости закачки. Основную часть окна занимает индикатор, на котором отображается график скорости закачки.
- Информирование о состоянии и проценте выполнения активных закачек. После старта закачки в нижней части плавающего окна появляется полоска, отображающая процент выполнения закачки, а также меняющая цвет в зависимости от того, передаются в данный момент данные или нет. Подведя указатель мыши к полоске, вы получите дополнительную информацию о закачке — название файла, точный процент выполнения и текущую скорость.
- Управление активными закачками. Щелкнув кнопкой мыши на одной из полосок в нижней части плавающего окна, вы откроете информационное окно закачки. Правым щелчком кнопкой мыши на полоске вы можете вызвать меню управления данной закачкой.
- Изменение скорости закачки. Нажав на верхнюю кнопку, вы сможете легко выбрать желаемый скоростной режим.
- Управление программой. Двойной щелчок кнопкой мыши на индикаторе скорости закачки приводит к открытию главного окна программы. Правым щелчком кнопкой мыши вы можете вызвать меню управления программой. Щелчком кнопкой мыши на значке скорости вызывается меню управления программой. Скорость переключается щелчком правой кнопкой мыши. Если

вы щелкнете левой кнопкой мыши на индикаторе скорости закачки, то появится краткий список закачек, доступных для старта/остановки, в котором, щелкнув на закачке, вы можете запустить/остановить ее.

- Добавление новых закачек. Вы можете добавить новые закачки, перетащив ссылку или выделенный текст, содержащий ссылки из браузера или другой программы, в плавающее окно.

СОВЕТ

Включить или отключить отображение плавающего окошка можно из контекстного меню или в меню Вид главного окна программы.

FTP Explorer

FTP Explorer предназначен для навигации по FTP-серверам и поиска файлов, которые необходимо закачать. Навигация при помощи FTP Explorer осуществляется аналогично навигации в **Проводнике** Windows.

Для добавления сайта введите его адрес в соответствующем поле и нажмите кнопку **Открыть**. Одновременно можно открыть несколько сайтов. Однажды задав параметры сайта (имя пользователя и пароль), можно сохранить их в менеджере сайтов (**Использовать для всего сервера**), и в дальнейшем они будут подставляться автоматически.

ПРИМЕЧАНИЕ

Введенные адреса автоматически сохраняются в истории. Для ее очистки используйте Инструменты ▸ Очистить историю URL.

Для закачки необходимо дважды щелкнуть кнопкой мыши на нужном файле либо выделить выбранные файлы в списке и нажать кнопку **Закачать** (можно выбрать аналогичный пункт в раскрывающемся меню). В качестве альтернативы можно перетащить мышью выбранные файлы из списка в плавающее окошко Download Master.

С помощью фильтра можно настроить отображение файлов определенных типов, например EXE и ZIP.

В меню **Избранное** вы можете хранить список наиболее часто посещаемых сайтов, для того чтобы не вводить их адреса вручную.

Для многих пользователей неоспоримое преимущество Download Master перед конкурентами — его полная бесплатность. И при этом никаких баннеров. Download Master за сравнительно короткое время смог завоевать расположение пользователей. И дело не только в бесплатном статусе, но и в том, что

разработчики программы постарались собрать в ней всевозможные настройки, доступные пользователям других менеджеров закачки. Большинству пользователей, судя по результатам опроса, функционала Download Master более чем достаточно. Если вы пользуетесь другим менеджером закачки, не пожалейте времени, скачайте бесплатный Download Master и оцените его преимущества.

FlashGet

Программа FlashGet (**www.amazesoft.com**) — давняя любимица публики, которая, тем не менее, в последнее время сдала позиции. При помощи FlashGet можно дозваниваться в Интернет, производить автоматический поиск зеркал и выбирать самый быстрый вариант загрузки. Программа предлагает три режима скорости закачки файлов: неограниченный, ручной и автоматический. В ручном режиме скорость загрузки определяется пользователем, а в автоматическом программа сама подбирает наилучшую скорость. По умолчанию FlashGet разбивает файл на пять частей, но это количество, равно как и размер одной части, можно изменить. Программа также позволяет просматривать содержимое HTTP- и FTP-серверов, создавать неограниченное количество тематических категорий, в которых для облегчения поиска могут располагаться задания на загрузку.

После завершения установки FlashGet будет запускаться автоматически всякий раз, когда будет предпринята попытка закачать файл через браузер. Для запуска загрузки нажмите кнопку **OK** в появляющемся окне свойств загрузки.

После добавления и настройки вашего прокси-сервера необходимо будет выбрать его в списке прокси-серверов и в окне свойств загрузки (**Сервис ▸ Настройки**).

Добавление задания. FlashGet перехватывает все щелчки кнопкой мыши, выполняемые в окне браузера. Когда выбрана ссылка URL, FlashGet проверяет соответствие расширения загружаемого файла тем, которые вы установите в настройках. Если соответствие найдено, то URL будет добавлен в список заданий. Для удобства можно настроить FlashGet, так чтобы программа перехватывала щелчки кнопкой мышью только тогда, когда нажата клавиша **Alt**.

При копировании адреса ссылки в буфер обмена она автоматически будет добавляться к списку заданий, но только в том случае, если расширение загружаемого файла соответствует указанным в настройках.

Для начала скачивания перетащите любой адрес из окна просмотра браузера в **Корзину** или основное окно FlashGet. Программа выдерживает также перетаскивание сразу нескольких ссылок из окна Internet Explorer.

Кроме того, вы можете ввести адрес вручную: выберите пункт меню **Задания**, затем **Новое задание** и введите адрес.

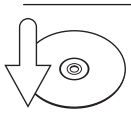
Свойства задания. Щелкните правой кнопкой мыши на неактивном задании в основном окне FlashGet и выберите **Свойства** для изменения свойств этой загрузки. Или просто щелкните кнопкой мыши на значке **Свойства** в панели инструментов FlashGet, чтобы открыть соответствующее окно. Ниже приведены настройки программы.

- **URL** — полный интернет-адрес файла.
- **Найти альтернативный URL через файл списка зеркал или FTP-поиск** — снятие этого флажка отключает список зеркал и FTP-поиск.
- **Ссылка** — некоторые серверы требуют указания этого пункта, для того чтобы запускать загрузку. Оставьте его пустым, FlashGet автоматически введет правильный адрес за вас.
- **Категория** — когда задание будет завершено, файл автоматически переместится в выбранную категорию. По умолчанию это **Принятые**.
- **Сохранить** — загрузка файла в определенную папку, эту настройку изменять не рекомендуется.
- **Переименовать** — сохранение загружаемого файла под другим именем.
- **Http и FTP proxy** — FlashGet имеет настраиваемый список прокси-серверов, из которого пользователь выбирает предпочтительный.
- **Разбить на** — делит файл на 1–10 частей, что значительно увеличивает скорость загрузки. Некоторые пользователи для еще большего увеличения скорости загрузки предлагают разбивать файл более чем на 10 частей. Однако это может привести и к обратному эффекту: скорость значительно уменьшится либо сервер вообще разорвет соединение. С целью предотвращения разрывов соединения не рекомендуется разбивать файлы на 10 частей. В большинстве случаев достаточно 3–5. FlashGet также поддерживает загрузку по расписанию, закачивая файлы в часы, когда загруженность канала минимальна либо дешевле тариф. Это экономит ваше время и деньги.
- **Вход на сервер** — некоторые серверы требуют идентификации пользователя. Введите в эти поля ваши имя пользователя и пароль.
- **Старт** — решите, как запускать загрузку. Если **Вручную**, то происходит только добавление адреса к списку загрузки, но сам процесс не начинается. **Немедленно** — загрузка начинается сразу. **По расписанию** — FlashGet начинает загрузку в запланированное время. Вы можете переключаться между тремя настройками в любой момент, когда это будет нужно.

ПРИМЕЧАНИЕ

При слишком низкой скорости есть возможность остановить загрузку и переключиться на загрузку по расписанию.

- **Сохранить по умолчанию** — сохранение выбранных настроек для использования по умолчанию в других заданиях на загрузку.



СОВЕТ

Настройки могут быть изменены в меню Свойства, если выбрать Параметры закачки по умолчанию.

- **Описание** — по прошествии некоторого времени вы можете забыть, что за файл загрузили. Поместите здесь свои комментарии, чтобы этого не произошло.
- **Удаленные** — все удаленные задания будут перемещены в папку **Удаленные**. Полностью удалить задание можно, удалив его снова уже в папке. Работает по принципу корзины Windows.

СОВЕТ

Можно удалить задание, минуя папку Удаленные, если одновременно нажать клавиши Shift и Delete.

Менеджер файлов. Управление файлами — одна из наиболее важных характеристик FlashGet. Программа распределяет файлы по категориям. Если определить папку для каждой категории, тогда всякий загружаемый файл, соответствующий определенной категории, будет перемещаться в заданное место на жестком диске.

Например, каждое задание, отнесенное к категории MP3, будет перемещаться на `c:\download\mp3`. В пределах каждой категории можно создать подкатегории. По умолчанию имеются три категории FlashGet: **Задания**, **Принятые** и **Удаленные**. Все незаконченные задания хранятся в категории **Задания**, все удаленные — в одноименной категории.

Существуют разные варианты перемещения и удаления заданий. Откройте меню **Сервис ▸ Настройки**, а затем выберите вкладку **Менеджер файлов**. Здесь вы сможете выбрать роль FlashGet при перемещении заданий в другие категории, а также его поведение, в случае если конечный файл уже существует.

Если вы хотите переместить загружаемые файлы на другой накопитель, рекомендуется делать это при помощи FlashGet, иначе могут возникнуть проблемы с базой данных загрузки:

- создайте временную категорию во FlashGet;
- переместите туда все файлы;
- для исходной категории измените папку по умолчанию на путь к другому накопителю (например, `e:\download`);
- переместите файлы в исходную категорию.

СОВЕТ

Можете не указывать категорию при загрузке. Позже можно будет перетащить в необходимую категорию уже готовое задание.

Бытует мнение, что время FlashGet уходит, и эту программу пользователи оставляют на компьютере, скорее, по привычке, чем из-за острой необходимости. Но решать, так это или нет, только вам. Кстати, судя по рейтингу популярности, многие не отказываются от FlashGet, несмотря на присутствие на рынке мощных конкурентов.

ReGet

Программа ReGet (**www.reget.com**) имеет три версии: Junior, Pro и Deluxe. Каждая из них ориентирована на свою категорию пользователей. Базовые функции у всех трех программ одинаковые — отличия только в дополнительных возможностях.

Все версии ReGet отличаются удобным интерфейсом, позволяют восстанавливать оборванные загрузки и производить загрузку в несколько потоков, кроме того, интегрируются с популярными браузерами и дают возможность загружать все ссылки одним щелчком кнопкой мыши.

- ReGet Junior ориентирована на начинающих пользователей и имеет минимальный набор функций. К ее особенностям можно отнести возможность изменения интерфейса при помощи «скинов», которая отсутствует в других версиях программы.
- ReGet Pro может предложить такие настройки, как управление скоростью загрузки, благодаря чему можно одновременно производить загрузку файла и открывать сайты; соединение с Интернетом в случае обрыва связи; управление настройками закачки для нескольких файлов одновременно. Кроме этого, с ее помощью можно автоматически скачивать галереи изображений и проверять загруженные файлы на вирусы.
- Однако для опытного пользователя, проводящего в Интернете много времени, наибольший интерес представляет версия ReGet Deluxe. В ней

пользователям предлагаются встроенный FTP-клиент, расширенные возможности планировщика (например, планирование загрузки на указанную дату, повторение загрузки в указанное время и дни, начало загрузки при выполнении заданных условий), выключение компьютера, возможность сортировки загруженных файлов по папкам и ведение истории закачек.

Если же вы хотите получить в свое распоряжение весь инструментарий программы, но при этом не уверены, нужно ли вам все это ежедневно, можно работать с ReGet Deluxe в упрощенном режиме. Всего в программе предусмотрено три режима: с отображением всех возможностей, большинства настроек или только базовых.

Потенциальным пользователям данной программы хотелось бы дать небольшой совет: не спешите сразу бросаться в бой, скармливая ей килограммы ссылок. Не поленитесь и потратьте пять минут на настройку. Для начала интегрируйте ReGet с используемым браузером, укажите типы расширений файлов, на которые программа реагировать не должна. Кстати, интеграция будет более гибкой, если установить в соответствующих настройках флажок **Добавлять только при нажатом Alt**. Теперь ReGet будет перехватывать ссылки из браузера только в том случае, если при щелчке кнопкой мыши вы удерживаете эту клавишу. Подобная избирательность может пригодиться в тех случаях, когда ReGet неправильно обрабатывает ссылку на файл (такое случается крайне редко).

Способы добавления закачки. Рассмотрим более детально работу с программой ReGet.

Пользователям Internet Explorer, MSN Explorer, NetCaptor или NeoPlanet достаточно щелкнуть кнопкой мыши на ссылке/кнопке закачки, и окно ReGet Deluxe появится вместо стандартного **Сохранить как**. Если этого не случилось, нажмите сочетание клавиш **Ctrl+Alt** и, не отпуская его, щелкните на ссылке еще раз. Выберите **Закачать с помощью ReGet Deluxe** в раскрывающемся меню (щелкните на ссылке правой кнопкой мыши, для того чтобы это окно появилось). Щелкните кнопкой мыши на ссылке, удерживая нажатой клавишу **Alt**, если вы используете Netscape Navigator или Opera.

СОВЕТ

Если вы пользуетесь браузером, основанным на Internet Explorer (например, NetCaptor или MSN Explorer), можно выделить часть текста и перетащить ее в плавающее окно ReGet Deluxe. Программа откроет окно Список ссылок, содержащее все ссылки, найденные в выбранном отрывке текста.

Перетащите ссылку из браузера и вставьте ее в плавающее прозрачное окно ReGet Deluxe.

Можно скопировать необходимый интернет-адрес в буфер обмена и нажать **Ctrl+V**, чтобы вставить его в окно закачек или в меню **Создать новую закачку**.

СОВЕТ

Удерживайте нажатыми клавиши Ctrl+Alt, когда щелкаете на ссылке/кнопке, чтобы вынудить ReGet перехватить закачку (если это не произошло автоматически).

Вы можете также щелкнуть правой кнопкой мыши на значке ReGet Deluxe в системном меню, а затем выбрать **Добавить закачку** из меню.

И наконец, можно вписать адрес вручную, нажав кнопку с изображением плюса. После этого появится окно **Свойства**, в котором вводятся свойства закачки. Если вы хотите сохранить файл под другим именем, введите желаемое имя в поле **Сохранить как**. Если сервер, с которого закачивается информация, требует логин/пароль, то введите их в соответствующие поля.

СОВЕТ

Нажмите одновременно клавишу Ctrl и кнопку Пауза на панели инструментов, чтобы остановить одну секцию выбранной закачки.
Для добавления еще одной секции к выбранной закачке одновременно нажмите клавишу Ctrl и кнопку Старт на панели инструментов.
Удалить не только закачку из очереди, но и закачанный файл с жесткого диска можно, нажав комбинацию клавиш Ctrl+Shift+Delete.

Интеграция с браузером. ReGet Deluxe может автоматически перехватывать закачки и интегрироваться в раскрывающееся меню браузеров, построенных на основе Internet Explorer, следить за буфером обмена (и автоматически предлагать создавать закачку, когда в буфер обмена помещается интернет-адрес). Программа ReGet может также перехватывать закачки из браузеров Netscape и Opera.

Обратите внимание, что интеграция с браузерами на основе Internet Explorer и всеми другими браузерами работает по-разному. В случае с Internet Explorer возможно выбрать один из двух методов интеграции: интеграцию на низком уровне или базовую интеграцию.

В случае использования интеграции на низком уровне ReGet перехватывает окно сохранения файла. Этот метод работает со всеми типами ссылок, включая сложные. Однако это может нарушить работу некоторых других приложений. При щелчке кнопкой мыши на ссылке держите нажатой клавишу **Ctrl**, чтобы избежать активации этого режима и передать ссылку для скачивания Internet Explorer.

СОВЕТ

Запретить перехват закачки можно, удерживая нажатой клавишу Ctrl, когда щелкаете мышью на ссылке/кнопке.
Вы можете передвигать выбранную закачку вверх (вниз), нажимая одновременно Alt и стрелку вверх/вниз.

Использовать базовую интеграцию рекомендуется только в том случае, если низкоуровневая вызывает ошибки в работе других приложений. Этот метод не позволяет перехватывать сложные ссылки — перехватывается лишь интернет-адрес, который затем анализируется, и, если расширение указанного в нем файла не находится в специальном списке **Игнорировать расширение**, появляется окно ReGet с предложением создать закачку (когда включены подтверждения добавления из браузера). Это необходимо, для того чтобы ReGet не пытался перехватывать файлы, предназначенные для интерпретации браузером, — HTML-документы, JAVA-сценарии и прочие.

Для настройки параметров интеграции выберите **Настройки ▸ Интеграция** в главном меню ReGet.

ПРИМЕЧАНИЕ

MSIE Spy — это приложение, которое позволяет отследить все адреса, запрашиваемые браузером Internet Explorer. Если установить на нем флажок в соответствующих настройках, то на панели инструментов Internet Explorer появится кнопка Spy, при нажатии которой станет активным модуль MSIE Spy. Должен быть включен либо MSIE Spy, либо перехват закачек из Internet Explorer, чтобы в ReGet работала возможность автоматического понижения приоритета по трафику во время активности браузера.

Менеджер сайтов. Менеджер сайтов позволяет пользователю установить собственные настройки (такие как логин и пароль, максимум возможных соединений и т. д.) для каждого сервера, с которого будет происходить закачка. Заметьте, менеджер сайтов используется всегда, если очередь закачек непуста: каждый раз, когда вы начинаете скачивать данные с нового сайта, менеджер сайтов создает временную запись для этого сайта (если она еще не существует), используя значения по умолчанию.

Временные записи удаляются из менеджера сайтов после выхода из ReGet Deluxe. Вы можете снять флажок **Временно** в свойствах сайта, чтобы сохранить информацию о нем и после завершения работы с ReGet Deluxe.

Менеджер сайтов может быть полезен в следующих случаях.

- Для работы с сервером требуются логин и пароль. Указать логин и пароль для конкретного сайта можно, установив флажок **Для работы с сервером**

требуется указать логин и пароль в свойствах сайта и указав логин и пароль в соответствующих полях.

- Сервер не позволяет более нескольких одновременных соединений. Многие FTP-серверы не позволяют более одного одновременного соединения. Используя поле **Количество одновременных соединений с этим сервером**, вы можете указать количество позволенных соединений (например, одно). Обратите внимание, что для вновь создаваемых записей для FTP-сайтов по умолчанию используется одно соединение.

Рассмотрим некоторые настройки в менеджере сайтов (меню **Свойства ▸ Все настройки**).

- **Путь в URL указан относительно домашнего каталога** — установите этот флажок, если хотите, чтобы ReGet воспринимала все вводимые адреса относительно домашнего каталога на FTP-серверах.
- **Не посылать команду LIST** — позволяет существенно увеличить скорость скачивания с FTP-серверов. Установка этого флажка может понадобиться при работе с некоторыми необычными FTP-серверами, которые не отвечают на команду `list`, хотя это может повлиять на способность корректно определять размер файла при скачивании с обычных FTP-серверов.
- **Использовать команду MDTM для получения информации о времени создания файла** — вынуждает ReGet Deluxe использовать команду `mdtm` для получения точной информации о времени создания/модификации файла. Это может незначительно замедлить скачивание с FTP-серверов, однако настройка очень важна, если вы хотите синхронизировать содержание удаленного и локального дисков.
- **Пауза между попытками** — время (в секундах), которое должно пройти, прежде чем ReGet Deluxe предпримет следующую попытку закачки.
- **Таймаут** — время (в секундах), которое должно пройти, прежде чем ReGet прервет закачку по тайм-ауту.
- **Таймаут незадействованных соединений** — время (в секундах), по истечении которого ReGet отсоединится от FTP-сервера, если нет активных закачек с этого сервера. Вы можете использовать данную возможность для ускорения закачки, если в очереди находится несколько закачек с одного FTP-сервера. Если этот параметр не равен нулю, то программа ReGet не будет отсоединяться от сервера после окончания закачки, и это позволит сэкономить время, не тратя его на установку соединения для новой закачки.

Поиск. Встроенная в ReGet Deluxe функция поиска позволяет искать в Интернете файлы для последующей закачки. Если вы хотите найти музыкальные файлы в MP3-формате, выберите **MP3** из раскрывающегося списка.

Поиск работает так: после введения ключевых слов в строку поиска и нажатия кнопки **Поиск** программа начинает рассылать запросы по выбранным поисковым системам (чтобы увидеть список поисковых систем и выбрать нужные, щелкните на кнопке **Поисковые системы**). Обратите внимание, что запрос выполняется с использованием логического оператора «И», то есть он включает в себя все введенные слова. После того как поисковые системы возвращают результат, ReGet Deluxe удаляет повторяющиеся ссылки и проверяет, работают ли серверы, на которых находятся найденные файлы.

В ReGet Deluxe предусмотрена возможность отсортировать список результатов поиска по любому из перечисленных выше критериев, чтобы было легче выбрать файл для скачивания. Щелкните кнопкой мыши на заголовке нужной колонки один раз, чтобы отсортировать результаты по восходящей, и два раза, чтобы отсортировать по нисходящей.

Обратите внимание, что некоторые из найденных файлов не могут быть скачаны непосредственно после поиска, так как находятся на ratio-сайтах, баннерных ресурсах, недоступных серверах или просто отсутствуют на сервере (были удалены или переименованы).

ПРИМЕЧАНИЕ

Ratio-сайты требуют сначала закачать на них один или несколько файлов, чтобы получить доступ к MP3, хранящимся на сервере.
Баннерные сайты требуют, чтобы вы прочитали приветственное сообщение и последовали содержащимся в нем инструкциям: например, щелкнули кнопкой мыши на баннере и посетили сайт, на который он ведет. Только после этого можно будет скачать нужный файл.

При поиске старайтесь менять пробелы на знаки подчеркивания в имени исполнителя и в названии песни. Например, если вы ищете «Foxy Lady» Дж. Хендрикса, введите в строке поиска: `Hedrix_-_Foxy_Lady.mp3`. Как правило, имена MP3-файлов конструируются именно таким способом.

Если вы хотите начать новый поиск, не удаляя результаты предыдущего, введите название песни или исполнителя и нажмите кнопку **Поиск**, удерживая нажатой клавишу **Shift**.

Если хотите найти фразу целиком, а не по отдельным словам, заключайте ее в кавычки (например, `"beautiful pictures"`).

Щелкните на файле правой кнопкой мыши и выберите команду **Проверить URL** из контекстного меню, чтобы проверить, можете ли вы закачать конкретный файл и на каком типе сервера он находится. Нажмите кнопку **Проверить все** на панели инструментов ReGet Deluxe или выберите команду **Проверить все** из контекстного меню, чтобы проверить таким образом все файлы из списка.

После проверки рядом с именем файла появляется значок, показывающий статус файла (сервера).

- **Хороший** — файл может быть скачан без проблем. Для этого выберите **Скачать** из контекстного меню или дважды щелкните на файле кнопкой мыши.
- **Доступ запрещен** — вы должны закачать один или несколько своих файлов на сервер, чтобы получить право скачать с него что-нибудь.
- **Плохой** — вы не можете скачать этот файл. Возможно, сервер, на котором находится файл, не отвечает, или файл на сервере не найден.
- **Занят** — сервер, на котором расположен файл, в данный момент занят (к нему подключено одновременно слишком много пользователей). Подождите некоторое время, прежде чем предпринять следующую попытку скачивания.

После завершения проверки на статус ReGet Deluxe также проверяет, поддерживают ли найденные серверы докачку после обрыва связи, и помещает рядом с именем файла соответствующий значок:

- **Докачка поддерживается** — этот сервер поддерживает докачку, так что после обрыва связи вы можете продолжить скачивание с того места, где связь оборвалась;
- **Докачка не поддерживается** — сервер не поддерживает докачку, поэтому после обрыва связи вам придется качать файл с самого начала.

FTP Explorer. В новой версии ReGet Deluxe появилась новая особенность — FTP Explorer, которая предназначена для облегчения скачивания файлов с FTP-серверов. Кнопка, активирующая панель **FTP Explorer**, расположена на панели ReGet (также можно воспользоваться сочетанием клавиш **Alt+7**). Чтобы начать навигацию по серверу, нужно ввести его адрес в поле **Address** и нажать клавишу **Enter** (или кнопку **Go**). Префикс `ftp://` вводить необязательно.

Список внизу будет содержать имена каталогов и файлов, расположенных на этом сервере. Имена каталогов выделены жирным шрифтом, имена файлов — курсивом. Для входа в директорию (или скачивания файла) нужно дважды

щелкнуть на ней (в случае щелчка кнопкой мыши на имени файла это приведет к созданию закачки). Если для работы с этим сервером необходимо указать какие-то специфические для сервера настройки, то для этого можно воспользоваться менеджером сайтов.

Увеличить скорость работы программы с большими очередями можно, воспользовавшись следующими советами:

- выключите автоматическое сохранение файла очереди (**Настройки ▸ Настройки программы ▸ Все настройки ▸ Общие настройки ▸ Автоматически сохранять файл очереди**);
- уменьшите количество сохраняемых строк в журнале каждой закачки, чтобы уменьшить использование памяти (**Настройки ▸ Настройки программы ▸ Все настройки ▸ Настройки лога ▸ Количество строк в логе закачки**);
- выключите возможность подсветки трафика для выделенных закачек (**Настройки ▸ Настройки программы ▸ Все настройки ▸ Внешний вид**);
- полезно также отключить настройку **Анимированная иконка** (**Настройки ▸ Настройки программы ▸ Все настройки ▸ Внешний вид ▸ Показывать иконку в панели задач ▸ Анимированная иконка**), чтобы уменьшить использование процессорного времени, что особенно заметно на компьютерах малой мощности.

Возможности браузеров

Глобализация семимильными шагами продолжает топтать индивидуальность, и это видно даже на программах. Создается впечатление, что скоро все программные решения будут уметь делать все, для чего ранее требовалось несколько разных программ. Например, Nero раньше умела записывать CD и DVD, сейчас же при помощи этой программы можно смотреть фильмы, слушать музыку и просматривать картинки. Winamp уже мало проигрывания музыкальных файлов — теперь с ее помощью можно смотреть фильмы.

Аналогично себя ведут и разработчики браузеров — обучают свои детища всему и сразу. Начинают усиливаться те функции, которые изначально не рассматривались в качестве основных. Например, функция загрузки файлов.

Разработчики расширений для браузера Firefox (**www.mozilla.com/firefox**) в этом отношении постарались на славу. Энтузиастами была создана целая серия расширений, позволяющих сделать процесс закачки более эффективным.

Самым популярным расширением является FlashGot (**addons.mozilla.org/firefox/220** или **www.flashgot.net/getit**). Оно добавляет в Firefox интеграцию

с менеджерами закачек Download Master, FlashGet, Free Download Manager, GetRight, Internet Download Accelerator, Leechget, Net Transport, Reget (Deluxe, Junior, Pro). Закачать ссылку при помощи FlashGot можно, выбрав соответствующий пункт меню, нажав сочетание клавиш **Ctrl+F1** или щелкнув кнопкой мыши на ссылке, удерживая нажатой клавишу **Alt**. Загрузка происходит через установленный по умолчанию менеджер загрузки.

FlashGot также захватывает ссылки в подсвеченном тексте или изображениях, пытаясь преобразовать чистый текст в ссылки. Производится до некоторой степени разумная замена, превращающая `hxxp://` в `http://` (адреса вида **hxxp://www.rapidshare.de** часто используются для маскировки от автоматических программ — так называемый «антилич»).

При помощи FlashGot можно закачать все ссылки, найденные на текущей странице (через раскрывающееся меню или одновременным нажатием клавиш **Ctrl+F3**).

FlashGot также перехватывает окно открытия файла Firefox, давая вам шанс подменить встроенный менеджер загрузки непосредственно перед его запуском. Если вы хотите, чтобы файлы данного типа всегда обрабатывались FlashGot, установите флажок **Выполнять для всех таких файлов автоматически** в нижней части окна.

FlashGot правильно посылает адрес источника ссылки, обнаруженного Firefox, внешнему менеджеру загрузки, что необходимо для многих сайтов, на которых строго отслеживаются адреса пользователей, загружающих файлы.

Файлы COOKIE текущего сеанса Firefox также сохраняются, чтобы избежать проблем с сайтами, которые требуют постоянного прослеживания учетной записи.

Если FlashGot выступает только в роли посредника, передавая указания менеджеру загрузки, то следующие расширения с готовностью выполняют функцию закачки файлов из Сети.

- DownloadStudio Integration (**addons.mozilla.org/firefox/627**) — это расширение интегрирует менеджер загрузки DownloadStudio в Firefox.
- SpiderZilla (**spiderzilla.mozdev.org**) — пригодится, если вы хотите скачать сайт целиком на локальный компьютер с рекурсивным построением структуры файлов и папок внутри. Есть возможность восстановления прерванной закачки и обновления ранее скачанного сайта.
- Download Manager Tweak (**addons.mozilla.org/firefox/256**) — модификация менеджера загрузки Firefox, которая позволяет сделать его более

функциональным и, самое главное, — добавить кнопку **Пауза** (возможность приостановить закачку).

Рекомендовать к ознакомительной установке можно также следующие расширения.

- Save Image in Folder (**addons.mozilla.org/firefox/614**) — позволяет сохранять картинки в заранее заданные папки.
- Backgroundimage Saver (**addons.mozilla.org/firefox/1853**) — это простое расширение помогает бороться с различными техниками защиты изображений от копирования. К примеру, часто искомое изображение «прячется» под прозрачной GIF-картинкой, в результате чего вы не можете щелкнуть правой кнопкой мыши и применить команду **Сохранить как**.
- VideoDownloader (**addons.mozilla.org/firefox/2390**) — позволяет закачивать видео, MP3, флэш-ролики с Google, Metacafe, iFilm, Dailymotion (всего около 60 подобных сервисов).

В контексте функциональности встроенного менеджера загрузки про Internet Explorer нельзя сказать ничего хорошего. Одна из лучших надстроек для Internet Explorer под названием Maxthon (**www.maxthon.com**) этого не исправляет. Приходится пользователям Internet Explorer в обязательном порядке использовать менеджер загрузки от стороннего производителя, другой альтернативы нет.

Как закачивать сайты целиком?

В Сети полно полезных ресурсов с ценными энциклопедическими данными, полезными книгами в HTML-формате, галереями фотографий и т. д. Порой бывает, что так и хочется получить сайт во владение, чтобы тщательно просмотреть, не беспокоясь о счете за Интернет. Конечно, можно сохранить несколько страниц на жесткий диск. Но если этих страниц десятки, а то и сотни, и сделаны они в виде базы данных? Очень скоро вы устанете сохранять страницы, а потом просто собьетесь со счету и элементарно запутаетесь.

Благодаря специальным программам, которые умеют сохранять на диск целые сайты, перенести содержимое любого ресурса с сохранением его структуры вполне возможно.

WebCopier

Поскольку программа WebCopier (**www.maximumsoft.com**) является разработкой отечественных программистов, то и с поддержкой русского языка нет ни-

каких проблем. Для ее активации нужно зайти в меню **Edit ▸ WebCoper options ▸ Language** и выбрать русский язык.

Для создания проекта по закачке сайта в главном окне программы WebCopier проследуйте в меню **Файл ▸ Создать**, и перед вами появится мастер, в котором необходимо задать основные настройки для успешного скачивания указанного ресурса. После создания проекта запустить процесс можно следующим образом: зайдите в меню **Проект ▸ Начать Загрузку**.

WebCopier во время загрузки показывает, какие файлы загружаются в данный момент.

Teleport Pro

Программа Teleport Pro (**www.tenmax.com**) отличается простым и логическим интерфейсом, а также большим количеством настроек. Создать новый проект для закачки можно как с помощью мастера, так и вручную. При создании нового проекта важно правильно установить глубину закачки. С помощью встроенного планировщика задается расписание, по которому скачиваются сайты. Teleport Pro может работать через прокси-сервер и поддерживает закачку в несколько потоков.

Создавая новый проект, на первом шаге вы выбираете структуру будущего сайта, затем вводите адрес ресурса, указываете, с какими расширениями файлы нужно скачивать, и все — мастер завершил работу, можно запускать проект на исполнение. Копирование из Сети сопровождается полной визуализацией рабочего процесса. После сохранения файла проекта в главном окне можно увидеть две панели. В левой панели показана древовидная структура сайта, а в правой — непосредственно файлы. Весь проект с любым количеством стартовых адресов сохраняется в одном файле, открыв который вы получите доступ ко всем скачанным страницам.

ПРИМЕЧАНИЕ

Некоторые сайты содержат прямой запрет на использование офлайн-браузеров. Teleport Pro умеет менять идентификацию и прикидываться, например, Internet Explorer или Opera для корректной работы с сайтами.

Teleport Pro может дозваниваться до провайдера при запуске, разъединяться по завершении задания или при закрытии. Программа также позволяет лимитировать место для закачки. Если объем закачиваемого сайта достигает указанной величины (по умолчанию 24 Мбайт), то скачивание приостанавливается.

В программу встроен планировщик — проекты автоматически запускаются и останавливаются в заданное время. Очень удобно для закачки по ночам (обычно ночью Интернет дешевле и скорость больше).

Можно ли организовать закачку прямо из командной строки?

Интернет в нашу жизнь, порой, чтобы быть «в курсе», приходится несколько раз в день соединяться с Сетью. Проще, когда речь идет о текстовой информации, сложнее, когда требуется регулярно обновлять базу данных или заархивированный прайс. Вот тут-то и поможет простая утилита командной строки под недвусмысленным названием URL2File (**www.chami.com/free/url2file_wincon.html**). Используя ее вместе с гибким планировщиком (например, nnCron), можно автоматизировать рутинные процессы. Предположим, вы занимаетесь перепродажей компьютерных комплектующих и нужно постоянно иметь у себя «свежие» прайсы. Закачать архив с прайсом с сайта какой-нибудь компании для URL2File — элементарная задача. В каталоге с программой выполните команду: `url2file.exe http://www.cpu.by/uni_price.ZIP price.ZIP`. Синтаксис таков: `адрес_с_которого_качать имя_под_которым_сохраняем`.

Еще одна консольная утилита — wGet (**users.ugent.be/~bpuype/wget**), которая умеет работать как с HTTP, так и с FTP-серверами. wGet поддерживает докачку при обрыве соединения. Простейший пример использования: `wget.exe -P "c:downloads" "http://download.ru/myfile.ZIP"` или `wget.exe -P "c:downloads" "ftp://download.ru/myfile.ZIP"`. Ключ `-P` указывает каталог, в который надо производить сохранение файла. Путь, как и адрес, рекомендуется заключать в кавычки, иначе файлы с пробелами в именах будут неправильно обрабатываться.

Средство очень гибкое в настройке, так как ключей у программы огромное количество. При помощи wGet можно даже закачивать сайты целиком.

Учет трафика

Если вас интересует вопрос — сколько мегабайт данных перекачивает ваш модем, то помогут специализированные программы. К сожалению, встроенные средства Windows не позволяют сделать это максимально комфортно.

Одна из наиболее известных программ в своем роде — TMeter (**www.tmeter.ru**). Она предоставляет возможность учета и контроля трафика. Собранная стати-

стика тут же отображается на экране (в графическом или цифровом виде). TMeter имеет немного сложную для освоения систему фильтров трафика, позволяющую считать только полезный трафик. В бесплатной версии количество фильтров ограничено, однако для домашнего использования их вполне достаточно.

Рассмотрим основные возможности программы:

- учет трафика по любому протоколу (TCP/UDP-порту);
- графический вид представления счетчиков в виде кривой линии;
- автоматическое ежедневное и/или ежемесячное формирование отчетов по счетчикам;
- протоколирование подсчитанных пакетов в файл или базу данных;
- возможность блокирования трафика при достижении заданного лимита;
- одновременный сбор трафика с нескольких сетевых адаптеров;
- удаленное администрирование;
- ограничение скорости.

Скорость доступа в Интернет очень маленькая, хотя провайдер обещал 256 Мбайт/с. Можно ли проверить провайдера?

При покупке у провайдера услуги доступа в Интернет пользователи, как правило, договариваются на какую-то скорость, например не ниже 128 Мбайт/с. Ежемесячно платят деньги, а скорость оценивают обычно «на глаз» — быстро, медленно, очень медленно. Перечисленные ниже онлайновые инструменты помогут провести тест скорости интернет-соединения и получить данные в цифрах, а не в абстрактных понятиях. Опираясь на эти цифры, можно либо ругаться с провайдером по поводу низкой скорости, либо искать нового. Итак: **www.speedtest.net**, **www.speed.yoip.ru**, **www.2ip.ru**, **www.computer.md** и **www.alvisnet.ru/useful**.

Воспользуйтесь показателем каждого ресурса, и получившаяся в результате средняя скорость как раз будет той самой усредненной цифрой, которую можно будет показать провайдеру.

Довольно полезным ресурсом является также **www.traceroute.org**, здесь вы можете посмотреть маршруты трассировок из любой страны.

Как узнать, каким шрифтом сделана надпись на картинке?

Поможет сайт **www.myfonts.com/WhatTheFont**. Для работы с ресурсом потребуется графическое изображение, содержащее анализируемый текст. Годятся картинки в форматах GIF, JPEG, TIFF и BMP, ограничен лишь максимальный размер: 360 × 275 пикселов. Оптимальным для системы является размер отдельного символа в пределах 100 пикселов (больший размер увеличивает время поиска совпадений). Ссылаясь на ограничение картинки по ширине, изображение будет содержать всего 3–4 символа, но этого вполне достаточно для определения похожих шрифтов.

Сервис успешно работает с цветными картинками, однако высокой точности можно добиться только на черно-белых изображениях.

Как можно обмениваться большими фрагментами текста через Интернет или совместно работать над документом?

Можно использовать сайт **docs.google.com**, но здесь нужна регистрация. Есть способ попроще: наберите в браузере `cl1p.net` и затем любую комбинацию символов (например, `cl1p.net/privet727`), и перед вами появится окно текстового редактора, в которое вы можете вставить любой текст, прикрепить вложение (не более 2 Мбайт) и указать, сколько хранить этот документ на сервере ресурса **www.cl1p.net**. Доступен будет документ по тому адресу, который вы указали после слэша. Полный адрес (например, `cl1p.net/privet727`) можно посылать друзьям, чтобы ознакомить их с какой-либо информацией.

С помощью каких программ можно отслеживать обновление сайтов?

«Что новенького?» — вопрос, который в нашем мире звучит все чаще. Человечество неудержимо гонится за новостями и новшествами, оставляя позади лишь прочитанные заголовки. На то, чтобы до конца осознать полученную информацию, не хватает времени.

Не пропускать ничего нового на любимых сайтах и своевременно реагировать на обновление контента вам поможет WebSite-Watcher (**www.aignes.com**). Главное окно программы разделено на две части. В левой — дерево папок со вкладками. В правой — собственно, сами вкладки сайтов. Импортировать вкладки

можно, отправившись в меню **Tool ▸ Im/Export**, спектр возможностей довольно широк (рис. 12.11). Останется только «расфасовать» свою коллекцию по соответствующим папкам.

Рис. 12.11. Окно программы WebSite-Watcher

К примеру, вы постоянный посетитель какого-либо сайта. Выберите в правом окне «жертву», щелкните на ней правой кнопкой мыши и затем в открывшемся меню выберите **Properties**. В появившемся окне на вкладке **AutoWatch** можно настроить интервал, с которым WebSite-Watcher будет проверять данную страницу, указать определенные дни недели. Еще одна приятная особенность есть на вкладке **Keywords**. Здесь можно указать ключевые слова, появление которых следует отслеживать. На вкладке **Actions** указывается действие, которое выполняется, если сайт обновился. Можно воспроизвести звук, отправить электронное письмо или запустить нужную программу (например, браузер). Выбирайте на свой вкус.

Начать можете с тотальной инспекции всех вкладок — меню **Bookmarks ▸ Check all Bookmarks** или нажмите клавишу **F9**. Появится окно с индикатором процесса. Программа зафиксирует все ошибки в специально отведенной для этих целей папке **Errors**. Для экономии времени воспользуйтесь выборочной проверкой. У любой папки в левой части окна есть всплывающее меню, в котором доступны команды **Check Folder** или **Check Folder and Subfolders**. Выделите мышью необходимые сайты, после чего опять отправляйтесь в меню **Bookmarks ▸ Check selected Bookmarks** и проверяйте выделенные вкладки.

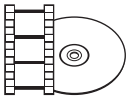
Временные интервалы проверок устанавливаются как для всех папок, так и для каждой закладки в отдельности, но можно проверить наличие обновлений принудительно в любое удобное для вас время при помощи пункта меню **Bookmarks ▸ Check Bookmarks (Extended options)**, здесь следует установить флажок **Ignore all time settings**.

Воспользоваться встроенным просмотром интернет-страницы можно, выбрав в правой части главного окна какой-либо адрес и дважды щелкнув на нем кнопкой мыши (либо нажав сочетание клавиш **Ctrl+0**). Установите флажок **Highlight changes** на панели инструментов внутреннего браузера, и все изменения будут подсвечиваться цветом.

В программе реализованы сразу два вида поиска.

- Первый — для начинающих пользователей. Он расположен в меню **Search ▸ Find**, здесь нет никаких настроек, ничего лишнего — одинокая строка для ввода поисковой фразы. WebSite-Watcher просматривает свою базу и автоматически перемещает указатель мыши на вкладку, где содержится указанное словосочетание.
- Второй вариант (**Search ▸ Extended Search**) позволяет искать в определенной папке, не учитывать регистр символов, проверять только новые или старые версии файлов. В общем, поиск для «продвинутых» с поддержкой регулярных выражений.

Программа WebSite-Watcher способна не только осуществлять контроль обычных сайтов, но и следить за обновлениями по FTP-серверам.



ВИДЕОКУРС

Просмотрите видеоурок «Урок 21. Программа WebSite-Watcher» и научитесь пользоваться описанной утилитой для отслеживания обновлений любимых сайтов.

Программа WatzNew (**www.watznew.com**) — более простая альтернатива WebSite-Watcher. WatzNew ведет себя гораздо скромнее: компактна, не отнимает лишней памяти и места на **Рабочем столе**. Несмотря на кажущуюся простоту интерфейса, WatzNew обладает широкими возможностями.

ПРИМЕЧАНИЕ

RSS — семейство XML-форматов, предназначенных для описания лент новостей, анонсов статей, изменений в блогах и т. п. Информация из различных источников, представленная в формате RSS, может быть собрана, обработана и представлена пользователю в удобном для него виде специальными программами-агрегаторами.

Для отслеживания обновлений также удобным будет использование RSS-ленты.

Feedreader (**www.feedreader.com**) — свободно распространяемая программа для Windows. Имеет систему обновления каналов и фильтрации с помощью ключевых слов. После установки программа не требует особой настройки. Достаточно лишь добавить RSS-ленту, на которую вы желаете подписаться. Пользователь может настроить внешний вид лент, выводить в них изображения и просматривать заголовки статей (рис. 12.12).

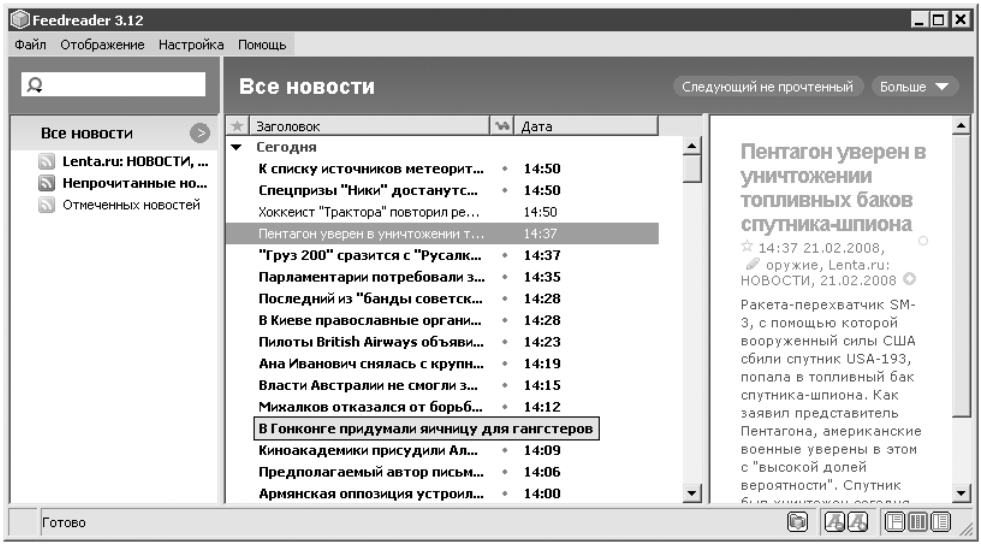


Рис. 12.12. Окно программы Feedreader

RssReader (**www.rssreader.com**) — утилита, мало отличающаяся от Feedreader по функционалу. Реализована на платформе .NET Framework 1.1.

Как узнать дату обновления страницы?

Не всегда авторы сайтов ставят дату обновления страницы, из-за чего пользователи тратят драгоценное время, «рыская» по старому контенту в поисках чего-нибудь новенького. Взять все в свои руки поможет JavaScript. Чтобы узнать дату обновления страницы, на которой вы находитесь, следует в адресной строке браузера набрать команду `javascript:alert(document.lastModified)` и нажать клавишу **Enter**.

Перетащите значок интернет-страницы (крайний левый угол в строке адреса) в **Избранное**, чтобы не запоминать эту команду и не набирать ее вручную.

При необходимости нужно будет просто щелкнуть кнопкой мыши на соответствующем элементе в меню **Избранное**.

Однако для динамических страниц дата обновления будет указана, скорее всего, неверно, так что использовать эту хитрость можно только на обычных HTML-страницах.

Что такое IP-телефония?

IP-телефония вызывает массу эмоций у пользователей и у операторов классической телефонной связи. У первых — эмоции в основном положительные, у вторых — сугубо отрицательные, потому что посредством IP-телефонии можно совершать звонки по всему миру в десятки раз дешевле, чем если бы вы звонили по обычному телефону. Кроме обычных телефонных разговоров, посредством IP-телефонии можно устраивать многопользовательские аудио- и видеоконференции (когда в разговоре участвует несколько человек), посылать факсы.

IP-телефония — это довольно обширное понятие. Наибольшего внимания заслуживает понятие технологии VoIP, или же просто интернет-телефонии. Это частный случай IP-телефонии, требующий от каждого из участников сетевого разговора подключенного к Сети компьютера (поэтому часто обозначается как схема «компьютер — компьютер»). В этом случае не требуется установки какого-либо оборудования, понадобится только специальное программное обеспечение. Возможны еще схемы «компьютер — телефон» и «телефон — телефон». Ниже схемы IP-телефонии описаны подробнее.

- При связи «компьютер — компьютер» используется следующий алгоритм. Записанная на микрофон речь отправителя преобразуется в цифровую. Затем оцифрованный сигнал сжимается в зависимости от алгоритмов сжатия в 4, 8 или 10 раз (удаляются ненужные шумы, оптимизируется кодирование), разбивается на пакеты данных и отправляется по назначению. Система IP-телефонии получателя принимает пакеты и отправляет закодированный голос на раскодирование, после чего цифровой сигнал конвертируется обратно в аналоговый, который уже выводится на колонки или наушники.
- Немного по-другому обстоит дело в простейшей схеме «компьютер — телефон». Пакеты отправляются не напрямую получателю, а провайдеру услуг IP-телефонии, который выступает в качестве посредника, — декодирует сигнал в аналоговый и передает его по телефонным сетям абоненту.
- И наконец, «телефон — телефон». Два абонента связываются по телефону, сигнал идет не по стандартным коммутационным телефонным сетям, а по их IP-аналогам, что является очень выгодным решением. Абонент по обычному

телефону получает доступ к шлюзу, заставляя последнего соединить его с нужным номером. Шлюз анализирует номер и решает, какой его собрат имеет с этим номером самую быструю связь. Далее два шлюза соединяются (может быть, даже через Интернет), и через выходной шлюз, связанный со своей телефонной сетью, вызывается требуемый абонент.

IP-телефония во много раз эффективнее в использовании, чем обычные телефонные линии. Дело в том, что классические телефонные сети для разговора двух абонентов нуждаются в физическом выделенном канале. Это неудобно и невыгодно сразу по двум причинам. Во-первых, кабель стоит денег, а его протягивание и, в случае чего, ремонт требуют времени и нудной работы. Во-вторых, в аналоговых системах присутствует эффект бесполезной траты ресурсов, которые можно было бы выгодно использовать, экономя значительную сумму. Даже если вы молчите в трубку, канал все равно занят. В сетях IP-телефонии вся информация передается по виртуальным каналам, не зависящим от каких-либо физических факторов.

Частный случай IP-телефонии — интернет-телефония — очень распространен и широко используется сотнями тысяч людей в разных странах, и выбор этот сделан неспроста. Позвонить через Интернет из России в Австралию будет стоить почти в несколько десятков раз дешевле, чем сделать это, прибегая к услугам обычной международной связи. Эта огромная разница в цене очень тревожит операторов традиционной телефонии, потому что представляет для нее реальную угрозу полного вытеснения.

Есть у IP-телефонии и свои недостатки: так как передача данных идет по протоколу TCP/IP, который изначально создавался для других целей, то плохая связь может привести к «глотанию» слов, бульканью и иногда к полной потере связи. Еще одно неудобство — динамичность телефонных IP-адресов. Это означает, что создать единую записную книжку, по которой из любой программы для интернет-телефонии можно вызвать абонента, невозможно. В рамках одной утилиты эта проблема решаема. Еще одним минусом IP-телефонии является безопасность работы. Существует несколько основных видов угроз, представляющих наибольшую опасность для абонентов:

- перехватить звонок абонента 1 к абоненту 2 можно, если просто войти в сеть, выдав себя за абонента 2 (так называемое «похищение звонка»);
- можно прослушать разговор двух абонентов, а также любой трафик в VoIP-сети, используя специальную программу.

Сооружение серьезной системы, построенной на базе IP-телефонии, обойдется в несколько десятков, а то и сотен тысяч долларов. Если же речь идет

об интернет-телефонии, то потребуется только одна из нижеперечисленных программ.

- Наиболее популярной и достойной программой для интернет-телефонии является Skype (**www.skype.com**). После установки она настраивается автоматически и работает по технологии, схожей с пиринговыми сетями, то есть у нее нет центрального сервера, который обрабатывает звонки. Все клиенты соединяются друг с другом напрямую (рис. 12.13). Программа Skype хорошо защищена с помощью самого современного алгоритма шифрования AES (Advanced Encription Standart) и не испытывает трудностей при работе с брандмауэрами. Качество голоса в Skype на высоте.

  Программу Skype использует много людей, она превращается в своеобразный стандарт. Нередко в подписи к электронному письму можно увидеть примерно такие строки: «Теперь вы можете общаться со мной не только по почте, ICQ, но и через Skype; мой ID — x403.minsk».

- Интернет-пейджер ICQ тоже предоставляет своим пользователям услуги интернет-телефонии. Для этого требуется плагин ICQ Phone, который изначально не идет в комплектации с ICQ. Настроить эту функцию можно, если зайти в пункт **Services ▸ Icq Phone** и, если плагин еще не установлен, скачать его.

  Пользователи, имеющие возможность принимать звонки по схеме «компьютер — компьютер», помечаются в контакте телефонной трубкой правее «ника». Вызвать абонента можно, щелкнув на его «нике» правой кнопкой мыши (или левой, в зависимости от того, как настроен клиент ICQ) и выбрав пункт меню **ICQPhone ▸ Send PC-to-PC call**. В ICQ также имеется возможность звонка в любую точку мира на обычный телефон, но за это придется заплатить.

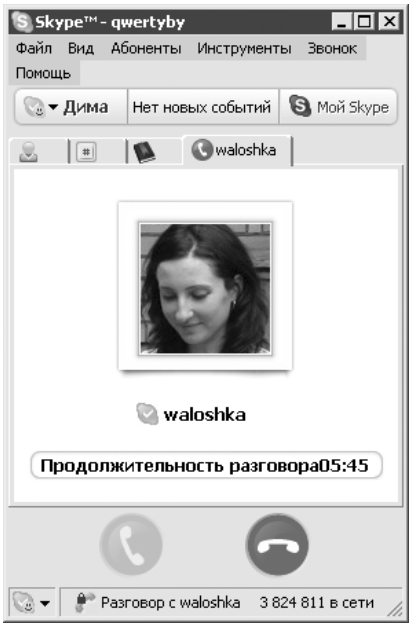
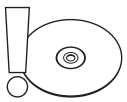


Рис. 12.13. Skype помогает общаться с любимыми

Что такое пиринговые сети?

Пиринговые сети основаны на таком механизме передачи информации: один пользователь позволяет скачивать у него файл (дает информацию), а другой, в свою очередь, тоже делится тем, что у него есть.



ВНИМАНИЕ

Довольно часто путают названия клиентских программ для пиринговых сетей с названиями самих P2P-сетей. К примеру, сеть FastTrack нередко называют Kazaa, хотя Kazaa — это всего лишь одна из нескольких клиентских программ для работы в сети FastTrack. Нередко также приходится слышать о несуществующей сети eMule. На самом деле сеть называется eDonkey2K, а eMule — самый популярный клиент для этой сети.

Ошибочно полагать, что пиринговые сети — это только обмен файлами. К данному классу сетей относятся и системы распределенных вычислений. Наверное, самая распространенная из них — SETI@Home (Search for Extra-Terrestrial Intelligence At Home — поиск инопланетного разума на дому). Этот проект, стартовавший в 1996 году, представлял собой хранитель экрана, который запускался во время простоя компьютера пользователя и обрабатывал данные, поступающие от радиотелескопа. Цель проекта — поиск внеземных цивилизаций. С тех пор SETI@Home заинтересовалось свыше 3 млн людей. Другим примером распределенных вычислений может послужить такой проект, как **www.distributed.net**, участники которого занимаются легальным взломом криптографических шифров, чтобы проверить их стойкость.

Примером так называемых смешанных пиринговых сетей является ICQ — детище израильских программистов (**www.icq.com**). ICQ позволяет своим пользователям быстро и без особых проблем находить собеседников и друзей по интересам для общения через Интернет. Помимо этого, пользователи могут обмениваться файлами. Центральный сервер Mirabilis используется как посредник. Вы с помощью сервера находите интересного вам человека и дальше устанавливаете соединение уже непосредственно с ним.

Проектов, подобных ICQ, на сегодняшний день существует достаточно много. Например, Yahoo! (**www.messanger.yahoo.com**), MSN Messanger (**www.msn.com**), AOL Internet Messanger (**www.aol.com/aim**).

Однако увидеть весь потенциал пиринговых сетей пользователи Интернета смогли, только когда 18-летний студент Ш. Феннинг представил бета-версию проекта, который вскоре получил название Napster. Студент бросил учебу, и уже в сентябре того же года служба была введена в эксплуатацию — она требовала наличия у пользователей специальной программы под названием Napster, позволявшей бесплатно скачивать через Интернет данные, предоставляемые другими пользователями.

Популярность Napster быстро возросла. В течение нескольких месяцев с момента начала работы она достигла колоссальных размеров: ежедневно через Napster проходили сотни тысяч файлов. Обмен большей их части осуществлялся

нелегально. Владельцы авторских прав (издательские фирмы, звукозаписывающие и другие компании) реагировали на сложившуюся ситуацию должным образом: через тринадцать месяцев с начала действия Napster было вынесено судебное постановление о запрете ее эксплуатации. На тот момент Napster имела уже 40 миллионов пользователей (как видите, именно файлообменная функция принесла пиринговым сетям настоящую популярность). И хотя руководство Napster пыталось противиться судебным решениям, одновременно ведя переговоры с истцами, обещая выплатить штраф, сделать службу платной и предпринимая попытки удержать проект на плаву, — Napster закрыли. Однако шествие пиринговых сетей по планете уже было не остановить.

ПРИМЕЧАНИЕ

Пиринговые сети часто обозначают как P2P. Суть данного сокращения становится понятна, если обратить внимание на оригинальное англоязычное название технологии — «peer to peer», что можно перевести как «равный к равному». Сейчас модно использовать вместо предлога «to» цифру 2 ввиду схожего произношения, в результате сокращенный вариант записывается как P2P.

Ниже приведены наиболее актуальные пиринговые сети.

BitTorrent

BitTorrent переводится как «битовый поток». Этот проект создал автор-одиночка, американский программист Бр. Коэн. Уже в 2001 году у него была готова первая версия BitTorrent (**www.bittorrent.com**), и Бр. Коэн всячески пытался привлечь к ней внимание. Старания не прошли даром — программу заметили, и в ноябре 2001 года **LinuxFund.org** выделил грант на ее доработку. После этого дела быстро пошли в гору. Через два месяца журнал New Scientist назвал BitTorrent практически готовым инструментом для обмена файлами. Еще через два месяца продукт одобрили завсегдатаи Slashdot, а спустя год, в марте 2003 года, фирма Red Hat начала раздавать по Сети свой вариант Linux именно с помощью BitTorrent.

Наиболее рейтинговые программы, созданные для работы в данной пиринговой сети: BitTorrent (программа, созданная разработчиками одноименной сети — **www.bittorrent.com**), BitTornado (**www.bittornado.com**), BitComet (**www.bitcomet.com**) и uTorrent (**www.utorrent.com**) (рис. 12.14).

ПРИМЕЧАНИЕ

Адреса наиболее популярных сайтов по поиску torrent-файлов: www.mininova.org, www.thepiratebay.org, www.mybittorrent.com, www.torrentz.com, www.isohunt.com, www.torrentspy.com, www.newtorrents.info, www.snarf-it.org, www.torrentbox.com, www.torrentreactor.net, www.fulldls.com, www.bushtorrent.com, www.torrentportal.com, www.novatina.com, www.yotoshi.com и www.torrents.ru.

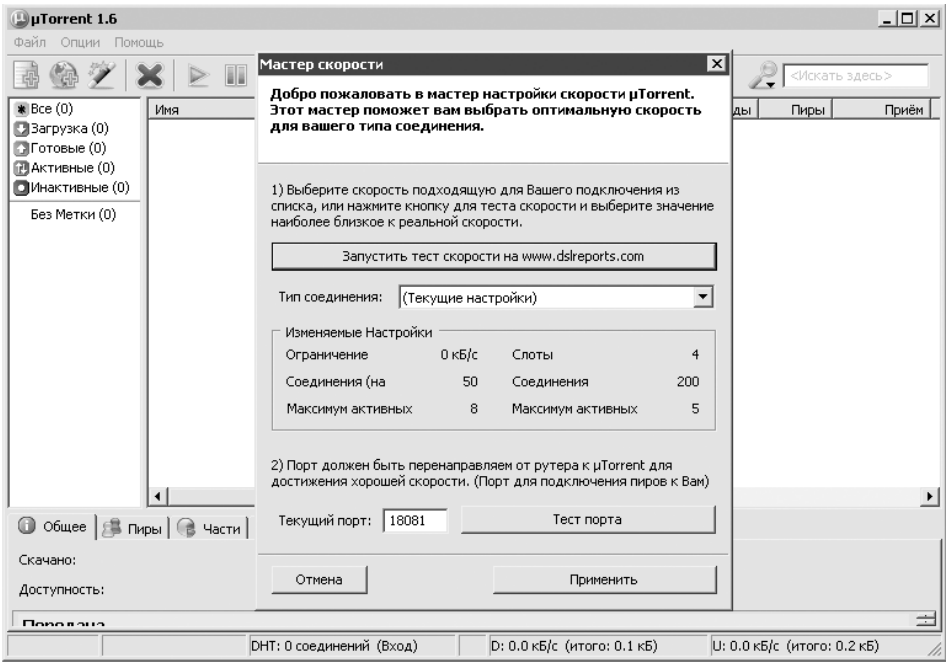


Рис. 12.14. Окно программы uTorrent

eDonkey

Пожалуй, BitTorrent и eDonkey2K (или eDonkey2000) — два основных игрока на поле пирингового файлообмена в настоящее время. Архитектура eDonkey2K (**www.edonkey.com**) смешанная. Сеть состоит из десятков независимо работающих серверов, обрабатывающих запросы подключенных к ним клиентов. Клиентами являются пользователи, загружающие файлы, и пользователи, имеющие полные версии файлов. Серверы позволяют находить опубликованные файлы и других пользователей, имеющих эти файлы (полностью или частично). Сами файлы не проходят через сервер.

ПРИМЕЧАНИЕ

Адреса сайтов-хранилищ ссылок eDonkey2K: www.shareconnector.com, www.filedonkey.com, sharereactor.revconnect.com, www.isoheaven.com, www.ac3-guru.com, www.ed2k-it.com, www.fileheaven.org, www.bucktv.net и www.musicdonkey.net.

Самые рейтинговые программы, созданные для работы в данной пиринговой сети: eMule (**www.emule-project.net**), Shareaza (**www.shareaza.com**) (рис. 12.15).

В качестве альтернативы Shareaza можно пользоваться Gnucleus (**www.gnucleus.com**) или Xolox (**www.xolox.nl**).

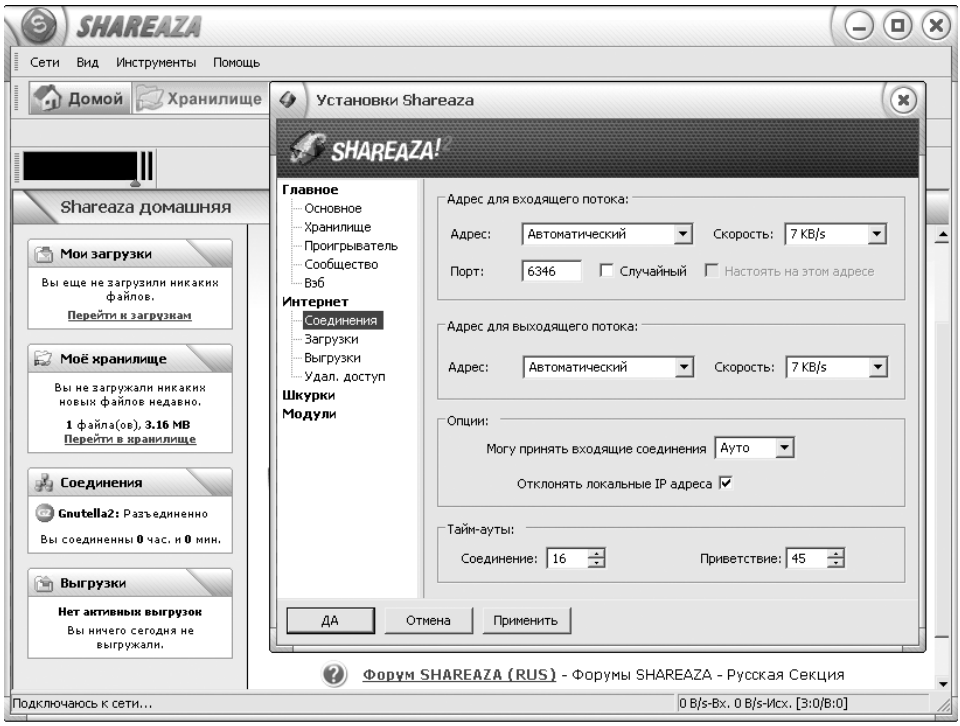


Рис. 12.15. Окно утилиты Shareaza

Gnutella

Gnutella по сравнению с другими пиринговыми сетями имеет весьма почтенный возраст. Но ни он, ни постоянные нападки звукозаписывающих компаний не мешают Gnutella существовать и иметь свой круг почитателей. Надо отметить, что в наших краях эта пиринговая сеть не особенно популярна: поклонниками Gnutella (**www.gnutella.com**) большей частью являются англоязычные пользователи.

Во многом данную P2P-сеть держит на плаву ее открытость — спецификация протокола находится в открытом доступе, и абсолютно любой желающий может в нем разобраться и написать собственную программу-клиент для работы в этой пиринговой сети.

DirectConnect

Пиринговая сеть DirectConnect (**www.neo-modus.com**) заметно отличается от всех остальных систем обмена файлами, благодаря тому что она функционирует на основе серверов. При этом каждый из серверов выступает в роли управ-

ляющего центра некоторой группы пользователей, подключенных к нему. Пользователи могут подключаться к разным серверам, причем можно сразу к нескольким одновременно.

Наиболее популярным клиентом для пиринговой сети DirectConnect является DC++ (**www.dcpp.net**), он абсолютно бесплатен, не содержит рекламных модулей и шпионских программ.

FastTrack

Пиринговая сеть, владельцев которой не любят, но которой активно пользуются. Это весьма похоже на ситуацию, когда пользователи Windows регулярно ругают Microsoft за создание такой плохой операционной системы, что не мешает им работать в Windows долгие годы. Люди парадоксальны, и с этим ничего не поделаешь.

Кстати, о парадоксах. В Сети последние несколько лет как-то немодно использовать официальные клиенты для сети FastTrack: Kazaa (**www.kazaa.com**), Grokster, iMesh. Связано это с тем, что в свое время бесплатные версии данных программ были дискредитированы наличием в них шпионских приложений, которые следили за пользователем. Поэтому большое распространение получили неофициальные программы для работы с FastTrack, к примеру Kazaa Lite K++, которая возникла в результате взлома оригинальной программы. По причине своего хакерского происхождения Kazaa Lite K++ не имеет домашней странички. Как только программу выкладывали на каком-либо сайте, вскоре он оказывался под угрозой закрытия.

FreeNet

Данная сеть призвана обеспечить конфиденциальность передаваемых по ней данных, в некотором смысле она перекликается с другой сетью — Tor (**www.torproject.org**).

Благодаря анонимности FreeNet (**www.freenetproject.org**) может избежать судебных исков, поскольку ни одни пользователь не знает, какие данные передаются через его компьютер. Однако жесткие требования к безопасности и мощные криптографические алгоритмы накладывают определенные ограничения — в использовании данная пиринговая сеть одна из самых сложных.

Клиентскую программу для сети FreeNet можно совершенно бесплатно раздобыть по адресу **www.freenetproject.org**, однако учтите, что для работы программы потребуется наличие на компьютере установленной виртуальной машины Java, взять ее (тоже совершенно бесплатно) можно по адресу **www.java.com**. Кстати,

во время установки клиент FreeNet докачает из сети недостающие модули, так что запаситесь терпением и трафиком.

SoulSeek

Пиринговая сеть довольно популярна среди поклонников электронной музыки. Представительство находится по адресу **www.slsknet.org**. Здесь располагаются просто залежи музыки разных направлений.

Одна из особенностей SoulSeek (рис. 12.16) в ее «общительности». Своеобразные виртуальные комнаты позволяют встречаться людям с похожими интересами, делиться информацией и общаться посредством встроенного чата.

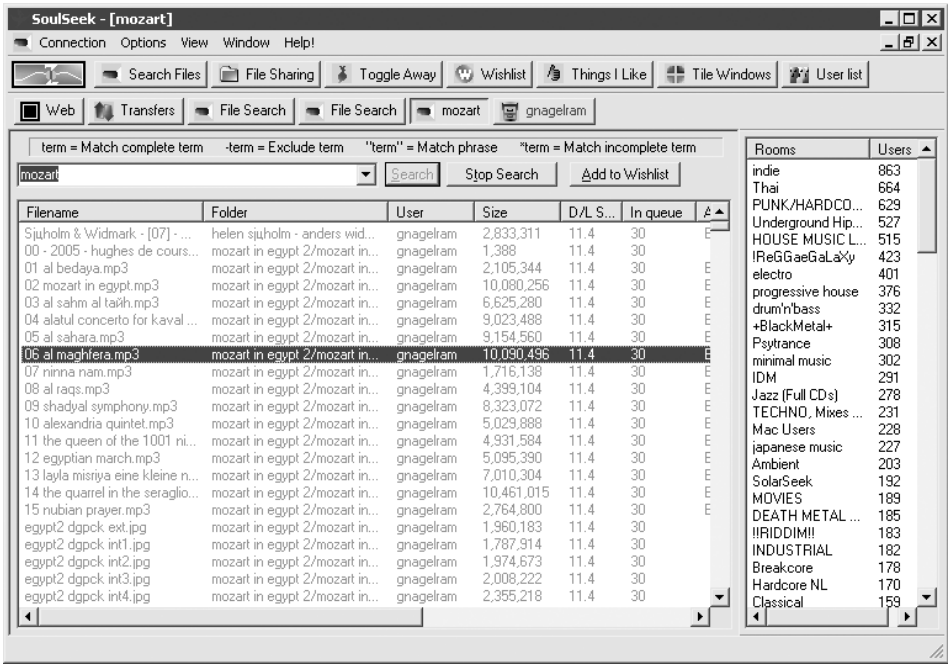


Рис. 12.16. Окно приложения SoulSeek

Скачать прграмму вы сможете на официальном сайте **www.slsknet.org**.

Пиринговое радио Mercora

Проект пирингового радио Mercora (**www.mercora.com**) (рис. 12.17) открыл бывший исполнительный директор и основатель антивирусной компании McAfee, видимо, посчитав, что этот бизнес является более перспективным. Принцип взаимодействия пользователей в Mercora тот же, что и в обычных

пиринговых сетях: архитектура сети децентрализована, а передача данных между пользователями ведется напрямую, без центрального сервера. Но пользователи Mercora передают не файлы, а потоковое аудио, причем выбирать, какую музыку транслировать, невозможно.

Mercora приобрела лицензии на неинтерактивную трансляцию цифрового звука (аналогичную лицензию получают владельцы интернет-радио). Пользователи Mercora должны транслировать только те песни, которые они самостоятельно оцифровали с компакт-дисков или скачали из Сети на законных основаниях.

Рис. 12.17. Пиринговое радио Mercora

Работа в Mercora происходит следующим образом. Как только вы установите клиент, он произведет поиск MP3-файлов на вашем жестком диске и начнет вещание по Интернету. Если вы желаете контролировать, какие песни будут отправлены на вещание, то запустите клиентскую программу. Там вы сможете собрать свои песни в списки проигрывания и создать до пяти каналов вещания. Mercora обходит проблемы других пиринговых сетей, поскольку MP3-файлы не передаются через Интернет: служба осуществляет только прямое вещание в реальном режиме времени.

Установка клиентской программы для пирингового радио Mercora не представляет сложностей. Достаточно лишь скачать клиент с сайта **www.mercora.com** и запустить установочный файл двойным щелчком кнопкой мыши.

Что такое подкастинг?

Термин «подкастинг» произошел от названия популярного имиджевого MP3-плейера от Apple — iPod и термина «broadcasting» (что означает «широковещание»). В настоящее время, чтобы слушать подкасты, плеер iPod не обязателен. Подойдет практически любой MP3-плеер (или любое устройство, способное воспроизводить MP3 или видео, в том числе и компьютер).

Подкастинг — это синтез двух технологий: хранение музыки и видео в цифровом формате и RSS. Именно благодаря RSS автоматизируется процесс закачки аудио- или видеофайлов на компьютер или мультимедийный плеер. Вы просто подписываетесь на что-то вроде рассылки, и когда автор выкладывает новый подкаст, то автоматически его получаете. В качестве подкаста может выступать короткий ролик с новостями, регулярно публикующийся в Сети, либо прочитанные вами советы компьютерным пользователям в формате MP3. В подкастинге главное — регулярность выхода и интересный контент.

Принцип работы

В специальном XML-документе на компьютер пользователя передаются ссылки на распространяемые файлы (как правило, это аудио в формате MP3) и краткая информация об их содержании и свойствах. Существуют специальные программы, которые автоматически отслеживают новые выпуски подкастов, скачивают и помещают их в плеер.

Иными словами, подкастинг — это радио, которое вы создаете сами, скачивая только те передачи, которые вам интересны. Записать собственный подкаст не сложнее, чем соорудить интернет-страницу.

Как пользоваться

Популяризация подкастинга как такового связана с компанией Apple, которая летом 2005 г. представила новую версию своего популярного аудиоплеера iTunes (**www.apple.com/itunes**), имеющую поддержку подкастов. С тех пор iTunes стал классической программой для работы с подкастами, но не единственной. В качестве альтернативы может выступать утилита с открытым кодом под названием Juice (**www.juicereceiver.sourceforge.net**).

Каталоги подкастов

В России подкасты только набирают популярность, поэтому стоящих проектов пока немного. Среди них можно отметить RussianPodcasting (**www.russianpodcasting.ru**), основанный теле- и радиоведущим В. Стрельниковым. Проект постепенно набирает популярность и на сегодняшний день имеет довольно солидную коллекцию (рис. 12.18). Можно также выделить Podcast.iXBT (**podcast.ixbt.com**) — подкаст авторитетного IT-ресурса iXBT, который постоянно обновляется.

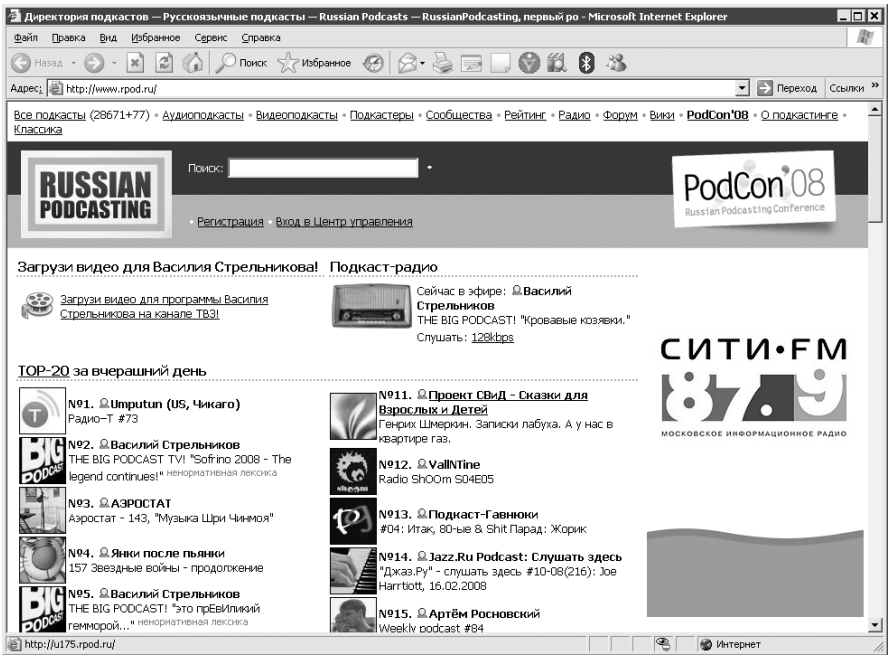


Рис. 12.18. Окно программы RussianPodcasting

Иностранные коллекции подкастов вы сможете найти на уже упомянутом Apple Music Store через программу iTunes, а также на сайтах Yahoo! Podcasts (**www.podcasts.yahoo.com**), Podcast.net (**www.podcast.net**), Podcast Alley (**www.podcastalley.com**).

Как избавиться от баннеров на сайтах? Не хочу тратить свой трафик

Серфинг по Интернету можно ускорить, используя файл **hosts** (у Windows XP он находится в папке **windows\system32\drivers\etc**). С его помощью можно

блокировать рекламные баннеры, которые замедляют открытие странички и расходуют трафик. Для этого необходимо по определенным правилам внести в файл **hosts** список адресов баннерных сетей. Например: `127.0.0.1 banner.list.ru`. В результате получится, что запросы к доменному имени **banner.list.ru** компьютер будет посылать самому себе, и баннер не загрузится (`127.0.0.1` — так называемый адрес обратной связи).

К сожалению, баннерных сетей развелось великое множество, и с развитием Интернета они плодятся все с большей скоростью. Записать все их адреса вручную — дело немыслимое, поэтому можно поискать в Интернете, где находятся ссылки на готовые файлы **hosts** со списками баннерных сетей.

Владельцы Firefox могут воспользоваться расширением AdBlock (**https://addons.mozilla.org/en-US/firefox/addon/1865**).

Можно также установить брандмауэр OutpostFirewall (**agnitum.ru**), который позволяет блокировать интернет-рекламу.

Можно ли к списку стандартных поисковых машин в Firefox добавить свои?

Поэксперементировать с настройками всегда интересно, благо программные продукты позволяют вам заняться этим увлекательным делом. Наберите в адресной строке команду `about:config`, Firefox загрузит содержимое файла **user.js** из папки пользователя, и вы получите возможность вносить в него изменения. Не забудьте, что при переносе параметров **user.js** необходимо будет скопировать в новое место. Создайте на всякий случай резервную копию файла.

Поле деятельности после выполнения `about:config` представляется широкое. Вы наверняка замечали, что если в адресной строке Firefox набрать неправильный адрес или поисковый запрос, то браузер переносит вас в Google. Изменить такое положение дел можно, если отредактировать два параметра: **keyword.URL** и **browser.search.defaulturl**. А теперь по порядку.

Например, вы хотите использовать для поиска через адресную строку «Яндекс», а не Google. В таком случае укажите в **keyword.URL** и **browser.search.defaulturl** значение `http://www.yandex.ru/yandsearch?text=`.

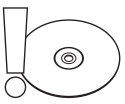
Все готово. Есть только одна мелочь. Для осуществления поиска в адресной строке надо набрать как минимум фразу, потому что одно слово Firefox тут же пытается преобразовать в интернет-адрес, добавляя впереди префикс «http».

Если вы желаете добавить «Яндекс», то проще всего будет установить «Яндекс. Бар» (**bar.yandex.ru**).

За моим компьютером работает несколько человек. Могу ли я в браузере создать несколько профилей пользователей, чтобы каждый из них мог хранить свои настройки рабочей среды?

Добиться этого можно, используя возможности команды `runas`, которая позволяет запускать программы от имени другого пользователя.

Например, вы используете браузер Firefox. Создайте в Windows пользователя, к примеру, **Вася**. Откройте **Блокнот** и наберите в нем: `runas /noprofile /user:Вася /savecred "C:\Program Files\Mozilla Firefox\firefox.exe"`. Сохраните файл с расширением CMD (например, **firefox_Вася.cmd**). Запуская браузер таким образом, вы получите новую рабочую среду, независимую от текущего пользователя. При первом запуске потребуется ввести пароль пользователя **Вася**, в дальнейшем он будет применяться для автоматической авторизации.



ВНИМАНИЕ

Необходимо запустить службу Вторичный вход в систему (Пуск ▸ Выполнить ▸ services.msc), чтобы данный способ работал.

Я слышал, что Firefox хорош тем, что к нему существует масса дополнений. Какие из них выбрать?

Достойные внимания разработки попадаются нечасто, потому имеет смысл перечислить наиболее полезные и качественные расширения для Firefox.

- Download Manager Tweak — делает менеджер закачек Firefox более «красивым» и работу с ним более приятной. Имеет возможность возобновления прерванной закачки, правда, она не всегда работает. Закачка продолжается (даже если вы закроете Firefox), пока вы не закроете окно Download Manager Tweak.
- Tweak Download Statusbar — позволяет следить за состоянием закачки, не прибегая к услугам соответствующего окна (вызывается нажатием сочетания клавиш **Ctrl+J**). В строке состояния отображаются количество закачанных данных, скорость и оставшееся время (все это можно настроить вручную).

- Fasterfox — действительно увеличивает скорость загрузки страниц в Firefox.
- FireFTP — если вы частенько путешествуете по FTP-ресурсам, то данный клиент поможет чувствовать себя на них более комфортно.
- Flashblock — блокирует все FLASH-ролики на страницах, вставляя вместо них свой значок. При необходимости достаточно щелкнуть кнопкой мыши по значку, и «флэшка» будет загружена. Поддерживает исключения.
- NoScript — блокирует все потенциально опасные компоненты на сайтах. Надежные ресурсы вы можете включить в «белый» список. Добавлять их можно прямо в процессе серфинга. Отлично блокирует назойливую флэш-рекламу.
- Adblock Plus — блокирует рекламу на сайтах. Пригодится тем пользователям, которые платят за трафик и не хотят скачивать бесполезные рекламные баннеры, а потом за них платить. Примечательно, что в расширении можно использовать специальные листы подписки, которые постоянно обновляются, позволяя блокировать 90 % рекламы. Есть листы как международные, так и сугубо для русскоязычных пользователей.

Все расширения вы найдете по адресу **addons.mozilla.org**. Кроме того, можно выбрать в меню Firefox **Инструменты ▸ Дополнения** и в появившемся окне нажать кнопку **Загрузить расширения**. Далее просто воспользуйтесь поиском и сможете установить все, здесь перечисленное.

Все обмениваются файлами через rapidshare.com, но на нем слишком много ограничений. Существуют ли в Сети аналоги RapidShare?

Действительно, не все пользователи довольны самым популярным на сегодняшний день файловым обменником. Ниже приведен список альтернативных сервисов, ничуть не хуже RapidShare и с поддержкой докачки: **www.bestsharing.com**, **www.easy-sharing.com**, **www.ifolder.ru**, **www.uploading.com**, **www.uploadyourfiles.de** и **depositfiles.com** (рис. 12.19).

Правда ли, что можно проверить файл на вирусы прямо в Интернете?

Неутомимые гении программистской мысли создали сервис с глобальными амбициями и таким же названием — VirusTotal (**www.virustotal.com**). «Скормите» любой файл этому ресурсу, и он тут же натравит на него более трех десятков антивирусов. Правда, из-за перегруженности сервера VirusTotal

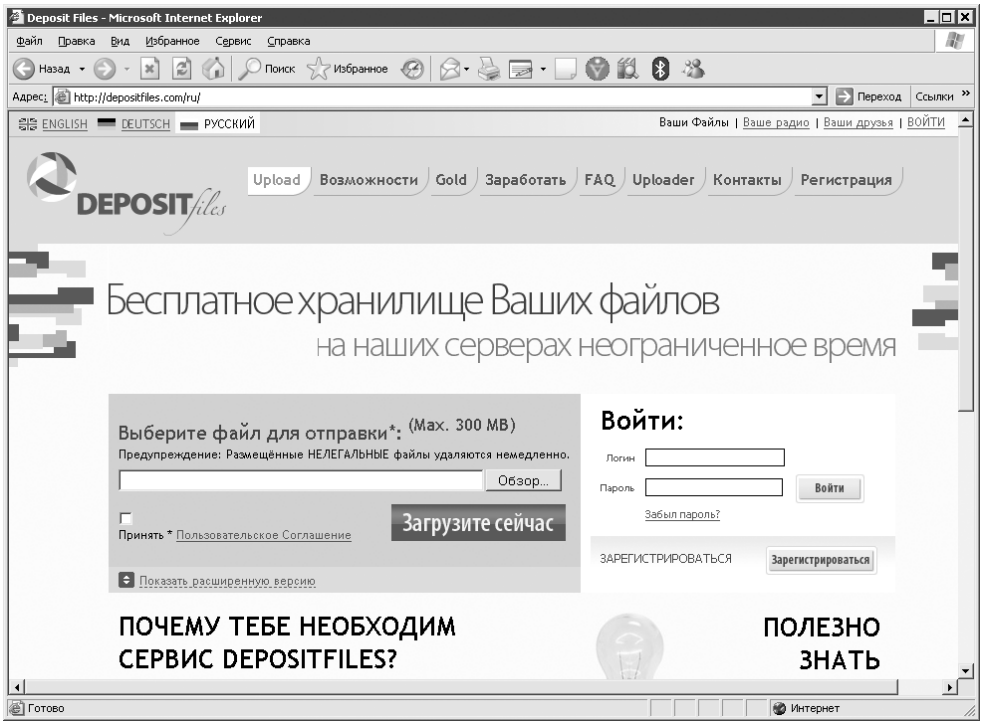


Рис. 12.19. Страница Depositfiles.com

не всегда получается проверить файл всеми 30 антивирусами, но и этого вполне достаточно.

Алгоритм работы с сервисом такой. Зайдите по адресу **www.virustotal.com**, нажмите кнопку **Обзор**, расположенную на сайте, и укажите подозрительный, по вашему мнению, файл. Он загружается на сервер VirusTotal, заказ ставится в очередь, вам сообщается примерное время ожидания, и по его истечении прямо у вас на глазах начинает формироваться таблица с результатами проверки (рис. 12.20).

Загрузить файл в сервис VirusTotal можно двумя способами — по электронной почте или через браузер. В первом случае требующий проверки объект отправляется почтовым вложением на адрес **scan@virustotal.com**. Размер анализируемого файла не должен превышать 10 Мбайт.

Кроме того, есть возможность воспользоваться утилитой VirusTotal Uploader. Ее установка добавляет в раскрывающееся меню Windows пункт VirusTotal для быстрой проверки выбранного файла через Интернет и просмотра отчета в окне браузера.

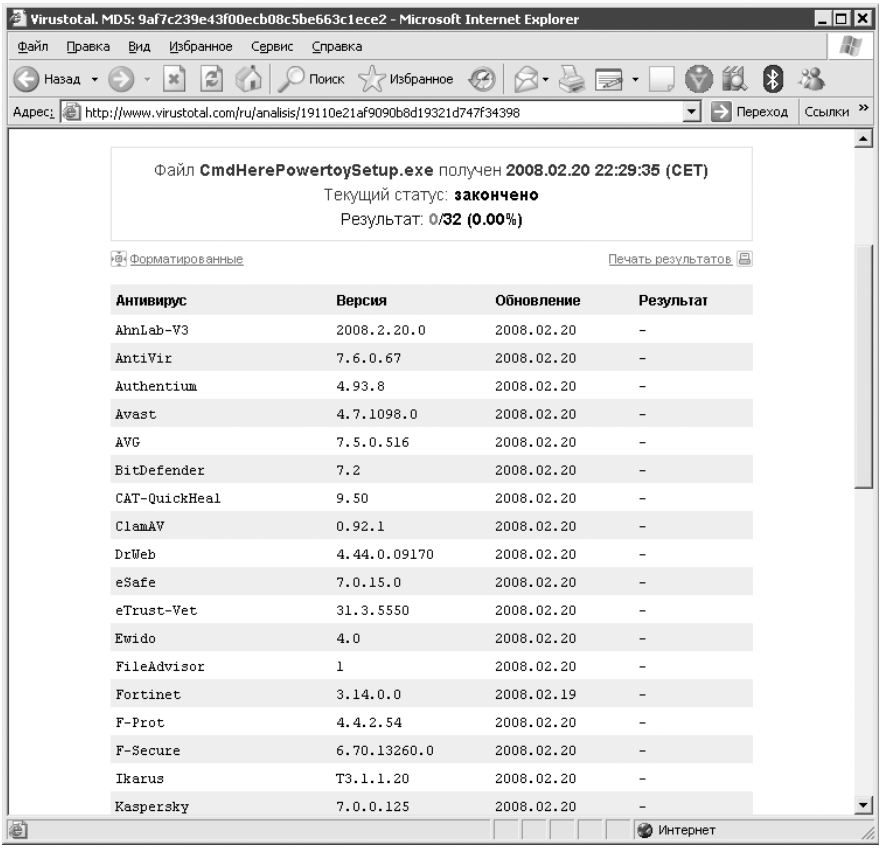


Рис. 12.20. Отчет о сканировании файла VirusTotal

Вы также можете проверить файл на сайтах некоторых антивирусных компаний, например **www.drweb.ru/scan/**.

На работе запретили ICQ. Можно ли подключить мобильный к рабочему компьютеру и пользоваться «аськой» через GPRS?

В последнее время на частных предприятиях практикуется блокирование ICQ и сайтов сомнительного содержания в целях повышения работоспособности сотрудников в рабочее время. Возьмите на вооружение хитрость, таблицу маршрутизации Windows и мобильный телефон с GPRS (либо обыкновенный модем). В данном случае вы сможете настроить компьютер так, что все запросы к определенным сайтам и ICQ будут уходить через модем или GPRS, то есть в обход системного администратора.

Предположим, вас интересует сайт **www.bardiyan.net**, и вы хотели бы посещать его втайне от руководства. Сначала потребуется выяснить IP-адрес данного ресурса, для чего выполните команду `ping bardiyan.net`. Результат: 212.98.162.115.

Теперь можно приступать ко второму этапу. Следует выяснить номер либо адрес интерфейса, посредством которого вы собираетесь подключаться к Интернету. Например, у вас есть модем (в данном случае нет принципиальной разницы, вы можете работать и с GPRS). Узнайте свой IP-адрес (в свойствах модемного подключения), когда вы подключились к провайдеру. В течение сеанса этот адрес будет идентифицировать интерфейс модема. К примеру, это будет адрес 177.7.7.7, именно через него вы и будете указывать маршруты к сайтам и ICQ.

Вам необходимо добавить новый маршрут в таблицу маршрутизации своего компьютера. Сделать это нужно таким образом, чтобы все обращения к сайту **www.bardiyan.net** шли не через интерфейс локальной сети, а через модем, то есть через интерфейс с адресом 177.7.7.7 (он будет использоваться в качестве шлюза). Для этого в консоли пишем следующее: `route add 212.98.162.115 177.7.7.7`. Но это еще не все: чтобы можно было обращаться к искомому сайту по DNS-имени (**bardiyan.net**), нужно добавить в файл **WINDOWS\system32\drivers\etc\hosts** строку: `212.98.162.115 bardiyan.net`.

Таким же образом можно привязать любой адрес к своему модемному подключению. Достаточно лишь знать его IP-адрес и адрес соответствующего интерфейса.

Как видите, с сайтами все просто. Что касается ICQ, то здесь все несколько сложнее. Дело в том, что: во-первых, при работе с ICQ происходит обращение к нескольким узлам; во-вторых, узел **login.icq.com** (с которым связывается интернет-пейджер) периодически меняет свой IP-адрес. Посему потребовалось провести следственный эксперимент, в результате которого выяснилось, что все возможные IP-адреса **login.icq.com** принадлежат двум подсетям: 64.12.0.0 либо 205.188.0.0. Вам этого вполне достаточно. Теперь задача состоит в том, чтобы обращения к адресам из этих подсетей шли не через локальную сеть, а перенаправлялись на модем. Для добавления к интерфейсу модема маршрута первой подсети в консоли пишем: `route add 64.12.0.0 mask 255.255.0.0 177.7.7.7`. Для второй: `route add 205.188.0.0 mask 255.255.0.0 177.7.7.7`. Дело сделано. Весь трафик ICQ теперь будет уходить мимо любопытных глаз, сохраняя конфиденциальность общения. Если вы собираетесь получать альтернативный доступ только к ICQ, то вариант с GPRS будет для вас наиболее выгодным в экономическом плане, поскольку в этом случае вы будете платить лишь за трафик (при работе с ICQ его генерируется совсем немного).

Не следует оставлять без внимания еще одну деталь, которая имеет принципиальное значение для вас. Отправьтесь на ее поиски в свойства нашего модемного подключения. Далее на вкладке **Сеть** выберите **Протокол Интернета (TCP/IP)** и нажмите кнопку **Свойства**. В появившемся окне нажимите кнопку **Дополнительно** и на вкладке **Общие** увидите флажок **Использовать основной шлюз в удаленной сети**, по умолчанию он установлен. Наверняка вы раньше не придавали ей особого значения. Если флажок будет установлен, то обращения ко всем узлам, находящимся за пределами вашей локальной сети, будут идти через данное подключение. Иными словами, весь интернет-трафик вашего компьютера направится на интерфейс модема. В случае с GPRS это скажется не только на скорости, но и на стоимости. Вашей задачей было создать более гибкую систему и направлять «в обход» только обращения к некоторым узлам сети, следовательно, флажок **Использовать основной шлюз в удаленной сети** рекомендуется снять (рис. 12.21).

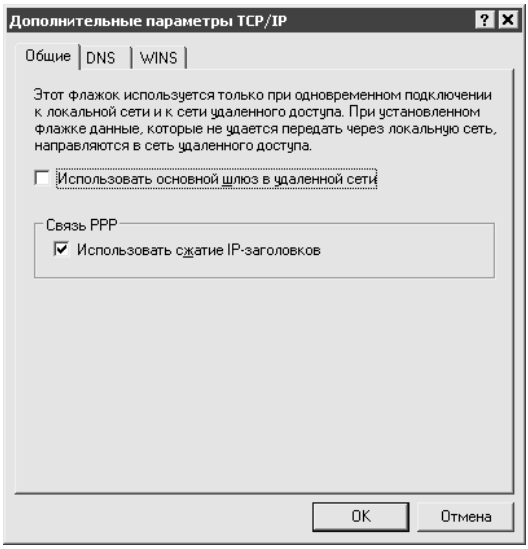


Рис. 12.21. Флажок Использовать основной шлюз в удаленной сети следует снять

Каждый раз, когда вы будете дозваниваться к провайдеру, вашему модему будет назначаться другой IP-адрес. Именно по этой причине мы не используем команду `route -p add` (ключ `-p` сохраняет добавленные маршруты даже после перезагрузки). Так как адрес интерфейса будет меняться, то будет меняться и адрес шлюза, через который мы оправляем в Интернет «особый» трафик. Следовательно, периодически придется снова вручную добавлять маршруты к сайтам и ICQ либо менять их командой `route change`. К примеру, ранее вы выполнили: `route -p add 64.12.0.0 mask 255.255.0.0 177.7.7.7`. На следующий день вновь подключились через модем (его адрес поменялся на 177.7.8.8). В этом слу-

чае напишите в консоли: `route -p change 64.12.0.0 mask 255.255.0.0 177.7.8.8`.

Все постоянные маршруты (добавленные с ключом `-p`) хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\PersistentRoutes`. В связи с этим возникает вопрос: почему бы вам не вносить изменения в таблицу маршрутизации напрямую через реестр? Причин этого не делать нет. Пример приведен с помощью ICQ.

Аналогом команды `route -p add 64.12.0.0 mask 255.255.0.0 177.7.7.7` будет служить следующая запись в файле с расширением REG (листинг 12.2).

Листинг 12.2. Добавление маршрутов через реестр

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\
PersistentRoutes]
«64.12.0.0,255.255.0.0,177.7.7.7,1"="»
```

Предположим, что вы внесли необходимую информацию в файл реестра (назовем его **routes.reg**), и вот пришло время менять адрес шлюза. Запускаете `ipconfig /all`, узнаете новый адрес (к примеру, 177.7.8.8). Затем открываете **routes.reg** в обычном **Блокноте** и следуете в меню **Правка ▸ Заменить**. В строке **Что** вводите `177.7.7.7`, а в строке **Чем** — `177.7.8.8`, после нажимаете кнопку **Заменить все** и сохраняете изменения. Осталось только двойным щелчком кнопкой мыши добавить новую информацию в реестр. Когда у вас прописано больше одного маршрута, этот способ быстрее и удобнее, нежели использование `route change` в случае, когда маршрутов несколько.

Вот, пожалуй, и все. Такими несложными манипуляциями вы можете достигнуть определенной независимости от администратора.

Правда ли, что можно отправлять электронную почту из командной строки?

Большинство пользователей привыкло отправлять электронную почту простым нажатием одной кнопки. Между тем существует масса альтернативных способов.

Электронную почту можно отправлять/получать через «Телнет». На заре Интернета это был самый ходовой способ. Сейчас о нем забывают, однако остались еще пользователи, верные старому доброму «Телнету». Происходит это следующим образом.

Прежде всего надо найти почтовый сервер, который позволяет работать с ним через «Телнет». Предположим, это будет **hotmail.com**.

В консоли введите: `telnet mail.hotmail.com 25` (25-порт используется для отправки почты). Сервер выдает приглашение. С ним нужно «поздороваться» командой `helo`. Далее необходимость «сказать» серверу, кому должно быть отослано сообщение: `rcpt to: x403@yandex.ru`. Если в ответ появится `OK`, можно начинать вводить текст вашего сообщения. Для этого наберите команду `data`, нажмите клавишу **Enter**. После этого можете набирать текст письма. Нужно поставить точку в самом конце вашего сообщения, чтобы отослать его. Обратите внимание, что финальная точка стоит на новой строке.

Для чтения почты через «Телнет» понадобится набрать в консоли: `telnet mail.hotmail.com 110` (теперь уже обращаемся к 110-му порту, по которому осуществляется прием почты). Появляется приглашение сервера. В ответ набираете сначала: `USER имя_пользователя`, затем вводите пароль: `PASS пароль`. При работе вам могут понадобиться команды:

- `stat` — запрашивает и выводит информацию о количестве непрочитанных сообщений и их размер в байтах;
- `retr n` — показывает сообщение номер N;
- `dele n` — удаляет сообщение номер N;
- `quit` — завершение сеанса.

Есть еще один вариант отправки почты — с использованием бесплатной программы Blat (есть на компакт-диске, который прилагается к книге). Пример использования: `Blat.exe body.txt -t bill@microsoft.com -subject "Windows "`.

Кстати, на основе Blat написан плагин для Total Commander, который позволяет посылать файлы почтой прямо из этой программы.

Помимо указанных способов, можно отправлять почту из PHP-сценария или из VBS.

Нужно контролировать присутствие определенного IP-адреса в Интернете. Как это сделать?

Можно самому написать простой, но работающий сценарий. Представленный ниже сценарий (листинг 12.3) пингует хост с IP-адресом 111.112.113.114 и записывает результат в файл **pingmodem.txt**. Перед запуском команды `ping`

отрабатывает команда `time`, которая показывает текущее системное время (оно тоже записывается в файл). Утилита `sleep.exe` позволяет сделать паузу в выполнении сценария на 55 секунд, взять ее можно из Windows Server 2003 Resource Kit tools.

Листинг 12.3. Запись результатов команды ping

```
:begin
time /t >> c:pingmodem.txt & ping 111.112.113.114 >> c:pingmodem.txt
c:sleep.exe 55
goto :begin
```

Как организовать резервное копирование данных на внешний FTP-сервер?

Секрет резервного архивирования данных достаточно прост. Например, вы известный писатель, который создает новый шедевр. Первоначальная идея такова: каждый день в назначенное время файлы с главами вашей книги должны архивироваться с паролем, затем новая версия архива должна копироваться на FTP-сервер в Интернете (причем копия и оригинал должны находиться как можно дальше друг от друга). Таким образом, даже если с вашим ноутбуком что-нибудь случится, то все равно можно продолжить работу над книгой за другим компьютером. Для воплощения этой идеи в жизнь понадобятся три утилиты, которые нетребовательны к системным ресурсам (за счет отсутствия интерфейса) и совершенно бесплатны. Вот их имена: nnBackup и nnCronLite (**www.nncron.ru**) и клиент FTP, входящий в дистрибутив Windows.

Шаг 1

nnBackup — это крошечная утилита командной строки, предназначенная для резервного копирования файлов и синхронизации содержимого каталогов. Поддерживает сжатие архивных данных по алгоритмам GZ или ZIP. nnBackup позволяет использовать все распространенные методы резервного копирования.

- Традиционное копирование файлов и каталогов. Это самый распространенный (но не самый надежный и не самый эффективный) способ резервного хранения данных. Режим копирования используется nnBackup по умолчанию, если пользователь не задал иной. Основное достоинство этого режима — простота. Для успешного копирования файлов из одного каталога в другой вам достаточно указать местоположение исходных данных и задать приемный каталог.

- Копирование данных в стек пронумерованных каталогов/ZIP-файлов заданной глубины. Это самый надежный режим резервного копирования (его и будем использовать). Он позволяет создавать неограниченное количество точных копий исходных данных, которые помещаются в пронумерованные каталоги (стек каталогов) или в пронумерованные ZIP-файлы (стек архивов). Вы сами выбираете глубину стека — сколько копий данных вы собираетесь хранить. Каждая новая копия исходных данных помещается в каталог/ZIP-файл с соответствующим номером (от 1 до N), причем в каталоге/ZIP-файле с номером 1 хранится самая последняя (самая свежая) копия источника. Как только количество копий превысит указанное значение (N), самая старая копия автоматически удаляется. В каждый из пронумерованных каталогов/ZIP-файлов копируются все файлы из источника данных в соответствии с заданными включающими и исключающими масками. Однако размер создаваемого ZIP-архива ограничен до размера в 2 Гбайт. Если вы работаете с большим объемом данных, целесообразно вместо копирования в стек архивов использовать копирование в стек каталогов.
- Инкрементное резервирование. Очень эффективный и вместе с тем надежный способ резервного копирования. Его основные преимущества: скорость и высокая степень настраиваемости. Режим инкрементного резервирования позволяет сначала выполнить резервное копирование всего исходного каталога и потом добавлять к нему те файлы, которые изменились со времени последнего резервного копирования. Сессию резервного копирования в таком режиме принято называть «дампом». Каждой сессии резервного копирования (дампу) присваивается свой номер (целое число от 0 до 9) — это уровень резервирования, который определяет, какие файлы будут скопированы. Дамп уровня 0 содержит все файлы из источника данных, дамп любого другого уровня (например, N) включает только файлы, которые появились или изменились с момента создания последнего дампа, чей уровень меньше или равен N. Если новых или измененных файлов нет, то дамп не создается. Каждый «дамп» упаковывается в один большой файл и сжимается по алгоритму ZIP.
- Синхронизация файлов и каталогов. Это режим, в котором nnBackup проверяет два указанных каталога на полную идентичность. Если в исходном каталоге появились новые файлы или какие-то файлы были изменены, то они копируются в приемный каталог. Если в приемном каталоге отсутствуют какие-то из файлов исходного каталога, то они тоже будут скопированы. Основные преимущества синхронизации каталогов по сравнению с остальными способами резервного копирования — это быстрота работы (копируются только новые или изменившиеся файлы) и экономия диско-

вого пространства, отводимого под резервную копию файлов (создается только одна резервная копия, которая постоянно поддерживается в актуальном состоянии).

Поскольку nnBackup — консольная утилита, то все аргументы в нее передаются через командную строку. Дать программе понять, какой режим копирования мы собираемся включить, можно, указав ключ `verz`. Это значит, что вы собираетесь использовать копирование данных в стек пронумерованных ZIP-файлов. Далее следует задать глубину стека `-n 2`. Потом после ключа `-i` надо указать исходный каталог (откуда берем данные), получается что-то вроде: `-i e:\work\book\`. Затем каталог-приемник: `-o f:\backup\work\book\`. Теперь надо указать маску, по которой будем выбирать интересующие нас документы: `-m ch*.doc`, ведь в каталоге наверняка будет полно других не таких важных файлов, которые только будут засорять архив и увеличивать время его создания. Поскольку архив будет храниться на FTP-сервере, к которому может получить доступ посторонний, при помощи ключа `-pw` установим на архив пароль: `-pw 834586x561`. Пароль лучше устанавливать длинный, чтобы затруднить взлом.

Как видите, параметров довольно много, строка запуска резервного архивирования будет иметь такой вид: `nnbackup.exe verz -n 2 -i e:\work\book\ -o f:\backup\work\book\ -m ch*.doc -pw 834586x561`. Получилось громоздко. Сократить можно, записав все параметры в текстовый файл (листинг 12.4), который передадим nnBackup в качестве аргумента: `nnbackup.exe -f book.txt`.

Листинг 12.4. book.txt

```
\ копируем в стек архивы
verz
\ глубина
-n 2
\ исходный каталог:
-i "e:\work\book\"
\ приемный каталог:
-o "f:\backup\work\book\"
-m ch*.doc
\ маска
-pw 834586x561
```

Файл `book.txt` следует сохранить в директории программы nnBackup. Запуск тоже следует осуществлять из директории nnBackup либо прописывать в командной строке полный путь к файлам `nnbackup.exe` и `book.txt`, например: `c:\nnbackup\nnbackup.exe -f c:\nnbackup\book.txt`.

Шаг 2

Обратите внимание на малоизвестную стандартную утилиту Windows, она понадобится вам для копирования архивов на FTP-сервер. Запустите консоль и введите команду `ftp`, после этого вы попадете в оболочку FTP-клиента Windows, о чем свидетельствует появление приглашения `ftp>`. Теперь можно вводить команды, а FTP-клиент будет их выполнять. Краткий список команд, которые нам понадобятся для осуществления задуманного:

- `open` — подключение к удаленному узлу по протоколу FTP;
- `cd` — изменение рабочего каталога на удаленном компьютере;
- `bin` — установка режима передачи файлов в двоичном формате;
- `put` — передача одного файла на сервер;
- `bye` — завершение сеанса FTP и выход.

Познакомиться с FTP-клиентом поближе и научиться работать с ним можно, если осуществить подключение к FTP-серверу в консольном режиме. Наверняка вам доводилось делать это ранее, используя Total Commander, Far или Internet Explorer, в командном режиме все выглядит несколько иначе. Итак, как выглядит подключение, например, в Internet Explorer: сначала к серверу надо подключиться (ввести его адрес), потом зайти в нужный каталог, скопировать туда файл, закрыть окно. Далее подробно рассмотрено, как происходит подключение в консоли.

Введите команду `open 72.9.255.178` (это IP-адрес FTP-сервера). Если сервер с таким адресом существует и поддерживает подключение по FTP, вам будет выдан запрос на имя пользователя, а затем на пароль. Когда авторизация пройдена, самое время создать папку для хранения ваших архивов, назовите ее, например, **backup** (папка создается командой `mkdir`). Теперь зайдите во вновь созданную папку командой `cd backup`. Осталось только скопировать нужный файл. Сделайте это, но сначала установите режим передачи файлов в двоичный формат командой `bin` без параметров. Введите `put f:/backup/work/book/1.ZIP`, где аргументом команды `put` выступает полный путь к копируемому файлу. После завершения копирования остается лишь попрощаться с сервером командой `bye`.

Клиент FTP будет совершать перечисленные действия автоматически, не задавая вопросов, если составить для него сценарий. Ниже представлен текстовый файл (например, `book.ftp`, сохраненный в каталоге `c:\nnbackup`), содержащий команды FTP, которые будут выполняться автоматически при запуске FTP-клиента (листинг 12.5).

Листинг 12.5. book.ftp

```
open 72.9.255.178
имя_пользователя
пароль
cd backup
bin
put f:/backup/work/book/1.ZIP
bye
```

Передать данный файл на исполнение можно, написав в консоли: `ftp -s:"c:\nnbackup\book.ftp"`.

Шаг 3

У вас есть две задачи: архивирование и последующее копирование на FTP-сервер. Осталось только запускать их в заданное время и в нужной последовательности. Эти задачи возложите на утилиту nnCronLite.

«Сердце» nnCronLite — файл `cron.tab`, в котором хранятся все необходимые программе данные: время старта приложения, периодичность выполнения, имя приложения и параметры его запуска. Это обычный текстовый файл, он может быть отредактирован в любом доступном текстовом редакторе. nnCronLite раз в минуту проверяет дату последней модификации `cron.tab` и, обнаружив обновление информации, автоматически перечитывает его.

Классический формат `cron.tab` таков: `минуты часы номер_дня_в_месяце номер_месяца номер_дня_в_неделе путь_к_выполняемому_приложению`. Рассмотрим пример рабочего файла настроек планировщика nnCronLite, где прописан поочередный запуск nnBackup и FTP-клиента (листинг 12.6).

Листинг 12.6. Файл cron.tab

```
#CRONTAB FILE
# Classic crontab format:
# Minutes Hours Days Months WeekDays Command
```

В 17 минут 17 часов каждый месяц (`*`) каждый рабочий день (`1-5`) вы запускаете архивирование средствами утилиты nnBackup, настройки которой прописаны в файле `book.txt` (см. листинг 12.4): `17 17 * * 1-5 c:\nnbackup\nnbackup.exe -f c:\nnbackup\book.txt`.

В 30 минут 17 часов каждый месяц (`*`) каждую пятницу (`5`) средствами утилиты `ftp.exe` вы производите копирование согласно сценарию, описанному в файле `book.ftp` (см. листинг 12.5): `30 17 * * 5 c:\winnt\system32\ftp.exe -s:"c:\nnbackup\book.ftp"`.

Чистота и порядок в доме —
признак неисправного компьютера

Глава 13

Сбой системы

Я слышал, что в Windows 2000/XP есть консоль восстановления. Как ей пользоваться?

Когда возникают проблемы с загрузкой Windows 2000/XP, вернуть операционную систему к жизни поможет консоль восстановления. Она разработана компанией Microsoft для устранения неполадок в аварийных ситуациях. Отсутствие дружественного к пользователю интерфейса компенсируется широкими возможностями консоли, которые позволяют получить прямой доступ к файловой системе, управлять загрузкой Windows и запуском системных служб.

Конкурирующих средств, предназначенных для восстановления Windows, довольно много. Каждое из них выполняет конкретные задачи, а консоль восстановления вполне можно назвать «лекарством» если не от всех, то от большинства компьютерных болезней. Консоль восстановления поставляется вместе с дистрибутивом Windows 2000/XP, легка в установке и занимает мало места на диске, потому она так популярна.

Инсталляция и запуск консоли

Уверенность, что сбой системы не застанет вас врасплох, лучше подкрепить установкой консоли восстановления на свой жесткий диск. Для начала процесса требуется запустить из дистрибутива Windows 2000/XP файл `winnt32.exe` с ключом `/cmdcons`. Для этого в меню **Пуск** выполните команду: `g:\i386\winnt32.exe /cmdcons`, где `g` — буква диска, на котором хранится дистрибутив (обычно это компакт-диск).

После завершения процедуры установки (рис. 13.1) компьютер следует перезагрузить. В загрузочном меню должна появиться строка с вариантом запуска консоли восстановления, выбрав ее, вы начнете запуск консоли. Если строку заметить не удалось, следуйте в **Панель управления ▸ Свойства системы ▸ Дополнительно ▸ Загрузка и восстановление** и увеличьте параметр **Задержка при отображении списка операционных систем**. Загрузочное меню будет отображаться указанное вами количество секунд.

Для работы с консолью предусмотрены два варианта. Один — это установка консоли на жесткий диск компьютера, другой — запуск консоли с установочного компакт-диска Windows 2000/XP. Воспользоваться вторым вариантом можно, если загрузиться с указанного компакт-диска и дождаться автоматического запуска программы установки. После этого в ее текстовой части появится возможность выбора между инсталляцией системы или восстановлением. Для запуска консоли нужно выбрать вариант восстановления (нажмите клавишу **R**). Далее в новом окне выбора следует указать режим восстановления с помощью консоли (нажмите клавишу **C**).

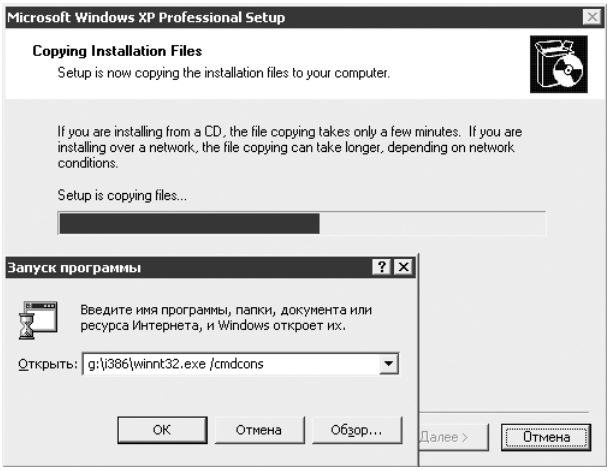


Рис. 13.1. Установка консоли восстановления

После запуска консоли любым из перечисленных методов появляется меню, в котором отображается пронумерованный список установленных на данном компьютере систем Windows. Выберите номер системы, в которую хотите войти, и нажмите клавишу **Enter**. Далее нужно ввести пароль локального администратора. Если пароль правильный, то появится приглашение на ввод команд, — это означает, что консоль восстановления готова к работе.

Замена поврежденного реестра

Застраховаться от порчи системного реестра очень сложно, ведь это большая база данных, с которой работают все программы. Умышленно или случайно одна из программ может повредить реестр, и не исключено, что после этого Windows перестанет загружаться. Единственный выход в такой ситуации — заменить поврежденные файлы реестра резервными копиями. Если на вашем компьютере до сбоя не была включена функция автоматического резервирования, то без консоли восстановления не обойтись.

На жестком диске реестр хранится в виде пяти файлов: `system`, `software`, `sam`, `security`, `default`. Они находятся в папке `windows\system32\config`.

Для восстановления реестра лучше всего заменять сразу все пять файлов, поскольку они взаимосвязаны. Если у вас нет их резервных копий, придется воспользоваться копиями, сделанными самой Windows при установке (они находятся в каталоге `windows\repair`). Возможно, что после этого некоторые программы потребуется переустановить, но ведь это сделать куда проще, чем заново устанавливать Windows.

Запустив консоль и введя пароль администратора, в командной строке можно начинать отдавать приказы. Для осуществления этого вам нужно выполнить следующую последовательность действий (листинг 13.1).

1. Вы создаете временную папку.
2. На всякий случай сохраняете в ней пять поврежденных файлов реестра.
3. Заменяете поврежденные файлы резервной копией из каталога **repair**.
4. Выходите из консоли и перезагружаете компьютер.

Листинг 13.1. Замена поврежденного реестра

```
md temp

copy system32\config\software temp
copy system32\config\security temp
copy system32\config\default temp
copy system32\config\system temp
copy system32\config\sam temp

copy repair\software system32\config
copy repair\security system32\config
copy repair\default system32\config
copy repair\system system32\config
copy repair\sam system32\config

exit
```

Следует отметить, что после запуска консоли по умолчанию вы находитесь в папке **windows**, поэтому в командах нет смысла писать полный путь (например, `c:\windows\system32\config`), а достаточно просто указать путь от каталога **windows** (например, `system32\config`).

СОВЕТ

По умолчанию из консоли восстановления можно обращаться только к файлам и папкам, находящимся в каталоге Windows, также запрещено копирование дискет средствами консоли.

Дать право пользователям консоли выполнять эти действия можно, проследовав по следующему маршруту: Панель управления ▸ Администрирование ▸ Локальная политика безопасности ▸ Локальные политики ▸ Параметры безопасности. В правом окне следует дважды щелкнуть кнопкой мыши на пункте Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и каталогам и в появившемся окне установить флажок Включен.

Блокирование служб, мешающих запуску системы

Бывают ситуации, когда причиной сбоя при загрузке являются дефекты служб или драйверов. В этом случае запуск неисправной службы или драйвера можно отключить через консоль восстановления. Показательное отключение приведено ниже (листинг 13.2).

Листинг 13.2. Блокирование ненужных служб

```
listsvc
disable cryptsvc
enable cryptsvc service_auto_start
```

Получаете список всех загружаемых служб. Выбираете из него ту, которая приводит к проблемам (например, служба криптографии — `cryptsvc`), и блокируете. После выполнения команды `disable` будут выведены старое и новое значения флага запуска. Старое значение следует запомнить или записать на тот случай, если в дальнейшем потребуется из консоли восстановления вновь разрешить запуск этой службы. Значение `service_auto_start` — это и есть флаг запуска, оно означает, что служба должна запускаться автоматически.

Восстановление загрузочного сектора

Виновником повреждения данных в загрузочном секторе жесткого диска может быть что угодно, даже программа установки Windows 9x. Если на компьютер с Windows 2000/XP в качестве второй системы устанавливается Windows 9x, то после этого загрузить Windows 2000/XP уже не удастся. При установке Windows 9x самым эгоистичным образом удаляет все записи из загрузочного сектора и вписывает туда только себя. Для приведения системы в норму в консоли восстановления нужно выполнить команду `fixboot c:`.

Данная команда перезаписывает загрузочный сектор жесткого диска сохраненной ранее копией. В результате записи, оставленные в секторе, Windows 2000/XP будут восстановлены, следовательно, система снова сможет загружаться.

Единственный аргумент команды — это буква устройства, на которое производится запись. В подавляющем большинстве случаев это системный диск.

Большинство команд консоли восстановления предоставляют сокращенные возможности по сравнению с их синонимами в Windows, хотя некоторые команды существуют только в консоли восстановления.

Для получения более подробной информации используйте утилиту `help`. Набрав `help`, вы получите перечень всех доступных команд. Информацию по

каждой конкретной команде (например, `diskpart`) можно получить, выполнив `help diskpart`. Ниже приведен список наиболее используемых команд консоли восстановления.

- `Batch` — команда запуска на исполнение файла пакетной обработки. Использует два аргумента: имя запускаемого файла и файла, в который будут выводиться данные, полученные в результате работы.
- `Disable` — отключает запуск указанной службы или драйвера при загрузке системы. Используется в том случае, если на стадии начальной загрузки системы происходит сбой в инициализации службы или драйвера устройства. В качестве аргумента используется название службы, запуск которой следует остановить.
- `Diskpart` — работает с разделами жесткого диска. Все параметры можно передавать из командной строки, однако проще с `diskpart` работать в диалоговом режиме.
- `Enable` — разрешает запуск ранее отключенных (возможно, командой `disable`) служб и драйверов.
- `Exit` — завершает работу консоли восстановления и перезагружает компьютер.
- `Expand` — распаковывает архивные файлы, в которых хранятся файлы в дистрибутиве Windows.
- `Fixmbr` — восстанавливает основную загрузочную запись в загрузочном разделе.
- `Fixboot` — запись нового загрузочного сектора в системный раздел (обычно диск **C:**): `fixboot c:`. Как правило, эту команду запускают, после того как выполнили `fixmbr` и перезагрузились.
- `Format` — позволяет форматировать диск или раздел.
- `Listsvc` — выводит на экран перечень всех используемых в системе служб и драйверов с указанием их флагов запуска.
- `Logon` — при использовании нескольких вариантов загрузки эта команда позволит подключаться к различным разделам. Выводит список разделов, позволяет выбрать нужный и запрашивает пароль администратора.
- `Map` — отображает список устройств жесткого диска, поставленных им в соответствие букв, используемую файловую систему, размеры дисков. Аргументом этой команды может быть ARC. В этом случае команда покажет разметку физического устройства в формате Advanced RISC Computing (ARC). В таком формате записана информация о дисках в файле `boot.ini`.

Удаление консоли

Установленную на жесткий диск консоль при необходимости можно без труда удалить. Просто удалите папку **cmdcons**, файл `cmldr` из корневого каталога системного диска и удалите в файле `boot.ini` запись с вариантом запуска консоли восстановления.

При включении компьютер выдал сообщение: «NTLDR is missing. Press Ctrl+Alt+Delete to restart». Что это значит?

Отсутствует загрузчик операционной системы (файл `ntldr`, который обычно находится в корне диска **C:**). Причиной этому может быть вирус или сбой файловой системы. Такая проблема может возникнуть, если у вас два винчестера в компьютере, а в BIOS выбрана загрузка с несистемного жесткого диска, либо вставлена дискета, «флэшка» или компакт-диск.

Загрузитесь с установочного компакт-диска, выберите параметр — восстановление (**R**) либо запустите консоль восстановления с жесткого диска. Попробуйте исправить ситуацию при помощи специальных команд.

Попробуйте взять файл `ntldr` с установочного диска. Команда, которая сделает это, выглядит так: `copy d:\i386\ntldr c:\ntldr`. В данном случае **D:** ассоциируется с компакт-диском. После этого введите `exit`, чтобы выйти из консоли, и перезагрузите компьютер.

Можно попробовать просто скопировать файл `ntldr` с другого компьютера в корень вашего диска **C:**. Сделать это можно, подключив свой жесткий диск к другому компьютеру, загрузив на исправном компьютере Windows в защищенном режиме, и скопировав файл `ntldr`. Есть и второй путь. Скопируйте данный файл со «здоровой» системы на «флэшку». Затем на своем компьютере загрузитесь со специализированного компакт-диска наподобие INFR@ или ERD Commander, который позволяет получать доступ к разделам NTFS. Затем перепишите искомый файл с «флэшки» в корень диска **C:**.

Загрузил консоль восстановления. Какие команды нужно использовать для восстановления системы?

Дать рекомендацию, подходящую для всех случаев, невозможно. Проблемы могут быть разного рода и решаться разными средствами. Однако в наиболее частых случаях помогает следующий набор команд, которые надо выполнять последовательно.

1. Полная проверка файловой системы, поверхности диска и исправления ошибок: `chkdsk /r`.
2. Восстановление основной загрузочной записи в загрузочном разделе: `fixmbr`.
3. Запись нового загрузочного сектора в системный раздел (обычно диск **C:**): `fixboot c:`. Эту команду нужно запускать, после того как вы выполнили предыдущие две и перезагрузили компьютер.

При загрузке появляется сообщение: «HAL.DLL is missing». Что делать?

Загрузите консоль восстановления с жесткого диска (если она у вас установлена) либо вставьте в привод компакт-диск с дистрибутивом Windows XP и загрузитесь с него. Выберите пункт — восстановить (нажмите клавишу **R**). Если на вашем компьютере установлено несколько операционных систем, выберите ту, к которой вы хотите иметь доступ из консоли восстановления. Если потребуется, введите пароль администратора (если вы не создавали пароль, нажмите клавишу **Enter**). Когда консоль загрузится, сделайте следующее. Вставьте диск с дистрибутивом (если он еще не там) в привод компакт-дисков, выполните команду: `expand d:\i386\hal.dl_ c:\windows\system32\hal.dll`. В данном случае считается, что буква **d** присвоена компакт-диску. После восстановления файла введите `exit`, чтобы выйти из консоли, и перезагрузите компьютер.

При загрузке Windows появляется сообщение: «Отсутствует или поврежден файл ntoskrnl.exe». Можно ли исправить ситуацию?

Дистрибутив Windows содержит оригинал данного файла, поэтому можно попробовать его скопировать. Как это можно сделать, описано в гл. 3. Команда будет выглядеть так: `expand d:\i386\ntoskrnl.ex_ c:\windows\system32\ntoskrnl.exe`.

Поэкспериментировал с файлом boot.ini, в результате не могу загрузить систему. Что делать?

Загрузите консоль восстановления и воспользуйтесь командой `bootcfg /rebuild`, которая осуществляет проход по всем установленным системам Windows на жестком диске и предоставляет возможность сделать запись о каждой в файл `boot.ini`.

Если вы использовали стандартную конфигурацию (размещение системы на диске **C:**, который физически размещен в начале жесткого диска; и название

каталога — **Windows**), то можно скопировать файл `boot.ini` с винчестера другого компьютера либо открыть данный файл в консоли восстановления и отредактировать его в соответствии с типичным файлом `boot.ini`.

«Полазил» в реестре, и Windows не грузится. Как восстановить работоспособность системы?

Первым делом попробуйте загрузить последнюю удачную конфигурацию Windows. Если была включена функция восстановления системы, то должно получится.

Если вы знаете, какие именно параметры реестра изменяли, то вернуть систему к жизни с сохранением прежних настроек можно. О том, как это сделать, будет сказано ниже. Если вы не помните, что меняли в реестре, то этот случай более печальный. Восстановить Windows можно из консоли восстановления, скопировав резервную копию реестра из папки `c:\windows\repair` в `c:\windows\system32\config`, однако при этом потеряется информация об установленных программах и настройках системы.

К сожалению, редактора реестра в консоли восстановления нет, поэтому придется воспользоваться услугами специализированного компакт-диска (например, iNFR@ или ERD Commander), которые имеют в своем наборе редактор реестра. Исправьте внесенные изменения, которые привели к сбою, и перезагрузитесь в штатном режиме. Можно также подключить винчестер к «здоровой» системе и загрузить дерево реестра с ошибочными данными.

ПРИМЕЧАНИЕ

В редакторе реестра есть возможность загрузить «чужой» для данной системы файл реестра. Выделите в списке слева ту ветвь реестра, аналог которой вам необходимо редактировать (скорее всего, это HKEY_LOCAL_MACHINE), и выберите в меню редактора: Файл ▸ Загрузить куст. Укажите путь к соответствующему (имена совпадают с названиями подразделов ветви HKEY_LOCAL_MACHINE: software, hardware и т. д.) файлу поврежденного реестра, который находится в папке Windows\system32\config (папка Windows должна принадлежать поврежденной системе). После выбора нужного файла вам потребуется ввести имя, под которым выбранный раздел будет представлен (оно может быть любым). Ищите нужный параметр и корректируете его.

Как работает функция восстановления Windows и как ее правильно использовать?

В Windows XP имеется встроенная функция восстановления. Под ее руководством происходит создание точки возврата, как только возникают потенциаль-

но опасные ситуации (например, установка неподписанного драйвера). Затем, если произошел сбой в системе, можно загрузить последнюю удачную конфигурацию и вернуть работоспособность.

ПРИМЕЧАНИЕ

Точка возврата — состояние системы, в которое она может вернуться, если текущая конфигурация окажется неустойчивой.

Функция восстановления непрерывно осуществляет мониторинг разделов жесткого диска. При этом вы можете определить для каждого логического диска необходимый объем пространства (рис. 13.2), которое система использует для сохранения точек восстановления. Для этого в окне **Свойства системы** (сочетание клавиш **Windows+Pause Break**) следуйте на вкладку **Восстановление системы** и, выбрав диск, нажмите кнопку **Параметры**. Если свободного места на диске мало, то можно отключить функцию **На всех дисках, кроме системного**, установив флажок **Отключить восстановление на всех дисках**.

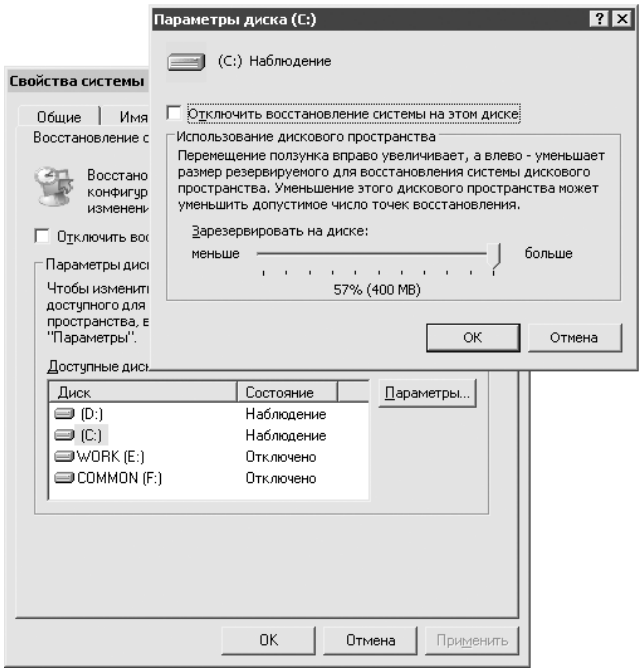


Рис. 13.2. Управление «аппетитами» функции восстановления

Пользоваться функцией восстановления предельно просто: для того чтобы вернуть систему к какой-либо точке, следует отправиться в меню **Пуск ▸ Программы ▸ Стандартные ▸ Служебные ▸ Восстановление системы**. В появившемся

окне выберите **Восстановление более раннего состояния компьютера** и нажмите кнопку **Далее** (рис. 13.3).

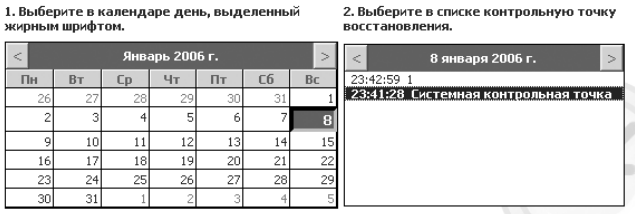


Рис. 13.3. Восстановление контрольной точки

Здесь же можно вручную создать точку восстановления (рекомендуется делать до начала экспериментов с реестром и системными настройками).

Свои обязанности рассматриваемая функция выполняет неплохо (если несильно урезать ее «аппетиты» по части дискового пространства), однако есть некоторые нюансы, которые могут показаться странными. Дело в том, что восстановленная система никогда не является точной копией оригинала. Функция восстановления не предназначена для того, чтобы вернуть Windows в то состояние, в котором она пребывала на момент создания точки восстановления. Ее главное назначение — возвратить утраченную работоспособность, поэтому все изменения касаются только системных файлов, не затрагивая пользовательские документы. Такое восстановление способно помочь при мелких проблемах, но оказывается бессильным при большом сбое. В таком случае вам повезет, если удастся хотя бы загрузить последнюю удачную конфигурацию и скопировать важные документы на сменный носитель, чтобы потом переустановить систему Windows.

При попытке переустановки Windows XP с загрузочного диска предлагается использовать Диск автоматического восстановления системы (ASR). Как его можно создать?

Вставьте чистую дискету в дисковод, далее следуйте в направлении: **Пуск ▸ Программы ▸ Стандартные ▸ Служебные ▸ Архивация данных**. Перейдите в расширенный режим. Следуйте в **Сервис ▸ Мастер аварийного восстановления системы**. Укажите путь для создаваемого архива (только не указывайте диск **C:**). После сбора необходимой информации начнется процесс архивации. Теперь вновь запустите **Мастер подготовки аварийного восстановления**. После создания архива вам будет предложено вставить дискету для записи на нее параметров восстановления. На этом создание набора ASR закончено.

Какие действия могут предотвратить сбой нестабильной системы?

Нестабильная работа может служить первым признаком того, что скоро вам понадобится применить на практике советы по восстановлению системы. Поэтому не дожидайтесь, когда Windows продемонстрирует вам «синий экран», начинайте активно действовать.

- Загрузитесь в защищенном режиме. Если компьютер продолжает работать нестабильно, то, скорее всего, проблема в аппаратной части. В противном случае пытайтесь локализовать проблему.
- Операционная система от Microsoft имеет в своем составе утилиту SFC. Ее задача — проверка всех защищенных системных файлов и замена неправильных либо поврежденных версий. Это утилита командной строки. Чтобы запустить ее, выполните в меню **Пуск** команду `sfc /scannow`. Обнаружив присутствие измененных файлов на диске, утилита предложит либо обновить данные о файле (не рекомендуется), либо восстановить файл с дистрибутивного диска (это и следует сделать). В последнем случае SFC заменит измененный системный файл оригинальным.
- Проверьте систему антивирусом.
- Исправьте ошибки в реестре, например, утилитой CCleaner (**www.ccleaner.com**) или более ранней NBG Clean Registry (рис. 13.4).

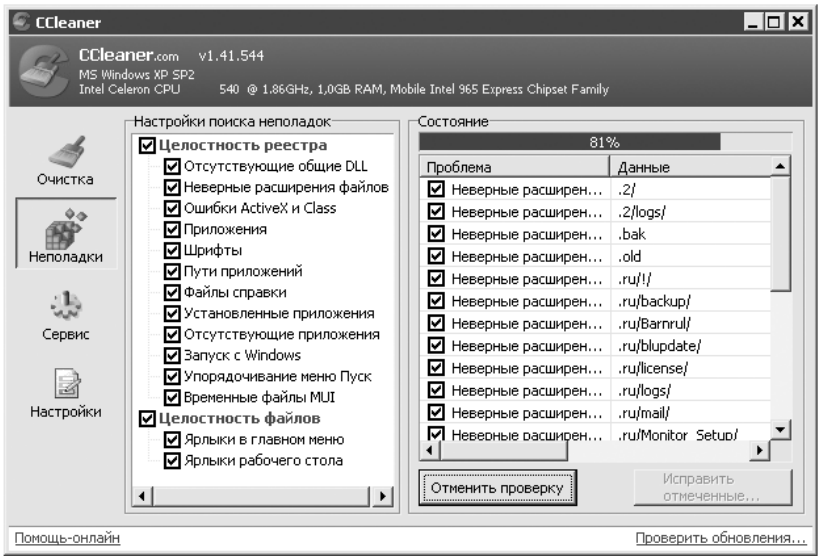


Рис. 13.4. Окно утилиты CCleaner

Если указанные экспресс-методы не помогли, то проблема находится достаточно глубоко и требуется детальный анализ. Перед тем как совершать более рискованное вмешательство в систему, рекомендуется создать резервную копию важных документов и сохранить драйверы.

При восстановлении защищенных файлов Windows командой sfc/scannow система просит установочный компакт-диск. Но у меня дистрибутив находится на жестком диске. Как перенаправить утилиту на него?

Самый очевидный способ — переписать дистрибутив на компакт-диск и «скормить» его системе. Но есть и другой выход. Запустите **Редактор реестра** (**Пуск ▸ Выполнить ▸ regedit**), откройте в нем ветвь **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup** и в параметре **SourcePath** укажите путь к папке с дистрибутивом.

Файл Word перестал открываться. Что делать?

В папке, где хранился этот файл, могут быть временные файлы с символом ~ в начале имени (например, `~wrl0002.tmp`) или с расширением TMP. Поочередно задайте для них расширение DOC и попробуйте открыть. Такие же файлы следует поискать в папке `C:\Documents and Settings\ваше_имя_пользователя\Local Settings\Temp`.

Какие программы, кроме консоли восстановления, можно использовать для «возвращения к жизни» Windows?

Для восстановления Windows можно использовать не только консоль, но и программы сторонних разработчиков. Большинство из них являются платными и, соответственно, предоставляют более широкий спектр возможностей по восстановлению. Программный пакет, имя которому Winternals Administrator's Pack, поможет вам справиться с проблемой. Несмотря на фигурирующее в названии слово «Administrator», работать с этим набором программ могут и обычные пользователи.

Как увидеть раздел NTFS в DOS?

При невозможности загрузить Windows прочитать данные с дисков, отформатированных под NTFS, непросто. Входящая в комплект от Winternals утилита

NTFSDOS Professional позволяет из MS-DOS получать доступ к дисковым разделам с файловой системой NTFS. При запуске NTFSDOS Professional монтирует ваши NTFS-разделы и, если находит возможность, дает им те же буквы, что были назначены в Windows.

Перед началом работы предлагается скопировать файлы NTFSDOS Professional на компакт-диск. Для начала запустите Boot Disk Wizard — этот мастер поможет создать необходимые файлы. Далее вам предстоит сделать следующее.

1. Указать кодировку, используемую в версии вашей MS-DOS. Поскольку наиболее распространена версия для США, то по умолчанию в NTFSDOS Professional используется кодовая страница 437. Если же у вас русская MS-DOS, то следует добавить русскую кодовую страницу 866. Однако нужно иметь в виду, что это действие не поможет прочитать в NTFS-разделах имена файлов, написанных русскими буквами, потому что для хранения имен файлов NTFS использует Unicode, а MS-DOS применяет OEM-кодировку.
2. Потребуется разыскать компакт-диск с дистрибутивом Windows 2000/XP/Server 2003 и вставить его в привод — Boot Disk Wizard нуждается в некоторых системных файлах.
3. Вам будет предложено выбрать директорию для установки NTFSDOS Professional. Это может быть либо дискета, либо каталог на жестком диске (второе предпочтительнее).

   Из каталога файлы NTFSDOS Professional можно скопировать на компакт-диск, а в качестве загрузчика использовать дискету с MS-DOS и драйверами для привода. Скачать различные версии MS-DOS можно на сайте **www.bootdisk.com**. Однако помните, что Winternals рекомендует использовать MS-DOS 7.0 (ту самую, которая была в Windows 98).
4. Подготовительные процедуры выполнены. После запуска файла `ntfspro.exe` происходит монтирование NTFS-разделов, и далее вы можете обращаться с ними как обычно, то есть создавать и удалять каталоги, файлы, пользоваться командами MS-DOS. Управлять работой программы можно, если при запуске к `ntfspro.exe` добавлять параметры. Например, ключ `/l:<буква>` заставит программу раздавать имена дискам начиная с заданной вами буквы.

Вторым компонентом NTFSDOS Professional является утилита NTFSCHK. Она предназначена для проверки NTFS-разделов на наличие ошибок. По умолчанию NTFSCHK работает в режиме «только чтение». Если вы запустите `ntfschk e:`, то получите только сведения об ошибках, но не сможете их исправить. Устранить их можно, если запустить утилиту с ключом `/f`. Получить информацию о доступных разделах можно, выполнив `ntfschk /s`.

Дисковые операции на расстоянии

Полный контроль над дисками удаленного компьютера передает в ваши руки программа Remote Recover. Список возможностей обширный: вы можете создавать на диске новые разделы и удалять старые, форматировать диски под FAT или NTFS, запускать проверку и дефрагментацию, заменять поврежденные системные файлы и удаленно менять пароль администратора.

Remote Recover состоит из двух частей: клиентской (устанавливается на компьютеры, нуждающиеся в восстановлении) и серверной (должна быть установлена на рабочей машине). Загрузка клиентов может производиться либо с загрузочной дискеты, либо через сеть по протоколу PXE (этот вариант годится только для сетей, в которых есть DHCP-сервер).

Процесс создания загрузочной дискеты классический, за исключением того, что на одном из этапов потребуется вставить в привод компакт-диск именно с Windows NT 4.0 Server, поскольку программа установки нуждается в Microsoft Network Client 3.0. Вот здесь-то и кроется неприятность для обладателей новых сетевых карт. Дело в том, что для работы потребуется самостоятельно найти драйверы под Microsoft Network Client для своих сетевых карт. А это трудно.

Всего этого можно избежать, если воспользоваться ERD Commander. Это мощнейшее по функциональности средство значительно опережает Remote Recover и, без преувеличения, является главным продуктом в программном пакете Administrator's Pack.

ERD Commander

При помощи ERD Commander можно получить полный доступ даже к «мертвой» системе. Интерфейс программы напоминает Windows XP — это удобно, поскольку не нужно привыкать к чему-то новому. В состав ERD Commander входят разнообразные инструменты: собственная консоль, менеджер загружаемых сервисов и драйверов, редактор реестра, файловый браузер, просмотрщик системных логов, текстовый редактор и утилита для изменения пароля локальной учетной записи.

Программа инсталляции ERD Commander создает ISO-образ, который нужно записать на компакт-диск, после чего с него можно осуществлять запуск. От пользователя этот процесс требует усилий не больше, чем загрузка Windows. Когда ERD Commander стартовала, первым делом нужно просмотреть системные папки при помощи кнопки **Event Log Viewer** и попытаться понять, отчего произошел сбой. Когда известно хотя бы направление, в котором сто-

ит двигаться, можно приступать к активному вмешательству в систему. Возможностей в ERD Commander для этого предостаточно.

Процесс удаления или блокирования неисправных драйверов реализован более удобно, чем в консоли восстановления, и позволяет отключать драйверы, мешающие загрузке Windows. Делается это на вкладке **Service and Driver Manager**, далее следует перейти к пункту **Drivers** и вызвать окно свойств подозрительного драйвера, после чего в поле **Startup type** можно будет указать нужный тип запуска (чтобы заблокировать драйвер, выбирайте **Disabled**).

Пользователи, которые имели дело с установкой прав доступа, знают, что Windows можно в два счета вывести из строя, установив неправильные права доступа к системным каталогам. Проблема довольно распространенная. Допустим, по неопытности или злому умыслу (кстати, так поступают некоторые вирусы) к каталогу `windows/system32` был запрещен доступ для всех. В этом случае система ведет себя довольно забавно — где-то на середине загрузки компьютер словно спотыкается и неожиданно начинает перезагружаться (то же происходит и в защищенном режиме). ERD Commander решает эту проблему быстро: в файловом менеджере вызовите свойства папки и в появившемся окне нажмите кнопку **Reset Permissions**, установите флажок **Reset Permissions for all child object**. То же можно проделать и с ключами реестра при помощи встроенного в ERD Commander редактора реестра. Вернуть доступ к ключу можно в меню **Edit**, выбрав пункт **Reset Permissions**.

Что касается реестра, то стоит упомянуть, что для редактирования в **ERD Commander** доступны только две корневые ветви: `HKEY_CLASSES_ROOT` (ассоциации файлов и объектов) и `HKEY_LOCAL_MACHINE` (информация о локальной системе).

Как известно, встроенная в Windows XP функция восстановления позволяет восстановить систему и вернуться к удачной конфигурации, если возникли ошибки после инсталляции программ или при установке нового оборудования. Тем не менее эта возможность доступна, только когда можно загрузить систему. Когда же загрузка невозможна, становится невозможным и восстановление средствами Windows. Утилита System Restore в ERD Commander позволяет получить доступ к точкам восстановления, созданным Windows XP, и вернуть систему к более благополучной конфигурации. Находится System Restore в разделе **Administrative Tools** в меню **Start**. Работа с утилитой похожа на работу с мастером восстановления Windows XP и не вызывает затруднений.

ERD Commander снабжена консолью. В ней функционирует разработанная Microsoft утилита Diskpart. Она позволяет проводить различные манипуляции

над разделами жесткого диска. Оснастка Disk Management в ERD Commander является графическим интерфейсом для этой утилиты, позволяя делать почти все то же, что и Diskpart. Отличия состоят только в том, что Diskpart работает в диалоговом режиме и позволяет взаимодействовать со сценариями.

Самое интересное в ERD Commander — утилита Locksmith. Она делает, казалось бы, невозможное: при включенной программе Syskey позволяет менять пароль для любой учетной записи, в том числе и администратора. Единственное условие: неповрежденные файлы реестра.

Бытует мнение, что в ERD Commander можно запускать любые Windows-приложения, но это не совсем так. Вот результаты нашего эксперимента. Программы из пакета Office работать не захотели, потребовав установки. Symantec Antivirus запустился, но старательно игнорировал диски компьютера, отказываясь их сканировать. Зато запустились Total Commander и WinRAR (правда, с русскими буквами в интерфейсе были проблемы, но русскоязычные названия папок и файлов отображались без проблем).

FileRestore. Неотложную помощь в восстановлении удаленных файлов окажет FileRestore, программа чем-то напоминает поиск в Windows. Вы можете разыскать на всех локальных дисках удаленные файлы. Задать можно довольно много условий, как, например, время последней модификации, ограничения на размер и т. д. Данная утилита полезна, когда в результате удаления или перезаписи важных файлов система стала неработоспособной.

Disk Commander. Одинаково эффективным и опасным средством для работы с вашим жестким диском является Disk Commander. Основное назначение программы — спасение данных с аварийных накопителей. Поставить под угрозу сохранность музыкальных коллекций, собраний фильмов и картинок, которые хранятся на винчестере, не так уж и сложно: всего за несколько мгновений этого эффекта можно добиться внезапным отключением электричества либо неосторожным обращением с командой `fdisk`. А терять данные совсем не хочется, поэтому и приходится обращаться к таким средствам, как Disk Commander. Программа умеет восстанавливать удаленные файлы как в существующих разделах, так и на неразмеченном пространстве диска. При запуске Disk Commander мастер интересуется, имеется ли буква (**`C`**, **`D`** и т. д.) у раздела с интересующими вас данными; если буква не назначена (в Windows вы не сможете прочитать данные с такого раздела), то Disk Commander может провести сканирование всего диска, чтобы получить доступ к таким областям. Опытные пользователи даже могут попытаться восстановить поврежденную структуру диска вручную, получив прямой доступ к таблицам разделов и загрузочным записям. Главное —

быть предельно осторожными, чтобы восстановленная система окончательно не утратила работоспособность.

Слежка

В комплект Administrator's Pack входят еще две утилиты: для наблюдения за реестром (Regmon) и файловой системой (Filemon). Небольшие по размеру, они иногда оказывают немалую помощь.

Filemon контролирует и отображает всю деятельность файловой системы на компьютере. Программа имеет расширенную фильтрацию и возможность поиска, показывает, файлы с каким расширением использует приложение.

После запуска Filemon появляется постоянно изменяющийся список из названий активных процессов, характеров их запросов к файлам (запись, чтение) и путей к используемым файлам.

При помощи Filemon можно отлавливать вредоносные программы-шпионы на вашем компьютере. Для этого нужно воспользоваться главным свойством клавиатурного шпиона — он должен сохранять введенные данные в какой-нибудь файл. Значит, чтобы выследить шпиона, достаточно просмотреть список файлов, в которые ведется запись при работе с клавиатурой. В программе Filemon нажмите сочетание клавиш **Ctrl+L**, в открывшемся окне настроек фильтров снимите флажки **Log Opens** и **Log Reads**, установите флажок **Log Writes**. Таким образом, вы будете получать информацию только об операциях записи.

Теперь запускайте любой текстовый редактор и набирайте в нем текст, а тем временем Filemon собирает нужные данные. Если клавиатурный шпион есть, то он обязательно проявит себя и осуществит запись в какой-нибудь подозрительный файл, что-нибудь вроде `ks000log.txt`. Проверить свои опасения можно, щелкнув правой кнопкой мыши на строке с названием процесса и в раскрывающемся меню выбрав **Process properties**. Если процесс запускается из несистемного каталога или имеет странное имя, то есть повод задуматься.

Утилита Filemon может применяться и в более мирных целях. К примеру, она способна помочь, когда из-за неправильной расстановки прав доступа возникают проблемы с запуском программ. Это актуально для многопользовательских систем с файловой системой NTFS.

Решить проблему можно, отслеживая файлы, к которым у тестируемой программы нет доступа (напротив них будет установлен флажок **Access denied**). Для удобства сортировки результатов следует использовать фильтр.

Утилита Regmon работает аналогично Filemon, только вместо файлов отслеживает операции с ключами реестра. Каждая из этих программ имеет возможность проводить мониторинг удаленного компьютера. В меню **Computer ▸ Connect** и далее в сетевом окружении выберите исследуемый компьютер. Если вы обладаете соответствующими правами, программы подключатся к удаленному компьютеру и начнут мониторинг (если после подключения в окне приложения ничего не отображается, нажмите сочетание клавиш **Ctrl+E**, чтобы начать сбор информации).

Какими программами делать резервное копирование?

Не проходит и минуты, чтобы в каком-то уголке нашей планеты не разразился проклятиями человек по поводу безвозвратно исчезнувших данных. Дабы не повторять их судьбу, необходимо делать резервное копирование. Программ для этого предостаточно. Одни создают образы целых разделов, вторые занимаются резервным копированием и архивированием важных файлов, третьи имеют еще более узкую специализацию, например делают копию реестра. Каждое из этих средств хорошо по-своему.

Однако разнообразие — это не всегда хорошо: такое важное дело, как резервное копирование, нельзя доверять первой попавшейся утилите — в Сети полным-полно полуфабрикатов, до конца не проверенных и работающих с ошибками. Такие программы противопоказаны к применению. Поэтому доверять нужно лишь устоявшимся брендам.

Полное резервное копирование

В последнее время все большую популярность приобретает утилита Acronis True Image (**www.acronis.ru**), разработанная нашими соотечественниками. Начиная с девятой версии, она совмещает в рамках одного продукта два взаимодополняющих способа резервного копирования:

- создание точного образа диска, который содержит все данные: операционную систему, реестр, драйверы устройств, приложения и данные, а также служебные области диска, скрытые от пользователя;
- резервное копирование любых файлов и папок по выбору пользователя.

Во время установки Acronis True Image будет предложено создать специальный загрузочный диск, этой возможностью лучше не пренебрегать. Вся процедура займет не более пары минут, зато в аварийной ситуации будет откуда загрузиться и восстановить поврежденную систему. Интерфейс утилиты прост и понятен.

Перейдите к созданию образа диска (рис. 13.5). Он может содержать копии сразу нескольких разделов винчестера. Причем в сам образ копируются данные только с занятых секторов раздела, попутно упаковываясь с заданной степенью компрессии. В итоге получается, что образ раздела в большинстве случаев имеет значительно меньший объем, нежели сам диск. При необходимости можно разделить получившийся файл на несколько более мелких (например, чтобы записать образ на несколько компакт-дисков).

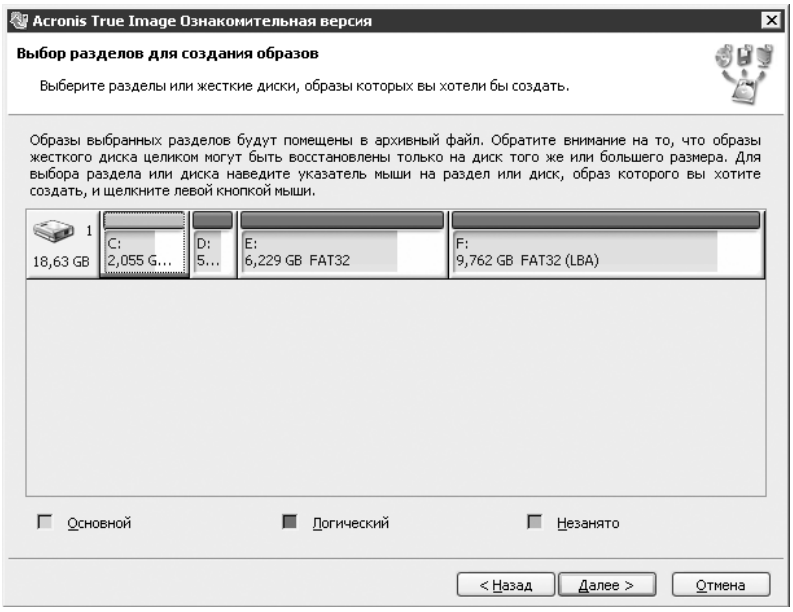
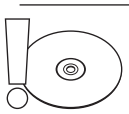


Рис. 13.5. Окно приложения Acronis True Image

Если вы копируете раздел не в первый раз, то можно создать так называемый инкрементный образ. Такой образ содержит данные только с тех секторов диска, которые были изменены с момента создания предыдущего. Получившийся в результате файл имеет куда меньший объем, нежели был бы у полной копии, и на его создание уходит значительно меньше времени. Однако следует иметь в виду, что его одного будет недостаточно, для последующего восстановления раздела потребуется еще и полный образ.



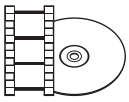
ВНИМАНИЕ

Будьте внимательны при работе с программами дефрагментации, если вы пользуетесь инкрементным копированием. Дефрагментация сильно меняет таблицу размещения файлов, что сказывается на последующем инкрементном образе: в него записывается существенно большее количество дополнительной информации, чем до дефрагментации.

Пользователи, у которых на винчестере много свободного места, могут воспользоваться Acronis Secure Zone — это специально созданная область на жестком диске, невидимая для операционной системы и приложений. Она доступна только для утилиты True Image, поэтому хранящиеся в ней образы более защищены от повреждения, чем если бы они хранились на этом же диске, но в обычном разделе.

Операция восстановления диска осуществляется несколькими способами. Так, если нужно восстановить обычный несистемный диск, действие осуществимо в режиме реального времени. Необходимый образ можно подключить в качестве виртуального диска и скопировать нужную информацию. В случае когда требуется восстановить раздел с установленной Windows, лучше использовать Acronis Startup Recovery Manager (во время загрузки компьютера нажмите клавишу **F11**). Если же компьютер совсем не загружается, то как раз для этого случая (еще при установке True Image) к данной книге прилагается специальный загрузочный диск.

Оболочка восстановления True Image очень похожа на интерфейс Windows XP, так что проблем с пониманием не возникнет. В случае использования с компакт-диска оболочка полностью загрузится в оперативную память компьютера, и загрузочный диск можно будет смело извлекать, чтобы вставить в привод компакт-диски с образами.



ВИДЕОКУРС

Научиться работать с программой вы сможете, просмотрев урок «Урок 22. Утилита Acronis True Image», расположенный на компакт-диске, прилагаемом к книге.

Сегодня достойных альтернатив у Acronis True Image три: Symantec Norton Ghost (**www.symantec.com**), Paragon Drive Backup (**www.paragon.ru**) и FarStone RestorIT (**www.farstone.com**). Что касается Norton Ghost, то эта утилита зарекомендовала себя как мощнейшее средство резервного копирования данных, именно из-за его мощи Norton Ghost не рекомендуется для домашних пользователей.

Компания Symantec для домашних пользователей предлагает утилиту Norton GoBack (**www.symantec.com**). Она обеспечивает постоянную защиту данных в автоматическом режиме почти незаметно для пользователя. Чтобы провести восстановление системы, не нужно вникать в причину неполадки. Возврат может быть осуществлен практически в любую конфигурацию, которую имела система после установки Norton GoBack. Восстановить можно и незагружаемую систему, для этого используется специальный загрузочный диск.

Кроме того, Norton GoBack дает пользователю возможность просмотреть и восстановить любые файлы, которые были ошибочно удалены из системы. Более

того, она позволяет в хронологическом порядке ознакомиться со всеми изменениями, которые происходили на жестком диске: пользователь видит окно, в правой части которого находится список измененных файлов, а в левой — календарь и циферблат. В придачу ко всему программа снабжена парольной защитой. Среди недостатков стоит отметить, что утилита очень громоздка и занимает много дискового пространства, а постоянный мониторинг требует значительных затрат системных ресурсов. Особенно это заметно в первые минуты после включения, когда компьютер начинает заметно «притормаживать».

Весьма хорошо зарекомендовала себя утилита Paragon Drive Backup. Работа с ней проста и надежна. Интерфейс Paragon Drive Backup чем-то напоминает Partition Magic в годы своей юности. Приятное впечатление оставляет скорость работы программы, она хорошо работает даже на компьютере слабой мощности и предъявляет довольно скромные требования к системным ресурсам. Paragon Drive Backup умеет работать по сети и поддерживает шифрование образов дисков.

Снимок реестра

Храните реестр в местах, недоступных для детей, и берегите от попадания прямых солнечных лучей. А если что-нибудь с ним все-таки случится, то доставайте снимки. Сделать их поможет, например, Advanced Registry Tracer (**www.elcomsoft.com**).

Сразу после запуска программа начинает проводить сканирование, и менее чем через минуту снимок реестра будет готов. Advanced Registry Tracer предоставляет много побочных сервисов по работе с реестром, но основное назначение утилиты — это возможность отмены изменений. Если компьютер стал работать нестабильно после установки какого-либо приложения, запустите Advanced Registry Tracer и нажмите сочетание клавиш **Ctrl+R**. Утилита создаст новый снимок реестра, и вы получите возможность отменить все сделанные ранее изменения, предварительно сравнив их нажатием клавиши **F10**.

Еще одна программа похожего назначения — RegSnap (**www.lastbit.com**); кроме снимков реестра, она умеет делать снимки системных файлов.

Частота использования перечисленных утилит линейно зависит от того, насколько часто вы устанавливаете новое программное обеспечение. В профилактических целях рекомендуется запускать одну из них хотя бы раз в неделю.

Файлы

После первого знакомства с утилитой APBackUp (**www.avpsoft.ru**) кажется, что она написана не профессиональными программистами, а студентами последних

курсов. Виной этому нескладный интерфейс программы, сразу видно, что с дизайном у разработчиков APBackUp дела обстоят неважно. Зато с функциональностью проблем нет. Приложение имеет богатый арсенал возможностей.

При создании резервной копии допускается обработка сразу нескольких директорий, как с локальных, так и с удаленных дисков, поддерживается копирование файлов по маске. К примеру, можно заархивировать все DOC-файлы из какой-либо директории и пропускать остальные. Есть свой планировщик, в котором указывается периодичность запуска задания. Создайте задание, щелкните кнопкой мыши по нему два раза, и вы поймете, что значит много настроек.

Кроме того, APBackUp умеет «складировать» резервные копии на FTP-сервере или на файл-сервере в локальной сети.

У данной утилиты, кроме внешнего вида, есть еще один недостаток — она платная. Пользователи, которым она действительно нужна, смогут раскошелиться на программу, а для экономных есть вариант попроще. Речь идет об утилите с названием, которое говорит само за себя: Save2FTP. Производитель тот же (**www.avpsoft.ru**), утилита бесплатная и с более аккуратным дизайном. Save2FTP создает резервную копию данных на FTP-сервере с заданной периодичностью. Это незаменимая утилита для пользователей, которые по-настоящему берегут свои данные, потому что с компакт-диском или резервным винчестером неприятность может случиться скорее, чем с целым FTP-сервером (особенно если к его выбору отнестись ответственно).

Застраховаться от утраты важных файлов поможет избирательное архивирование, которое позволяет сэкономить место на диске, выделяемое под резервные копии. Программа Smart Data Backuper, которую вы найдете на прилагающемся к этой книге компакт-диске, собирает все важные файлы с различных директорий и записывает их в один архив. Утилита поддерживает четыре вида архивации: полную, быструю, выборочную и архивацию с обновлением. Быстрая архивация, к примеру, работает только с новыми и измененными файлами, что позволяет сэкономить и время, затрачиваемое на архивацию, и дисковое пространство.

Планировщик утилиты Smart Data Backuper предоставляет пользователю свободу выбора: благодаря системе исключений есть возможность задавать любые временные отрезки и условия. Исключения работают и при определении заданий, можно приказать утилите копировать всю директорию, за исключением «тяжелых» PSD-файлов. Можно также задавать так называемую глубину архивов, то есть указывать количество архивов, которые необходимо оставлять в директории архивации.

СОВЕТ

Хранение копии на одном разделе с данными, которые нужно сохранить, — вариант далеко не самый лучший. Стремитесь к тому, чтобы копия и оригинал находились как можно дальше друг от друга. Объяснение этому очень простое: если жесткий диск откажется работать, то восстановить данные с копии, находящейся на нем, будет проблематично. Хорошими местами для хранения резервных копий являются сменные носители, сетевой файл-сервер либо второй жесткий диск.
Даже при использовании встроенной функции восстановления Windows не следует пренебрегать архивированием наиболее важных документов, поскольку функция восстановления Windows не делает копии всех файлов.
Всегда старайтесь делать мониторинг системы перед масштабной установкой каких-либо программ или началом экспериментов с настройками системы. Восстановить систему из образа быстрее, чем возвращать большое количество настроек в исходную позицию либо деинсталлировать много программ.

Как восстановить данные после форматирования?

К сожалению, данные теряются не реже, чем ключи, перчатки и зажигалки. Происходит это порой по вине самих пользователей, а иногда из-за странных совпадений.

Вопрос восстановления удаленных данных уже поднимался в разделе второй главы, посвященном безопасности. Как выяснилось, вернуть данные после форматирования все-таки можно.

Утилита GetDataBack (**www.runtime.org**) призвана восстановить данные после всевозможных катаклизмов: удаления, повреждения загрузочного сектора и таблицы размещения файлов, системных ошибок файловой системы. И самое главное — GetDataBack возвращает данные даже после форматирования диска.

СОВЕТ

По умолчанию интерфейс GetDataBack на немецком языке. Пользователям, более сильным в английском, следует направляться в пункт меню Werkzeuge ▸ Sprache и здесь выбрать Englisch.

После более близкого знакомства GetDataBack начинает производить впечатление серьезного продукта. С течением времени это впечатление только усиливается. Ниже приведен пример работы с утилитой.

Предположим, вы отформатировали диск (например, HDD2) с важными данными. Первое, что вы делаете, — это подключаете его в качестве второго диска к другому компьютеру. Обязательно проверьте в BIOS, чтобы он не был загрузочным, система должна стартовать со «здорового» диска (к примеру, HDD1).

Далее вспоминаете, какая файловая система была на HDD2 до форматирования, и выбираете соответствующую ей версию утилиты на сайте **www.runtime.org** или на прилагающемся компакт-диске (GetDataBack выпускается в двух вариантах — для каждой файловой системы своя версия).

Устанавливайте утилиту на HDD1 и запускайте. На первом шаге выберите отформатированный диск (обычно это HD129).

На втором шаге выберите раздел жесткого диска HDD2, который был отформатирован. Если диск не содержит более одного раздела, выберите целый диск.

На третьем шаге утилита поинтересуется по поводу диапазона, в котором следует производить сканирование. Обычно здесь ничего не нужно выбирать, оставьте предопределенные установки и нажмите кнопку Next. Теперь GetDataBack начнет сканирование (рис. 13.6). Это займет какое-то время в зависимости от размера области сканирования.

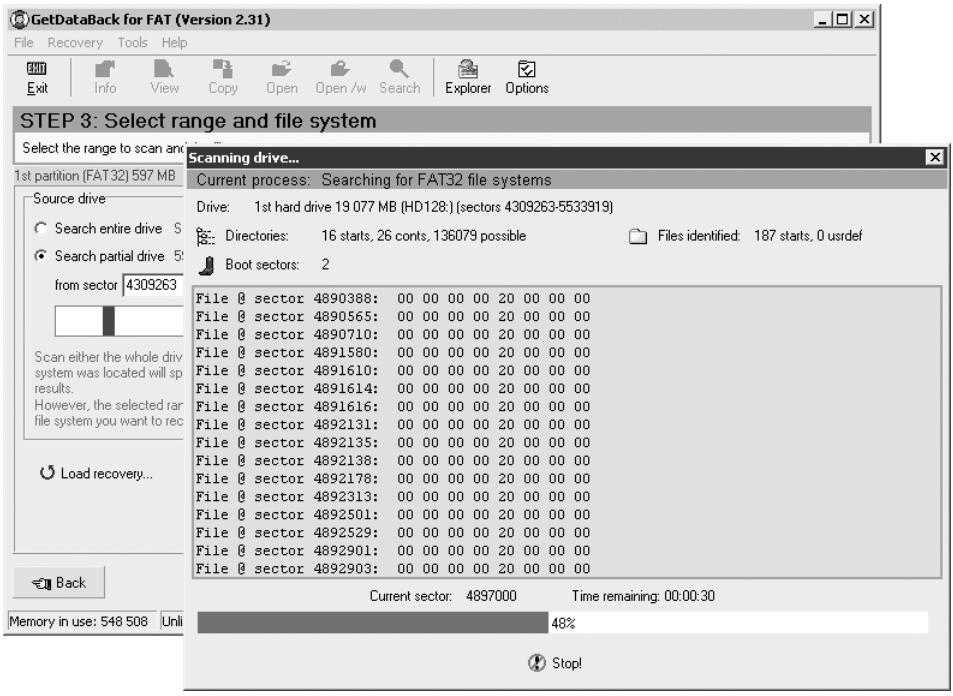


Рис. 13.6. GetDataBack сканирует диск

Как только процесс завершится, вы сможете увидеть список файловых систем, найденных утилитой. Обычно следует выбирать первую систему в списке.

На четвертом шаге GetDataBack отобразит дерево восстановленных файлов и папок (рис. 13.7). После того как появилось дерево, самое время приступать к восстановлению. Найдя интересующий файл, вы можете оценить качество восстановления, выделив его и нажав клавишу F3. Запустится встроенный в GetDataBack просмотрщик файлов. Если два раза щелкнуть кнопкой мыши по искомому файлу, то он откроется в соответствующей программе. Например, DOC-файл — в Word, а HTML — в Internet Explorer. Кстати, потом из этих программ беспрепятственно можно сохранить восстановленные файлы.

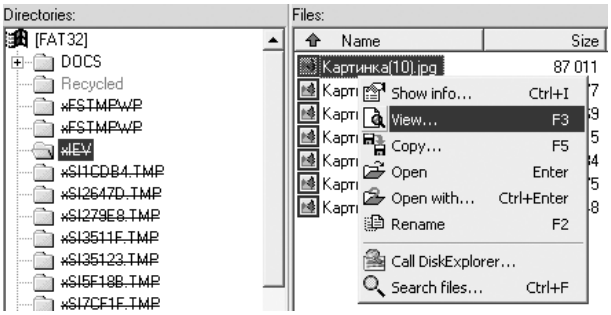


Рис. 13.7. Дерево восстановленных документов в GetDataBack

Еще одна утилита для восстановления данных после форматирования — Restorer2000 (**www.restorer2000.com**). Выступает в качестве более дешевой альтернативы предыдущему продукту. Restorer2000 работает медленнее, чем GetDataBack, да и впечатление от нее остается не такое хорошее, но это и понятно: цена утилиты Restorer2000 в четыре раза меньше. Несмотря на более низкую стоимость, Restorer2000 старается изо всех сил и восстанавливает все, что попадается под руку: файлы, папки и даже вирусы.

Как и предыдущая, программа Restorer2000 поставляется в двух вариантах: для FAT- и для NTFS-систем.

Можно ли вернуть случайно удаленные файлы?

Случайно удаленные файлы можно вернуть при помощи специальных программ.

- В арсенале Back2Life (**www.grandutils.com**) предусмотрены два метода восстановления: стандартный (standard recovery) и «умный» (smart recovery). При восстановлении стандартным методом считывается последовательная цепочка кластеров вне зависимости от того, свободны они или нет. При «умном» читаются только свободные кластеры. Таким образом, стандартный

лучше использовать, если вы уверены, что файл не был фрагментирован (то есть хранился на диске в одном месте), иначе производителем рекомендуется применить «умный» метод. Когда ущерб, нанесенный файлу, оценивается программой в 0 %, то оба метода дают одинаковый результат.

Кстати, на дисках с NTFS используется только стандартный метод, поскольку даже в случае удаления файла на диске хранится запись о последовательности его кластеров. Поэтому всегда известно, какие считывать. Щелкнув кнопкой мыши на интересующем вас файле, выбрав в раскрывающемся меню пункт **Properties** и перейдя на вкладку **Clusters**, можно просмотреть карту, где указано, сколько кластеров (хранящих данные удаленного файла) свободно, а сколько уже занято другими данными.

Опытным путем в незарегистрированной версии удалось восстанавливать только каталоги, файлы по отдельности не получилось.

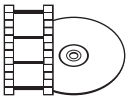
- Возможности восстановления у Handy Recovery (**www.handyrecovery.com**) не хуже, чем у Back2Life. Интерфейс красивый, все понятно. Особенно порадовала кнопка **Filter**, нажатие которой оставляет на экране только удаленные файлы, а объекты, существующие в данный момент на диске, исчезают. Отличное средство, чтобы не запутаться.

  Handy Recovery сканирует диски и в результате выдает полную структуру удаленных данных. Для каждого файла и папки указана дата их создания и последнего изменения (это и есть дата удаления). Восстановленные файлы и папки копируются в любой другой каталог, который выберет пользователь.

  Утилита может возвращать к жизни файлы, удаленные вирусами или утерянные в результате сбоя системы. Handy Recovery восстанавливает и файлы, удаленные в обход мусорной корзины (нажатием сочетания клавиш **Shift+Delete**). Без труда восстанавливается структура вложенных папок, которые были удалены неосторожным движением. Достаточно установить флажок **Restore Folder Structure** в окне **Recover**.

  Как и в Back2Life, предусмотрены два метода восстановления. Первый используется в NTFS и позволяет восстанавливать дополнительную информацию о файле, такую как пользовательские комментарии. Второй метод применяется, если снять флажок **Recover alternative data streams**.

Программ восстановления стертых данных, которые распространяются бесплатно, очень мало. Это и понятно: чтобы восстановить свою информацию, многие пользователи готовы платить. Handy Recovery не исключение — версия 2.0 позволяет восстанавливать только по одному файлу в день. Более ранняя версия распространяется бесплатно, и ее функциональность не ограничена.



ВИДЕОКУРС

На компакт-диске вы найдете урок «Урок 23. Восстановление файлов», демонстрирующий работу программ для восстановления удаленных файлов.

Если я повредил компакт-диск, можно ли прочитать с него данные?

Чего только не делают пользователи с компакт-дисками по неосторожности: ставят на них кофе, роняют на асфальт, вешают на стену в качестве зеркальца. А потом внезапно вспоминают, что на этих истерзанных дисках записана копия курсового проекта, который больше нигде не найти, или файл с паролями от почтового ящика. Что касается паролей, то их еще можно восставить (об этом — в соответствующем совете), а вот с документами уже никуда не деться — надо использовать специальные утилиты.

DVD Data Rescue (**www.naltech.com**) применяется для восстановления данных с поврежденных носителей, поцарапанных или дефектных компакт-дисков. DVD Data Rescue может восстановить диски, записанные в форматах ISO-9660 (обычно используется в коммерческих компакт-дисках и для записи программного обеспечения) и UDF (этот формат использует пакетную запись, применяется в программах, которые работают с компакт-дисками как с дискетами). Кроме того, DVD Data Rescue поддерживает работу с мультисессионными дисками (сканируется каждая сессия), также утилита восстанавливает файлы после быстрого форматирования компакт-дисков.

ПРИМЕЧАНИЕ

Следует различать понятия быстрой очистки (Quick Erasing) и быстрого форматирования (Quick Formatting). После Quick Erasing данные не могут быть восстановлены, а после Quick Formatting — могут. Для восстановления в этом случае надо использовать режим Mode B, Full scan или UltraRescue.

Разработчики DVD Data Rescue очень гордятся режимом восстановления UltraRescue, который позволяет восстанавливать файлы, записанные на поврежденных дисках, когда другие методы оказываются неэффективными.

По умолчанию при запуске утилиты появляется мастер Recovery Wizard, который поможет вам делать первые шаги при сканировании поврежденного компакт-диска.

1. На первом шаге надо указать восстанавливаемое устройство. Изменять настройки стоит, только если в системе установлены два привода для компакт-дисков.

2. На втором шаге будет просканирована структура поврежденного компакт-диска (рис. 13.8).

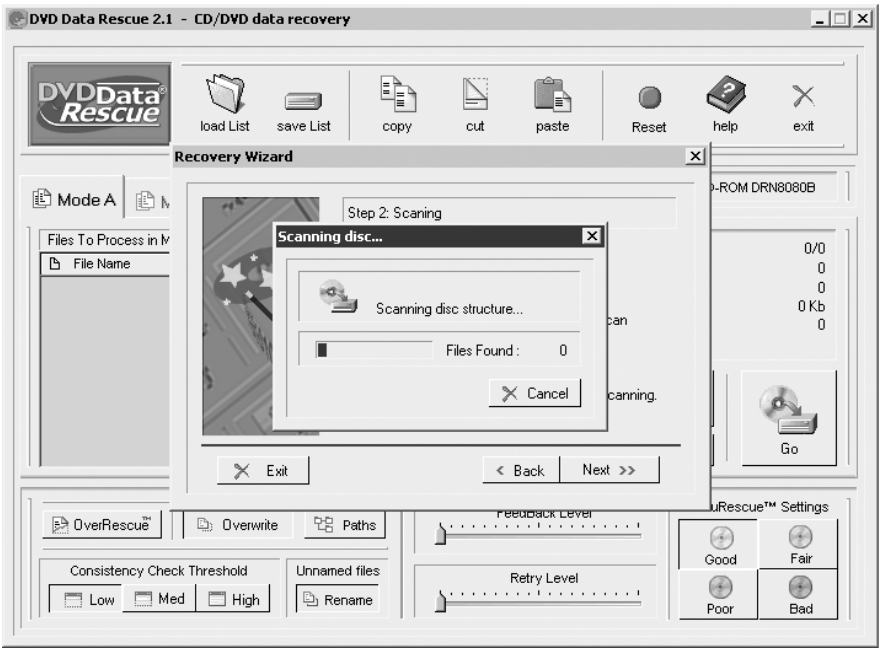


Рис. 13.8. DVD Data Rescue сканирует поврежденный компакт-диск

3. Заключительный шаг служит для определения режима восстановления: Mode A, Mode B или UltraRescue.

Recovery Wizard сделала свое дело, теперь вам предстоит работать с основным окном программы. Оно не содержит списка файлов, подлежащих восстановлению. Нужно нажать кнопку **Add Files** и добавить в главное окно документы, которые вы хотите восстановить. Далее нажмите кнопку **Dst Folder** (она находится рядом), чтобы указать папку, в которую следует сохранять восстановленные файлы.

Перед тем как приступить непосредственно к процессу, обратите внимание на вкладку **AccuRescue settings**. При нажатии одной из четырех кнопок должным образом конфигурируются настройки:

- **good** — используйте, когда пытаетесь восстановить файлы с компакт-диска в нормальном состоянии;
- **fair** — выбирайте, когда пробуете восстановить данные с умеренно поврежденного диска;

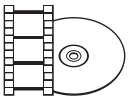
- **poor** — эти настройки следует применять, когда пытаетесь восстановить файлы с сильно поврежденного компакт-диска;
- **bad** — используйте для самых безнадежных случаев, когда повреждения носят экстремальный характер.

Восстановление музыкальных файлов

Новое — это плохо удаленное старое. Особенно справедливо данное утверждение для музыки. Если вас замучила ностальгия и хочется послушать чего-нибудь старенького, отправляйтесь на сайт **www.dtidata.com** либо на прилагающийся к данной книге компакт-диск в поисках утилиты Digital Music Recovery. Она умеет восстанавливать не только музыкальные файлы, но и видео.

Работа с Digital Music Recovery сводится к тому, что вам надо будет выбрать диск и папку, из которой следует производить восстановление, а затем нажимать стилизованную кнопку **Next** и ждать на некоторых этапах. В общем, ничего сложного и почти никаких настроек. Единственное, что можно установить в меню **Program Settings**, — типы медиафайлов, на которые Digital Music Recovery следует обращать внимание.

При просмотре списка восстановленных файлов не обращайте внимание на расширение, которое им даст Digital Music Recovery. Например, у автора файл видеоклипа оказался с расширением WMA, которое в расшифровке читается как Windows Media Audio.



ВИДЕОКУРС

Просмотрев видеоурок «Урок 24. Приложение Digital Music Recovery», вы научитесь восстанавливать музыкальные файлы.

Человеку свойственно ошибаться, но с помощью компьютера это ему удается лучше...

Глава 14

Безопасность и приватность

Откуда берутся вирусы?

Компьютерные вирусы создают люди, долго и целенаправленно разрабатывая маленькую вредоносную программу, которая потом отформатирует чей-то жесткий диск, украдет документы или стащит пароли.

Пользователи привыкли называть вирусом любую вредоносную программу, однако это не совсем правильно. На самом деле компьютерные вирусы — это всего лишь одна из трех групп вредоносных программ. Есть еще троянские программы и черви (сетевые, почтовые и т. д.).

Большинство подобных приложений распространяется через Интернет и локальную сеть, однако каждому типу вредоносных программ присущи и свои излюбленные методы проникновения в компьютер.

Вирусы сценариев распространяются в документах Word и Excel, которые можно получить как угодно. Файловые вирусы и троянские программы приходят по почте, оказываются на компьютерных компакт-дисках либо на дискетах и «флэшках».

Активировать вредоносную программу обычно можно, запустив ее самостоятельно либо щелкнув по зараженному файлу. Но есть и исключения: особую категорию составляют программы, которые запускаются без ведома пользователя, — это загрузочные вирусы и черви.

Загрузочные вирусы стартуют автоматически при просмотре содержимого зараженного компакт-диска, «флэшки» или дискеты.

Черви страшны только для пользователей, подключенных к Интернету: они сканируют всю Сеть на наличие уязвимых компьютеров и проникают на них через бреши в безопасности. Владелец об этом даже и не подозревает. Более подробную информацию о вирусах можно получить в Интернете: **www.viruslist.com/ru/**.

Есть ряд признаков, предположительно свидетельствующих о заражении компьютера. Компьютер заражен, если вы замечаете, что с ним происходят «странные» вещи, например:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие привода для компакт-дисков;
- произвольный запуск на компьютере каких-либо программ.

Кроме того, есть некоторые характерные признаки поражения вирусом через электронную почту:

- друзья или знакомые говорят вам о получении от вас сообщений, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Существуют также косвенные признаки заражения компьютера:

- частые «зависания» и сбои в работе;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке).

В большинстве случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуется провести полную проверку вашего компьютера антивирусным программным обеспечением.

Что делать при заражении вирусом?

Не поддаваться панике — это самое главное правило, которое может избавить вас от потери важных данных. Просто хладнокровно выполните следующие действия.

1. Отключите компьютер от Интернета.
2. Отключите компьютер от локальной сети, если он к ней был подключен.
3. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев.
4. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, компакт-диск или «флэшку»).
5. Установите антивирус с последними обновлениями антивирусных баз. Если это возможно, для их получения выходите в Интернет не со своего компьютера, а с незараженного компьютера знакомых, из интернет-кафе

или с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к Интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги.

6. Если на компьютере найдены вирусы, антивирус сообщит вам об этом и предложит на выбор несколько вариантов обработки зараженных объектов. Довольно часто в результате лечения зараженные данные могут быть успешно восстановлены.
7. После ликвидации последствий заражения на компьютере проверьте все компакт-диски и дискеты, которые могут оказаться зараженными вирусом.

Я слышал, что в Windows XP можно использовать учетные записи с разными правами. Как воспользоваться данной возможностью?

Системы Windows NT/2000/XP/2003 являются многопользовательскими. Обычно под этим определением понимают, что такие системы предназначены для работы нескольких пользователей за одним компьютером. Однако идея многопользовательских систем шире. На компьютере всегда должно быть две учетные записи, даже если за ним работает один человек. Первая запись — входит в группу администраторов и обладает неограниченными правами (под ней производятся настройка системы, установка утилит, антивирусов, брандмауэра). Вторая — принадлежит группе пользователей или опытных пользователей и обладает ограниченными правами (под ней происходит повседневная работа).

Концепция такого разделения прав применяется в операционных системах вроде Unix, Linux и очень важна. Ведь большинство вредоносных программ попадают к вам на компьютер во время повседневной работы. Если же вы находитесь под ограниченной в правах учетной записью, то даже запущенный вирус вряд ли сможет причинить вред, поскольку вы не имеете права изменять системные настройки, а значит, и программа, запущенная вами, — тоже. Ниже многопользовательские возможности Windows рассмотрены более детально.

Добавление пользователей

В системе Windows есть семь групп безопасности. Самые интересные из них четыре: **Администратор**, **Опытный пользователь**, **Пользователь**, **Гость**. Каждой группе соответствует свой набор прав. Добавляя пользователя в ту или иную группу, вы тем самым ограничиваете/увеличиваете его права на использование и настройку компонентов операционной системы.

- **Администратор** — обладает полным контролем над локальным компьютером и правами на совершение любых действий.
- **Опытный пользователь** — обладает правами на чтение и запись файлов не только в личных папках, но и за их пределами. Он может устанавливать приложения и выполнять многие административные действия.
- **Пользователь** — в отношении большей части системы имеет право только на чтение. У него есть право на чтение и запись только файлов его личных папок. **Пользователь** не может читать данные других пользователей (если они не находятся в общей папке), устанавливать приложения, требующие модификации системных каталогов или реестра.
- **Гость** — может выполнять очень ограниченный набор действий, в том числе выключать компьютер.

После установки Windows 2000/XP в систему, кроме пользователя **Администратор**, добавляется ваша пользовательская запись, например **Дима**. По умолчанию она имеет неограниченные права, то есть ничем не отличается от пользователя **Администратор**. С точки зрения безопасности это неправильно. Наверняка разработчики Windows пошли на такую меру только из жалости к своей службе технической поддержки, иначе у пользователей Windows по всему миру возникло бы слишком много вопросов.

Действительно, здесь нужна подготовка. Освоив концепцию многопользовательского режима на практике, вы переходите на более высокий уровень знаний и представлений о работе системы.

Не исправляйте сразу ошибку Microsoft. Для начала попытайтесь создать нового пользователя. Следуйте по маршруту **Пуск ▸ Настройка ▸ Панель управления ▸ Администрирование** и запускайте вкладку **Управление компьютером** (либо в меню **Пуск** выполните команду `compmgmt.msc`). В открывшемся окне раскройте ветвь **Локальные пользователи и группы ▸ Пользователи**. Щелкните правой кнопкой мыши по полю с перечисленными пользователями и из раскрывающегося списка выберите **Новый пользователь**. Появится окно **Новый пользователь**, введите имя, например **Тестер**.

После нажатия на кнопку **Создать** в списке появится учетная запись нового пользователя. Щелкните на ней кнопкой мыши, в открывшемся окне свойств перейдите на вкладку **Членство в группах**. По умолчанию ваш **Тестер** будет принадлежать к группе **Пользователи**. Добавить или удалить группу можно здесь же соответствующими кнопками (рис. 14.1).

Завершите сеанс текущего пользователя (например, **Дима**) и войдите в систему под именем **Тестер**. Вот ваша защищенная учетная запись, под которой и следует

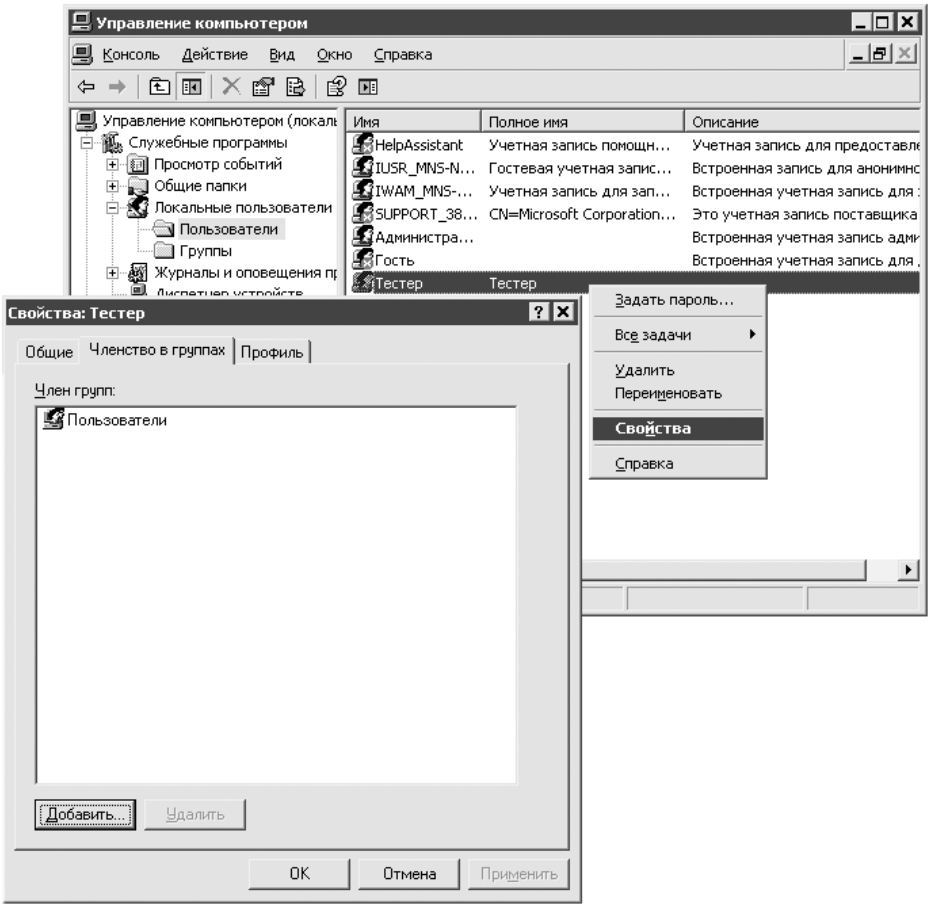
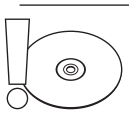


Рис. 14.1. Членство в группах безопасности

работать. Чтобы скопировать со старой учетной записи настройки программ и значки с **Рабочего стола**, завершите сеанс **Тестер**, войдите в систему как **Администратор** (пароль вы задали при установке, его может и не быть). Теперь в окне свойств системы (сочетание клавиш **Windows+Pause Break**) откройте вкладку **Профили пользователей**, выберите профиль пользователя **Дима**, нажмите кнопку **Копировать** и выберите `Documents and Settings\Тестер` в качестве папки назначения. Только не забудьте в группе **Разрешить использование** нажать кнопку **Изменить**. И выберите пользователя **Тестер**, чтобы дать ему доступ к скопированным файлам.



ВНИМАНИЕ

Скопировать текущий профиль пользователя нельзя. Это нужно делать обязательно из-под другой административной записи.

Попробуйте работать под учетной записью **Тестер**. К сожалению, из-за безграмотности разработчиков некоторые программы могут не запускаться. Если это критичные для вас приложения, сделайте следующее. Удерживая нажатой клавишу **Shift**, щелкните правой кнопкой мыши на ярлыке проблемного приложения и в раскрывающемся списке выберите пункт **Запуск от имени**. Появится окно, в котором нужно указать имя пользователя из административной группы (обычно это **Администратор**) и соответствующий пароль (рис. 14.2). В результате программа запустится с правами администратора.

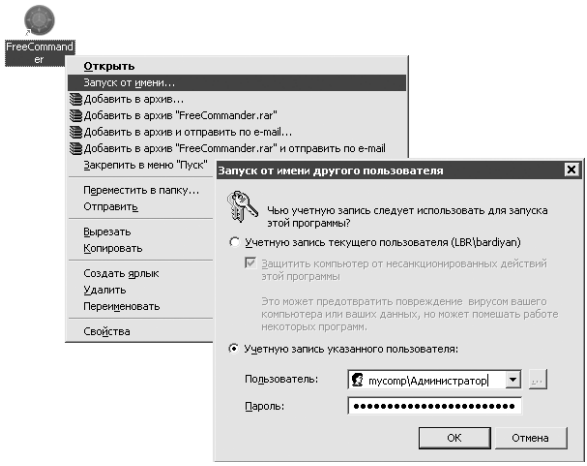


Рис. 14.2. Запуск с правами администратора

Если будет сложно, снова зайдите под именем **Администратор** и добавьте **Тестер** в группу **Опытные пользователи**, это будет компромиссное решение: не такое удачное, как членство только в группе **Пользователи**, но и не такое незащищенное, как **Администраторы**.

Данный метод кажется непривычным, но на самом деле он является общепринятым в мире серверных и профессиональных операционных систем (Unix, Linux, FreeBSD и т. д.).

Я знаю, что правильнее работать под ограниченной учетной записью, однако это не всегда возможно. Есть ли другой способ, более удобный, но такой же безопасный?

Каждодневную работу хорошо выполнять как непривилегированный пользователь, чтобы вирусы не смогли воспользоваться администраторскими полномо-

чиями. В этом случае поступайте наоборот: запускайте потенциально уязвимые приложения от имени непривилегированного пользователя. Иными словами, работая под учетной записью **Администратор**, вы будете запускать некоторые программы от имени ограниченного в правах пользователя, например **Тестер**. Данный метод не обещает стопроцентную надежность, но все же достаточно безопасен.

Сначала определите набор приложений, через которые к вам может пробраться зловредная программа. В общем случае это все программы из пакета Microsoft Office (Word, Excel, Outlook), браузер (особенно уязвим Internet Explorer), почтовый клиент (Outlook Express или The Bat!), файловый менеджер (Total Commander).

Есть два способа сделать такой старт для себя менее утомительным.

- В свойствах ярлыка каждого приложения нажать кнопку **Дополнительно** и установить флажок **Запускать от имени другого пользователя** (рис. 14.3). После щелчка правой кнопкой мыши на ярлыке появляется окно с требованием ввести имя и пароль пользователя.

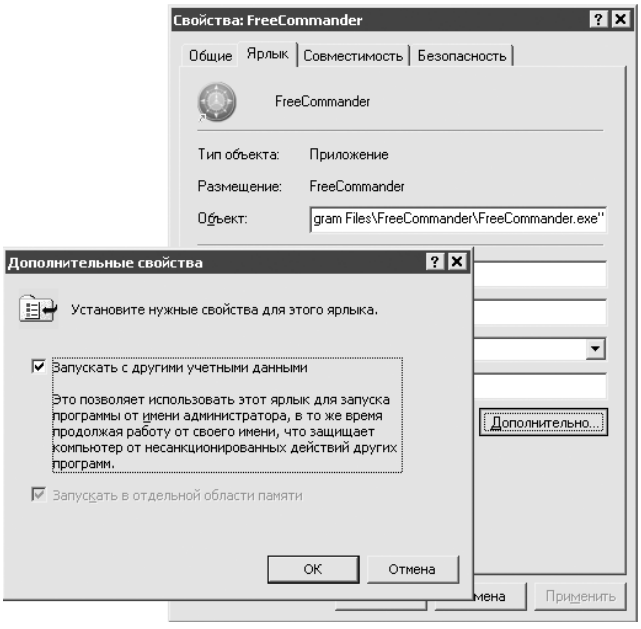


Рис. 14.3. Окно свойств ярлыка

- Второй способ заключается в использовании команды `runas`. Вы можете создать командный файл, в котором укажете, что нужное приложение должно запускаться от имени другого пользователя. Затем создайте ярлык

этого файла и запустите его. Например, вы создаете командный файл, предназначенный для запуска менеджера Total Commander: `runas /user:тестер c:\program files\totalcmd\totalcmd.exe`. Сохраните этот файл под именем `total.cmd`, и все готово. Аналогично поступаете с остальными потенциально уязвимыми приложениями.

Если проделать эти действия в Windows 2000, то обойтись без ввода пароля никак не удастся. В Windows XP Professional и версий выше у команды `runas` появился новый ключ, который эту проблему решает. Выглядит он так: `/savecred`. Если вы укажете ключ в команде `runas`, то пароль будет предложено ввести только один раз. Дальнейшие запуски программ от имени этого пользователя через команду `runas` пароля запрашивать не будут.

Непривилегированный старт

Ниже приведены некоторые рекомендации на примере ICQ о том, как правильно производить непривилегированный старт и как сделать этот процесс наиболее удобным.

1. Создайте пользователя (к примеру, **Тестер**) и определите его в группу **Пользователи**. Можно, конечно, попробовать зачислить его в группу **Гости**, но в этом случае могут возникнуть непредвиденные трудности, среди которых и снижение скорости работы.
2. Далее создайте командный файл, из которого вы и будете производить ограниченный запуск. Для общего случая команда запуска ICQ будет иметь такой вид: `runas /profile /savecred /user:тестер "c:\program files\icq\icq.exe"`. Ключ `/profile` означает, что при работе программы будет использоваться профиль указанного пользователя (то есть будут применяться настройки пользователя US, сделанные для этой программы), `/savecred` позволяет ввести пароль для пользователя US только один раз, и далее система будет подхватывать его автоматически (пустой пароль использовать не получится — запрещено политикой безопасности, хотя это исправимо). Сохраните приведенную строку в файле `icq.cmd` и поместите его, например, в каталог **Program Files**.
3. Создайте для файла `icq.cmd` ярлык на **Рабочем столе**. Щелкните на ярлыке правой кнопкой мыши и выберите **Свойства ▸ Сменить значок**. Далее следует указать путь к файлу `icq.exe` и выбрать стандарнтый значок. Теперь ярлык не отличить от обычного.
4. В свойствах ярлыка в поле **Run** установите переключатель в положение **Minimized**, чтобы после запуска ICQ на экране не появлялось окно командной строки.

По этому алгоритму можно «оформить» любые приложения. Особого падения производительности при этом не происходит, а безопасность улучшается. Этот метод нужно применять, даже если вы пользуетесь для работы в Интернете альтернативными программами (такими как Firefox, The Bat! и Miranda), хоть они и менее подвержены атакам. Помните, неуязвимых программ нет.

Пользователям Internet Explorer, Outlook Express и стандартного клиента ICQ прислушаться к данному совету просто жизненно необходимо.

Правда ли, что Windows XP позволяет ограничивать доступ к файлам для некоторых пользователей? Как это использовать для увеличения безопасности?

Одним из главных достоинств файловой системы NTFS является возможность ограничивать права пользователей. Хоть Windows XP и навязывает NTFS при установке, но, руководствуясь своей загадочной логикой, не дает воспользоваться основным плюсом NTFS в полной мере.

В Windows XP при установленном флажке **Использовать простой общий доступ ко всем файлам** возможности по изменению прав весьма ограничены. Сняв этот флажок в меню **Проводника**: **Сервис ▸ Свойства папки ▸ Вид**, вы получите доступ к набору прав NTFS (пользователям XP Home Edition, чтобы блокировать простой общий доступ, придется перезагружаться в безопасном режиме). Дальнейшее управление правами производится во вкладке **Безопасность** в свойствах объекта.

ПРИМЕЧАНИЕ

Для каждого объекта, который хранится на диске в NTFS, поддерживается контрольный список доступа (ACL). Он определяет перечень пользователей, которым разрешен доступ к данному объекту, а также тех, кому запрещен. Каждая запись в таком списке называется записью, контролирующей доступ ACE (Access Control Entry). В ней содержатся: SID пользователя или группы пользователей; список разрешений доступа (например, на чтение и запись); данные о наследовании, которые определяют, будет ли Windows использовать разрешения из родительской папки, и флажок, снятие или установка которого указывают на разрешение или запрет доступа.

Чтобы разрешить или отказать в доступе к объекту (файлу или папке), необходимо модифицировать ACE. Делать это могут владельцы объекта, члены группы Администраторы и обычные пользователи, которым это сделать разрешено.

Управление доступом к ресурсам реализовано с помощью набора предопределенных базовых прав доступа (их шесть): полный доступ, чтение, запись и т. д. Но есть еще и двенадцать специальных прав доступа, с помощью которых

разрешения настраиваются более тонко. Добраться до них можно, нажав кнопку **Дополнительно** на вкладке **Безопасность**, после чего нужно два раза щелкнуть кнопкой мыши на имени пользователя. Использование предопределенных прав упрощает процесс администрирования. На самом деле, если вы устанавливаете флажок **Чтение и выполнение**, операционная система сама назначает пять отдельных прав доступа: выполнение файлов, чтение данных, атрибутов, дополнительных атрибутов, разрешений. Считается, что шести предопределенных прав в обычных случаях вполне достаточно.

Права доступа предоставляются установкой флажка **Разрешить**. Флажки **Запретить** устанавливаются, когда требуется явно запретить применение указанного права доступа пользователю. Они имеют высший приоритет по сравнению с разрешениями и применяются в основном для внесения ясности при наложении прав нескольких пользователей. Если требуется полностью блокировать доступ к объекту, для нежелательного пользователя установите флажок **Запретить** в строке **Полный доступ**. Таким образом вы можете полностью запретить другим пользователям читать ваши личные документы.

ПРИМЕЧАНИЕ

В разделе NTFS каждый файл или папка имеют владельца, который может предоставлять или отказывать в правах доступа другим пользователям или группам. Владельцы могут заблокировать любого пользователя, включая членов группы Администраторы. Владелец объекта может предоставлять свои права другому пользователю, если тот является членом группы Администраторы. Сменить владельца можно на вкладке Безопасность ▸ Дополнительно ▸ Владелец. Кроме того, администратор системы может получить право собственности на любой объект.

С расстановкой прав надо быть очень осторожным. Не все начинающие администраторы способны установить права доступа к папкам так, чтобы сохранилась работоспособность всех программ. Обо всех тонкостях не расскажешь, их слишком много. Единственное, что можно посоветовать, — экспериментируйте, со временем придет опыт. И еще одно — всегда оставляйте группу **Администраторы** и **Система** в контрольном списке прав доступа. Довольно распространена ошибка, когда в порыве выставляются такие жесткие ограничения на папку **Windows** и системный диск, что потом нет возможности даже загрузить систему.

Верным помощником вам в этом нелегком деле будет утилита Filemon (**www.sysinternals.com**). Она позволяет отслеживать все файлы, с которыми работают запущенные в данный момент приложения. В списке также показано, удачно ли закончилась попытка открыть тот или иной файл. Если у вас не запускается какое-то приложение, к примеру CorelDRAW, вы просто отсле-

живаете, к каким файлам/папкам CorelDRAW не смог получить доступ, а потом даете текущему пользователю права на этот файл/папку. Какие права давать (на запись, удаление и вообще полный доступ), определяется экспериментальным путем.

ПРИМЕЧАНИЕ

Наряду с визуальными утилитами, в Windows XP есть возможность пользоваться для администрирования приложениями командной строки, например Cacls. Эта программа позволяет организовывать просмотр существующих прав доступа к файлам и папкам путем ввода в консоли команды cacls имя_файла. Права доступа к указанному файлу изменяются добавлением соответствующих параметров в конце строки. При просмотре разрешений с помощью Cacls отображается сокращенный список прав доступа для каждого файла, указанного в качестве аргумента. Каждый такой список включает имя пользователя и одну букву для любой из стандартных настроек прав доступа: F (full control) — полный контроль, C (change) — изменение и т. д.

Кстати, разрешения можно указывать не только для файлов и папок, но и для реестра. В Windows 2000 для этого следует выполнить из меню **Пуск** команду `regedt32` (рис. 14.4), а в Windows XP данные операции можно проводить в обычном редакторе реестра, щелкнув правой кнопкой мыши на нужной ветви.

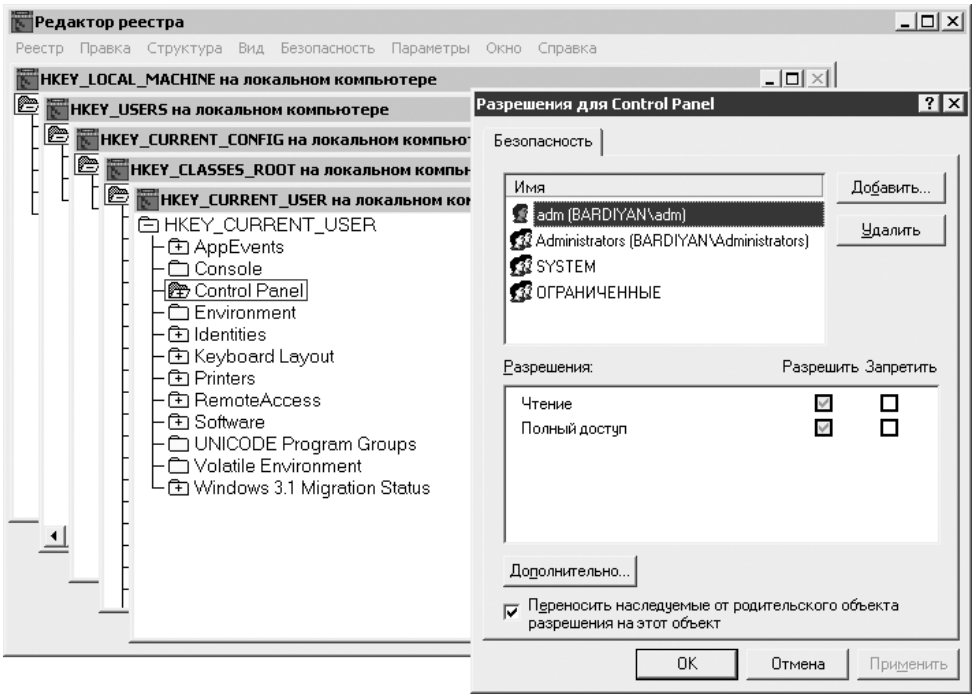
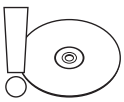


Рис. 14.4. Установка прав на ветви реестра



ВНИМАНИЕ

Работая с реестром, будьте вдвойне осмотрительны и не запрещайте доступ кому-либо без веских на то причин.

Как можно защитить учетную запись администратора от хакеров?

Учетная запись администратора чаще всего становится целью различного рода атак и домогательств со стороны злоумышленников. Это и понятно: имеющий права администратора получает полную власть над компьютером. Немного повысить уровень защиты этой записи можно, просто изменив ее имя.

Можно делать это в политиках безопасности или выполнить в меню **Пуск** команду `control userpasswords` для Windows 2000 (`control userpasswords2` для Windows XP). Во вкладке **Пользователи и пароли** выберите учетную запись администратора и нажмите кнопку **Свойства**.

После переименования можно создать учетную запись с именем **Администратор** (это будет приманка) и дать ей минимальные права, добавив в группу **Гости**. Задайте длинный пароль для фиктивной записи, чтобы окончательно «добить» предполагаемого взломщика.

Какие способы чаще всего применяют для взлома компьютера?

Есть два наиболее распространенных способа, которые не требуют от взломщика высокой квалификации и очень легко устранимы. Однако за счет того, что они малоизвестны (хотя легко предположить их использование), данные методы являются самыми действенными.

- Пустой или простой пароль администратора. На каждом компьютере есть административная учетная запись, в зависимости от языковой версии системы она называется либо **Администратор**, либо **Administrator**. Если злоумышленник имеет непосредственный доступ к компьютеру, то ему достаточно попробовать каждое из этих имен пользователей с пустым паролем. Дело в том, что пользователи довольно часто устанавливают пароль на свою учетную запись, а на встроенную запись **Администратор** забывают либо устанавливают слишком простой (например, `123456` или `qwerty`).

  Кроме того, велика опасность проникновения в ваш компьютер через сеть, используя данную учетную запись. Например, злоумышленник (зная ваш IP-адрес или имя компьютера) набирает на своем компьютере:

`\\computer17\c$` или `\\192.168.0.93\c$`, чтобы получить доступ к вашему диску **C:**. Ваша система потребует авторизоваться от злоумышленника и выдаст окно с запросом имени пользователя и пароля. В нем злоумышленник введет имя пользователя: `computer17\администратор` и какой-нибудь распространенный пароль: `123456` или `qwerty`. Если при установке вы задали первый пришедший в голову пароль (что большинство и делает), то доступ к вашим документам получен. Защититься от данного способа поможет установка сложного пароля на учетную запись администратора: **Пуск ▸ Выполнить ▸ compmgmt.msc ▸ Служебные программы ▸ Локальные пользователи ▸ Пользователи** (рис. 14.5).

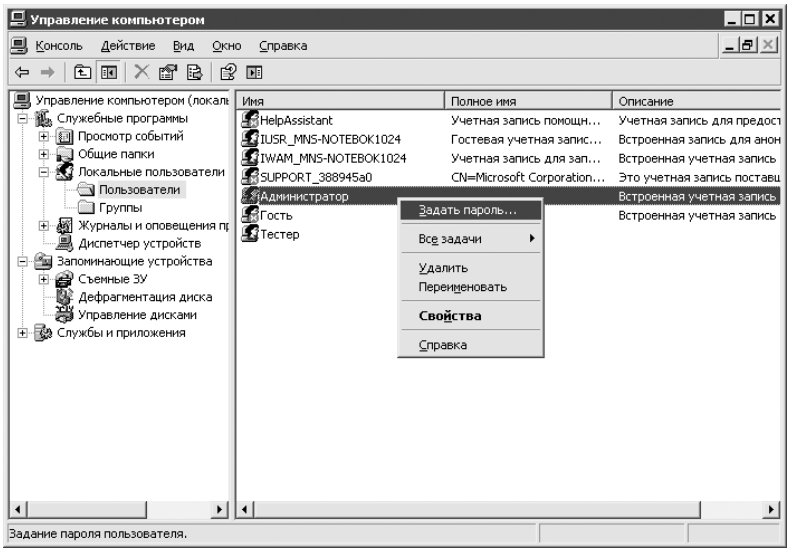
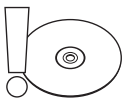


Рис. 14.5. Смена пароля встроенной учетной записи администратора

- Порой после установки операционной системы, кроме стандартных записей (**Гость**, **Администратор**), в системе обнаруживаются еще и другие учетные записи, которые не используются и, скорее всего, защищены слабым паролем (или вовсе пустым). Все неиспользуемые учетные записи следует удалить или отключить, чтобы избежать их использования злоумышленником. Не исключено, что некоторые были созданы специально, чтобы в дальнейшем через них можно было проникнуть на ваш компьютер через сеть. Поэтому следуйте по пути **Пуск ▸ Выполнить ▸ compmgmt.msc ▸ Служебные программы ▸ Локальные пользователи ▸ Пользователи** в окно **Управление компьютером** и начинайте удалять лишние учетные записи из своего компьютера, выбирая из раскрывающегося списка пункт **Удалить**. Либо зайдите в **Свойства** и установите флажок **Отключить учетную запись**.



ВНИМАНИЕ

Не удаляйте встроенную учетную запись Гость. Лучше заблокируйте ее в окне управления компьютером (меню Пуск ▸ compmgmt.msc). Если вдруг понадобится, запись можно будет легко восстановить.

Правда ли, что можно расшифровать базу данных Windows, в которой хранятся все пароли? И как это делается?

Противостояние попыткам нарушить безопасность системы по-настоящему эффективно, когда вам уже известны слабые места в ее защите, — в таком случае действия злоумышленника всегда можно предупредить.

Вскрыть базу данных с паролями пользователей — пожалуй, заветная мечта любого злоумышленника. В Windows XP информация о пользовательских учетных записях хранится в базе данных SAM (Security Accounts Manager). Резервная копия базы, созданная при установке, находится в каталоге `windows/repair`, оригинал в — `windows/system32/config`. В реестре база находится в ветви `HKEY_LOCAL_MACHINE\SAM`.

Отвечая требованиям модели безопасности, еще со времен Windows NT пароли в SAM хранятся не в открытом виде, а в виде хэша (зашифрованы при помощи односторонней функции). Расшифровать хэш можно только методом прямого перебора или зная ключ (если функция неуязвима).

С появлением утилиты Syskey вскрытие базы SAM стало занятием весьма утомительным. Но если в Windows NT Syskey можно было отключить, то в Windows XP утилита всегда работает по умолчанию и дополнительно шифрует хэш паролей так называемым стартовым ключом, который случайным образом генерируется компьютером. Бесплатные программы, которые способны взломать SAM и зашифрованную утилиту Syskey без использования прав администратора, неизвестны.

При возможности кратковременного доступа с правами администратора порядок действий следующий. Утилитой Pwdump2 нужно создать дамп базы SAM: выполните `pwdump2.exe ▸ pwd.txt` (в этот файл будут записаны результаты). Далее можно продолжать работать с правами обычного пользователя. В программе LCP следуйте в меню **Импорт ▸ Импорт PwDump-файла** и укажите путь к `pwd.txt`. Успех мероприятия будет зависеть от настроек LCP, длины паролей и наличия специального LM-хеша пароля.

Для защиты базы с паролями пользователей первым делом следует отказаться от использования LM-хэша. Эта мера приемлема для компьютеров, которым

не требуется сетевое взаимодействие с Windows 9x/3.11. Выполните в меню **Пуск** команду `secpol.msc` и на вкладке **Локальные параметры безопасности** следуйте по маршруту **Локальные политики ▸ Параметры безопасности**, здесь установите флажок **Сетевая безопасность: не хранить хэш значений LAN Manager при следующей смене пароля**. Теперь вам потребуется заново установить пароли для каждого пользователя (или переустановить старые) — смысл этого действия в том, чтобы обновить информацию в базе SAM и заменить предыдущий LM-хэш паролей на пустую строку.

Обязательное использование Syskey повысило защищенность SAM и, как следствие, общий уровень безопасности всей системы. Теперь условия взлома ужесточились, и для успеха требуется либо получение прав администратора (чтобы создать дамп), либо использование платных программ. В частности, утилита SAMInside может выполнять подбор паролей, если с атакуемого компьютера удается скопировать файлы реестра **sam** и **system**. Обезвредить такие программы очень просто. Обратите внимание на этот способ — он хоть и прост, но весьма эффективен. Итак, выполняем в меню **Пуск** команду `syskey`, в появившемся окне **Защита БД учетных записей Windows XP** нажимаем кнопку **Обновить** и самостоятельно указываем пароль запуска (для простоты он может быть таким же, как пароль администратора), затем нажимаем кнопку **OK**.

При следующей загрузке Windows вам просто придется вводить пароль два раза — для однопользовательских компьютеров это очень надежное решение. Администраторам многопользовательских систем следует указать пароль запуска, отличный от своего, а затем сообщить его всем пользователям компьютера. Даже зная пароль запуска, хакер средней руки не сумеет использовать его себе во благо, поскольку программ, позволяющих это сделать, пока нет.

Пустые пароли не кэшируются Windows XP, безразлично к ним относится и Syskey. Благодаря этому недостатку можно несанкционированно сбросить пароль администратора. Эту задачу успешно решает программа Offline NT Password and Registry Editor. Утилиту для создания загрузочной дискеты с данной утилитой можно скачать на сайте **home.eunet.no/~pnordahl/ntpasswd**.

Утилита работает в диалоговом режиме, и вам потребуется только выбрать монтируемый диск, на котором расположен системный реестр, — программа сама найдет местоположение файла реестра SAM. Для установки пустого пароля потребуется выбрать лишь соответствующий пункт меню. Даже при включенном Syskey метод срабатывает, и учетная запись оказывается без пароля. Какие могут быть последствия, догадаться нетрудно.

Оказать противодействие такого рода атакам можно, полностью запретив на компьютере загрузку со сменных носителей путем их физического удаления

из системного блока приводов для компакт-дисков и дискет. Мера крайняя и подходит скорее для серверов, чем для домашних компьютеров. Для последних будет полезным установить пароль в BIOS как на изменение настроек, так и на загрузку. Но, к сожалению, такая защита убирается нехитрой манипуляцией с батарейкой.

ПРИМЕЧАНИЕ

Обычно, чтобы сбросить настройки BIOS, из материнской платы достают батарейку на продолжительное время: 30 минут — 2 часа (чем современнее материнская плата, тем время больше). Перед процедурой необходимо выключить компьютер из сети.

Как выбрать надежный пароль и защититься от подбора?

Блокировать учетную запись после определенного количества попыток ввода неправильного пароля можно и даже нужно, дабы предотвратить попытки его подбора. Следуйте по пути **Локальные параметры безопасности** (**Пуск** ▸ `secpol.msc`) и зайдите в **Политики учетных записей** ▸ **Политика блокировки учетной записи**, где следует установить параметр **Пороговое значение блокировки** (обычно ставят 3).

Устанавливая пароль, не забывайте, что в Windows XP/2000 его длина может достигать 128 символов. Маленький, хорошо известный отрывок из «Евгения Онегина» со всеми знаками препинания, набранный русскими буквами в латинской раскладке и установленный в качестве пароля, может привести в трепет любого взломщика. Посудите сами: `Vjq lzlz cfvs[ xtcnys[ ghfdbk, Rjulf yt d ienre pfytvju, Jy edf; fnm ct, z pfcnfdbk B kexit dslevfnm yt vju`. Пароль воистину исполинский и выглядит угрожающе, а запомнить его совсем несложно: «Мой дядя самых честных правил, Когда не в шутку занемог, Он уважать себя заставил И лучше выдумать не мог».

Кроме того, специалистами были разработаны рекомендации по созданию усиленных паролей, использование которых уменьшает вероятность успешной атаки взломщика:

- пароль должен содержать не менее шести символов, и среди них должны быть символы по крайней мере трех типов из следующих четырех: заглавные буквы, строчные буквы, цифры и специальные символы (то есть *, %, &, !);
- пароль не может включать учетное имя пользователя;

- пароль не может содержать частей полного имени пользователя;
- если пользователь создает пароль, который не отвечает перечисленным требованиям, операционная система выдает сообщение об ошибке и не принимает пароль.

Заставить Windows автоматически проверять устанавливаемые пароли на соответствие данным правилам можно на вкладке **Групповая политика**: **Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Политики учетных записей ▸ Политика паролей**, где следует установить флажок **Пароль должен отвечать требованиям сложности**.

Кстати, пароль на основе «Евгения Онегина» удовлетворяет требованиям данной политики.

Я слышал, что в Windows XP есть криптографическая файловая система. Что это?

Криптографическая файловая система — это новшество, введенное в Windows 2000 и доступное теперь во всех версиях Windows XP кроме Home Edition. Полное название — Encrypted File System (EFS). По своей сути EFS не является самостоятельной файловой системой: она очень тесно связана с NTFS, можно даже сказать, является «криптографической надстройкой» NTFS.

Попробуйте что-нибудь зашифровать встроенными средствами Windows, например один файл. Сделать это очень просто: щелкните правой кнопкой мыши на данном файле и выберите из раскрывающегося списка **Свойства**, в появившемся окне нажмите кнопку **Дополнительно** и в следующем открывшемся окне установите флажок **Шифровать содержимое для защиты данных** (рис. 14.6). Теперь, если еще раз открыть свойства уже зашифрованного объекта, появится новая вкладка **Детали**, где можно выбрать зарегистрированных в компьютере пользователей, которые в дальнейшем смогут пользоваться зашифрованным файлом (доступно только в Windows XP). Для расшифровки требуется всего-навсего снять соответствующий флажок.

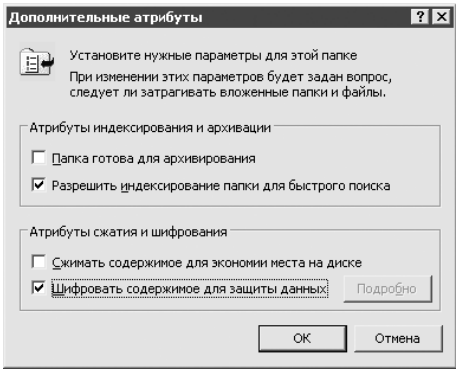
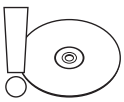


Рис. 14.6. Включение шифрования



ВНИМАНИЕ

Разрешая другим пользоваться зашифрованным файлом, вы предоставляете тот же уровень контроля над шифрованием, который имеете сами. Пользователь получает возможность так же, как и вы, добавлять или удалять других пользователей, имеющих доступ к файлу, и самостоятельно расшифровывать файл. Если после этого он зашифрует его заново из-под своей учетной записи, то вы потеряете доступ к собственному файлу.

Стандартные возможности шифрования доступны из контекстного меню файла. Для более тонкого управления шифрованием можно посоветовать команду `cipher`. Запустите консоль и наберите в командной строке `cipher /?`, а дальше руководствуйтесь приведенными выше инструкциями.

Работа с зашифрованным файлом почти ничем не отличается от работы с любым другим файлом — шифрование и расшифровка производятся «на лету». Однако есть некоторые особенности. При копировании зашифрованного файла с NTFS-раздела куда-либо еще файл расшифровывается. Соответственно, если пользователь не может расшифровать файл, то он не сможет и скопировать его в раздел, не отформатированный под NTFS (например, на дискету). Также имеет место правило: любой файл, попавший в зашифрованную папку, автоматически шифруется и таким остается даже после того, как покинет эту папку.

Как это ни удивительно, но то, что вы зашифровали файлы в Windows XP, совсем не значит, что их никто не прочтет. Может получиться даже так, что злоумышленнику и не придется взламывать зашифрованный файл. Дело в том, что в процессе работы ваши файлы вполне могут оказаться и в других местах, например во временных папках (**TEMP** или **TMP**). Кроме того, некоторые программы (например, из семейства Microsoft Office) при работе делают временные копии файлов, с которыми работают в той же директории, где находится и оригинальный файл (для восстановления данных в случае сбоя). Эти копии не шифруются автоматически. Поэтому лучше шифровать не отдельные файлы, а директории, где они хранятся. Кроме того, можно посоветовать зашифровать и папку **TEMP**. Тогда временные файлы и копии ваших данных будут автоматически зашифрованы.

ПРИМЕЧАНИЕ

Если «Пользователь 1» зашифрует папку, а «Пользователь 2» поместит в нее свой файл, то файл автоматически зашифруется, но с ключом «Пользователя 2», который поместил файл в папку. В результате «Пользователь 1» не сможет прочитать или расшифровать его. К тому же «Пользователь 1» может в любой момент снять флажок Зашифровано с папки, зашифрованной с его ключом, но это не окажет никакого влияния на находящиеся в папке файлы, как зашифрованные самим «Пользователем 1», так и кем-либо другим. Снятие с папки флажка Зашифровано приводит к тому, что скопированные в эту папку файлы уже не будут зашифровываться автоматически.

Использование EFS наверняка повысит уровень защищенности ваших данных, однако не стоит по этому поводу сильно обольщаться. Шифрование средствами EFS защитит лишь от непрофессионалов. Используемые в Windows XP алгоритмы шифрования на основе DES вряд ли будут неразрешимой задачей для спецслужб или профессиональных взломщиков.

Кража зашифрованных данных

Конфиденциальность данных, обеспечиваемая применением шифрованной файловой системы (EFS), не является гарантированной. После шифрования файла на диске остается его первоначальный образ, который можно восстановить программой для работы с жестким диском на низком уровне (например, утилитой Diskedit из пакета Norton Utilities). После восстановления можно беспрепятственно прочесть незашифрованные данные. Зашифрованный исходный файл лишь помечается как удаленный, а на самом деле продолжает существовать на жестком диске, пока на его место не будет записана другая информация. Исправить такое положение можно, запустив после шифрования утилиту командной строки **Cipher** с ключом `/w`. Она заполняет случайными значениями все неиспользуемое дисковое пространство, исключая восстановление первоначального образа.

Программа Advanced EFS Data Recovery (**www.elcomsoft.com/aefsdr.html**) позволяет расшифровывать данные, закодированные при помощи EFS в версиях Windows XP/2000 (рис. 14.7).

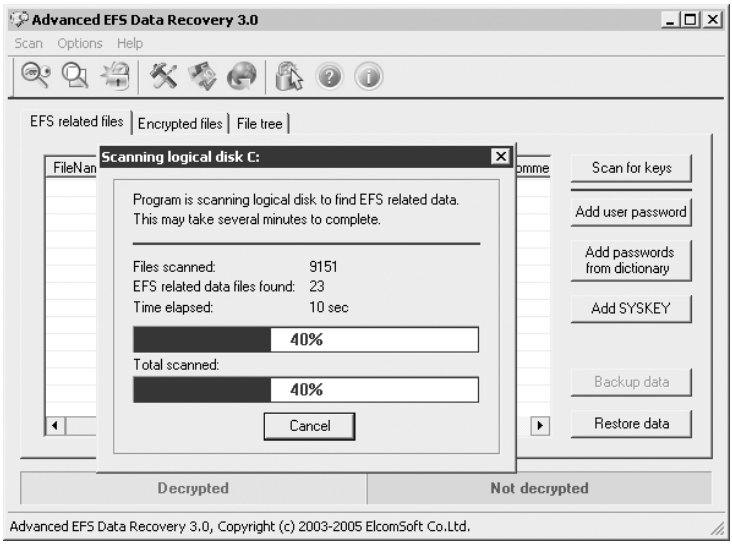


Рис. 14.7. Advanced EFS Data Recovery ищет зашифрованные файлы

Как сделать, чтобы все пользователи, кроме администратора, не смогли форматировать диски или выполнять другие операции?

Задавать ограничения для других учетных записей (не обладающих администраторскими правами) можно на вкладке **Локальные параметры безопасности** (**Панель управления ▸ Администрирование ▸ Локальные параметры безопасности**) по маршруту: **Локальные политики ▸ Назначения прав пользователя** и **Локальные политики ▸ Параметры безопасности**.

ПРИМЕЧАНИЕ

Вкладка Локальные параметры безопасности является частью вкладки Групповая политика (которая включает в себя большое число настроек), в данном случае вам достаточно возможностей первой вкладки, которую к тому же можно легко вызвать из Панели управления (групповую политику можно вызвать только командой gpedit.msc из меню Пуск ▸ Выполнить).

Как запретить пользователям изменять настройки Рабочего стола, Проводника и системы?

Помогут в этом, опять же, политики безопасности, воспользуйтесь услугами вкладки **Групповые политики** (**Пуск ▸ Выполнить ▸** `gpedit.msc`). Задать желаемые ограничения вы сможете по маршруту: **Конфигурация пользователя ▸ Административные шаблоны** — здесь расположено наибольшее скопление настроек доступа и управления основными компонентами системы (**Рабочий стол**, **Экран**, **Панель управления**, **Сеть** и т. д), меньшая часть настроек расположена в других ветвях: **Конфигурация пользователя ▸ Конфигурация Windows**, **Конфигурация компьютера ▸ Административные шаблоны**.

Говорят, после обычного удаления файл можно восстановить. Как же его удалить навсегда?

Если произошла перезапись удаленного файла новым, данные все равно можно восстановить, применяя специальное оборудование. Его работа основывается на том, что при записи на диск одного бита информации на головку чтения/записи подается недостаточно мощный сигнал. В результате на абсолютную величину записанного сигнала оказывают влияние данные, которые ранее хранились на этом месте. Иными словами, когда бит `0` замещается на `1`, интенсивность сигнала слабее, чем в случае, когда бит `1` замещается на `1`. С помощью специальных аппаратных средств можно замерять текущую интенсивность сигнала и на ее основании получить «тень» прежних данных.

ПРИМЕЧАНИЕ

На жестких дисках есть области, где можно преднамеренно прятать данные. Секторы на жестком диске формируются в процессе низкоуровневого форматирования, обычно выполняемого на заводе. Дефектные секторы помечаются, и поэтому обычно контроллер жесткого диска даже не пытается производить на них запись и чтение (хотя теоретически там могут храниться данные). Специальными средствами можно записать секретную информацию и в дефектные кластеры (если в нем есть исправные секторы).

Для доступа к таким скрытым частям жесткого диска необходимы программы, которые действуют в обход операционной системы. Профессиональные приложения криминалистов обычно очень дорогие: две-три тысячи долларов. Например, EnCase Forensic Edition (www.guidancesoftware.com).

Поэтому для сохранения конфиденциальности разработаны более надежные способы уничтожения файлов.

- Удалите файл и запустите команду `cipher /w:диск` (рис. 14.8), где `диск` — имя логического диска, с которого был удален файл. Проведите полную дефрагментацию.

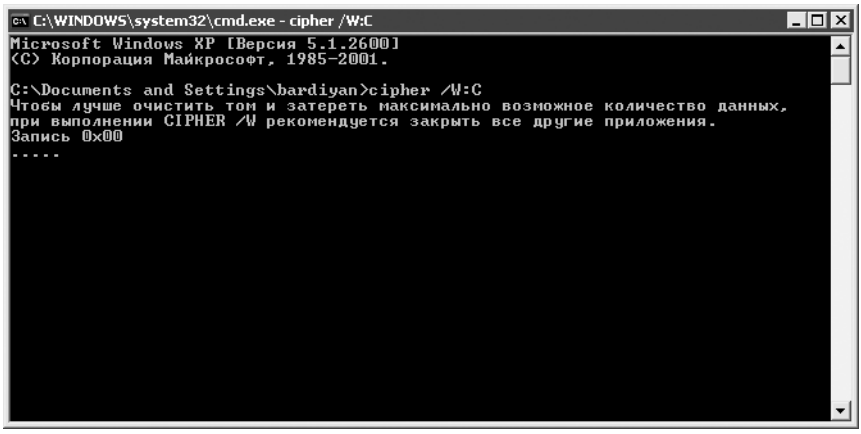


Рис. 14.8. Cipher удаляет файл окончательно

- Создайте в другой папке файл большего объема, чем тот, который надо удалить. Переименуйте его так, чтобы имя этого файла совпадало с именем файла, который вы хотите удалить. Перезапишите файл, который надо удалить, б**о**льшим файлом (просто скопируйте б**о**льший файл в папку с секретным). Для верности желательно запустить команду `cipher` и провести дефрагментацию. В этом случае способ будет более надежным.
- Используйте специальные утилиты для уничтожения файлов без возможности восстановления. BCWipe (**www.jetico.com**) пригодится для этих целей (рис. 14.9).

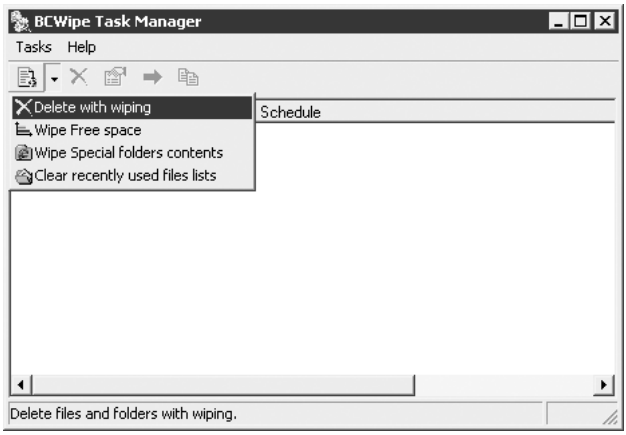


Рис. 14.9. Создание задачи на уничтожение в BCWipe

Утилитой KillDisk (**www.killdisk.com**) можно воспользоваться для надежного удаления данных с целого диска.

Программам, которые могут с высокой степенью надежности удалить файл или «затереть» целый раздел жесткого диска BCWipe и KillDisk, не хватает скорости.

Возможность избавиться от данных в любой момент, не теряя ни секунды драгоценного времени, — это и есть экстремальное уничтожение. Если вы храните информацию, которая может вас скомпрометировать, и за вами в любой момент могут прийти, зашторьте окна и читайте дальше. Есть приложения, которые могут помочь.

Hara-Kiri (**www.cyteg.com**) — так называется программа, которая удаляет данные из указанной папки, если после загрузки не нажать определенную комбинацию клавиш. Риск случайно потерять данные велик, так что подходит Hara-Kiri только тем пользователям, которым жизненно необходимо иметь возможность такого удаления. Принцип работы следующий. После каждой перезагрузки системы необходимо нажимать определенную комбинацию клавиш. Программа ожидает нажатия этой комбинации в течение указанного вами промежутка времени, иначе из выбранной ранее папки надежно удаляются все файлы. В программе предусмотрено появление сообщения (его текст можно изменять), чтобы застраховаться от удаления данных во время случайной перезагрузки. После закрытия «фальшивого» окна (неважно, ответите вы **Да** или **Нет**) Hara-Kiri начнет отсчет времени, прервать который можно нажатием заданного сочетания клавиш. Программа эффективна, когда о ней не знает потенциальный похититель данных, поскольку она видна в диспетчере задач, и процесс `harakiri.exe` можно за-

вершить до того, как он успеет удалить данные. Кроме того, при настройке Hara-Kiri в Windows 2000 постоянно возникают сообщения об ошибках.

Программа RedBut (**www.redjsoft.com**) обладает большей функциональностью, чем Hara-Kiri, и вызывает больше доверия. Утилита Red But предназначена для экстренного удаления, шифрования, подмены файлов и папок, очистки следов активности системы и пользователя. Может запускаться от нажатия сочетания клавиш, при получении сигнала по локальной сети или после запуска Windows. Для блокировки случайного удаления можно использовать предохранители.

Кроме удаления, вы можете зашифровать данные в архив нажатием заданного сочетания клавиш или подменить какой-либо файл заранее указанным.

В главном окне RedBut на вкладке **Следы активности** задается список временных файлов, ключей реестра и других следов деятельности на компьютере, которые будут очищены по вашему сигналу.

Стоит отметить забавную функцию «Анти-Босс»: в ее настройках задаются список программ, которые будут мгновенно завершены, и список файлов и приложений, которые откроются по сигналу, чтобы создать видимость работы.

Как сделать, чтобы перед выключением/включением из определенной папки вся информация из нее автоматически стиралась?

Вас выручит **Блокнот**. Предположим, вы хотите перед завершением работы автоматически удалять все файлы в папке `d:\secret`. Напишите в **Блокноте** следующее: `del /f /q d:\secret\*.*`. Сохраните файл, например, под именем `kill.cmd` в корень диска **C:**. Затем запустите редактор групповых политик (**Пуск ▸ Выполнить ▸** `gpedit.msc`) и найдите ветвь **Конфигурация компьютера ▸ Конфигурация Windows ▸ Сценарии**. В правой части два раза щелкните кнопкой мыши на параметре **Завершение работы** (или **Автозагрузка**, если хотите делать это при запуске). Используя кнопку **Добавить**, укажите на выполнение созданного вами командного файла `c:\kill.cmd` при выключении компьютера.

В качестве альтернативы можно также воспользоваться командой `attrib`, которая назначает атрибуты файлам и папкам. Установив для секретной папки атрибут **Скрытый** (`attrib +h d:\secret`), вы можете скрыть файл или папку от неопытных пользователей. Воспользоваться данной папкой вам самим можно, либо указав полный путь к ней в **Проводнике**, либо выполнив команду `attrib -h d:\secret`, чтобы снять атрибут **Скрытый**.

Сейчас существует много программ, позволяющих удаленно управлять компьютером. Как узнать, какая из запущенных утилит ожидает моих команд с удаленного компьютера?

Наблюдать за системой можно и встроенными средствами. В Windows 2000/XP можно добавить предупреждение в мониторе производительности (**Панель управления ▸ Администрирование ▸ Производительность**). Индикатором сетевого трафика могут выступать счетчики **TCP-Segments/Sec** или **Network Interface-Packets/Sec**. Сканирование портов обычно проявляется как устойчивое увеличение трафика в течение нескольких минут.

Другой встроенный инструмент контроля — утилита командной строки `netstat`. Если вы подозреваете о сканировании, то можете использовать команду: `netstat -p tcp -n`. Признаком того, что ваш компьютер сканируют, будет подозрительная последовательность открытых портов, например **4131**, **4132** или **4133**. Также следует обратить внимание на количество открытых портов (во время сканирования это число резко возрастает). Если ваши подозрения оправдались, то источник сканирования можно определить по IP-адресу в столбце **Foreign Address**.

Что касается программ, ожидающих команд с удаленного компьютера, то обнаружить их можно при помощи команды `netstat -a`, обратите внимание на столбец **Состояние**, значение `Listening` означает, что данный порт (столбец **Локальный адрес**) контролируется каким-то приложением. Узнать, каким именно, можно, воспользовавшись командой `netstat -a -b`. Ключ `-b` вызывает отображение исполняемого файла, участвующего в создании каждого подключения или ожидающего порта. Иногда известные исполняемые файлы содержат множественные независимые компоненты, тогда отображается последовательность компонентов, участвующих в создании подключения, либо ожидающий порт. В этом случае имя исполняемого файла находится снизу в скобках, сверху — компонент, который им вызывается, и так до тех пор, пока не достигается TCP/IP. Выполнение такой команды может занять много времени.

Любители графического интерфейса могут попробовать утилиту CurrPorts (**www.nirsoft.net/utils/cports.html**), которая наиболее наглядно предоставляет эти данные. Она может отображать список открытых портов; тип протокола (TCP/UDP); программы, которые используют эти порты, включая иконку, полный путь к исполняемому файлу, название продукта и описание. Кроме того, CurrPorts может постоянно обновлять список открытых портов и осуществлять подсветку изменений в нем. Теперь одного беглого взгляда будет

достаточно, для того чтобы суметь быстро оценить наличие потенциальной угрозы на компьютере в виде программ удаленного управления.

Что такое брандмауэр и как он работает в Windows XP?

В Интернете наиболее часто используются три протокола передачи данных.

- TCP — используется для установки долговременного соединения, обеспечивает надежную передачу данных.
- UDP — протокол для обмена простыми однопакетными сообщениями, об утере пакетов не сообщается. Главное преимущество заключается в том, что он не предъявляет особых требований к ресурсам компьютера.
- ICMP — протокол управляющих сообщений; является вспомогательным протоколом, с его помощью можно получать различные данные о состоянии объектов сети, маршрутизатор может обмениваться информацией с узлом.

Порты и протоколы довольно тесно связаны между собой. Термин порта является абстрактным понятием, фактически порт — это канал передачи данных. В большинстве случаев для получения и отправки данных каждому приложению назначается определенный порт. Например, среднестатистический интернет-сервер прослушивает 80-й порт, на который Internet Explorer посылает свои запросы. В то же время браузер Internet Explorer на клиентском компьютере может «висеть» на любом незанятом порте из диапазона 1023 — 16384.

Сканирование удаленных портов

Сканирование портов позволяет осуществлять поиск каналов передачи данных. Идея заключается в том, чтобы исследовать как можно больше потенциальных каналов связи и определить, какие именно находятся в состоянии ожидания соединения (открыты). Каждый открытый порт — это сервисная программа, установленная на сервере, к которой можно подключиться и выполнить определенные действия. Например, на 21-м порте «висит» FTP-сервис. Если к нему удается подключиться (пройти авторизацию, указав верные имя и пароль), то появляется возможность скачивания и закачивания файлов данного компьютера. Наибольший интерес представляют первые 1024 порта, поскольку среди них много стандартных сервисов вроде FTP, HTTP, Telnet и т. д., к которым потенциально можно подключиться (полный список на **www.iana.org/assignments/port-numbers**). К тому же в Windows 98/95 известна уязвимость следующего характера: послав на открытый 139-й порт специальный пакет, можно «выбросить» пользователя из Интернета, заставив операционную систему закрыть соединение.

В настоящее время разработано большое количество методов сканирования открытых портов удаленного компьютера. Перед началом процесса следует определить, находится ли «потенциальная жертва» в Сети. Для этого в консоли выполните команду `ping`, параметром в которой является искомый IP-адрес. В результате выполнения данной команды ваш компьютер отправляет «жертве» ICMP-сообщение и ожидает получения ответа (так называемое ICMP-эхо). Полученный ответ говорит о том, что компьютер с таким адресом к Сети действительно подключен. Следующий за этим процесс сканирования TCP- и UDP-портов может быть весьма изощренным и сложным.

Рассмотрим принцип работы встроенного в Windows XP брандмауэра.

Алгоритм работы брандмауэра Windows XP

Встроенный в Windows XP брандмауэр подключения к Интернету является брандмауэром фильтрации пакетов на основе измененного состояния. Суть данного определения становится понятной, если разобраться с алгоритмом.

В поле браузера вводится URL.

Браузер посылает пакеты, например, с 3126-го порта интернет-серверу на 80-й порт.

Брандмауэр сохраняет информацию о подключении в так называемой таблице состояний. В дальнейшем она будет использована для подтверждения возвращаемого входящего трафика.

Интернет-сервер посылает ответ на IP-адрес и исходный 3126 порт запросившего соединение компьютера.

Брандмауэр принимает ответ (входящий трафик) и сравнивает адрес источника трафика с адресом назначения пакетов из таблицы состояний; кроме того, сравниваются и номера портов. Если все совпало, то пакет идет беспрепятственно, иначе — блокируется. Информацию о пропущенных пакетах и подключениях можно просмотреть в журнале безопасности: `Windows\pfirewall.log`. Если данный файл пустой, следуйте в **Свойства соединения ▸ Дополнительно ▸ Параметры ▸ Ведение журнала безопасности** и устанавливайте соответствующие флажки.

Браузер отображает информацию интернет-сервера.

Если вы желаете сделать свой компьютер сервером и предоставлять с него доступ к службам FTP, HTTP и т. д., в окне **Дополнительные параметры** вам следует установить соответствующие флажки, иначе брандмауэр будет блокировать попытки подключиться к портам, которые прослушивают эти службы.

Часто приходится встречать в Интернете информацию, что компьютер, защищенный встроенным в Windows XP брандмауэром, невидим для различных сканеров портов. Представьте себе случай, когда хакеры сканируют диапазон IP-адресов, принадлежащих какому-либо предприятию, в надежде найти уязвимый компьютер и скачать с него всю нужную информацию. Но вначале из нескольких сотен нужно выбрать один IP-адрес подключенного в данный момент к Сети компьютера. Поэтому, чтобы не тратить силы попусту, они посылают по всем IP-адресам диапазона ICMP-сообщение: кто «откликнется», того и будут сканировать. По умолчанию компьютер должен в ответ послать ICMP-эхо. Брандмауэр заставит компьютер молчать, и, не получив ответа, хакеры просто его не заметят. Этот способ не единственный, но и в других случаях компьютер должен оставаться невидимым, так как брандмауэр отклоняет «незваные» пакеты максимально тихо.

Недостатки у встроенного брандмауэра, безусловно, есть: это узкий спектр настроек, отсутствие визуализации и невозможность блокировать исходящий трафик.

Фильтрация входящего трафика средствами TCP/IP

На компьютерах под управлением Windows 2000 и версий выше можно создать примитивный брандмауэр, используя фильтрацию TCP/IP. Она полезна с точки зрения безопасности, поскольку работает в режиме ядра, другие же методы контроля входящего доступа зависят от процессов пользователя или служб рабочих станций и серверов. Фильтрация TCP/IP позволяет следить только за входящим доступом. Для настройки безопасности протокола TCP/IP необходимо выполнить следующие действия.

Установите параметр **Фильтрация TCP/IP** в свойствах протокола Интернета (TCP/IP) и нажмите кнопку **Свойства**.

В появившемся окне нажмите кнопку **Дополнительно**, перейдите на вкладку **Общие** и выберите параметр.

Нажмите кнопку **Свойства** и установите соответствующий флажок. В окне имеются три столбца со следующими именами: TCP-порты, UDP-порты, IP-протоколы.

Для разрешения всех пакетов трафика по протоколу TCP или UDP необходимо выбрать значение **Можно все**. Пропускать только определенный трафик по протоколу TCP или UDP можно, установив значение **Только** и добавив нужный порт (чтобы блокировать весь трафик по этим протоколам, не добавляйте номера портов). Имейте в виду, что таким способом нельзя заблокировать

сообщения ICMP, для этого потребуется использовать брандмауэр или политику безопасности IP.

Я слышал, что в Windows XP можно создать брандмауэр при помощи IPSec. Как это сделать?

Протокол IP Security (далее — IPSec) обладает замечательным свойством — помимо того что он обеспечивает безопасную передачу данных, при помощи его фильтров можно контролировать исходящий и входящий трафик различных протоколов, в том числе ICMP (TCP/IP-фильтрация этого лишена).

Для работы с IPSec вам нужно запустить вкладку **Локальные параметры безопасности** (**Пуск** ▸ **Выполнить** ▸ `secpol.msc`) и перейти к параметру **Политики безопасности IP**.

По умолчанию определены три политики, они используются при выполнении запросов авторизации средствами IPSec (конечно, если вы пользуетесь данным протоколом). Но в любом случае изменять предопределенные политики не стоит, лучше создать собственную. Каждая политика состоит из списка фильтров, их может быть несколько. Каждый список фильтров выполняет определенное действие.

Теперь сформулируйте задачу: блокировать нежелательный исходящий трафик (с блокировкой входящего справится встроенный брандмауэр). Замечательным примером нежелательного исходящего трафика может являться троянский вирус, который посылает данные о вашем компьютере злоумышленнику.

Далее приведен список портов, которые наиболее часто используют распространенные троянские вирусы:

- TCP 21 — используется программами: Back Construction, Blade Runner, Doly Trojan, Fore, FTP Trojan, Invisible FTP, Larva, MBT, Motiv, Net Administrator, Senna Spy FTP Server, WebEx, WinCrash;
- TCP 23 — Tint Telnet Server, Truva Atl;
- TCP 25 — Ajan, Antigen, Email Password Sender, Gip, Haebu Coceda, Happy 99, I Love You, Kaung2, Pro Mail Trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy;
- TCP 666 — Attack FTP, Back Construction, Cain & Able, NokNok, Satanz Backdoor, ServeU, Shadow Phyre;
- TCP 1243, 2773 — используется SubSeven;
- TCP 12345 — NetBus, GabanBus, X-Bill, Pie Bill Gates;

- TCP 12346 — NetBus 1.0, GabanBus, X-Bill;
- TCP 5000 — Bubbel, Back Door Setup, S ockets de Troie, Socket 23;
- TCP/UDP 31337 — Back fire, Back Orifice, Deep BO;
- TCP/UDP 31338 — Back Orifice, Deep BO;
- TCP 54320 — Back Orifice 2000;
- TCP 54321 — Back Orifice 2000, SchoolBus v1.6 и v2.0.

Блокировать нежелательный исходящий трафик можно двумя способами, далее о каждом в отдельности.

Способ первый

Запретите исходящий трафик из списка портов, которые наиболее часто используются троянскими программами. Данная мера позволит защититься от неопытных компьютерных хулиганов, которые обычно не догадываются изменить стандартные порты в своих программах.

На вкладке **Локальные параметры безопасности** перейдите к параметру **Политики безопасности IP**. Создать новую политику можно правым щелчком кнопкой мыши. В запустившемся мастере снимите флажок **Использовать правило по умолчанию**, следуйте далее и в свойствах новой политики снимите флажок **Использовать мастер**. Нажмите кнопку **Добавить**, затем щелкните кнопкой мыши на закладке **Список фильтров**, снова нажмите кнопку **Добавить**, и откроется окно списка фильтров. Теперь вы можете создавать и включать в список собственные фильтры, нажав кнопку **Добавить**. Адрес источника пакетов устанавите в **Мой IP-адрес**, адрес назначения — **Любой IP-адрес**; флажок **Отраженный** можно снять.

Продолжайте настройку фильтра. Следуйте на вкладку **Протокол** и выберите **TCP** (хотя многие троянские программы умеют работать и через UDP), установите флажок **Пакеты из этого порта в 31337** — тем самым вы заблокировали TCP-порт для троянского вируса Back Orifice. И так нужно будет сделать для каждого.

Создав нужное количество фильтров, выберите для вашего списка действие **Запретить**, и политика готова. Назначить ее можно правым щелчком кнопкой мыши и выбором одноименного пункта в меню.

Способ второй

Этот подход предназначен для серверов. В данном случае создается два списка фильтров: один — запретительный, а второй — разрешительный. Логика такова: сначала запретить все, а потом разрешить только нужное.

По адресам приоритеты в политике безопасности IP распределены так:

- ваш IP-адрес;
- определенный IP-адрес;
- определенная IP-подсеть;
- любой IP-адрес.

По протоколам ситуация выглядит следующим образом:

- определенный протокол и определенный порт;
- определенный протокол и любой порт;
- любой протокол.

Фильтры выполняются в порядке следования приоритетов. Фильтр с наиболее общими параметрами выполняется самым последним, а фильтр с более конкретными параметрами — перед ним, тем самым его перекрывая.

Теперь за дело. Создайте фильтр, запрещающий все. Для этого в свойствах политики, когда создадите новый список, следует перейти на вкладку **Действия фильтра** и **Добавить новое** нажатием кнопки **Добавить**. В появившемся окне уставите переключатель в положение **Блокировать**. Теперь это действие можно назначать запретительному списку фильтров. В списке фильтр будет только один: источник пакетов — **Мой IP-адрес**, адрес назначения — **Любой IP-адрес**, протокол — **Любой**. С запретами покончено.

Создав список разрешающих фильтров, где будет указаны определенный протокол и определенный порт, вы добьетесь того, что данный список будет иметь более высокий приоритет. В него и следует включить разрешенные программы, которые будут использовать сетевые ресурсы.

ПРИМЕЧАНИЕ

Перечислим порты, которые используют стандартные службы: DNS-сервер — 53-й порт протокола UDP; интернет-сервер — 80-й порт TCP 80; FTP — порты протокола TCP: 20-й и 21-й; SMTP (для отправки писем) — порт TCP 25; POP3 (для приема писем) — порт TCP 110; IMAP (для приема писем) — порт TCP 143; ICQ — TCP, порт 5190.

На локальном компьютере нет смысла использовать данный способ, поскольку в этом случае не будет возможности воспользоваться даже Internet Explorer, ведь он взаимодействует не с одним конкретный портом, а любым из диапазона 1023 — 16384. По этой причине его невозможно разрешить.

Как работает сканер безопасности?

Связанный с внешним миром компьютер приходится защищать — это необходимость, которую диктует время. Справиться с поставленной задачей помогут программы двух типов: для анализа существующих уязвимостей и для обнаружения атак.

Принцип работы сканера безопасности

Программы для поиска уязвимостей обычно называют сканерами безопасности, кратко их назначение можно сформулировать так: они позволяют взглянуть на систему «глазами хакера». Это без преувеличений, ведь бреши в программном обеспечении всегда найдутся, и буквально с каждым днем обнаруживаются новые. Можно находиться в счастливом неведении и не проверять свою систему, руководствуясь принципом «все работает, ну и ладно». Однако следует иметь в виду: если сканером безопасности не воспользуетесь вы, то за вас это сделает хакер.

Сканер ищет открытые порты, сообщает о величине риска, проверяет наличие известных ему «уязвимостей» на исследуемом компьютере и выдает информацию об их устранении.

Обнаружение открытых портов — это ключевой механизм, на котором строится работа любого сканера безопасности.

Процесс, получающий или отправляющий данные через Сеть, идентифицируется номером порта; чтобы установить соединение с какой-либо сетевой службой, соответствующий ей порт должен быть открыт. В самом простом случае определить, закрыт порт или открыт, можно по следующему алгоритму.

1. Формируется TCP-пакет с установленным флажком SYN (запрос соединения) и посылается на исследуемый порт компьютера, например 23.
2. Если порт, на который пришел запрос соединения, открыт, то компьютер посылает ответный пакет с установленным флажком ACK (подтверждение соединения); если порт закрыт, отправляется пакет с флажком RST (сброс).
3. Получив пакет с флажком ACK, можно быть уверенным, что 23-й порт открыт; если же пришел ответ с флажком RST или вообще нет ответа в течение установленного времени, то значит, соединение разорвано и 23-й порт закрыт.

Именно таким способом и пользовались на заре сканирования. Но когда от него начали защищаться, было разработано множество более хитроумных

методов. Например, когда пакет с флажком SYN предварительно фрагментируется, а затем отправляется на сканируемый компьютер. Затем на его стороне IP-фрагменты собираются в один пакет, и производится его обработка. В результате выполняются те же действия, что и выше, однако использование фрагментации затрудняет обнаружение сканирования специальными фильтрами.

Наиболее распространенные методы осуществляют открытое сканирование — это значит, что пользователь, который сканирует, может быть определен по IP-адресу приходящих запросов. Но существуют еще и методы анонимного сканирования, истинно хакерские. Один из таких способов основан на использовании серверов, предоставляющих бесплатный анонимный доступ по протоколу Telnet. Подключившись к такому серверу, можно от его имени вести анонимное сканирование любого компьютера в Интернете. Для этого достаточно выполнить команду: `telnet адрес_сканируемого_компьютера номер_порта`. Если порт закрыт, будет выдана ошибка (что-нибудь вроде **Could not open a connection**), иначе — порт открыт. При использовании такого метода определить инициатора сканирования довольно сложно.

Анализ защищенности

Алгоритмы выявления и поиска «уязвимостей» становятся все более запутанными, но в тоже время работать современным сканером безопасности совсем несложно. Понятный интерфейс и подробные описания проблем делают его легким в обращении. Просканировать небольшую сеть или свой домашний компьютер не составит особого труда. Начать можно с самых простых утилит, которые нельзя даже назвать сканерами безопасности.

LanScope (**www.lantricks.com**) — многопотоковый сканер Сети. Осуществляет мониторинг в Интернете на наличие доступных ресурсов NetBios (Samba), FTP и HTTP, сканируя заданные диапазоны IP-адресов (рис. 14.11). Показывает права доступа к ресурсам, например чтение или запись. Сканер ресурсов выполняет поиск по заданному имени ресурса, например **music**, **video** и т. д.

LanSpy (**www.lantricks.com**) — это сканер безопасности для исследования Сети. Осуществляет сбор информации о компьютере: доменное и NetBios-имена, MAC-адрес, сетевые адаптеры, пользователи, настройки безопасности, разделяемые ресурсы, сервисы, информация из реестра и журнала событий (рис. 14.12).

Из профессиональных продуктов можно отметить российскую разработку XSpider (**www.ptsecurity.ru**) или сканер Retina (**www.eeye.com**).

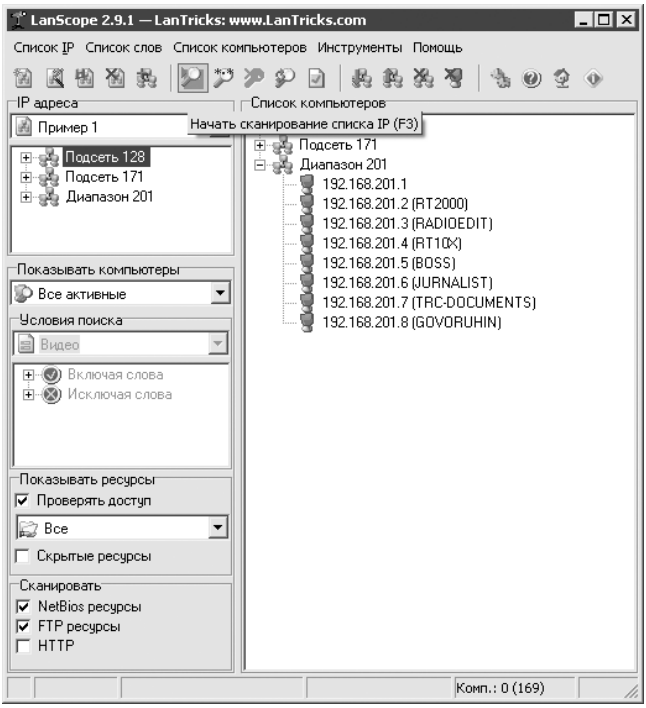


Рис. 14.11. Окно программы LanScope

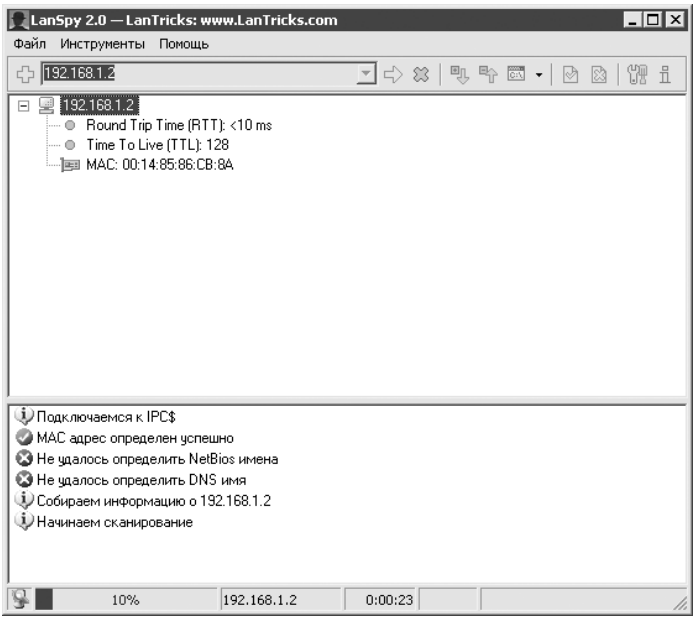


Рис. 14.12. Окно утилиты LanSpy

Обнаружение вторжений

Если вы обнаружите несанкционированную попытку сканирования, то получите предупреждение о готовящейся атаке. Помощь в этом окажет Snort (**www.snort.org**) — система обнаружения вторжений, предназначенная для мониторинга небольших сетей.

Snort позволяет в режиме реального времени анализировать сетевой трафик, проверяя соответствие содержимого пакетов определенным правилам. Для описания правил используется собственный язык сценариев. Встроенная база знаний определяет распространенные типы сканирования и сетевых нападений.

После установки Snort установите низкоуровневые сетевые драйверы WinPcap (**winpcap.polito.it**), скопируйте из директории `snort\bin` файл `libnetNT.dll` в директорию `windows\system32`.

Программа работает в режимах снифера и детектора вторжений. При работе в первом режиме Snort перехватывает сетевые пакеты. Режим устанавливается ключом `-v`. Если необходимо увидеть передаваемые в сетевом пакете данные, используйте совместно ключи `-v` и `-d`. Например, команда `snort -vd -i eth1 src host 192.1.2.3` приводит к отображению данных о пакетах, отправленных с IP-адресом 192.1.2.3 и полученных на сетевом интерфейсе ETH1. Если использовать ключ `-l`, то данные будут сохраняться в файл.

Для перевода Snort в режим детектора вторжений укажите конфигурационный файл, описывающий набор правил (обычно используется `snort.conf`): `snort -c ./etc/snort.conf -l ./log`. Правила хранятся в каталоге **rules**, их там около пятидесяти. На сайте **www.snort.org/snort-db** постоянно пополняются сигнатуры для обнаружения новых атак, их достаточно добавить в уже существующие файлы из каталога **rules**.

Файлы в логах разделяются по IP-адресам, создается один общий файл `alerts.ids`, в котором содержатся все возможные вторжения. Snort нуждается в настройке. Для упрощения работы установите графическую оболочку IDScenter (**www.engagesecurity.com**). Она облегчает задачи управления Snort, включает в себя функции диагностики конфигурации, поддерживает сигналы тревоги (при определении атаки запустите внешнее приложение).

Как сохранить анонимность в Интернете?

Протестировать уровень защиты своей системы вы можете на сайте **secyrity.symantec.com** (рис. 14.13).

Рис. 14.13. Secyrity.symantec.com позволяет протестировать безопасность

Специальные приложения на этом ресурсе проверят, насколько уязвим ваш компьютер в Сети.

На сегодняшний день анонимный серфинг вполне возможен. Проще всего замаскироваться можно, используя так называемые анонимайзеры. На каждом таком сайте есть форма для ввода адреса, набрав в ней, например, **www.xxx.com**, вы попадете на страницу издательства, однако уже как бы от имени анонимайзера. В результате будет сложнее выследить, по каким сайтам вы путешествовали, потому что большинство анонимазеров скрывают адрес сайта, на который они переходят.

Список адресов анонимайзеров, которыми вы можете воспользоваться: **www.anonymizer.com**, **www.anonymouse.org**, **www.all-nettools.com/toolbox,privacy**.

Пользователи браузера Firefox могут сделать работу с **www.anonymouse.org** удобнее, установив специальное расширение для этого браузера — Anonymouser (**https://addons.mozilla.org/ru/firefox/addon/1415**). После установки расширения перезапустите браузер. Теперь в контекстном меню для каждой ссылки

будет появляться пункт **Open with Anonymouser**, выбрав который вы откроете выделенную ссылку анонимно.

Метод использования анонимайзеров настолько же легок, как и ненадежен, поскольку большинство из ресурсов подобного рода были в свое время дискредитированы при независимых тестах, с легкостью выявивших IP-адреса их пользователей.

Более эффективный способ — использовать те минимальные возможности по сокрытию истинного IP-адреса вашего компьютера, которые уже встроены в Internet Explorer и другие популярные браузеры. Для этого в настройках браузера задайте использование любого общедоступного анонимного прокси-сервера. Анонимный (или непрозрачный) прокси-сервер заменяет в каждом проходящем через него пакете ваш IP-адрес на свой собственный, в результате чего в интернет-серверах, которые вы посещаете, записан уже не ваш адрес, а IP-адрес прокси-сервера. В Internet Explorer прокси-серверы устанавливаются в меню **Сервис ▸ Свойства обозревателя ▸ Подключения ▸ Настройка LAN**. В появившемся окне следует записать адрес прокси-сервера и порт, на котором он работает. В других браузерах запись прописывается аналогичным способом.

Уже готовые списки таких серверов можно без труда найти в Интернете (например, на сайтах: **www.freeproxy.ru**, **proxylist.virtualave.net**, **www.multiproxy.org**) либо при помощи программ. К примеру, ProxyGrab (**proxygrab.msk.ru**). Достаточно один раз занести в ее базу данных адреса популярных ресурсов, содержащих прокси-листы, и программа сама извлечет адреса прокси-серверов со всех ресурсов и оформит их в виде стандартного списка. Проверить все из списка на анонимность поможет программа Proxy Analyzer (**www.glocksoft.com**). Желательно использовать прокси-серверы с поддержкой SSL, в этом случае передаваемые данные будут зашифрованы серьезным алгоритмом, и вашему провайдеру перехватить их не удастся.

Если для вас крайне важно оставаться анонимным, следует обратить внимание на A4Proxy (**www.inetprivacy.com/a4proxy/**). Программа изначально имеет небольшую базу анонимных прокси-серверов. Другие серверы в A4Proxy можно добавлять либо поштучно, либо массово (импортируя их из текстового файла). Причем все можно тут же проверить на анонимность. Используемые прокси-серверы выбираются как вручную, так и автоматически. С ручной установкой все предельно понятно (достаточно буквально нескольких щелчков кнопкой мыши). Что касатеся автоматического выбора, то программа способна сама выбирать подходящие заданным критериям серверы исходя из результатов проверки на анонимность. В настройках A4Proxy можно задать необходимость тестирования прокси-сервера перед каждым его использованием.

Единственный нюанс — обычные прокси-серверы ведут протоколы всех действий, совершаемых пользователем, при этом, естественно, ваш IP-адрес оказывается в протоколах самого сервера, администрация которого может выдать вас. Как вы уже поняли, есть и «необычные» прокси-серверы. Платный доступ к ним предоставляют специализированные сервисы. Большинство из таких прокси-серверов установлены на компьютерах-зомби (зараженных троянским вирусом), а их хозяева даже не подозревают об этом. Такие компьютеры в огромных количествах разбросаны по всему миру, поэтому найти их следы невозможно.

Еще один сервис, на который следует обратить внимание пользователям, заботящимся о своей безопасности, — Tor (**www.torproject.org/index.html.ru**). Технология Tor предназначена для защиты пользователей Сети от анализа потока данных, разновидности сетевого надзора, который угрожает персональной анонимности и приватности, конфиденциальности бизнес-деятельности и отношений. Ваш трафик становится безопасней при использовании Tor, поскольку обмен информацией проходит через распределенную сеть серверов. Надежность программы возрастает с ростом числа пользователей, запустивших Tor.

Что делать, если администратор заблокировал доступ к любимому сайту?

Можно обойти интернет-фильтр, открывая сайты через другие. Иными словами, есть специальные эмуляторы браузеров, которые в виде JAVA-апплетов размещены на специальных ресурсах. Именно ими и следует пользоваться, чтобы посещать заблокированные администраторами сайты. Для этих целей замечательно подходят анонимайзеры. Используйте ресурс **www.operamini.com/demo/** или службу Google Translate. Достаточно ввести в адресной строке браузера ссылку вида `www.google.com/translate?langpair=en|ru&u=www.bardiyan.net`, чтобы получить доступ к заблокированному сайту, например **bardiyan.net** (рис. 14.14).

Как сохранить конфиденциальность и не дать хакерам и администраторам доступ к личной информации?

Наверняка вам есть, что скрывать от руководства, как и миллионам других людей, втайне подыскивающих новую работу или спутницу жизни через сайты знакомств.

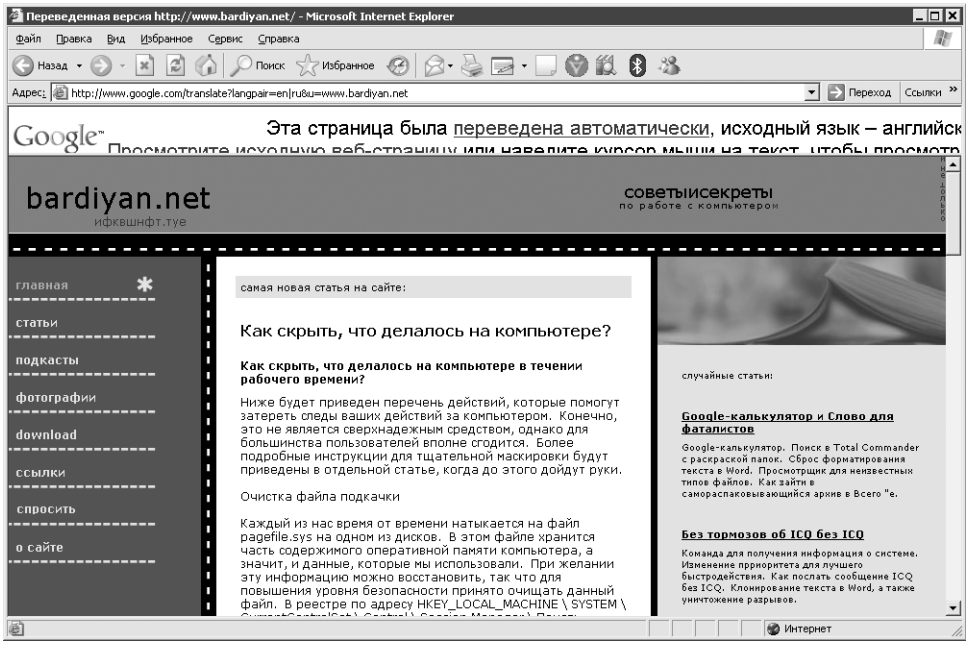


Рис. 14.14. Использование Google для обхода ограничений

Поскольку обычно вся личная информация хранится на компьютере, посягательства через него и осуществляются. Далее приведен комплекс мер, который поможет добиться решения конкретной задачи — защиты рабочего компьютера от системного администратора, поскольку именно он обычно выполняет оперативно-розыскные мероприятия на компьютерах подозреваемых сотрудников.

Для осуществления задуманного вам потребуются права локального администратора. В противном случае бороться с надзором весьма сложно.

Хороший администратор может взломать пароль и войти в компьютер под вашей учетной записью. Средства вроде установки пароля в BIOS на загрузку компьютера не остановят толкового специалиста.

Более эффективное малоизвестное решение — утилита Syskey в Windows 2000/XP. Ее назначение — шифровать пароли всех учетных записей, в таком виде они и хранятся в базе данных учетных записей Windows. По умолчанию Syskey шифрует пароли ключом, который генерируется автоматически, но существует возможность делать это вручную. В таком случае при запуске Windows вам потребуется ввести пароль, который будет использоваться для расшифровки паролей всех учетных записей вашего компьютера. Это будет происходить еще до появ-

ления окна входа в систему. Сбить пароль Syskey не под силу ни одному системному администратору. При такой защите специализированные дискеты или компакт-диски для сброса пароля локального администратора приведут лишь к сбою системы. Для осуществления задуманного в меню **Пуск** выполните команду `syskey`. В появившемся окне нажмите кнопку **Обновить** и установите переключатель в положение **Пароль запуска** (рис. 14.15). Введите пароль два раза и нажмите кнопку **OK**.

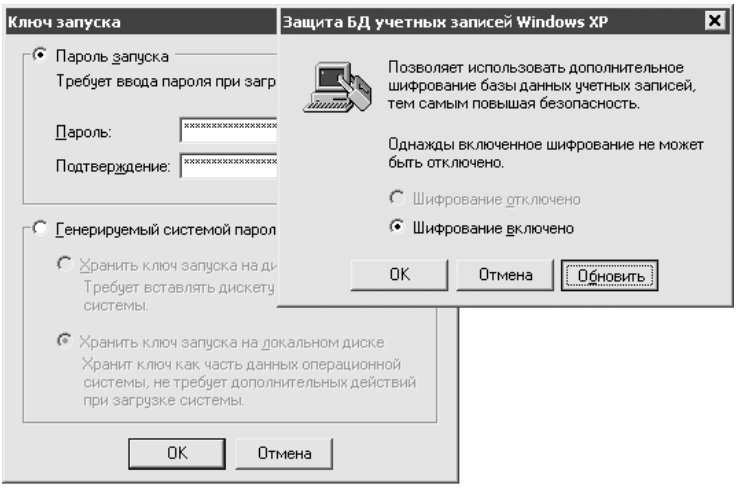


Рис. 14.15. Использование Syskey

ПРИМЕЧАНИЕ

Информация о пользовательских учетных записях хранится в защищенной базе данных SAM. В качестве усиления защиты SAM и была разработана утилита Syskey. Используя несколько уровней кодирования, она защищает информацию, сохраняемую в базе данных SAM. Данные о пароле пользователя кодируются Syskey при помощи ключа шифрования, присущего учетной записи данного пользователя. В результате использования Syskey даже при краже базы SAM взломать ее практически невозможно. При наличии физического доступа к компьютеру эта задача становится более реальной, поэтому для обеспечения высокого уровня надежности стартовый ключ следует хранить отдельно от компьютера. При вводе верного ключа произойдет разблокирование базы данных и отображение регистрационного экрана.

Теперь взломать вашу систему будет непросто. В таком случае системный администратор обычно снимает жесткий диск с вашего компьютера и подключает его к другому, чтобы прочесть содержимое всех папок и файлов.

Выход есть всегда: всю приватную информацию следует хранить на зашифрованном диске PGP (**www.pgp.com**), который при старте системы после ввода

пароля выглядит как обычный локальный диск. Получить к нему доступ по сети или подключив ваш жесткий диск к другому компьютеру не получится. Все содержимое зашифрованного диска будет находиться в файле с расширением PGD, который можно хранить на виду. Расшифровать данный файл практически невозможно.

TrueCrypt (**www.truecrypt.org**) — бесплатная утилита для создания шифрованных дисков, поддерживает алгоритмы AES-256, Serpent и Twofish. На производительности компьютера утилита сказывается меньше, чем аналогичный продукт PGP (рис. 14.16).

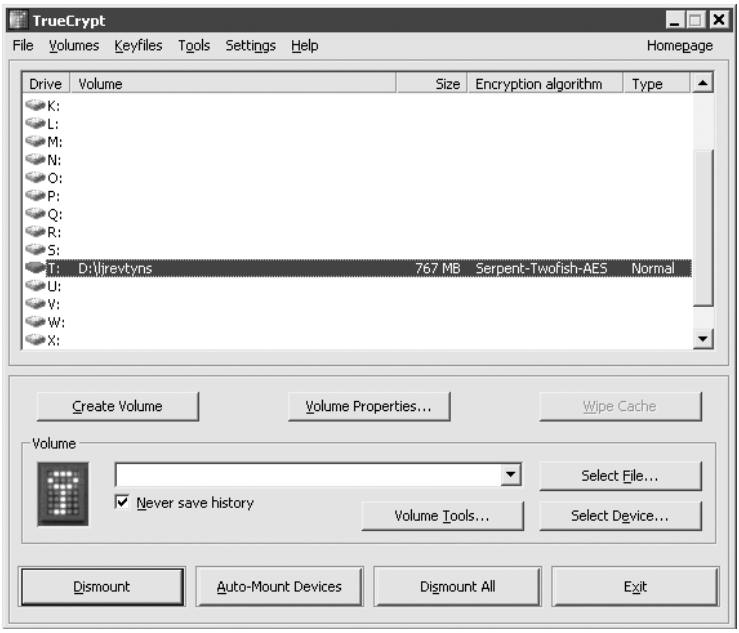


Рис. 14.16. Окно программы TrueCrypt

Папки **Documents and Settings** и **Windows/Temp** следует зашифровать с использованием EFS. Щелкните на нужной папке правой кнопкой мыши, выберите из раскрывающегося списка **Свойства**. В появившемся окне нажмите кнопку **Другие** и установите флажок **Шифровать содержимое для защиты данных**. Необходимо, чтобы жесткий диск был отформатирован в NTFS. Это пригодится, в случае если важные данные попадут во временные папки и что-нибудь «засветится» в истории браузера или почтовой базе (лучше работать с личным электронным ящиком через шифрованное соединение — перед адресом нужно указать вместо «HTTP» «HTTPS»). Использование EFS не так ресурсоемко, как PGP, и абсолютно незаметно при работе. EFS взламывается при наличии

определенных программ (**www.elcomsoft.com/prs.html**), так что доверяйте этой файловой системе лишь данные вторичной важности, самое ценное следует хранить на зашифрованном диске.

Если системному администратору не удалось получить доступ к папкам с секретной информацией, то он, скорее всего, прибегнет к последнему средству — восстановлению удаленных файлов в надежде, что «всплывут» ваши приватные документы, которые вы удалили с обычного диска после переноса на зашифрованный.

ПРИМЕЧАНИЕ

Установка таких программ, как интернет-пейджер и браузер, на зашифрованный диск, уменьшит вероятность утечки важных данных, поскольку после демонтирования зашифрованного диска получить доступ к данным программам и их истории почти невозможно. Браузер Firefox и интернет-пейджер Miranda без проблем можно установить на зашифрованный диск. Для решения проблем с другими программами можно использовать специально модифицированные приложения — www.portableapps.com.

Окончательно удалить файлы вам поможет команда `cipher /w` (работает в Windows XP и версиях выше), выполненная для каждого логического диска, или дефрагментация.

Небольшие заметки неудобно хранить на зашифрованном диске, поскольку они всегда должны быть под рукой. Поэтому можно воспользоваться программой fSekrit (**www.donationcoder.com/software/other/fSekrit/**) — это нечто вроде зашифрованного **Блокнота**. Несмотря на маленький размер программы, содержимое файла надежно шифруется по серьезному алгоритму AES. Результирующий файл сохраняется с расширением EXE, благодаря чему открыть его вы сможете на любом компьютере. После двойного щелчка кнопкой мыши по нему потребуется ввести пароль.

Для общения в ICQ на приватные темы желательно использовать программу Miranda (**www.miranda-im.org**) с плагином Acrypter (**addons.miranda-im.org**), который шифрует сообщения между вами и выбранным собеседником (у него тоже должен быть этот плагин). Щелкните на значке Miranda на **Панели задач** правой кнопкой мыши, выберите **Главное меню ▸ Acrypter Plugin** и устанавите значок ключа напротив любого из контактов. Miranda лучше целиком хранить на зашифрованном диске, тогда нет опасности, что кто-то прочтет историю сообщений.

Если вы отлучаетесь от компьютера даже на пару минут, его нужно блокировать, используя сочетание клавиш **Windows+L** или **Ctrl+Alt+Delete** и появившуюся в окне кнопку **Блокировка**.

Настройте параметры безопасности в групповых политиках: запустите **Пуск ▸ Выполнить ▸** `gpedit.msc`. В древовидном меню, расположенном в левой части окна, откройте: **Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Назначение прав пользователя**. На вкладке **Доступ к компьютеру из сети** желательно убрать все учетные записи, кроме своей (если у вас нет сетевых папок на компьютере, к которым подключаются другие пользователи). Лучше оставить только свою учетную запись в политике **Локальный вход в систему**.

Далее следуйте в направлении: **Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Параметры безопасности**. Установите флажок **Завершение работы: очистка страничного файла виртуальной памяти** (замедляет выключение машины, но не позволяет восстановить часть информации по файлу подкачки), в политике **Сетевая безопасность: уровень проверки подлинности LAN Manager** установите переключатель **отправлять только NTLM ответ** — это позволит усложнить перехват паролей по сети и не даст взломать базу SAM, в которой хранятся пароли. Если компьютер входит в домен, установите флажок **Член домена: требует стойкого ключа сеанса (Windows 2000 и выше)**.

Установите в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache` значение `Persistent=0`, это вынудит Internet Explorer удалять все временные файлы, оставшиеся после работы в Сети.

Отменить сохранение списка документов, с которыми вы работали, позволит установка переключателя `1` в области `NoRecentDocsHistory`. Адрес в реестре: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`.

Значение параметра `NoInstrumentation`, равное `1`, запрещает записывать, с какими приложениями недавно работал пользователь и к каким документам он получал доступ. Адрес в реестре: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`.

Оказывается, ядро Windows написано с использованием технологии искусственного интеллекта! И как любое разумное существо, оно пытается работать как можно меньше

Глава 15

Windows Vista

В переводе на русский язык «Vista» означает «новые возможности», «открывающиеся перспективы». Как заявляют в Microsoft, название новой операционной системы выбиралось очень тщательно: сначала оно было протестировано среди сотрудников корпорации, а затем в нескольких регионах мира методом фокус-групп и «глубинных» интервью.

Весьма интересно, что «Vista» — это название салона на горнолыжном курорте, расположенном недалеко от штаб-квартиры Microsoft. Кодовое имя «Whistler», которое во время разработки носила Windows XP, является также названием горы, расположенной все на том же горнолыжном курорте.

Как отключить службу ограничения привилегий?

Причин отключать механизм контроля учетной записи пользователя User Account Control (далее — UAC) может быть несколько: слабые нервы пользователей, которых раздражает постоянно появляющееся окно с предупреждением, либо полная уверенность в совершаемых действиях, когда опека со стороны операционной системы излишняя. Для отключения UAC следует нажать сочетание клавиш **Windows+R**. В появившемся окне **Выполнить** наберите команду `msconfig`. Появится окно **Конфигурация системы.** Следуйте на вкладку Сервис, в раскрывающемся списке выберите пункт **Отключить контроль учетных записей (UAC)** и нажмите кнопку **Запуск** (рис. 15.1). Перезагрузите компьютер.

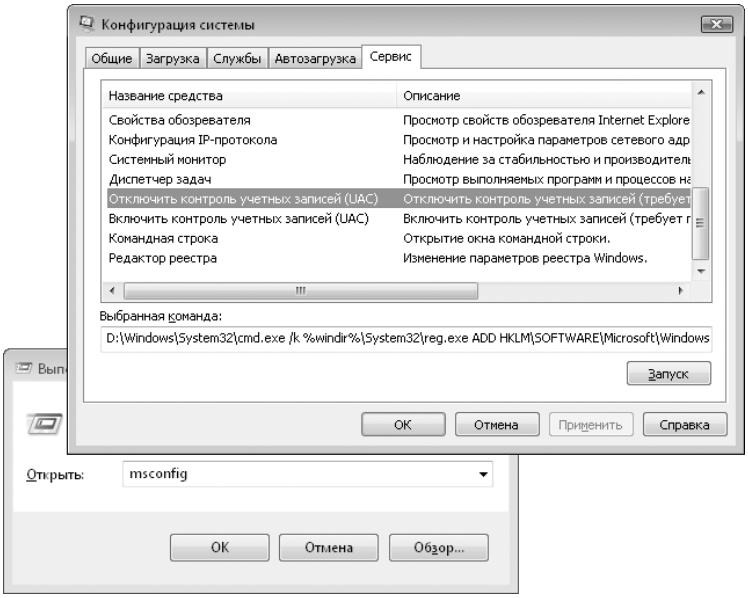


Рис. 15.1. Отключение UAC

Можно ли убрать визуальные эффекты? Компьютер не справляется с нагрузкой

Отключить некоторые эффекты визуализации можно, отправившись в следующем направлении: **Панель управления ▸ Система ▸ Дополнительные параметры системы** (либо нажав сочетание клавиш **Windows+Pause Break**). В появившемся окне **Свойства системы** на вкладке **Дополнительно** в блоке **Быстродействие** нажмите кнопку **Параметры**. Перед вами появится окно **Параметры быстродействия**, открытое на вкладке **Визуальные эффекты**. Здесь же будет представлен список визуальных эффектов, которые можно отключить.

Как изменить объем виртуальной памяти в Vista?

Управление памятью в Windows Vista очень похоже на аналогичное в Windows XP. Единственное исключение — технология Superfetch и использование индексации. Все операции проводятся в окне **Параметры быстродействия**, которое вы открыли при настройке визуальных эффектов, зайдите на вкладку **Дополнительно** и нажмите кнопку **Изменить** (рис. 15.2). Перед установкой размера файла подкачки необходимо очистить имеющийся. Выполнить это действие можно, установив флажок **Без файла подкачки** и нажав кнопку **Установить**, после чего перезагрузить компьютер. Данная операция одновременно выполняет два действия: во-первых, удаляет файл подкачки, избавляет от потенциальных повреждений файла подкачки, которые могут быть вызваны неправильным завершением работы (это поможет избавиться от многих проблем в будущем); во-вторых, размещает вновь созданный файл подкачки в одном нефрагментированном блоке на жестком диске, что опять же увеличивает производительность системы памяти.

После того как файл подкачки очищен, можно приступать к созданию нового. На каком диске или разделе должен располагаться файл подкачки, можно выбрать, исходя из следующих вариантов.

- Один жесткий диск и один раздел. В этом случае файл подкачки располагается на основном разделе жесткого диска.
- Один жесткий диск и несколько разделов. В этом случае файл подкачки должен располагаться на первом из разделов, потому что он самый быстрый. Размещение на другом разделе уменьшает преимущества создания нескольких разделов, так как головка чтения жесткого диска не может находиться в двух местах одновременно.
- Два и более жестких диска. В этом случае файл подкачки должен размещаться на физическом диске, на который не установлены Windows Vista

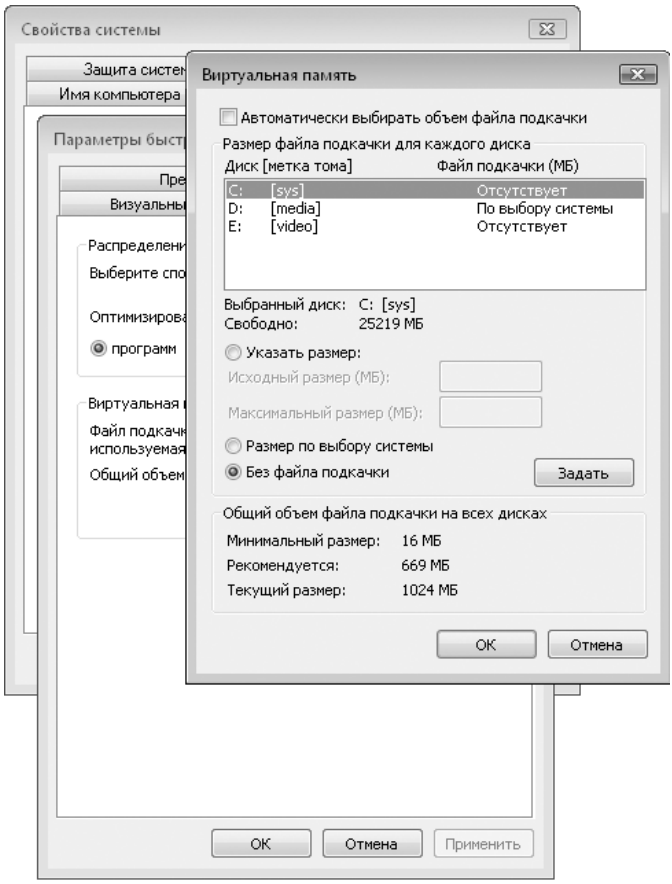


Рис. 15.2. Управление файлом подкачки

и иные приложения. Это снизит количество перемещений головки чтения основного диска и ускорит время доступа к файлу подкачки.

Какие службы можно отключить, чтобы освободить память?

Отключение некоторых служб может увеличить производительность вашего компьютера, но, с другой стороны, это может привести к некорректной работе отдельных приложений. Поэтому не бросайтесь в крайности и вместо отключения службы (установка переключателя **Тип запуска** в области **Отключена**) присвойте ей тип запуска **Вручную**, что позволит запускать данную службу, если она понадобится какому-то приложению. Отключение служб — довольно эффективный механизм оптимизации, который был успешно опробован на

Windows XP. Получить доступ к окну **Службы** можно, нажав сочетание клавиш **Windows+R** и выполнив команду `services.msc` (рис. 15.3).

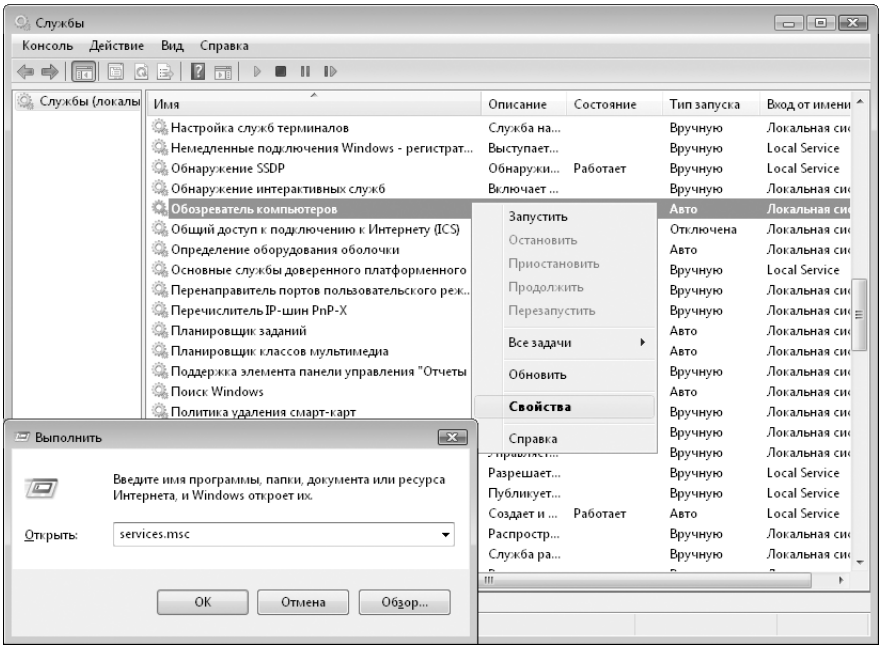


Рис. 15.3. Окно Службы

Ниже перечислены службы, которые можно отключать без вреда для работы компьютера.

- **Обозреватель компьютеров** — отвечает за составление текущего списка компьютеров сети и предоставляет его запрашивающим программам. **Обозреватель компьютеров** используется на компьютерах под управлением операционных систем Windows для просмотра сетевых доменов и ресурсов. Компьютеры, которые выступают в роли обозревателей, составляют списки просмотра, содержащие все общие ресурсы сети. Функции просмотра необходимы таким средствам Windows, как **Сетевое окружение**, команде `netview` и **Проводнику** Windows.
- **Вспомогательная служба IP** — обеспечивает автоматическую работу IPv6 на базе IPv4-сетей. Если вам не требуется поддержка IPv6, отключайте.
- **Диспетчер печати** — является ключевым компонентом системы печати в Windows. Он управляет очередями печати в системе, а также взаимодействует с драйверами принтеров и компонентами ввода-вывода, например USB-портами и протоколами семейства TCP/IP. Если вы не используете

печать и у вас в системе не установлено ни одного принтера, то отключите данную службу.

- **ReadyBoost** — обеспечивает поддержку технологии ReadyBoost. Если вы не пользуетесь USB-устройствами для повышения производительности системы, отключайте.
- **Центр обеспечения безопасности** — наблюдает за настройками безопасности. Если вы самостоятельно наблюдаете за безопасностью своего компьютера и используете антивирус или брандмауэр от сторонних производителей, то в работе данной службы нет необходимости.
- **Модуль поддержки NetBIOS через TCP/IP** — данная служба необходима для нормальной поддержки NetBIOS через TCP/IP. Если ваш компьютер не подключен к сети, то отключите данную службу.
- **Служба терминалов** — позволяет интерактивное подключение к удаленному компьютеру. Если вы никогда не подключаетесь к удаленным компьютерам, то данную службу можно отключить.
- **Веб-клиент** — позволяет Windows-программам создавать и изменять файлы, хранящиеся в Интернете. Служба интернет-клиента обеспечивает интеграцию WebDAV (Web Distributed Authoring and Versioning) в оболочку Internet Explorer/**Проводник**. Благодаря службе появляется возможность использования интернет-папок и просмотра файловых систем интернет-серверов в окне **Проводник**. Для большинства пользователей это неактуально. На обычном серфинге в Интернете отключение службы не сказывается.
- **Защитник Windows (Windows Defender)** — сканирует компьютер на наличие вирусов, позволяет делать это по расписанию и загружает собственные обновления. Некоторые пользователи отключают ее и используют сторонние приложения для обеспечения безопасности системы. Выбор за вами, но лучше использовать **Защитник Windows**, чем не использовать ничего.
- **Служба регистрации ошибок Windows** — при возникновении ошибки отправляет информацию о ней в корпорацию Microsoft (при этом появляется специальное окно). Если вы устали от него или просто не хотите сообщать о своих ошибках, отключайте. Но имейте в виду, что если система постоянно дает сбои, то данная служба является одним из лучших способов решить ваши проблемы.
- **Центр обновления Windows** — обнаруживает, загружает и устанавливает обновления Windows и других программ. Понятно, что вы не каждый день устанавливаете обновления, но служба остается запущенной в течение 24 часов 7 дней в неделю. Рекомендуется устанавливать тип запуска **Вручную** и самостоятельно проверять обновления раз в неделю или в 15 дней.

Обратите внимание, что установка типа запуска **Вручную** не позволяет службе загружаться вместе с Windows, но служба запускается, когда вы запускаете Windows Update.

- **Темы** — для максимального быстродействия мало отключить все визуальные эффекты, надо еще остановить и данную службу, которая управляет темами оформления.
- **Служба ввода планшетного ПК** — обеспечивает функционирование пера и рукописного ввода на планшетных компьютерах. Обладатели стандартных домашних компьютеров без перечисленных возможностей могут не беспокоится по этому поводу и устанавливать тип запуска службы **Вручную**.
- **Обнаружение SSDP** — обнаруживает сетевые устройства и службы, использующие протокол SSDP, такие как UPnP. В большинстве случаев обладатели домашних компьютеров могут отключать эту службу.
- **Планировщик заданий** — позволяет настраивать расписание автоматического выполнения задач на компьютере. Если в ваши планы такое не входит, можете устанавливать тип запуска службы **Вручную**.
- **Телефония** — управляет телефонным оборудованием. Если в компьютере не установлен модем и нет Сети, то можно отключить.
- **Служба списка сетей**, **Служба сведений о подключенных сетях** — если вы не используете ни локальную сеть, ни Интернет, то эти службы можно отключить.

Как оптимизировать производительность винчестера?

Щелкните два раза на значке **Диспетчер устройств** на **Панели управления** (либо выполните команду `devmgmt.msc`). В появившемся окне в древовидном списке требуется проследовать в раздел **Дисковые устройства** и раскрыть его. Щелкните правой кнопкой мыши на каждом имеющемся жестком диске, в открывшемся списке выберите пункт **Свойства**. В появившемся окне выберите вкладку **Политика** (рис. 15.4).

Проверьте, установлен ли флажок **Оптимизировать для выполнения**. Рекомендуется установить флажки **Разрешить кэширование записи на диск** и **Включить дополнительную производительность**. Цель установки этих параметров — позволить диску использовать кэш — маленькую область памяти на жестком диске, которая дает возможность заметно увеличить его производительность (особенно скорость записи). Обратите внимание, что данные установки нельзя

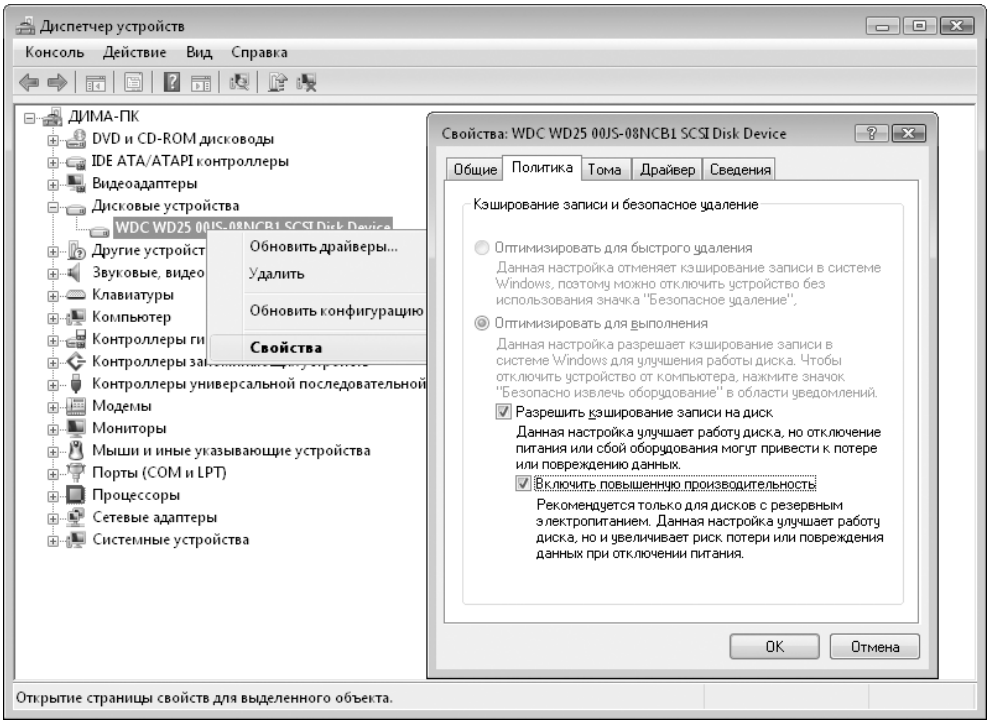


Рис. 15.4. Политика жесткого диска

будет изменить, если вы пользуетесь SCSI-дисками или некоторыми дисками Serial ATA (SATA).

Как превратить Windows XP в Windows Vista?

Интерфейс Aero

Чтобы имитировать интерфейс Aero в Windows XP, потребуется инструмент под названием Vista Customization Pack (**www.bardiyan.net**). Будьте аккуратны — перед началом эксперимента сохраните все важные данные или задайте точку восстановления системы. Учтите, что сделанные вами изменения будут проникать в систему очень глубоко. Даже после деинсталляции Vista Customization Pack нет полной уверенности, что все вернется на свои места.

Придется временно отключить брандмауэр и антивирус, чтобы не возникло проблем с установкой Vista Customization Pack. Во время инсталляции окно командной строки отображает названия изменяемых файлов. Затем компьютер автоматически перезагружается.

После этого вы можете приступать к изменению фонового изображения и окон. Щелкните правой кнопкой мыши на **Рабочем столе** и выберите **Свойства**. В появившемся окне на вкладке **Рабочий стол** нажмите кнопку **Обзор** и перейдите в каталог **Customization Pack**. Там вы найдете фоновый рисунок **Bliss5259**. Теперь перейдите на вкладку **Заставка** и выберите **aurora_5xxx**. Увидеть заставку в окне предварительного просмотра можно с помощью бесплатного кодека XviD, который можно отыскать на сайте **www.free-codecs.com**. Теперь на вкладке **Оформление** выберите тему под названием **Aero Style Vista** и, нажав кнопку **Применить**, активируйте новый интерфейс.

Панель задач и окна

Для внесения изменений в **Панель задач**, стартовое меню и шрифт понадобится инструмент Vista Visual Styles Pack (**www.bardiyan.net** или **www.tcmagazine.info/modules.php?modid=4&action=show&id=413**). Он содержит эффекты и подсветки для темной **Панели задач**, улучшенное отображение окон и новый шрифт Vista, который называется Segoe.

Распакуйте ZIP-архив и запустите программу. Затем откройте **Панель управления ▸ Экран**. На вкладке **Оформление** выберите **Aero Style Vista**. Шрифт Segoe будет установлен автоматически. Для того чтобы увидеть световой эффект на **Панели задач**, нужно всего лишь провести курсором по свернутому окну. Если раньше вы работали с классическим видом меню **Пуск**, то потребуется включить его для Windows XP. Сделать это можно, щелкнув кнопкой мыши в **Панели управления** на значке **Панель задач** и меню **Пуск**.

Поиск

В Windows Vista существует такое понятие, как функция быстрого поиска. Ее довольно успешно можно имитировать в Windows XP с помощью бесплатной программы Copernic Desktop Search. При установке программы оставьте активными все настройки браузера. Таким образом, вы сможете (как и в Windows Vista) вести поиск из браузера.

Теперь вам надо заменить в меню **Пуск** обычную функцию поиска Windows на Copernic Desktop. Для этого откройте **Редактор реестра** и найдите ключ `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Создайте новый параметр типа `DWORD` с названием **NoFind** и задайте для него значение `1`. В результате стандартный поиск Windows будет удален из меню **Пуск**. Правда, результат вы увидите только после перезагрузки компьютера.

Чтобы взамен интегрировать новую функцию поиска, щелкните правой кнопкой мыши на ярлыке **Copernic Desktop** и в раскрывающемся меню выберите пункт **Свойства**. На вкладке **Ярлык** нажмите кнопку **Сменить значок**. Затем через **Найти объект** перейдите к папке `Windows\srchasst` и откройте файл с названием `srchui.dll`. Теперь выберите обычный для Windows символ поиска — лупу. Назовите получившийся ярлык **Search** и еще раз щелкните по нему правой кнопкой мыши. С помощью пункта **Добавить в меню Пуск** вы получите доступ к новой функции поиска через меню **Пуск**.

Приветствие

За внешний вид окна входа в Windows XP отвечает файл `logonui.exe`. Если заменить данный файл, можно изменить окно приветствия системы. В данном случае приведен пример подмены `logonui.exe` модифицированным файлом, предназначенным для Windows Vista.

Прежде чем использовать новый файл, необходимо деактивировать старый. Для этого откройте **Проводник** и перейдите к каталогу `Windows\System32`, переименуйте `logonui.exe` в `logonui.old`. В процессе система выдаст предупреждение об экстремальности таких действий, не обращайте на это внимания.

Измененный файл `logonui.exe` можно найти на сайте **www.bardiyan.net** в разделе **Download**. Скопируйте его в папку `Windows\System32` и перезагрузите компьютер.

Начиная с этого момента вы будете при каждой загрузке системы видеть окно приветствия Vista.

Логотип при загрузке

Замена логотипа, появляющегося при загрузке, представляет некоторую сложность, поскольку разработчики включили его в ядро операционной системы. Однако с помощью программы Resource Hacker можно извлечь стартовую картинку из системных файлов и заменить ее другой.

Для начала подстрахуйтесь и сделайте резервную копию ядра системы, в которое вы впоследствии будете вмешиваться. Для этого разыщите в каталоге `Windows\System32` файл `ntoskrnl.exe`, скопируйте его в этот же каталог под именем `vistaoskrnl.exe`. Теперь вам понадобится загрузочный логотип, на который вы желаете поменять стандартную загрузочную картинку для Windows XP. Разыскать нужный вы сможете на сайте **www.vistaultimate.com**.

Запустите Resource Hacker и откройте (**File ▸ Open**) в ней файл `vistaoskrnl.exe`. Выберите **Action ▸ Replace Bitmap** и с помощью кнопки **Open file with new bitmap** скачайте из Интернета загрузочный логотип Windows Vista. Нажмите кнопку **Replace** и сохраните измененный файл ядра. Осталось только отредактировать файл `boot.ini`, чтобы получить возможность использовать вместо файла ядра по умолчанию файл `vistaoskrnl.exe`.

Для редактирования `boot.ini` следует совершить следующие действия. Щелкните правой кнопкой мыши на значке **Мой компьютер** и в раскрывающемся списке выберите **Свойства**. На вкладке **Дополнительно** в разделе **Загрузка и восстановление** перейдите к пункту **Параметры**. После нажатия кнопки **Правка** в **Блокноте** откроется файл `boot.ini`. Скопируйте стартовую строку и в конце добавьте параметр `/kernel=vistaoskrnl.exe`. Теперь при загрузке компьютера у вас будет появляться меню, в котором можно будет выбрать, с каким ядром (а значит, и стартовой картинкой) вы желаете загружаться. При выборе второго пункта должен появиться логотип Windows Vista.

Проводник

Интегрировать новые кнопки из Windows Vista в Windows XP можно, отправившись по адресу **www.themexp.org** и через ссылку **Explorer Bar Icons** скачав коллекцию WinVista. Она представляет собой самораспаковывающийся архив, который преобразуется в обычный ZIP, после того как вы установите идущие в комплекте две рекламные программы. Теперь вам потребуется бесплатная версия программы StyleXP. Как только вы ее запустите, выберите **Explorer Bar** и подтвердите свой выбор нажатием кнопки **OK**. Через **Add an Explorer Bar Set** загрузите ZIP-файл, который вы недавно скачали, и перезагрузите компьютер. В **Проводнике** появятся новые кнопки.

ПРИМЕЧАНИЕ

Кстати, рекламные программы, которые вам пришлось установить, легко удаляются утилитой Ad-Adware.

Объемное переключение

Бесплатная программа Top Desk поможет пользователям Windows XP создать объемный интерфейс при переключении между окнами запущенных приложений. Обладателям Vista данная возможность известна как Flip 3D.

После установки Top Desk на **Панели задач** появится новый значок. Для получения объемного эффекта откройте несколько окон и нажмите сочетание клавиш **Alt+Tab**.

Боковая панель

Боковая панель — одно из самых заметных нововведений в Windows Vista. Этот элемент может появиться на вашем **Рабочем столе** благодаря программе Desktop Sidebar, которую вы можете скачать с сайта **www.bardiyan.net**.

После установки запустите ее. Поначалу панель все еще будет иметь дизайн Windows XP. Щелкните правой кнопкой мыши по свободному месту на ней и в раскрывающемся списке выберите пункт **Настройки программы**. Далее на вкладке **Появление** выберите пункт **Download more skins** и на открывшейся интернет-странице перейдите в низ окна. Загрузите интерфейс Aero, тогда оформление панели будет соответствовать дизайну Windows Vista.

Защита от шпионов

Как известно, от вирусов Windows Vista защищается с помощью утилиты Windows Defender. Но «защитник» доступен не только обладателям Vista, пользователи лицензионных версий Windows XP также могут воспользоваться данной утилитой (**www.microsoft.com**).

Internet Explorer 7

Вы сможете найти версию Internet Explorer 7.0 для Windows XP на сайте **www.microsoft.com**. В качестве альтернативы можно попробовать браузер Firefox с темой Longfiber (**www.lynchknot.com**), который весьма удачно гармонирует по цвету с боковой панелью и панелью задач Vista. Выберите в браузере **Extras ▸ Themes** и перетащите файл **Longfiber.jar** в открывшееся окно, чтобы установить тему в Firefox. Затем активируйте тему. Firefox готов к работе.