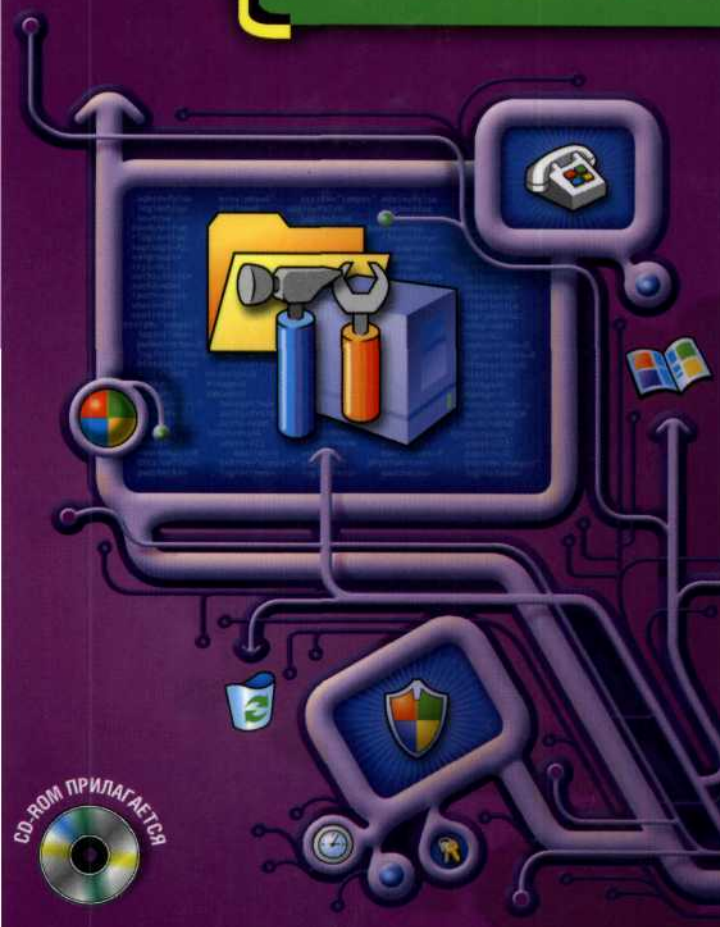
Сергей Бормотов

Системное администрирование

на 100 %



Овладейте на 100 %:

- конфигурированием сетей
- настройкой реестра Windows XP
- способами защиты информации
- методиками повышения надежности и быстродействия сети

CD-ROM ПРИЛАГАЕТСЯ

ПИТЕР®

Сергей Бормотов

Системное администрирование

на 100 %

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Новосибирск · Ростов-на-Дону · Екатеринбург · Самара
Киев · Харьков · Минск
2006

Сергей Витальевич Бормотов

Системное администрирование на 100 % (+CD)

Заведующий редакцией	*Д. Гурский*
Руководитель проекта	*Е. Каляева*
Литературные редакторы	*А. Алехна, Н. Гринчик*
Художник	*А. Татарко*
Корректоры	*Т. Курьянович, Т. Лаврович*
Верстка	*Г. Блинов, В. Поживилко*

ББК 32.988.02
УДК 004.45

Бормотов С. В.

Б82 Системное администрирование на 100 % (+CD). — СПб.: Питер, 2006. — 256 с.: ил.

ISBN 5-469-01220-4

В книге детально рассмотрены практические задачи, с которыми ежедневно сталкивается системный администратор: от настройки сети, организации антивирусной защиты и обновления системы до защиты информации. Основной упор сделан на решение практических задач, однако приводятся и необходимые теоретические сведения для понимания вопроса.

© ЗАО Издательский дом «Питер», 2006

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 5-469-01220-4

ООО «Питер Принт». 194044, Санкт-Петербург, Б. Сампсониевский пр., 29а.

Лицензия ИД № 05784 от 07.09.01.

Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2; 953005 — литература учебная.

Подписано в печать 28.09.05. Формат 70×100$^{1}/_{16}$. Усл. п. л. 20,64. Тираж 3500 экз. Заказ № 6062.

Отпечатано с диапозитивов в ФГУП «Печатный двор» им. А. М. Горького
Федерального агентства по печати и массовым коммуникациям.

197110, Санкт-Петербург, Чкаловский пр., 15.

Краткое содержание

Оглавление

Введение

Книга, которую вы держите в руках, посвящена системному администрированию локальных сетей на базе операционной системы Windows XP.

Эта книга ориентирована на системных администраторов небольших офисных или домашних локальных сетей. Как правило, сейчас в каждом офисе, где есть хотя бы два компьютера, организуется локальная сеть. После того как немного возрастет количество компьютеров в такой сети, в штате сотрудников появляется системный администратор, который призван следить за работоспособностью сети и рабочих станций.

Почему в этой книге рассматривается именно Windows XP? Потому что на сегодняшний день это самая распространенная операционная система в мире. По некоторым данным, около 60 % компьютеров на планете работают под управлением именно операционной системы Windows XP. Это объясняется легкостью в настройке, неприхотливостью в использовании и администрировании, высоким уровнем надежности и безотказности. Несмотря на то что в данной книге приведена информация для Windows XP, полученные сведения (за некоторым исключением) можно использовать для настройки и администрирования Windows 2000 и Windows Server 2003.

Что же называется системным администрированием? Это все то, что требуется для поддержки работоспособности компьютерной системы (например, создание резервных копий некоторых файлов, установка новых программ, создание и удаление учетных записей пользователей, проверка целостности файловой системы и т. д.). Если сравнивать компьютер с домом, то системное администрирование можно назвать содержанием этого дома, включающим в себя уборку, устранение различных неисправностей, проведение ремонта и т. д.

В этой книге рассмотрены все вопросы, с которыми может столкнуться системный администратор: приемы установки и настройки Windows XP, способы оптимизации ее работы, полезные приемы организации резервного копирования, работа с драйверами, организация локальной сети и т. д.

Книга написана таким образом, что главы не зависят друг от друга и могут быть рассмотрены отдельно. Например, для получения информации по организации локальной сети копий вы можете прочесть только главу 2. Это очень удобно и позволяет использовать книгу в качестве справочного пособия, а также избежать чтения всего руководства вместо нескольких разделов. Такая организация книги позволит читателю углубиться во всестороннее изучение какого-либо аспекта

Windows XP, а также быстро найти необходимую информацию, не тратя много времени на поиск и чтение.

Однако прежде всего это книга, а затем уже справочник. Если вы не считаете себя опытным системным администратором, я бы рекомендовал прочитать всю книгу. Она построена таким образом, что новые и полезные сведения из нее смогут почерпнуть как начинающие, так и опытные системные администраторы.

Первая глава содержит общие сведения о Windows XP. Кратко рассмотрены история разработки системы, а также отличия Windows XP Home Edition и Windows XP Professional. Здесь же описаны полезные приемы установки операционной системы, отличия файловых систем FAT и NTFS, особенности выбора размера кластера для файловой системы. Вместе с тем рассматриваются некоторые приемы, позволяющие уменьшить объем дискового пространства, занимаемого Windows XP.

Вторая глава целиком посвящена сетевым технологиям. В ней приведено описание всех сетевых технологий и протоколов, применяемых в локальных сетях. Отдельно рассмотрены типы применяемого сетевого оборудования и принципы прокладки и монтажа сети. В этой главе также рассмотрена настройка Windows XP для работы в локальной сети, организация общего доступа к файлам и принтерам, настройка программы Traffic Inspector для учета потребляемого трафика.

В третьей главе рассказывается о средствах администрирования Windows. Прочитав ее, вы узнаете, какое программное обеспечение используется для системного администрирования, познакомитесь со службами Windows XP, изучите системный реестр, научитесь пользоваться консолью восстановления системы. Кроме того, в этой главе рассматриваются приемы настройки Windows XP для работы с максимальной производительностью.

Четвертая глава посвящена полезным приемам системного администрирования. В ней рассмотрены приемы работы с драйверами (создание резервных копий драйверов системы, корректное удаление), организация автоматической установки и клонирования Windows. Вы сможете изучить принципы работы с программой Acronis TrueImage, позволяющей создавать резервные копии целых дисковых разделов. Кроме того, вы познакомитесь с программой Remote Administrator, позволяющей удаленно администрировать локальную сеть, не вставая с любимого кресла. Я думаю, многих заинтересует технология смены ядра операционной системы. Она позволяет клонировать Windows на компьютеры с отличающимся аппаратным обеспечением.

Прочитав пятую главу, вы узнаете, как защищать информацию в вашей сети. Рассмотрены приемы организации антивирусной защиты рабочих станций сети, установки и настройки межсетевого экрана (брандмауэра). Кроме того, в этой главе рассказывается, как проверить защищенность вашей сети, а также как зашифровать важные данные средствами операционной системы и дополнительного программного обеспечения.

В шестой главе рассмотрено, как сделать компьютер более надежным и быстрым. Прочитав ее, вы узнаете, как предотвратить системные сбои, научитесь тестировать систему и организовывать дисковый массив RAID.

В последней, седьмой, главе описываются программы для создания виртуальных машин. Рассмотрено, для каких задач в области системного администрирования могут использоваться виртуальные машины, технология их создания, настройки и использования с помощью программ VMware и VirtualPC. Кроме того, вы научитесь подключать виртуальные машины к локальной сети.

Отдельно следует сказать о компакт-диске, который вы получили вместе с этой книгой. На нем находятся все программы, упомянутые в книге. Программное обеспечение располагается в папках, рассортированных по главам. Например, чтобы найти программное обеспечение, рассматриваемое в третьей главе, нужно открыть папку ch03 на компакт-диске.

Кроме того, в папке utils на компакт-диске расположены утилиты и программы, полезные системному администратору, описание которых не вошло в эту книгу. Полное содержание компакт-диска приведено в приложении.

Итак, настало время перевернуть страницу и углубиться в чтение. Я надеюсь, что эта книга поможет вам в нелегком деле системного администрирования и что с ее помощью вы узнаете что-то новое и полезное.

Благодарности

Хочу поблагодарить сотрудников издательства, благодаря которым данная книга увидела свет. Огромное спасибо за предложение написать эту книгу, а также за советы относительно ее содержания.

Особая благодарность родным за терпение, проявленное во время моей работы над книгой.

И, конечно же, я благодарю всех, кто купил эту книгу.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты gurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

ГЛАВА 1 С чего начинается Windows?

- Краткий экскурс в историю Windows XP
- Особенности Windows XP
- Четыре способа установки Windows XP
- Файловая система: FAT или NTFS?
- Разберемся с кластерами
- Как уменьшить объем только что инсталлированной Windows XP

В этой главе мы познакомимся с историей операционной системы Windows, рассмотрим особенности работы с Windows XP. Здесь рассмотрены различные приемы установки операционной системы, особенности и недостатки различных файловых систем. Кроме того, вы узнаете, как уменьшить объем, занимаемый системой Windows XP на жестком диске.

Краткий экскурс в историю Windows XP

Первая версия Windows появилась в 1985 году. На тот момент она представляла собой всего лишь набор утилит, которые расширяли возможности очень распространенной в то время операционной системы MS-DOS.

Спустя некоторое время вышла система Windows 2.0, но, точно так же, как и Windows 1.0, она не стала популярной. В 1990 году Microsoft предприняла еще одну попытку завоевать компьютерный рынок: была выпущена операционная система Windows 3.0, которую стали активно использовать на многих компьютерах.

Популярность новой версии Windows легко объяснить, если внимательнее присмотреться к ее особенностям. Графический интерфейс дает возможность работать с компьютером не только с помощью текстовых команд, использующихся в MS-DOS, но также выполняя простые и понятные действия с меню и значками. Поддержка многозадачности значительно повысила эффективность и скорость работы. Кроме того, легкость написания приложений для Windows привела к появлению разнообразных программ, которые работали в среде этой операционной системы. Следующие версии Windows были направлены на повышение стабильности и надежности работы системы, а также на поддержку разнообразных мультимедийных устройств (версия 3.1) и работу в локальной сети (версия 3.11).

В 1988 году компания Microsoft начала работу над своей очередной операционной системой, которая получила название Windows NT. С самого начала эта операционная система разрабатывалась как серверная, поэтому ее задачей было существенное повышение надежности и эффективная поддержка сетевой работы. Интерфейс Windows NT не должен был существенно отличаться от интерфейса Windows 3.0. В 1992 году увидела свет Windows NT 3.0, а через год — Windows NT 3.5.

В 1995 году была выпущена радикально новая по тем временам операционная система Windows 95. В этой версии был значительно переработан графический интерфейс, выросла скорость работы приложений. Одной из главных возможностей Windows 95 стала автоматическая установка и настройка устройств и оборудования компьютера для работы без конфликтов. Еще одной существенной особенностью новой системы стала возможность работы с локальной сетью и Интернетом без необходимости установки дополнительных утилит и сетевых протоколов.

Интерфейс Windows 95 стал очень популярным и надолго обосновался в семействе Windows. В 1996 году выходит новая версия Windows NT 4.0, которая обладает таким же интерфейсом, как и Windows 95. На тот момент Windows NT 4.0 стала самой удачной серверной операционной системой, она могла работать с многопроцессорными системами и большими объемами оперативной памяти, имела серьезную защиту от атак хакеров и несанкционированного доступа. Windows NT достаточно

быстро стала основной операционной системой на множестве серверов по всему миру (на некоторых из них она установлена до сих пор). О популярности новой системы свидетельствует и тот факт, что официальная поддержка разработчиков и выпуск обновлений были прекращены лишь в 2004 году.

В 1998 году вышла Windows 98, которая стала продолжением легендарной Windows 95. Структура и состав новой операционной системы были значительно улучшены по сравнению с ее предшественницей. Было исправлено множество ошибок, упрощена работа с локальной сетью и Интернетом, а также добавлена поддержка новых протоколов транспортировки данных — стандартов, которые обеспечивают обмен информацией между разными системами. Кроме того, в Windows 98 была добавлена возможность работы с несколькими мониторами одновременно.

В 2000 году были выпущены сразу две операционные системы — Windows 2000 и Windows Me (Millennium Edition — редакция тысячелетия). Windows 2000 являлась продолжением систем семейства Windows NT и унаследовала от этой серии высокую стабильность и надежность защиты данных. Эта операционная система нашла применение на серверах и рабочих компьютерах требовательных пользователей.

Windows Me была написана для выполнения задач домашних компьютеров — игр, мультимедиа и Интернета. Фундаментом новой системы стала Windows 98, однако по сравнению с ней Windows Me приобрела множество новых функций, среди которых улучшенная работа с мультимедийными данными и устройствами, средства восстановления данных после ошибок и т. д.

25 октября 2001 года Microsoft выпустила новую операционною систему — Windows XP, которая была призвана заменить Windows 2000 на пользовательских компьютерах. Сотрудники Microsoft расшифровывают аббревиатуру XP как «eXPerience» — опыт. Windows XP построена на основе модифицированного ядра Windows 2000 и имеет совершенно новый удобный интерфейс, получивший название «Luna». Этот интерфейс значительно упрощает работу с операционной системой и легко изменяется с помощью установки новых тем Рабочего стола.

ПРИМЕЧАНИЕ

Над созданием Windows XP работало около пяти с половиной тысяч человек. За это время было выпито более 86 тысяч чашек кофе и у группы разработчиков родилось 452 ребенка.

Windows XP — универсальная система, которая соединяет в себе преимущества серверной и пользовательской операционных систем. Она дает возможность работать в режиме терминала, поддерживает одновременную работу большого количества пользователей. С помощью программы Desktop manager данная система позволяет использовать одновременно до четырех Рабочих столов, она способна корректно работать как на серверах, так и на рабочих станциях.

Продолжением серии операционных систем Windows должна стать Windows Vista (до недавнего времени будущая операционная система имела рабочее название Longhorn).

Первоначально выпуск этой операционной системы планировался на конец 2002 или начало 2003 года. Однако планы Microsoft изменились, и теперь мы можем ожидать появления совершенно новой системы в 2005–2006 году. Значительно переработанный графический интерфейс, более высокая надежность, новая структура файловой системы (структура реляционной базы данных), значительно увеличивающая скорость поиска и повышающая производительность, — это только часть списка коренных изменений, которые разработчики обещают внести в новую операционную систему.

Особенности Windows XP

Несмотря на то что Microsoft Windows XP создана на основе Windows NT и является логическим продолжением системы Windows 2000, она содержит в себе все лучшие нововведения, включенные в Windows Me. Оставляя на высоте показатели стабильности, безопасности и быстродействия, данная система стала проще в работе, в ней появилось множество программ и утилит, предназначенных для большинства домашних пользователей.

Существует несколько вариантов поставки системы, ориентированных на разные сферы применения. Microsoft Windows XP Home Edition разработана для домашних пользователей, которые чаще всего работают с мультимедийными данными и играми. В этой версии наибольшее внимание уделено работе с изображениями, звуком и видео. Microsoft Windows XP Professional написана для профессионального использования. Данная версия чаще всего используется в организациях. Впрочем, она может управлять и домашним компьютером при условии высокой сложности выполняемых задач.

Существует также Microsoft Windows XP Server, оптимизированная для установки на сервере, который организовывает работу большого количества пользователей в локальной сети и Интернете. В книге описана основная версия операционной системы — Windows XP Professional. Windows XP Home Edition практически не отличается от нее. В табл. 1.1 сравниваются эти версии операционной системы. Характеристики взяты с официального сайта Microsoft.

Таблица 1.1. Сравнительные характеристики версий Professional и Home Edition Windows XP

Возможности и средства	Windows XP Home	Windows XP Professional
Новый графический интерфейс Luna	+	+
Надежность платформы (стабильная работа возможна даже в самых сложных условиях)	+	+
Наличие Проигрывателя Windows Media для Windows XP (полнофункционального средства, обеспечивающего поиск, воспроизведение, сортировку и хранение цифровых мультимедиаданных)	+	+

Продолжение ⇩

Таблица 1.1. Сравнительные характеристики версий Professional и Home Edition Windows XP (Продолжение)

Возможности и средства	Windows XP Home	Windows XP Professional
Мастер установки сети (возможность легко подключать и совместно использовать компьютеры и устройства, которые применяются в домашних условиях и офисе)	+	+
Windows Messenger (средство связи и совместной работы, которое поддерживает передачу моментальных сообщений, проведение голосовых и видеоконференций)	+	+
Центр справки и поддержки (способен упростить решение большинства проблем и помочь своевременно получать необходимую техническую поддержку)	+	+
Поддержка переносных компьютеров (технологии ClearType и DualView, а также усовершенствованное управление питанием компьютера)	+	+
Беспроводное подключение (автоматическая конфигурация сети с использованием стандарта 802.1x)	+	+
Удаленный доступ к компьютеру. Позволяет подключаться в удаленном режиме к компьютеру, работающему под управлением Windows XP Professional, с любого другого компьютера, работающего под управлением операционной системы Windows. Таким образом, можно работать с необходимыми приложениями и данными, находясь вне рабочего места	–	+
Автономные файлы и папки (доступ к файлам и папкам, которые хранятся на общем сетевом диске даже в то время, когда компьютер отключен от сервера)	–	+
Усовершенствованное управление электропитанием и быстрый отклик системы (эти возможности значительно ускоряют загрузку системы и переход из спящего режима в рабочий)	+	+
Многозадачность (возможность выполнять несколько приложений одновременно)	+	+
Масштабируемая поддержка процессора (вплоть до поддержки двусторонней многопроцессорной обработки)	–	+
Брандмауэр Интернет-подключений (защищает подключенный к Интернету компьютер от взлома и внешних атак)	+	+

Возможности и средства	Windows XP Home	Windows XP Professional
Технологии безопасности Internet Explorer 6 (контроль использования личных данных во время посещения интернет-сайтов)	+	+
Шифрование файловой системы (защита важной информации, которая содержится в файлах, хранящихся на диске, использующем файловую систему NTFS)	–	+
Управление доступом (запрещение доступа к выбранным файлам, программам и прочим ресурсам)	–	+
Централизованное администрирование (подключение систем, работающих под управлением Windows XP Professional, к домену Windows Server открывает доступ к разнообразным эффективным средствам управления и обеспечения безопасности)	–	+
Групповая политика (значительно упрощает управление группами пользователей и отдельных компьютеров)	–	+
Установка и поддержка программного обеспечения (автоматическая установка, настройка, удаление и восстановление приложений)	–	+
Перемещаемые профили пользователей (доступ к личным документам и настройкам вне зависимости от того, какой компьютер используется для входа в систему)	–	+
Служба удаленной установки (поддержка установки операционной системы на компьютеры с помощью сервера, к которому они подключены)	–	+
Отображение текста на большинстве языков мира (технология Single Worldwide Binary)	+	+
Многоязычный пользовательский интерфейс (возможность смены языка интерфейса, чтобы работать с локализованными меню и диалогами, справкой, словарями, средствами проверки правописания и т. д.)	–	+

Для комфортной работы с операционной системой Windows XP потребуется достаточно мощный компьютер. В системе должно быть установлено не менее 128 Мбайт оперативной памяти (для более быстрой работы необходимо иметь 256 Мбайт и более). Минимальная тактовая частота процессора — 233 МГц, однако для полноценной работы потребуется процессор с тактовой частотой не менее 400 МГц. Жесткий диск должен иметь достаточный объем, чтобы вместить не только файлы

операционной системы и временные файлы, но и дополнительные программы (например, Microsoft Office). Понадобится винчестер размером не менее 3 Гбайт, однако практика показывает, что и 10 Гбайт может оказаться недостаточно (впрочем, все зависит от того, что именно вы собираетесь хранить на своем жестком диске).

Интерфейс Windows XP сильно переработан. Кнопки, значки, панели выглядят несколько по-другому. Вместе с тем большинство элементов перекочевало из Windows 95, хоть и со значительными визуальными изменениями. У вас также имеется возможность использовать старый привычный интерфейс, если вам проще работать с ним. Следует обратить внимание на работу приложений в режиме совместимости со старыми версиями Windows. Вы можете запускать даже те программы, которые написаны для Windows 95 и не работают в Windows 2000/NT.

Сильно усовершенствованы и средства для работы с Интернетом. Переработана справочная система, улучшена система, отвечающая за безопасность во время работы в сети. Значительно изменены средства администрирования и управления работой групп пользователей в локальной сети.

В новой операционной системе имеются и другие нововведения, о которых вы сможете узнать в процессе прочтения книги и при знакомстве с Windows XP.

Четыре способа установки Windows XP

Многие опытные пользователи множество раз устанавливали и переустанавливали Windows на своих компьютерах и компьютерах своих знакомых. В этом подразделе мы рассмотрим особенности установки Windows XP, о которых не всегда знают даже опытные пользователи.

Следуют обратить внимание на то, что существует несколько вариантов установки Windows XP (а не один, как считают некоторые).

Первый способ: загрузочный диск

Чтобы начать установку операционной системы (ОС) с загрузочного диска, в BIOS необходимо установить значение параметра `First Boot Device` равным `CD-ROM`, сохранить установки, вставить компакт-диск в привод и перезагрузить компьютер. Запустится программа установки. Далее необходимо следовать инструкциям.

ПРИМЕЧАНИЕ

Описанные выше действия — единственный метод загрузить непосредственно программу-установщик, имея только компакт-диск. Компания Microsoft считает, что наличие привода компакт-дисков является неотъемлемой деталью компьютера, на который устанавливается Windows XP, поэтому официальных средств для загрузки системы с помощью системной дискеты не предусмотрено.

Второй способ: системная дискета

Если загрузка с компакт-диска по каким-то причинам невозможна, *попробуйте* загрузиться с системной дискеты MS-DOS, содержащей драйвер привода компакт-дисков. Далее запустите файл `winnt.exe` в директории `i386` с диска, на котором находится дистрибутив Windows XP. Данный файл можно запускать со следующими ключами:

- `/?` — показывает справку;
- `/a` — использует специальные средства для пользователей с ограниченными физическими возможностями;
- `/e` — задает команду, которая будет выполняться по окончании стадии установки операционной системы в графическом режиме;
- `/r` — создает папку в каталоге Windows, которая остается после окончания установки системы;
- `/rx` — создает временную папку в каталоге Windows, которая будет автоматически удалена по окончании процесса установки;
- `/s` — указывает путь к установочным файлам Windows XP; этот ключ применяется при установке с системы сервера локальной сети;
- `/t` — задает диск, на котором будут размещаться временные файлы; при отсутствии этого параметра будет использоваться диск, на котором больше всего места;
- `/u:` — файл_ответов; создает файл ответов для приложения, выполняющего инсталляцию Windows XP;
- `/udf:id[,UDF_файл]` — указывает идентификатор ID, с помощью которого программа установки Windows сможет определить значения в UDF-файле (Uniqueness Database File) для изменения файла ответов каждого компьютера при инсталляции операционной системы на несколько компьютеров; если UDF-файл не указан, то система попросит вставить дискету, на которой находится файл `$Unique$.udb`.

ПРИМЕЧАНИЕ

Если ваш винчестер подключен к внешнему контроллеру (SCSI или Serial-ATA), то вам необходимо скачать для него новый драйвер, написанный под Windows XP, и записать его на дискету. Он понадобится, если программа установки по каким-то причинам не сможет правильно определить и настроить данное устройство. В такой ситуации нужно нажать клавишу F6 во время поиска таких устройств.

Третий способ: обновление

Обновить свою текущую версию Windows до Windows XP можно, если в Windows 95/98/NT4/2000 запустить программу `setup.exe` из корневого каталога установочного компакт-диска или `winnt32.exe` из директории `i386`. Процесс

обновления проходит достаточно просто. Перед перезагрузкой операционная система выдаст список программ и драйверов, которые по каким-то причинам несовместимы с Windows XP. Можно использовать следующие параметры командной строки `winnt32.exe`.

- `/?` — справка.
- `/checkupgradeonly` — тестирует возможности обновления текущей версии Windows. После данного теста вам предложат ознакомиться с отчетом о возможности установки Windows XP.
- `/cmd:command_line` — устанавливает команду, которая должна быть выполнена в процессе последней стадии установки операционной системы.
- `/cmdcons` — инсталлирует консоль восстановления системы и добавляет ее вызов в загрузочное меню операционной системы. Windows при этом не установится.
- `/copydir:i386\folder_name` — создает дополнительную директорию с указанным именем в каталоге Windows.
- `/copysource:folder_name` — создает временную директорию в каталоге Windows, по окончании установки данная директория будет автоматически удалена.
- `/debug[level]:[filename]` — создает протокол отладки (первоначально — `C:\systemroot\Winnt32.log`) с заданным уровнем (первоначально — `2`). Возможные уровни: `0` — критические ошибки или сбои, `1` — обычные ошибки или сбои, `2` — предупреждения, `3` — информация, `4` — детальная информация, необходимая для отладки.
- `/dudisable` — запрещает производить динамическое обновление (Update Microsoft Windows). Установка произойдет с настройками, выставленными по умолчанию.
- `/duprepare:pathname` — изменяет установочный ресурс таким образом, чтобы использовать необходимые файлы обновления с сервера Windows Update.
- `/dushare:pathname` — указывает сервер, на котором расположены необходимые обновления.
- `/m:folder_name` — в процессе установки копируются файлы из дополнительно указанной папки. В случае их наличия они будут использованы вместо аналогичных файлов из директории, заданной по умолчанию.
- `/makelocalsource` — принуждает программу инсталляции скопировать все используемые файлы на локальный жесткий диск. Данный параметр используется тогда, когда компакт-диск недоступен во время установки.
- `/noreboot` — запрещает автоматический перезапуск системы по окончании копирования файлов.
- `/s:sourcepath` — задает папку, в которой размещены файлы инсталляции Windows XP (как правило, на локальном сервере).

- `/syspart:drive_letter` — копирует файлы установки Windows XP на жесткий диск, делает его активным, переносит на другой ПК и продолжает инсталляцию на этом компьютере. Данный параметр должен использоваться одновременно с параметром `/tempdrive`.
- `/tempdrive:drive_letter` — данный ключ используется вместе с ключом `/syspart` для установки основного раздела, который предназначен для размещения файлов и дальнейшей инсталляции Windows XP.
- `/udf:id [,UDB_file]` — указывает программе установки файл базы данных уникальности, изменяющий файл ответов.
- `/unattend` — обновляет текущую версию Windows в автоматическом режиме. При этом все настройки пользователя будут сохранены.
- `/unattend[num]:[answer_file]` — данный ключ следует указать в случае автоматизированной установки. Имя файла можно не указывать, если будет использоваться файл `Unattend.txt` (установлен по умолчанию).

Между тем обновление более ранней версии Windows до Windows XP не является оптимальным способом установки. Несмотря на тот факт, что Windows XP будет пытаться автоматически определить список приложений и драйверов, которые не смогут корректно работать под ее управлением, достаточно часто происходят ошибки. Во избежание проблем с совместимостью старых приложений и драйверов с новой операционной системой я рекомендую устанавливать систему заново.

Четвертый способ: установка второй ОС

В случае установки системы поверх существующей у вас появится возможность при загрузке компьютера выбирать нужную операционную систему (Dual boot).

ПРИМЕЧАНИЕ

После установки Windows XP в качестве отдельной операционной системы будет невозможна корректная работа таких приложений, как Outlook Express и Internet Explorer в Windows 95/98, так как Windows XP их заменит. Эта проблема возникает, только если обе ОС устанавливаются на один и тот же раздел жесткого диска. Данная проблема решается путем копирования некоторых DLL из папки WinXP\System32 в папку Windows\System. Чтобы определить список нужных библиотек, ознакомьтесь с тем, что показывает программа Outlook Express в окне «О программе».

Многие программы придется устанавливать по два раза: один для Windows XP и еще один для Windows 95/98. Иногда такие программы можно установить даже в один каталог (например, Office 2000 при повторной установке способен определить, что он уже был инсталлирован, и в итоге дополнительно установится всего около 18 Мбайт).

Файловая система: FAT или NTFS?

В самом начале установки Windows XP инсталлятор ОС предлагает отформатировать раздел, на который будет производиться установка, под одну из двух возможных файловых систем — FAT32 или NTFS. Ваш выбор должен зависеть прежде всего от того, сколько оперативной памяти установлено на компьютере. Обратите внимание, что NTFS работает медленнее, чем FAT, из-за дополнительно загружаемых сервисов и ее мощной системы безопасности. NTFS следует ставить, только если у вас минимум 128 Мбайт оперативной памяти. Необходимо взвесить преимущества и недостатки данной файловой системы и решить, что именно вам необходимо.

Одним из главных преимуществ FAT32 является то, что эта файловая система работает быстрее и требует меньше ресурсов для нормальной работы. Если ваш компьютер работает только с FAT32, то в память не загружаются дополнительные драйверы и сервисы, которые необходимы для работы NTFS. К тому же при использовании FAT32 возможен доступ к жесткому диску при загрузке с помощью специальной загрузочной дискеты Windows 95/98.

Главное преимущество NTFS — надежность и сохранение целостности файловой системы. Эту файловую систему повредить чрезвычайно сложно, однако возможно. В ходе проверки надежности NTFS запускалось множество различных программ, и в самые неподходящие моменты система принудительно перезагружалась с помощью кнопки Reset. Повторение этого эксперимента более десяти раз системе не повредило, и она продолжала работать без ошибок. Следует обратить внимание и на то, что NTFS имеет внутренние средства шифрования файлов, что обеспечивает уверенность в сохранности данных.

NTFS является продолжением файловой системы HPFS, совместной разработки IBM и Microsoft для проекта OS/2. Эта операционная система должна была стать конкурентом серверам на базе NetWare и UNIX, поэтому NTFS использовала все новейшие технологические разработки того времени. Файловая система NTFS имеет очень много возможностей.

Существует возможность работы с дисками большого объема. Размер кластера NTFS составляет 512 байт, однако его можно изменить вплоть до 64 Кбайт. Важно и то, что NTFS способна работать с томами, размер которых приближается к 17 Тбайт (16 777 216 Тбайт).

NTFS включает в себя две копии аналога таблицы размещения файлов (FAT), которые носят название MFT (Master File Table). В отличие от FAT MS-DOS, MFT скорее похож на таблицу из базы данных. Если оригинальный MFT будет поврежден в случае аппаратной ошибки (например, появления сбойного сектора), то система будет использовать его копию и автоматически создаст новый оригинал, однако с учетом всех повреждений. NTFS использует целую систему транзакций в процессе записи файлов на жесткий диск. Данная система пришла из системы управления базами данных (СУБД), где принцип защиты целостности данных является одним из главных приоритетов. В упрощенном виде она работает следующим образом.

1. Драйвер ввода/вывода NTFS инициирует процесс записи, при этом отдавая команду сервису Log File Service вести лог всего, что происходит (лог — специальный системный файл, в который автоматически пишется различная системная информация, он подобен «черному ящику» в самолете. В случае аварий или сбоев системы анализ логов позволяет выявить причину сбоев).
2. Данные записываются в кэш, который находится под управлением специального сервиса — Cache Manager.
3. Cache Manager посылает информацию Virtual Memory Manager (менеджеру виртуальной памяти) для записи на жесткий диск в фоновом режиме.
4. Virtual Memory Manager отправляет информацию драйверу жесткого диска, предварительно пропустив ее через драйвер Fault Tolerant (если у вас присутствует массив дисков RAID).
5. Драйвер жесткого диска передает данные контроллеру, который уже пишет их либо в кэш, либо непосредственно на жесткий диск.
6. Если данная операция проходит без сбоев, соответствующая запись лога будет удалена.
7. Если происходит ошибка, запись лога остается в таблице транзакций, и при любом следующем доступе к жесткому диску Log File Service обнаружит эту запись и восстановит все до состояния, которое было до операции.

Данная последовательность действий гарантирует полную сохранность информации в процессе копирования, перемещения и удаления файлов или папок. В случае внесения изменений в файл вы потеряете лишь те изменения, которые находились в момент сбоя в памяти или в кэше контроллера и не были записаны на жесткий диск.

NTFS рассматривает все файлы как отдельные объекты. Каждый файловый объект имеет свои свойства, такие как имя, дата создания, дата последнего обновления, архивный статус, а также дескриптор безопасности. Любой файловый объект содержит набор методов, которые дают возможность с ним работать: open, close, read и write. Для обращения к файлу пользователи, в том числе и работающие по локальной сети, могут вызывать все эти методы, а служба Security Reference Monitor определяет, имеет ли конкретный пользователь права, необходимые для вызова какого-либо из перечисленных методов.

Более того, файлы можно шифровать. Данная функция очень полезна, однако с шифрованием файлов нужно быть предельно осторожным. Если по каким-то причинам у вас перестанет работать система и вы ее переустановите, то прочитать зашифрованные файлы впоследствии не получится.

NTFS позволяет сжимать произвольные папки и файлы (в этом и состоит его отличие от DriveSpace в Windows 95/98, который мог сжать только целый раздел). Это достаточно удобно, так как у вас появляется возможность сжимать «на лету» файлы большого размера, причем для пользователя все это будет выполняться прозрачно (в фоновом режиме).

NTFS поддерживает формат ISO Unicode. Данный формат использует 16 бит для кодировки каждого символа (ASCII, например, использовал 8 или 7 бит). В конечном итоге это означает то, что теперь пользователь может называть файлы на любом доступном языке, и система будет работать с этими файлами, не требуя изменения кодовой страницы.

СОВЕТ

Чтобы преобразовать файловую систему из FAT (FAT32) в NTFS, можно использовать утилиту Convert, которая входит в состав Windows XP. Синтаксис использования данной команды следующий:

CONVERT *том*: /FS:NTFS [/V] [/CvtArea:*имя_файла*] [/NoSecurity] [/X],

где *том* определяет букву логического диска, точку подключения или конкретное имя тома; /FS:NTFS — файловая система, в которую производится преобразование: NTFS; /V — включение функции отображения сообщений; /Cvtarea:*имя_файла* — непрерывный файл, который создается в корневой директории для сохранения места, предназначенного для системных файлов NTFS; /NoSecurity — все параметры безопасности для файлов и папок, которые преобразуются, будут доступны для редактирования любому пользователю; /X — принудительное отключение данного тома (если он был подключен). Любой открытый дескриптор этого тома станет недоступным.

Разберемся с кластерами

Большинство показателей файловой системы (в частности, скорость ее работы) во многом определяет размер кластера. Кластер — наименьший объем места на жестком диске, который может быть предоставлен файловой системой для хранения одного файла. В большинстве случаев он определяется автоматически в процессе форматировании винчестера (зависимость указана в табл. 1.2).

Таблица 1.2. Размеры кластеров

Размер раздела	*Секторов в разделе*	*Размер кластера*
<512 Мбайт	1	512 байт
<1024 Мбайт	2	1 Кбайт
<2048 Мбайт	4	2 Кбайт
<4096 Мбайт	8	4 Кбайт
<8192 Мбайт	16	8 Кбайт
<16 384 Мбайт	32	16 Кбайт
<32 768 Мбайт	64	32 Кбайт
>32 768 Мбайт	128	64 Кбайт

Существует только одно исключение из правил для системного раздела: если данный раздел меньше 2048 Мбайт, то размер кластера при использовании NTFS всегда будет составлять 512 байт. Кроме того, в процессе трансформации раздела FAT32 в NTFS утилитой `convert`, входящей в состав Windows XP, размер кластера всегда будет составлять 512 байт. Чтобы этого избежать, придется воспользоваться услугами внешних программ, например Partition Magic.

Существует несколько способов, позволяющих узнать размер кластера в Windows XP. Во-первых, можно зайти в Панель управления ▸ Администрирование ▸ Управление компьютером ▸ Запоминающие устройства ▸ Дефрагментация диска. В этом окне необходимо выбрать нужный диск и нажать кнопку Анализ. Через несколько секунд появится таблица, внизу которой находятся три кнопки. Нажатие кнопки Вывести отчет отобразит окно, в котором содержится множество полезной информации о выбранном диске, в том числе и о размере кластера (рис. 1.1).

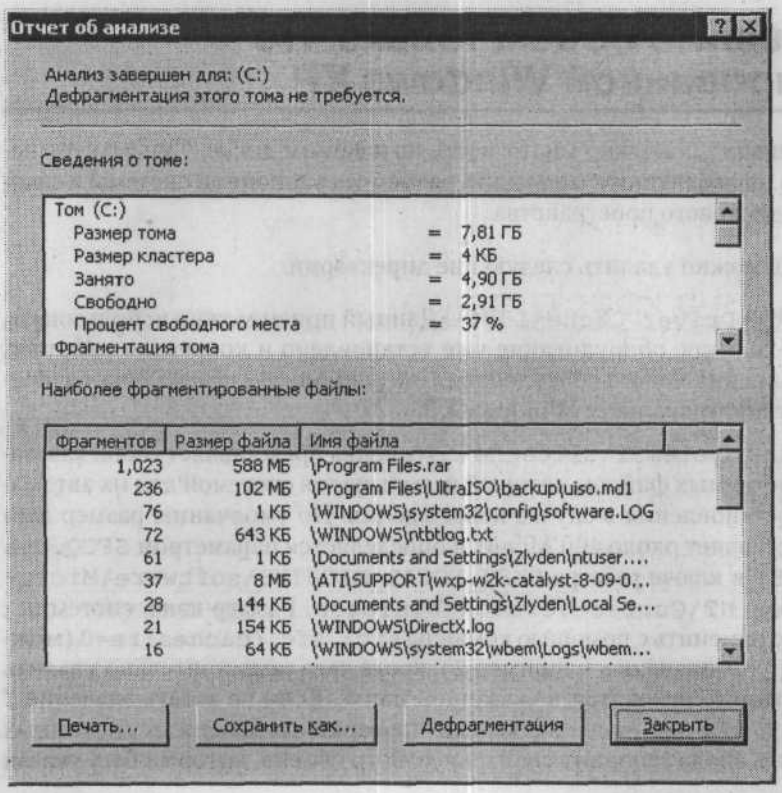


Рис. 1.1. Отчет об анализе диска

Существует еще один метод, который подойдет не только для Windows XP. Необходимо создать или взять готовый файл, размеры которого составляют от 1 байт до 500 байт. Нажатием правой кнопки мыши вызывается контекстное меню, где нужно выбрать пункт Свойства. Нам понадобится информация, которая содержится

в пунктах Размер и На диске. Размер должен быть чем-то вроде 10 байт (реальный размер файла), а На диске будет, например, 4096 байт, что соответствует размеру кластера, то есть 4 Кбайт. Размер кластера можно выбрать и самому, вручную, правда, только при форматировании. Это делается так:

```
format d: /A:size,
```

где `size` — это размер кластера в байтах.

Существуют некоторые правила, которых следует придерживаться: размер кластера должен быть кратным размеру физического сектора (в большинстве случаев 512 байт); есть ограничения по количеству кластеров в разделе. Следует учитывать и то, что если кластер будет больше 4 Кбайт, то в разделе, использующем NTFS, не будут работать функции сжатия, которые интегрированы с файловой системой.

Как уменьшить объем только что инсталлированной Windows XP

Windows XP занимает довольно много места на жестком диске. Существует несколько приемов, позволяющих уменьшить размер операционной системы и сэкономить немного дискового пространства.

В первую очередь можно удалить следующие директории.

- `%SystemRoot%\Driver Cache\i386\`. Данный прием можно использовать, если все необходимое оборудование уже установлено и корректно работает. В случае добавления нового оборудования операционная система будет запрашивать диск с дистрибутивом Windows XP.
- `%SystemRoot%\system32\dllcache\`. Эта папка представляет собой кэш защищенных системных файлов, который используется системой для их автоматического восстановления в случае повреждения. По умолчанию размер данной папки составляет около 400 Мбайт и определяется параметром `SFCQuota (0xFFFFFFFF)` в ключе реестра `HKEY_LOCAL_MACHINE\software\Microsoft\Windows NT\CurrentVersion\Winlogon`. Размер кэша системных файлов можно изменить с помощью команды `sfc: sfc /cachesize=0` (можно ввести и другое значение, например 2), после чего самостоятельно удалить все файлы, которые находятся в указанной папке. Если не задать значение `/cachesize=0`, то в процессе следующей проверки защищенных системных файлов система снова заполнит свой кэш до того объема, который был указан ранее.

Кроме того, существует возможность отключения службы System Restore. Это можно сделать, выполнив команду Мой компьютер ▸ Свойства ▸ Восстановление системы ▸ Отключить восстановление системы на всех дисках. Такими действиями вы сотрете все данные, которые занесены в System Restore и хранятся в System Volume Information (рис 1.2).

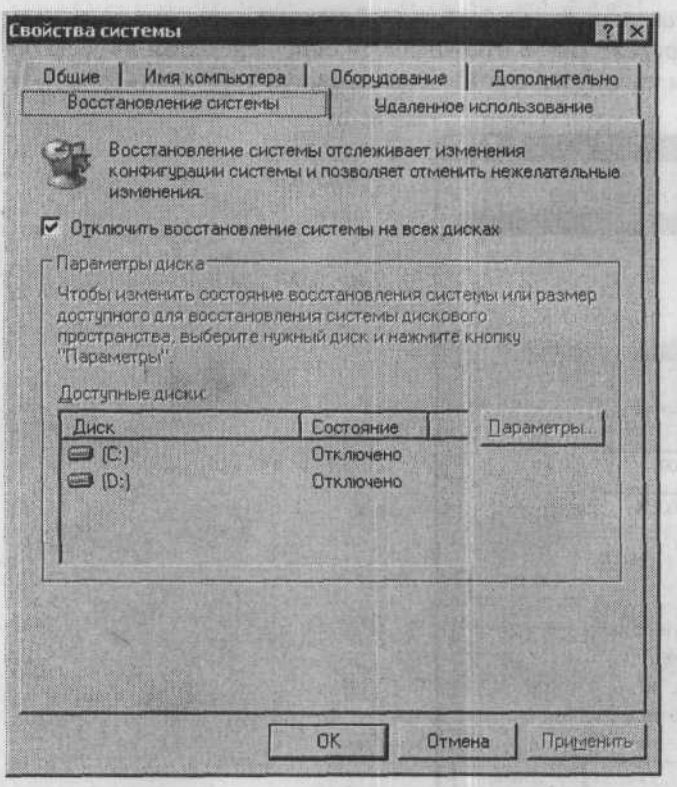


Рис. 1.2. Отключаем восстановление системы

Если вы не используете технологию Hibernate, то ее можно отключить, освободив тем самым немного места на жестком диске. Данная технология позволяет быстро выключать и включать ваш компьютер с сохранением всего, что содержится в оперативной памяти, в виде отдельного файла на жестком диске. При использовании Hibernate в корне системного диска всегда находится файл, который называется `hiberfil.sys` и имеет объем, равный оперативной памяти. Стирать его самостоятельно не имеет смысла по нескольким причинам: во-первых, это можно сделать только под другой ОС, а во-вторых, при повторной загрузке данный файл будет создан снова, даже если компьютер не переходил в «спящий» режим. Это сделано для того, чтобы на жестком диске всегда было достаточно места для сохранения информации из оперативной памяти. Чтобы удалить этот файл совсем, нужно отключить Hibernate, выполнив команду Панель управления ▸ Электропитание ▸ Спящий режим и сняв флажок Разрешить использование спящего режима.

Кроме того, можно уменьшить размер файла подкачки. По умолчанию Windows XP создает файл подкачки, размер которого в полтора раза превышает объем оперативной памяти. Учитывая современные объемы оперативной памяти, которые даже на домашних компьютерах могут превышать 1 Гбайт, можно сделать вывод, что размер файла подкачки, который Windows XP выставит для такого компьютера по умолчанию, большинству пользователей не нужен. Размер файла подкачки

можно изменить в окне Мой компьютер ▸ Свойства ▸ Дополнительные, нажав кнопку Параметры в области Быстродействие. В открывшемся окне переходим на вкладку Дополнительно и нажимаем кнопку Изменить в области Виртуальная память (рис. 1.3).

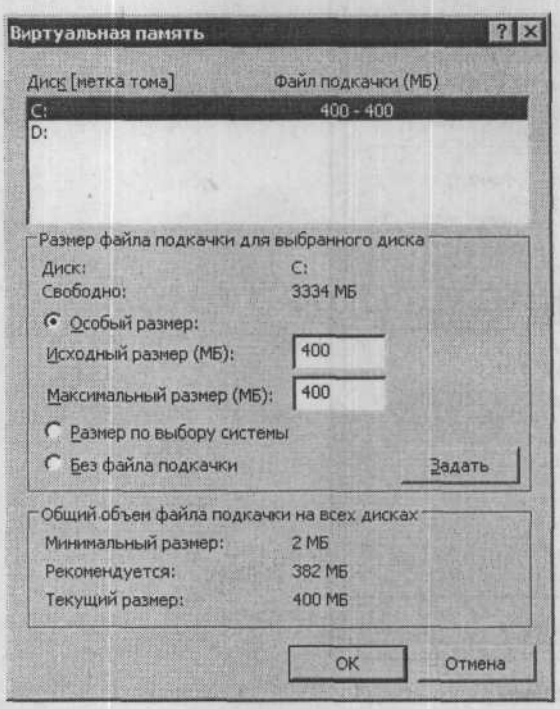


Рис. 1.3. Окно управления файлом подкачки

В окне, которое при этом откроется, следует выбрать диск или раздел, на котором требуется изменить размер файла подкачки, ввести требуемые значения и нажать кнопку Задать. После проделанных действий необходимо лишь перезагрузить компьютер.

ГЛАВА 2 Секреты локальной сети

- Какими бывают сети
- Как устроена сеть
- «Железо» для сети
- Искусство плетения сетевой паутины
- Совершенствуем сеть: модель OSI
- TCP/IP: протоколы бывают не только в милиции
- Погружаемся в Ethernet
- Не запутайся в кабелях!
- Если что-то не работает...
- Готовим систему для работы в локальной сети
- Сосчитаем каждый байт
- Война со спамом

В этой главе рассмотрим основные принципы организации локальных сетей, познакомимся с распространенными технологиями локальных сетей, подробно остановившись на самой известной — Ethernet. Вы узнаете, чем различаются марки сетевого кабеля, и научитесь выбирать сетевое оборудование. Кроме того, в данной главе рассказывается, как настроить Windows XP для работы в локальной сети и наладить учет трафика пользователей, работающих в Интернете.

Какими бывают сети

Сеть — группа компьютеров, соединенных друг с другом с помощью специального оборудования, обеспечивающего обмен информацией между ними. Соединение между двумя компьютерами может быть непосредственным (двухточечное соединение) или с использованием дополнительных узлов связи.

В дальнейшем компьютер, который подключен к сети, называется рабочей станцией (Workstation). Как правило, с этим компьютером работает человек. В сети присутствуют и такие компьютеры, на которых никто не работает. Они используются в качестве управляющих центров в сети и как накопители информации. Такие компьютеры называют серверами.

Если компьютеры расположены сравнительно недалеко друг от друга и соединены с помощью высокоскоростных сетевых адаптеров (скорость передачи данных — 10–100 Мбит/с), то такие сети называются локальными. При использовании локальной сети компьютеры, как правило, расположены в пределах одной комнаты, здания или в нескольких близко расположенных домах.

Для объединения компьютеров или целых локальных сетей, которые расположены на значительном расстоянии друг от друга, используются модемы, а также выделенные или спутниковые каналы связи. Такие сети носят название глобальных. Обычно скорость передачи данных в таких сетях значительно ниже, чем в локальных.

Как устроена сеть

Существуют два вида архитектуры сети: одноранговая (Peer-to-peer) и клиент/сервер (Client/Server). На данный момент архитектура клиент/сервер практически вытеснила одноранговую.

Если используется одноранговая сеть, то все компьютеры, входящие в нее, имеют одинаковые права. Соответственно, любой компьютер может выступать в роли сервера, предоставляющего доступ к своим ресурсам, или клиента, использующего ресурсы других серверов.

В сети, построенной на архитектуре клиент/сервер, существует несколько основных компьютеров — серверов. Остальные компьютеры, которые входят в сеть, носят название клиентов, или рабочих станций.

Сервер — это компьютер, который обслуживает другие компьютеры в сети. Существуют разнообразные виды серверов, отличающиеся друг от друга услугами, ко-

торые они предоставляют: серверы баз данных, файловые серверы, принт-серверы, почтовые серверы, веб-серверы и т. д.

Одноранговая архитектура получила распространение в небольших офисах или в домашних локальных сетях. В большинстве случаев, чтобы создать такую сеть, вам понадобится пара компьютеров, которые снабжены сетевыми картами, и кабель. В качестве кабеля используют витую пару четвертой или пятой категории. Витая пара получила такое название потому, что пары проводов внутри кабеля перекручены (это позволяет избежать помех и внешнего влияния). Все еще можно встретить достаточно старые сети, которые используют коаксиальный кабель. Такие сети морально устарели, а скорость передачи информации в них не превышает 10 Мбит/с.

После того как сеть будет создана, а компьютеры соединены между собой, нужно настроить все необходимые параметры программно. Прежде всего убедитесь, что на соединяемых компьютерах были установлены операционные системы с поддержкой работы в сети (Linux, FreeBSD, Windows NT, Windows XP) или системы с поддержкой сетевых функций (Windows 95, Windows for Workgroups).

Все компьютеры в одноранговой сети объединяются в рабочие группы, которые имеют свои имена (идентификаторы).

В случае использования архитектуры сети клиент/сервер управление доступом осуществляется на уровне пользователей. У администратора появляется возможность разрешить доступ к ресурсу только некоторым пользователям. Предположим, что вы делаете свой принтер доступным для пользователей сети. Если вы не хотите, чтобы кто угодно печатал на вашем принтере, то следует установить пароль для работы с этим ресурсом. При одноранговой сети любой пользователь, который узнает ваш пароль, сможет получить доступ к вашему принтеру. В сети клиент/сервер вы можете ограничить использование принтера для некоторых пользователей вне зависимости от того, знают они пароль или нет.

Чтобы получить доступ к ресурсу в локальной сети, построенной на архитектуре клиент/сервер, пользователь обязан ввести имя пользователя (Login — логин) и пароль (Password). Следует отметить, что имя пользователя является открытой информацией (например, вам обязательно нужно знать имя пользователя, чтобы отправить ему электронное письмо), а пароль — конфиденциальной.

Процесс проверки имени пользователя называется идентификацией. Процесс проверки соответствия введенного пароля имени пользователя — аутентификацией. Вместе идентификация и аутентификация составляют процесс авторизации. Часто термин «аутентификация» используется в широком смысле: для обозначения проверки подлинности.

Из всего сказанного можно сделать вывод о том, что единственное преимущество одноранговой архитектуры — это ее простота и невысокая стоимость. Сети клиент/сервер обеспечивают более высокий уровень быстродействия и защиты.

Архитектура клиент/сервер предусматривает использование одного или нескольких серверов. В зависимости от предоставляемых услуг существуют различные виды серверов: серверы печати, баз данных, почтовые, веб-серверы и т. п.

Достаточно часто один и тот же сервер может выполнять функции нескольких серверов, например файлового и веб-сервера. Естественно, общее количество функций, которые будет выполнять сервер, зависит от нагрузки и его возможностей. Чем выше мощность сервера, тем больше клиентов он сможет обслужить и тем большее количество услуг предоставить. Поэтому в качестве сервера практически всегда назначают мощный компьютер с большим объемом памяти и быстрым процессором (как правило, для решения серьезных задач используются многопроцессорные системы).

«Железо» для сети

В самом простом случае для работы сети достаточно сетевых карт и кабеля. Если же вам необходимо создать достаточно сложную сеть, то понадобится специальное сетевое оборудование.

Кабель

Компьютеры внутри локальной сети соединяются с помощью кабелей, которые передают сигналы. Кабель, соединяющий два компонента сети (например, два компьютера), называется сегментом. Кабели классифицируются в зависимости от возможных значений скорости передачи информации и частоты возникновения сбоев и ошибок. Наиболее часто используются кабели трех основных категорий:

- витая пара;
- коаксиальный кабель;
- оптоволоконный кабель.

Для построения локальных сетей сейчас наиболее широко используется витая пара. Внутри такой кабель состоит из двух или четырех пар медного провода, перекрученных между собой. Витая пара также имеет свои разновидности: UTP (Unshielded Twisted Pair — неэкранированная витая пара) и STP (Shielded Twisted Pair — экранированная витая пара). Эти разновидности кабеля способны передавать сигналы на расстояние порядка 100 м. Как правило, в локальных сетях используется именно UTP. STP имеет плетеную оболочку из медной нити, которая имеет более высокий уровень защиты и качества, чем оболочка кабеля UTP.

В кабеле STP каждая пара проводов дополнительно экранирована (она обернута слоем фольги), что защищает данные, которые передаются, от внешних помех. Такое решение позволяет поддерживать высокие скорости передачи на более значительные расстояния, чем в случае использования кабеля UTP. Витая пара подключается к компьютеру с помощью разъема RJ-45 (Registered Jack 45), который очень напоминает телефонный разъем RJ-11 (Registered Jack 11).

Витая пара способна обеспечивать работу сети на скоростях 10, 100 и 1000 Мбит/с.

Коаксиальный кабель состоит из медного провода, покрытого изоляцией, экранирующей металлической оплеткой и внешней оболочкой. По центральному прово-

ду кабеля передаются сигналы, в которые предварительно были преобразованы данные. Такой провод может быть как цельным, так и многожильным. Для организации локальной сети применяются два типа коаксиального кабеля: ThinNet (тонкий, 10Base2) и ThickNet (толстый, 10Base5). В данный момент локальные сети на основе коаксиального кабеля практически не встречаются. Скорость передачи информации в такой сети не превышает 10 Мбит/с.

Обе разновидности кабеля, ThinNet и ThickNet, подключаются к разъему BNC, а на обоих концах кабеля должны быть установлены терминаторы.

В основе оптоволоконного кабеля находятся оптические волокна (световоды), данные по которым передаются в виде импульсов света. Электрические сигналы по оптоволоконному кабелю не передаются, поэтому сигнал нельзя перехватить, что практически исключает несанкционированный доступ к данным. Оптоволоконный кабель используют для транспортировки больших объемов информации на максимально доступных скоростях.

Главным недостатком такого кабеля является его хрупкость: его легко повредить, а монтировать и соединять можно только с помощью специального оборудования.

Сетевые карты

Сетевые карты делают возможным соединение компьютера и сетевого кабеля. Сетевая карта преобразует информацию, которая предназначена для отправки, в специальные пакеты. Пакет — логическая совокупность данных, в которую входят заголовок с адресными сведениями и непосредственно информация. В заголовке присутствуют поля адреса, где находится информация о месте отправления и пункте назначения данных. Сетевая плата анализирует адрес назначения полученного пакета и определяет, действительно ли пакет направлялся данному компьютеру. Если вывод будет положительным, то плата передаст пакет операционной системе. В противном случае пакет обрабатываться не будет. Специальное программное обеспечение позволяет обрабатывать все пакеты, которые проходят внутри сети. Такую возможность используют системные администраторы, когда анализируют работу сети, и злоумышленники для кражи данных, проходящих по ней.

Любая сетевая карта имеет индивидуальный адрес, встроенный в ее микросхемы. Этот адрес называется физическим, или MAC-адресом (Media Access Control — управление доступом к среде передачи).

Порядок действий, совершаемых сетевой картой, такой.

1. Получение информации от операционной системы и преобразование ее в электрические сигналы для дальнейшей отправки по кабелю.
2. Получение электрических сигналов по кабелю и преобразование их обратно в данные, с которыми способна работать операционная система.
3. Определение, предназначен ли принятый пакет данных именно для этого компьютера.
4. Управление потоком информации, которая проходит между компьютером и сетью.

Повторители

Локальная сеть может быть расширена за счет использования специального устройства, которое носит название «репитер» (Repeater — повторитель). Его основная функция состоит в том, чтобы, получив данные на одном из портов, перенаправить их на остальные порты. Данные порты могут быть произвольного типа: AUI, BNC, RJ-45 или Fiber-Optic. Комбинации также роли не играют, что позволяет объединять элементы сети, которые построены на основе различных типов кабеля. Информация в процессе передачи на другие порты восстанавливается, чтобы исключить отклонения, которые могут появиться в процессе движения сигнала от источника.

Повторители могут выполнять функцию разделения. Если повторитель определяет, что на каком-то из портов происходит слишком много коллизий, он делает вывод, что на этом сегменте произошла неполадка, и изолирует его. Данная функция предотвращает распространение сбоев одного из сегментов на всю сеть.

Повторитель позволяет:

- соединять два сегмента сети с одинаковыми или различными видами кабеля;
- регенерировать сигнал для увеличения максимального расстояния его передачи;
- передавать поток данных в обоих направлениях.

Концентраторы

Концентратор (хаб) — устройство, способное объединить компьютеры в физическую звездообразную топологию. Концентратор имеет несколько портов, позволяющих подключить сетевые компоненты. Концентратор, имеющий всего два порта, называют мостом. Мост необходим для соединения двух элементов сети.

Сеть вместе с концентратором представляет собой «общую шину». Пакеты данных при передаче через концентратор будут доставлены на все компьютеры, подключенные к локальной сети.

Существует два вида концентраторов.

- Пассивные концентраторы. Такие устройства отправляют полученный сигнал без его предварительной обработки.
- Активные концентраторы (многопортовые повторители). Принимают входящие сигналы, обрабатывают их и передают в подключенные компьютеры.

Коммутаторы

Коммутаторы необходимы для организации более тесного сетевого соединения между компьютером-отправителем и конечным компьютером. В процессе передачи данных через коммутатор в его память записывается информация о MAC-адресах компьютеров. С помощью этой информации коммутатор составляет таблицу маршрутизации, в которой для каждого из компьютеров указана его принадлежность определенному сегменту сети.

При получении коммутатором пакетов данных он создает специальное внутреннее соединение (сегмент) между двумя своими портами, используя таблицу маршрутизации. Затем отправляет пакет данных в соответствующий порт конечного компьютера, опираясь на информацию, описанную в заголовке пакета.

Таким образом, данное соединение оказывается изолированным от других портов, что позволяет компьютерам обмениваться информацией с максимальной скоростью, которая доступна для данной сети. Если у коммутатора присутствуют только два порта, он называется мостом.

Коммутатор предоставляет следующие возможности:

- послать пакет с данными с одного компьютера на конечный компьютер;
- увеличить скорость передачи данных.

Маршрутизаторы

Маршрутизатор по принципу работы напоминает коммутатор, однако имеет больший набор функциональных возможностей. Он изучает не только MAC, но и IP-адреса обоих компьютеров, участвующих в передаче данных. Транспортируя информацию между различными сегментами сети, маршрутизаторы анализируют заголовок пакета и стараются вычислить оптимальный путь перемещения данного пакета. Маршрутизатор способен определить путь к произвольному сегменту сети, используя информацию из таблицы маршрутов, что позволяет создавать общее подключение к Интернету или глобальной сети.

Маршрутизаторы позволяют произвести доставку пакета наиболее быстрым путем, что позволяет повысить пропускную способность больших сетей. Если какой-то сегмент сети перегружен, поток данных пойдет по другому пути.

Искусство плетения сетевой паутины

Порядок расположения и подключения компьютеров и прочих элементов в сети называют сетевой топологией. Топологию можно сравнить с картой сети, на которой отображены рабочие станции, серверы и прочее сетевое оборудование. Выбранная топология влияет на общие возможности сети, протоколы и сетевое оборудование, которые будут применяться, а также на возможность дальнейшего расширения сети.

Физическая топология — это описание того, каким образом будут соединены физические элементы сети. Логическая топология определяет маршруты прохождения пакетов данных внутри сети.

Выделяют пять видов топологии сети:

- общая шина;
- звезда;
- кольцо;

- ячеистая;
- смешанная.

Остановимся на каждой из них.

Общая шина

В этом случае все компьютеры подключаются к одному кабелю, который называется шиной данных. При этом пакет будет приниматься всеми компьютерами, которые подключены к данному сегменту сети.

Быстродействие сети во многом определяется числом подключенных к общей шине компьютеров. Чем больше таких компьютеров, тем медленнее работает сеть. Кроме того, подобная топология может стать причиной разнообразных коллизий, которые возникают, когда несколько компьютеров одновременно пытаются передать информацию в сеть. Вероятность появления коллизии возрастает с увеличением количества подключенных к шине компьютеров. Схема данной топологии изображена на рис. 2.1.

Рис. 2.1. Сеть с топологией «общая шина»

На рисунке также изображены терминаторы. Такие устройства устанавливаются на концах сети и ограничивают распространение сигнала, замыкая сегмент сети. Если где-то произойдет обрыв кабеля или хотя бы на одном конце сети не будет установлен терминатор, сигнал начнет отражаться от места обрыва и соответствующего конца сети, что приведет к нарушению связи.

Преимущества использования сетей с топологией «общая шина» следующие:

- значительная экономия кабеля;
- простота создания и управления.

Основные недостатки:

- вероятность появления коллизий при увеличении числа компьютеров в сети;
- обрыв кабеля приведет к отключению множества компьютеров;
- низкий уровень защиты передаваемой информации. Любой компьютер может получить данные, которые передаются по сети.

Звезда

При использовании звездообразной топологии каждый кабельный сегмент, идущий от любого компьютера сети, будет подключаться к центральному коммутатору или концентратору. Все пакеты будут транспортироваться от одного компьютера к другому через это устройство. Допускается использование как активных, так и пассивных концентраторов. В случае разрыва соединения между компьютером и концентратором остальная сеть продолжает работать. Если же концентратор выйдет из строя, то сеть работать перестанет. С помощью звездообразной структуры можно подключать друг к другу даже локальные сети. Сеть с такой топологией изображена на рис. 2.2.

Рис. 2.2. Сеть с топологией «звезда»

Использование данной топологии удобно при поиске поврежденных элементов: кабеля, сетевых адаптеров или разъемов. «Звезда» намного удобнее «общей шины» и в случае добавления новых устройств. Следует учесть и то, что сети со скоростью передачи 100 и 1000 Мбит/с построены по топологии «звезда».

Если в самом центре «звезды» расположить концентратор, то логическая топология изменится на «общую шину».

Преимущества «звезды»:

- простота создания и управления;
- высокий уровень надежности сети;
- высокая защищенность информации, которая передается внутри сети (если в центре звезды расположен коммутатор).

Основной недостаток — поломка концентратора приводит к прекращению работы всей сети.

Кольцевая топология

В случае использования кольцевой топологии все компьютеры сети подключаются к единому кольцевому кабелю. Пакеты проходят по кольцу в одном направлении через все сетевые платы подключенных к сети компьютеров. Каждый компьютер

будет усиливать сигнал и отправлять его дальше по кольцу. Сеть с такой топологией изображена на рис. 2.3.

Рис. 2.3. Сеть с кольцевой топологией

В представленной топологии передача пакетов по кольцу организована маркерным методом. Маркер представляет собой определенную последовательность двоичных разрядов, содержащих управляющие данные. Если сетевое устройство имеет маркер, то у него появляется право на отправку информации в сеть. Внутри кольца может передаваться всего один маркер.

Компьютер, который собирается транспортировать данные, забирает маркер из сети и отправляет запрошенную информацию по кольцу. Каждый следующий компьютер будет передавать данные дальше, пока этот пакет не дойдет до адресата. После получения адресат вернет подтверждение о получении компьютеру-отправителю, а последний создаст новый маркер и вернет его в сеть.

Преимущества данной топологии следующие:

- эффективнее, чем в случае с общей шиной, обслуживаются большие объемы данных;
- каждый компьютер является повторителем: он усиливает сигнал перед отправкой следующей машине, что позволяет значительно увеличить размер сети;
- возможность задать различные приоритеты доступа к сети; при этом компьютер, имеющий больший приоритет, сможет дольше задерживать маркер и передавать больше информации.

Недостатки:

- обрыв сетевого кабеля приводит к неработоспособности всей сети;
- произвольный компьютер может получить данные, которые передаются по сети.

Ячеистая топология

Данная топология подразумевает подключение каждого компьютера через отдельный кабель ко всем остальным компьютерам, находящимся в сети. Применение

этого метода позволяет использовать дополнительные пути транспортировки данных. В случае обрыва какого-либо кабеля поток данных пойдет по другому пути, а сеть сможет нормально функционировать далее. Такая топология характерна для глобальных сетей и объединения нескольких удаленных сетей с применением оптоволоконных, выделенных или спутниковых каналов связи. Для локальных сетей данная топология не используется, так как требует присутствия одновременно нескольких сетевых интерфейсов на одной машине и больших объемов кабеля. Схема данной топологии изображена на рис. 2.4.

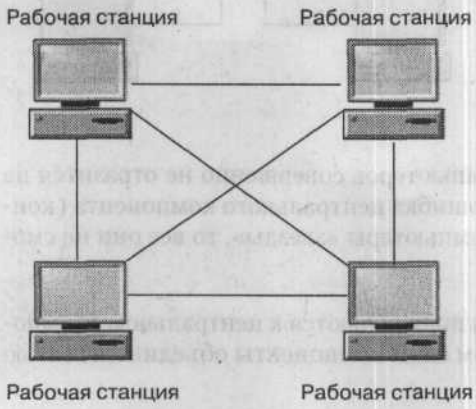


Рис. 2.4. Сеть с ячеистой топологией

Преимущества ячеистой топологии:

- эффективная работа с большими потоками данных;
- высокий уровень стабильности сети из-за использования дополнительных каналов связи;
- высокий уровень безопасности; поток информации идет от компьютера-отправителя к получателю напрямую, что теоретически исключает перехват данных.

Недостатки:

- потребность в наличии нескольких сетевых интерфейсов на компьютерах, входящих в сеть;
- большая стоимость организации сети.

Смешанная топология

Смешанная топология соединяет в себе две или более топологии, образуя тем самым завершенную сетевую структуру. На данный момент такая сеть является самой распространенной; наиболее часто объединяют звездообразную и шинную топологии.

При использовании топологии «звезда-шина» несколько сетей, имеющих звездообразную топологию, подключены к одной шине (рис. 2.5).

Рис. 2.5. Сеть с топологией «звезда-шина»

В данной топологии сбой на одном из компьютеров совершенно не отразится на работе сети в целом. Если же произойдет ошибка центрального компонента (концентратора), к которому подключаются компьютеры «звезды», то все они не смогут больше поддерживать связь.

В топологии «звезда-кольцо» компьютеры подключаются к центральному компоненту, как в звездообразной сети. При этом сами компоненты объединены сетью с кольцевой топологией (рис. 2.6).

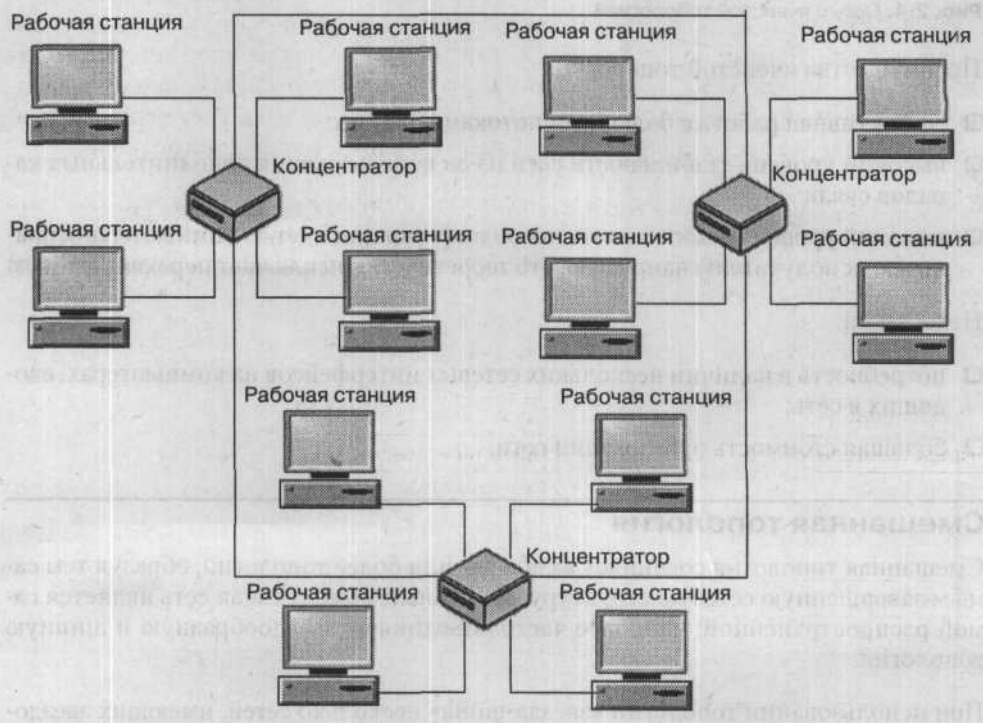


Рис. 2.6. Сеть с топологией «звезда-кольцо»

Точно так же, как и в предыдущем случае, сбой одного из компьютеров сети не отразится на ее работе. Учитывая использование методики передачи свободного маркера, все компьютеры сети имеют равные возможности по передаче информации, что приводит к увеличению потока данных внутри сети.

Совершенствуем сеть: модель OSI

В начале 1980-х годов некоторые интернациональные организации по стандартизации совместно с несколькими крупными компаниями разработали новую модель, сыгравшую впоследствии значительную роль в усовершенствовании компьютерных сетей. Данная модель получила название модели взаимодействия открытых систем (Open System Interconnection, OSI), или модели OSI. Модель OSI способна определять уровни взаимодействия систем в сетях с коммутацией пакетов, она присваивает им определенные имена и назначает функции, которые должен выполнять каждый уровень.

Общая характеристика модели OSI

Модель OSI разрабатывалась на основе большого опыта, который был получен в процессе создания компьютерных сетей (как правило, глобальных) в 1970-х годах.

Модель OSI описывает исключительно те средства взаимодействия, которые реализовывает операционная система, служебные утилиты и системное аппаратное оборудование, однако не включает средства взаимодействия программ и утилит пользователей сети. Собственные протоколы взаимодействия программы выполняют, осуществляя запросы к средствам системы. В этом и состоит основное различие уровня совместной работы программ и утилит и прикладного уровня.

В модели OSI (рис. 2.7) все средства взаимодействия разделены на семь базовых уровней: прикладной, представительский, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень связан с каким-то конкретным аспектом взаимодействия сетевого оборудования.

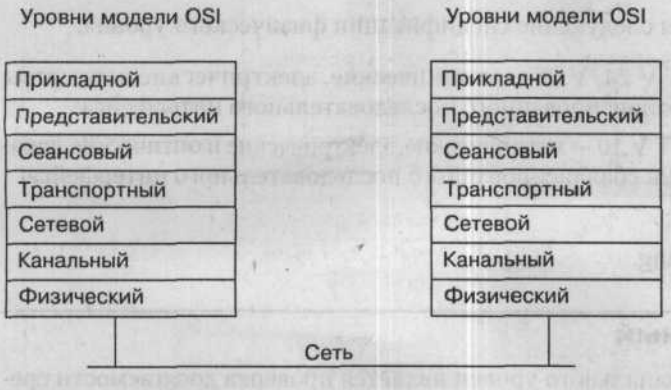


Рис. 2.7. Модель OSI

Данная модель имеет два подтипа:

- горизонтальная модель, которая основана на протоколах, обеспечивающих механизм совместной работы приложений и процессов на различных компьютерах;
- вертикальная модель, основанная на услугах, которые соседние уровни обеспечивают друг другу в пределах одного компьютера.

В случае использования горизонтальной модели двум приложениям понадобится один общий протокол для обмена информацией. Если же используется вертикальная модель, то соседние уровни будут обмениваться информацией, используя интерфейсы API.

Уровень 1: физический

Физический уровень устанавливает параметры передачи электрических сигналов по физическим каналам связи (коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал). На данном этапе определяются параметры физической среды передачи информации (полоса пропускания, защита от помех, волновое сопротивление), а также свойства электрических сигналов, которые передают цифровые данные (крутизна фронтов импульсов, уровни напряжения или тока сигнала, который передается, тип кодирования, скорость транспортировки сигналов). Кроме того, на этом уровне обозначаются и стандартизируются типы разъемов и предназначение всех контактов.

Устройства, принадлежащие к физическому уровню, получают пакеты данных от оборудования более высокого канального уровня, после чего превращают их в оптические или электрические сигналы, которые отвечают 0 и 1 бинарного потока. Данные сигналы отправляются через среду передачи на узел приема. Электрические и оптические характеристики среды передачи стандартизированы на физическом уровне и включают:

- разводку контактов в разъемах;
- тип используемых кабелей и разъемов;
- схему кодирования сигналов для значений 0 и 1.

Наиболее распространены следующие спецификации физического уровня:

- EIA-RS-232-C, CCITT V.24/V.28 — механические, электрические параметры и характеристики несбалансированного последовательного интерфейса;
- EIA-RS-422/449, CCITT V.10 — механические, электрические и оптические параметры и характеристики сбалансированного последовательного интерфейса;
- IEEE 802.3 — Ethernet;
- IEEE 802.5 — Token Ring.

Уровень 2: канальный

Одной из главных задач канального уровня является проверка досягаемости среды транспортировки. Следующей задачей канального уровня является исполне-

ние механизмов выявления и исправления ошибок. Для проведения данной операции на канальном уровне биты упорядочиваются в наборах, которые называются кадрами.

Канальный уровень обрабатывает запросы сетевого уровня и использует сервис физического уровня, чтобы принимать и передавать пакеты данных. Канальный уровень реализовывает создание, передачу и прием кадров данных. Он также обеспечивает правильность транспортировки каждого кадра, располагая контрольный набор битов в начале и конце каждого кадра для его отделения, определяет контрольную сумму кадров, используя специальный алгоритм, и добавляет ее к кадру.

По спецификации IEEE 802.x канальный уровень разделяется на два подуровня: контроль и управление логическим каналом (LLC) и управление доступом к среде (MAC). Подуровень LLC реализовывает обслуживание сетевого уровня, а подуровень MAC контролирует доступ к разделяемой физической среде.

Протоколы, которые наиболее часто используются на канальном уровне, включают:

- HDLC для последовательных соединений;
- IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;
- Ethernet;
- Token ring;
- FDDI;
- X.25;
- frame relay.

Уровень 3: сетевой

Сетевой уровень отвечает за управление транспортировкой пакетов по сети, а сама сеть может состоять из набора сетей, использующих различные принципы передачи пакетов между узлами, и иметь любую структуру связей. На данном уровне реализовывается маршрутизация пакетов на основе трансформации MAC-адресов сетевых карт в сетевые адреса. Сетевой уровень также занимается передачей пакетов на вышестоящий уровень в фоновом режиме.

Вот несколько протоколов, работающих на сетевом уровне:

- IP — протокол Интернета;
- IPX — протокол межсетевого обмена;
- X.25;
- CLNP — сетевой протокол без организации соединений.

Уровень 4: транспортный

Транспортный уровень отвечает за надежное соединение приложений или верхних уровней модели OSI. Он обеспечивает передачу информации с тем уровнем надежности, которая необходима верхним уровням модели OSI. Транспортный

уровень разбивает потоки данных на небольшие пакеты для последующей транспортировки на сетевой уровень.

Модель OSI производит стандартизацию пяти классов сервиса, которые предоставляет транспортный уровень. Отличие данных видов сервисов состоит в качестве услуг: возможность восстановления связи в случае обрыва, скорость, присутствие утилит для мультиплексирования нескольких соединений между разными прикладными протоколами через один транспортный протокол, а главное — способности к нахождению и исправлению искажений, потерь и повторения отправки пакетов.

Как правило, на транспортном уровне используются следующие протоколы:

- TCP (Transmission Control Protocol) — протокол управления передачей;
- NCP (Netware Core Protocol) — протокол ядра Netware;
- SPX (Sequenced Packet eXchange) — упорядоченный обмен пакетами;
- TP4 (Transmission Protocol 4) — протокол передачи класса 4.

Уровень 5: сеансовый

Сеансовый уровень отвечает за управление соединением. Он занимается мониторингом передачи, определяет, какая из сторон является активной на данный момент, и обеспечивает синхронизацию. Между тем, не так много приложений используют данный уровень, поэтому он достаточно редко исполняется в виде отдельных протоколов. Функции данного уровня нередко используются вместе с функциями прикладного уровня и реализовываются в одном протоколе. Протоколы сеансового уровня, как правило, являются составляющей функций трех предыдущих уровней модели.

Уровень 6: представительский

Представительский уровень предназначен для обмена информацией между программами на разных компьютерах. Данный уровень отвечает за трансформацию данных прикладного уровня в поток информации для транспортного уровня. Протоколы уровня представления входят в набор функций трех верхних уровней модели.

Уровень 7: прикладной

Прикладной уровень отвечает за сетевое взаимодействие приложений. На этом уровне происходит передача файлов, обмен электронными сообщениями и управление сетью.

С помощью возможностей данного уровня протоколы прикладных уровней различных машин в сети могут обойти различия в представлении информации или же несоответствия в кодах символов. На этом же уровне может происходить шифрование передаваемой информации, обеспечивая безопасную транспортировку данных через сеть для всех приложений одновременно.

Вот некоторые протоколы прикладного уровня:

- FTP — протокол передачи файлов;
- X.400 — электронная почта;
- TELNET — протокол виртуального терминала;
- SMTP — простой протокол почтового обмена;
- CMIP — общий протокол управления данными;
- SNMP — простой протокол управления сетью;
- NFS — сетевая файловая система.

TCP/IP: протоколы бывают не только в милиции

TCP/IP (Transmission Control Protocol/Internet Protocol) по своей сути является стеком протоколов, которые были разработаны специально для обеспечения связи компьютеров в условиях глобальной сети. Инициатором данной разработки более 20 лет назад стало Министерство обороны США, преследовавшее цель установить связи внутри экспериментальной сети ARPAnet и соединить ее с другими сетями.

Связь между элементами сети ARPA реализовывалась с помощью протокола IP (Internet Protocol), который до сих пор является одним из основных в стеке TCP/IP.

Стандарты TCP/IP подробно описаны в документации, носящей название Request for Comment (RFC). Документы RFC регулируют стандарты работы в Интернете. Некоторые RFC подробно описывают сетевые сервисы или протоколы и их исполнение, другие — рассматривают условия их реализации.

Стек TCP/IP на нижнем уровне способен работать со всеми распространенными стандартами физического и канального уровней модели OSI: Ethernet, Token Ring, FDDI, SLIP, PPP, протоколы территориальных сетей X.25 и ISDN.

Протоколами, которые выступают фундаментом стека TCP/IP, являются IP и TCP, которые и дали ему название. В системе понятий модели OSI они относятся к сетевому и транспортному уровням. Протокол IP реализует транспортировку пакета по сети, а TCP обеспечивает стабильность процесса его доставки.

На данном этапе развития глобальных сетей только Интернетом объединено более 10 млн компьютеров, которые взаимодействуют друг с другом с помощью стека протоколов TCP/IP.

Так как стек TCP/IP был разработан несколько ранее появления модели OSI, его соответствие уровням данной модели несколько условно, хотя его структура тоже делится на уровни. Протоколы TCP/IP делятся на четыре уровня (рис. 2.8).

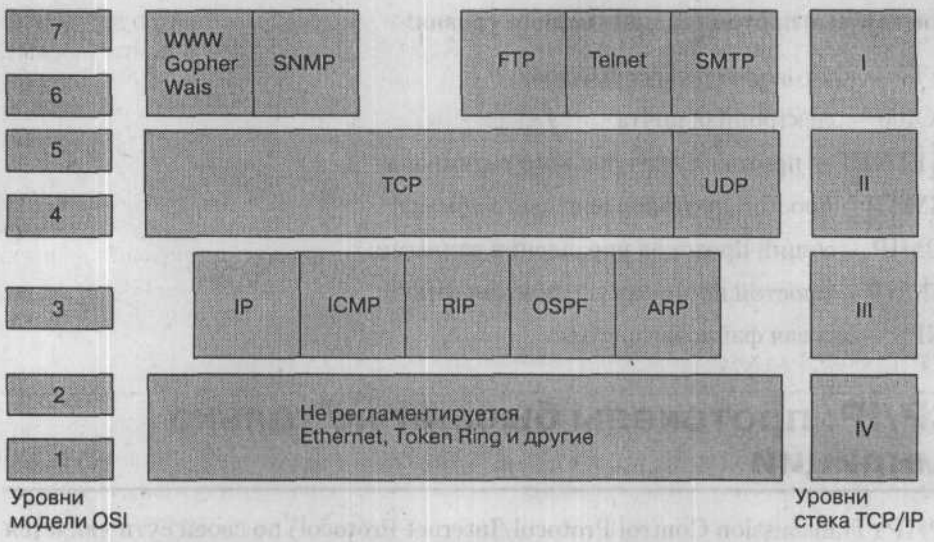


Рис. 2.8. Уровни стека TCP/IP и их соответствие уровням модели OSI

Нижний уровень (IV) аналогичен физическому и канальному уровням модели OSI. Он реализует передачу и прием информации от сетевой среды передачи. Данный уровень может работать со всеми популярными стандартами физического и канального уровней: Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, протоколы SLIP и PPP, протоколы сетей с коммутацией пакетов X.25, frame relay.

В процессе разработки новой технологии локальных или глобальных сетей рассматриваемая технология добавляется в стек TCP/IP сразу после того, как будет реализован метод инкапсуляции пакетов IP в ее кадры.

Следующий уровень (III) предназначен для обеспечения межсетевого взаимодействия, для передачи пакетов с использованием разнообразных транспортных технологий локальных и глобальных сетей. Данный уровень обеспечивает адресацию, упаковку и маршрутизацию информации, которую необходимо передать.

Протоколом сетевого уровня (в терминах модели OSI) является протокол IP, основным заданием которого является реализация возможности работы в локальных и глобальных сетях, использующих топологию произвольной сложности. IP — дейтаграммный протокол, а следовательно, он не гарантирует доставку информации адресату, однако пытается это сделать. Протокол IP старается экономно использовать пропускную способность каналов связи. Данный уровень также содержит протоколы, предназначенные для сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Протокол ICMP обеспечивает обмен данными о всевозможных сбоях между маршрутизаторами сети и источником пакета. Протокол, используя специальные пакеты, уведомляет о невозможности доставки пакета, об окончании времени существования или продолжительности сборки пакета из частей, об уточнении маршрута отправки и общем состоянии системы.

Следующий уровень (II) — основной. На данном уровне функционируют протокол TCP (контроль передачи) и протокол UDP (пользовательские дейтаграммы). TCP отвечает за передачу сообщений между компьютерами сети, используя виртуальные соединения. Протокол UDP передает пакеты с данными дейтаграммным способом, выполняя функции промежуточного звена между сетевым протоколом и разнообразными процессами системы.

Наивысший уровень (I) — прикладной. Данный уровень включает множество разнообразных протоколов и сервисов, включая протокол транспортировки файлов (FTP), протокол эмуляции терминала TELNET, SMTP, WWW и прочие.

Погружаемся в Ethernet

На данный момент Ethernet является самой распространенной технологией в локальных сетях. На базе этой технологии работает более 7 млн локальных сетей и более 80 млн компьютеров, имеющих сетевую карту, поддерживающую данную технологию. Существуют несколько подтипов Ethernet в зависимости от быстродействия и типов используемого кабеля.

Одним из основоположников данной технологии является фирма Xerox, разработавшая и создавшая в 1975 году тестовую сеть Ethernet Network. Большинство принципов, реализованных в упомянутой сети, используются и сегодня.

Постепенно технология совершенствовалась, отвечая возрастающему уровню запросов пользователей. Это привело к тому, что технология расширила сферу своего применения до такой среды передачи данных, как оптическое волокно или неэкранированная витая пара.

Причиной начала использования названных кабельных систем стало достаточно быстрое увеличение количества локальных сетей в различных организациях, а также низкая производительность локальных сетей, использующих коаксиальный кабель. Вместе с тем возникла необходимость в удобном и экономичном управлении и обслуживании данных сетей, чего уже не могли обеспечить устаревшие сети.

Остановимся на основных принципах работы Ethernet. Все компьютеры, входящие в сеть, подключены к общему кабелю, который называется общей шиной. Кабель является средой передачи, и его может использовать для получения или передачи информации любой компьютер данной сети.

Сети Ethernet используют метод пакетной передачи данных. Компьютер-отправитель отбирает данные, которые нужно отправить. Эти данные преобразуются в короткие пакеты (иногда их называют кадрами), которые содержат адреса отправителя и получателя. Пакет снабжен служебной информацией — преамбулой (отмечает начало пакета) — и информацией о значении контрольной суммы пакета, которая необходима для проверки правильности передачи пакета по сети.

Перед тем как отправить пакет, компьютер-отправитель проверяет кабель, контролируя в нем отсутствие несущей частоты, на которой и будет происходить передача. Если такая частота не наблюдается, то он начинает передачу пакета в сеть.

Пакет будет принят всеми сетевыми платами компьютеров, которые подключены к этому сегменту сети. Сетевые карты контролируют адрес назначения пакета. Если адрес назначения не совпадает с адресом данного компьютера, то пакет отклоняется без обработки. Если же адреса совпадают, то компьютер примет и обработает пакет, удаляя из него все служебные данные и транспортируя необходимую информацию «вверх» по уровням модели OSI вплоть до прикладного.

После того как компьютер передаст пакет, он выдерживает небольшую паузу, равную 9,6 мкс, после чего опять повторяет алгоритм передачи пакета вплоть до полной транспортировки необходимых данных. Пауза нужна для того, чтобы один компьютер не имел физической возможности заблокировать сеть при передаче большого количества информации. Пока длится такая технологическая пауза, канал сможет использовать любой другой компьютер сети.

Если два компьютера одновременно проверяют канал и делают попытку отправить пакеты данных по общему кабелю, то в результате этих действий происходит коллизия, так как содержимое обоих кадров сталкивается на общем кабеле, что значительно искажает передаваемые данные.

Коллизия — нормальное явление, которое появляется при работе сети. Чтобы проанализировать и устранить коллизию, все компьютеры одновременно изучают возникающие на кабеле сигналы. Если сигналы, которые передаются и реально наблюдаются, не совпадают, то отмечается присутствие коллизии. Те компьютеры, которые заметили коллизию, отправляют в сеть 32-битную последовательность, которая называется jam-последовательностью.

После того как коллизия будет найдена, передающий компьютер обязан остановить передачу на небольшой случайный интервал времени.

Важным условием корректной работы сети является обязательное распознавание коллизий всеми компьютерами одновременно. Если любой передающий компьютер не вычислит коллизию и сделает вывод о правильности передачи пакета, то данный пакет попросту пропадет из-за того, что будет сильно искажен и отклонен принимающим компьютером (несовпадение контрольной суммы).

Вероятно, что утерянную или искаженную информацию повторно передаст протокол верхнего уровня, который работает с установлением соединения и идентификацией своих сообщений. Следует учитывать и то, что повторная передача произойдет через достаточно длительный интервал времени (десятки секунд), что приведет к значительному снижению пропускной способности конкретной сети. Именно поэтому своевременное распознание коллизий крайне важно для стабильности работы сети.

Все параметры Ethernet составлены так, чтобы коллизии всегда четко определялись. Именно поэтому минимальная длина поля данных кадра составляет не менее 46 байт (а с учетом служебной информации — 72 байта или 576 бит). Длина кабельной системы рассчитывается таким образом, чтобы за то время, пока транспортируется кадр минимальной длины, сигнал о коллизии успел дойти до са-

мого отдаленного компьютера сети. Исходя из этого при скорости в 10 Мбит/с максимальное расстояние между произвольными элементами сети не может превышать 2500 м. Чем выше скорость передачи данных, тем меньше максимальная длина сети (уменьшается пропорционально). Используя стандарт Fast Ethernet, вы ограничиваете максимальный размер 250 м, а в случае с гигабитным Ethernet — 25 м.

Таким образом, вероятность успешного получения общей среды напрямую зависит от загруженности сети (интенсивности возникновения потребности передачи кадров).

Правило 5-4-3

Сеть Ethernet может состоять из нескольких сегментов, которые соединены повторителями.

Напомню, что повторитель Ethernet представляет собой устройство, имеющее несколько Ethernet-портов, которое соединяет несколько элементов сети. Ethernet-порты могут быть произвольного типа: AUI, BNC, RJ-45 или для оптоволоконного кабеля.

Основная задача репитера — немедленное перенаправление на все остальные порты полученной информации. В процессе передачи данные восстанавливаются, чтобы избежать искажений, которые могут появиться во время движения сигнала от источника.

Если повторитель обнаруживает большое количество коллизий, которые появляются на одном из портов, то он делает вывод о сбое на этом сегменте и отделяет его от основной сети. Данная функция призвана ограничить распространение сбоев конкретного сегмента на всю сеть.

Исходя из расчетов, проведенных разработчиками Ethernet, в сети не может быть более пяти сегментов и четырех репитеров, и только к трем из них можно подключать оборудование. Данные выводы называются «правило 5-4-3». Такое ограничение существует из-за того, что посылаемые пакеты не могут моментально попасть во все точки сети, и проходит небольшой отрезок времени, пока сигнал пройдет по кабелю через каждый репитер в сети.

Описанный отрезок времени называют «задержкой распространения сигнала». Если такая «задержка» между источником сигнала и максимально удаленным компьютером сети больше, чем половина времени передачи минимально допустимого пакета, то компьютеры не смогут корректно определить коллизию. В этом случае информация в сети может быть потеряна или искажена.

Данный метод можно использовать только тогда, когда сеть построена по топологии «общая шина» с использованием репитеров. Если будут использованы маршрутизаторы, то топология сети или отдельных ее элементов будет соответствовать «звезде» и данные ограничения можно будет обойти.

Спецификации сетей Ethernet указаны в табл. 2.1–2.4. Тут же приводятся типы необходимых кабелей, максимальное количество сегментов и их длин, а также применяемая топология.

Таблица 2.1. Спецификация 10Base-5

Характеристики	Значения
Тип кабеля	Толстый коаксиальный кабель RG-8/11 (желтый ethernet)
Топология	Шина
Максимальное число узлов на сегменте	100
Максимальное количество сегментов	5 (4 репитера, 2 сегмента без узлов)
Максимальная длина сегмента	500 м
Максимальная длина сети	2500 м (300 узлов)
Минимальное расстояние между точками включения	2,5 м
Максимальная длина трансиверного кабеля	50 м

Таблица 2.2. Спецификация 10Base-2

Характеристики	Значения
Тип кабеля	Тонкий коаксиальный кабель RG-58/U или RG-58A/U
Топология	Шина
Максимальное число узлов на сегменте	30
Максимальное количество сегментов	5 (4 репитера, 2 сегмента без узлов)
Максимальная длина сегмента	185 м
Максимальная длина сети	925 м
Минимальное расстояние между точками включения	0,5 м
Способ подсоединения узла	BNC T-коннектор

Таблица 2.3. Спецификация 10Base-T

Характеристики	Значения
Тип кабеля	UTP3, UTP4, UTP5
Топология	Звезда
Максимальное число узлов на сегменте	1024
Максимальное количество сегментов	5 (последовательно)
Максимальная длина сегмента	100 м
Максимальная длина сети	500 м
Способ подсоединения узла	RJ-45
Количество используемых пар кабеля	2

Таблица 2.4. Спецификация 10Base-F

Характеристики	Значения
Тип кабеля	Одномодовый и многомодовый оптический кабель
Топология	Звезда
Максимальное число узлов на сегменте	1024
Максимальная длина сегмента	Для одномодового — 5 км, для многомодового — 1 км
Способ подсоединения узла	ST-коннектор
Количество используемых пар кабеля	1
Тип кабеля	Одномодовый и многомодовый оптический кабель

Технология Fast Ethernet

Постоянное возрастание уровня требований к пропускной способности сети послужило причиной разработки технологии Ethernet, скорость передачи в которой превышала 10 Мбит/с. В 1992 году был реализован стандарт Fast Ethernet, поддерживающий транспортировку информации со скоростью 100 Мбит/с. Большинство принципов работы Ethernet остались без изменений.

Некоторые изменения произошли в кабельной системе. Коаксиальный кабель был не в состоянии обеспечить скорость передачи информации в 100 Мбит/с, поэтому ему на смену в Fast Ethernet приходят экранированные и неэкранированные кабели типа витая пара, а также оптоволоконный кабель.

Выделяют три вида Fast Ethernet:

- 100Base-TX;
- 100Base-T4;
- 100Base-FX.

Стандарт 100Base-TX использует сразу две пары кабеля: UTP (неэкранированный кабель) или STP (экранированный кабель). Одна пара необходима для передачи данных, а вторая — для приема. Перечисленным требованиям соответствуют два кабельных стандарта: EIA/TIA-568 UTP категории 5 и STP Типа 1 компании IBM. В 100Base-TX предоставляется возможность полнодуплексного режима в процессе работы с сетевыми серверами, а также применение всего двух из четырех пар восьмижильного кабеля — две оставшиеся пары будут свободными и в дальнейшем могут быть использованы для расширения функциональности данной сети (например, на их основе возможна организация телефонной сети).

Стандарт 100Base-T4 позволяет использовать кабели категорий 3 и 5. Это происходит из-за того, что в 100Base-T4 используются четыре пары восьмижильного кабеля: одна — для передачи, а другая — для приема, остальные могут использоваться как для передачи, так и для приема. Соответственно, как прием, так и передача

данных могут проводиться сразу по трем парам. Если общая пропускная способность в 100 Мбит/с распределяется на три пары, то 100Base-T4 снижает частоту сигнала, поэтому для нормальной работы вполне достаточно и менее качественного кабеля. Для организации сетей 100Base-T4 могут использоваться кабели UTP категорий 3 и 5, точно так же, как и UTP категории 5 и STP типа 1.

Стандарт 100Base-FX использует для передачи данных многомодовое оптоволокно с 62,5-микронным ядром и 125-микронной оболочкой. Данный стандарт предназначен для магистралей — соединения репитеров Fast Ethernet в пределах одного помещения. Основные преимущества оптического кабеля передались и рассматриваемому стандарту 100Base-FX: невосприимчивость к электромагнитным шумам, повышенный уровень защиты информации и увеличенные расстояния между сетевыми устройствами.

Различные спецификации сетей Ethernet представлены в табл. 2.5–2.8.

Таблица 2.5. Спецификация 100Base-TX

Характеристики	Значения
Тип кабеля	UTP5, STP тип 1
Топология	Звезда
Максимальное число узлов на сегменте	1024
Максимальное количество сегментов	3 (последовательно)
Максимальная длина кабеля между концентраторами	5 м
Максимальная длина сегмента	100 м
Максимальная длина сети	205 м
Способ подсоединения узла	RJ-45
Количество используемых пар кабеля	2

Таблица 2.6. Спецификация 100VG-AnyLAN

Характеристики	Значения
Тип кабеля	UTP3, UTP4, UTP5
Топология	Звезда
Максимальное количество узлов на сегменте	1024
Максимальное количество сегментов	4 (последовательно)
Максимальная длина кабеля между концентраторами	5 м
Максимальная длина сегмента (только для оборудования HP)	225 м
Максимальная длина сети	1100 м
Способ подсоединения узла	RJ-45
Количество используемых пар кабеля	4

Таблица 2.7. Спецификация 100Base-FX

Характеристики	Значения
Тип кабеля	Одномодовый оптический кабель
Топология	Звезда
Максимальное количество узлов на сегменте	1024
Максимальная длина сегмента	Коммутатор-коммутатор, full duplex — 2 км; коммутатор-коммутатор, half duplex — 412 м; коммутатор-узел, full duplex — 2 км; коммутатор-узел, half duplex — 412 м.

Таблица 2.8. Спецификация 100Base-T4

Характеристики	Значения
Тип кабеля	UTP3, UTP4, UTP5
Топология	Звезда
Максимальное количество узлов на сегменте	1024
Максимальное количество сегментов	3 (последовательно)
Максимальная длина кабеля между концентраторами	5 м
Максимальная длина сегмента	100 м
Максимальная длина сети	205 м
Способ подсоединения узла	RJ-45
Количество используемых пар кабеля	4 (3 — обмен данными, 1 — определение коллизий)

Gigabit Ethernet: знакомимся со стандартом

Несколько лет назад был разработан новый стандарт Ethernet — Gigabit Ethernet. На данный момент он пока еще не имеет широкого распространения. Технология Gigabit Ethernet в качестве среды транспортировки информации использует оптические каналы и экранированную витую пару. Такая среда способна десятикратно повысить скорость передачи данных, что является необходимым условием для проведения видеоконференций или работы сложных программ, оперирующих большими объемами информации.

Данная технология использует те же принципы, что и более ранние стандарты Ethernet. Кроме того, если у вас уже функционирует сеть, которая базируется на основе экранированной витой пары, вы сможете осуществить переход на технологию Gigabit Ethernet путем замены сетевых плат и сетевого оборудования, которые используются в вашей сети.

1000Base-X содержит сразу три физических интерфейса, параметры и характеристики которых указаны ниже.

- Интерфейс 1000Base-SX определяет лазеры с допустимой длиной излучения в промежутке 770-860 нм, мощность излучения передатчика в диапазоне от 10 до 0 дБм, при существующем соотношении ON/OFF (есть сигнал/нет сигнала) не менее 9 дБ. Чувствительность такого приемника — 17 дБм, а его насыщение — 0 дБм.
- Интерфейс 1000Base-LX определяет лазеры с допустимой длиной излучения в промежутке 1270–1355 нм, мощность излучения передатчика в диапазоне от 13,5 до 3 дБм, при существующем соотношении ON/OFF (есть сигнал/нет сигнала) не менее 9 дБ. Чувствительность такого приемника — 19 дБм, а его насыщение — 3 дБм.
- 1000Base-CX — экранированная витая пара, предназначенная для транспортировки данных на небольшие расстояния. Для транспортировки данных используются все четыре пары медного кабеля, а скорость передачи по одной паре составляет 250 Мбит/с.

Технология Gigabit Ethernet — самая быстрая из всех существующих на данный момент технологий локальных сетей. Достаточно скоро большинство сетей будут создаваться на основе данной технологии.

Технические характеристики сетей Ethernet представлены в табл. 2.9–2.12.

Таблица 2.9. Технические характеристики 1000Base-LX

Характеристики	Значения
Тип кабеля	Одномодовый и многомодовый оптический кабель, используются трансиверы на длинноволновом лазере
Топология	Звезда
Максимальное число узлов на сегменте	2
Максимальная длина сегмента	Для одномодового — 3 км, для многомодового — 550 м

Таблица 2.10. Технические характеристики 1000Base-SX

Характеристики	Значения
Тип кабеля	Многомодовый оптический кабель, используются трансиверы на коротковолновом лазере
Топология	Звезда
Максимальное число узлов на сегменте	2
Максимальная длина сегмента	Для многомодового диаметром 62,5 мкм — 300 м для многомодового диаметром 50,0 мкм — 550 м

Таблица 2.11. Технические характеристики 1000Base-CX

Характеристики	Значения
Тип кабеля	UTP5 (используется экранированная витая пара)
Топология	Звезда
Максимальное число узлов на сегменте	2
Максимальная длина сегмента	100 м

Таблица 2.12. Технические характеристики 1000Base-T

Характеристики	Значения
Тип кабеля	STP (используется неэкранированная витая пара)
Топология	Звезда
Максимальное число узлов на сегменте	2
Максимальная длина сегмента	25 м

Не запутайся в кабелях!

Большинство локальных сетей на данный момент создаются на основе кабеля UTP, а оптические и коаксиальные кабели используются крайне редко. Оптические кабели пока что являются достаточно редким явлением из-за своей высокой стоимости и определенных трудностей, возникающих в процессе монтажа. Коаксиальные кабели не используются, так как они уже устарели и не в состоянии обеспечить пропускную способность сети выше чем 10 Мбит/с.

Учитывая это, подробно остановимся на особенностях создания сети на основе кабеля «витая пара».

Неэкранированная витая пара UTP

Кабель «витая пара» состоит из нескольких пар проводов, которые закручены друг вокруг друга и вместе вокруг других пар внутри кабеля.

Любая пара состоит из двух проводов: Ring и Tip (данные названия пришли еще из телефонии).

Каждая пара имеет свой индивидуальный номер, чтобы любой провод можно было определить как Ring1, Tip1, Ring2, Tip2 и т. д. Как правило, провода в кабеле не нумеруют, а применяют специальную цветовую схему. Внешний вид кабеля изображен на рис. 2.9.

На данной цветовой схеме провод Ring окрашен в основной цвет с полосками дополнительного, а провод Tip — в дополнительный цвет с полосками основного. Например, первая пара содержит Ring-провод, окрашенный в синий цвет с белыми полосками, и Tip-провод белого цвета с синими полосками.

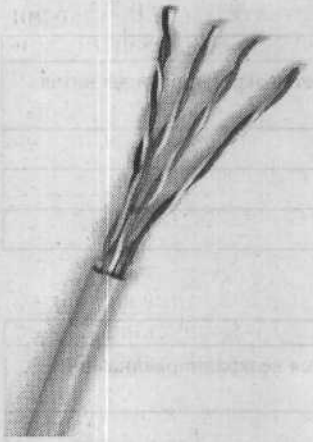


Рис. 2.9. Внешний вид кабеля «витая пара»

Если количество пар небольшое (четыре пары), то чередование основного и дополнительного цветов несколько изменяется.

В таком случае пары будут окрашены следующим образом:

- первая пара — синий и белый с синими полосками;
- вторая пара — оранжевый и белый с оранжевыми полосками;
- третья пара — зеленый и белый с зелеными полосками;
- четвертая пара — коричневый и белый с коричневыми полосками.

В соответствии со стандартами ANSI/EIA/TIA-568, ISO/IEC 11801 виды кабеля разбиваются на несколько групп в зависимости от пропускной способности (табл. 2.13).

Таблица 2.13. Категории кабелей UTP

Категория кабеля	Область применения
1 категория	Стандартный телефонный кабель. Не подходит для передачи данных
2 категория	Применяется в локальных сетях с пропускной способностью до 4 Мбит/с
3 категория	Применяется в локальных сетях с пропускной способностью до 10 Мбит/с. Используется в сетях 10Base-T
4 категория	Применяется в локальных сетях с пропускной способностью до 16 Мбит/с. Используется в сетях Token Ring
5 категория	Применяется в локальных сетях с пропускной способностью до 100 Мбит/с. Используется в сетях 100Base-TX. Является наиболее распространенным видом кабеля, который применяется на данный момент для создания локальной сети
5+ категория	Сертифицирован для частот до 300 МГц
6 категория	Сертифицирован для частот до 600 МГц

Кроме того, может быть использована экранированная витая пара (STP — экранирование медной оплеткой, FTP — экранирование фольгой, SFTP — экранирование медной оплеткой и фольгой), обладающая значительно улучшенными характеристиками по защищенности от всевозможных помех. Ее использование оправдано в разветвленных сетях Fast и Gigabit Ethernet.

Основные эксплуатационные требования к кабелям на основе витой пары

Каждый кабель должен иметь витые пары проводов, а использование кабеля, который не отвечает этому условию, не допускается, так как его пропускная способность и устойчивость к помехам не будет отвечать установленным стандартам.

Если применяются экранированные кабели на витой паре, то их элементы следует заземлять только на одном из концов. Эту операцию удобнее производить с тем концом, который присоединен к концентратору.

Наименьший допустимый радиус изгиба кабеля должен быть не больше 5 см.

При работе и хранении кабеля допустимыми являются следующие температуры:

- –35...+60 °C — для кабеля, находящегося в поливинилхлоридной оболочке;
- –55...+200 °C — для кабеля, находящегося в тефлоновой оболочке.

Допустимая температура в процессе монтажа:

- –20...+60 °C — для кабеля в поливинилхлоридной оболочке;
- –35...+200 °C — для кабеля в тефлоновой оболочке.

Использование вне помещения:

- запрещено — для кабеля в поливинилхлоридной оболочке;
- разрешено — для кабеля в тефлоновой оболочке.

В соответствии с правилами противопожарной безопасности выделяют кабели общего применения и пленумные (прокладка которых разрешена в вентиляционных шахтах). Это разделение производится в зависимости от материалов, которые применяются при производстве кабеля. Как правило, чаще всего используются пластики на основе поливинилхлорида, который при горении выделяет токсичные газы. Соответственно, данные кабели нельзя прокладывать в вентиляционных шахтах. В пленумных пространствах необходимо применять кабели, изоляция которых изготовляется с использованием тефлона.

Разъемы для кабеля

Существует два типа разъемов, которые используются в сетях, основанных на витой паре. В сетевых платах компьютеров, хабах и на стенах находятся розетки, предназначенные для вилок стандарта RJ-45.

Вилка RJ-45 напоминает телефонный разъем, однако содержит восемь контактов и немного шире (рис. 2.10).

Рис. 2.10. Внешний вид разъема RJ-45

Вилки бывают экранированными и неэкранированными, с использованием вставки или без нее, предназначенные для круглого или плоского кабеля, с двумя и тремя зубцами. Свой выбор вы должны делать прежде всего исходя из цены. Не нужно приобретать дешевую кабельную продукцию, так как последствия могут стоить вам значительно дороже.

Чтобы соединить вилку и кабель, вам понадобится обжимной инструмент (рис. 2.11).

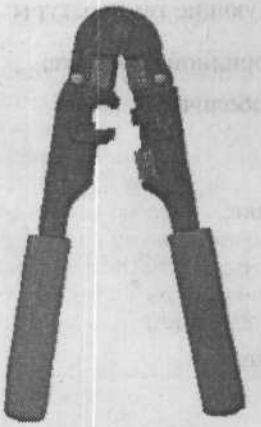


Рис. 2.11. Обжимной инструмент для витой пары

Чтобы обжать вилку, удалите оболочку кабеля приблизительно на 12 мм. В обжимном инструменте находятся специальные нож и ограничитель, так что трудностей возникнуть не должно. Зачистку проводов производить не нужно.

Отделите провода друг от друга и расположите их в порядке, который соответствует выбранной вами схеме заделки. Учтите, что длина расплетенных концов проводов не должна превышать 12,5 мм.

Расположите вилку контактами к себе (рис. 2.12) и осторожно наденьте ее на кабель до упора, чтобы провода оказались под контактами.

Обожмите вилку с помощью специального гнезда на обжимном инструменте, в которое вставляется вилка с проводами. В процессе обжима контакты будут вдавле-

ны внутрь корпуса и пробьют оболочку проводов. Фиксатор провода также должен быть утоплен внутрь корпуса.

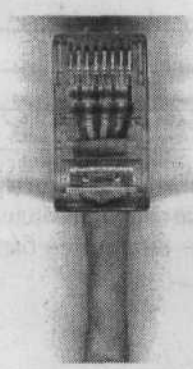


Рис. 2.12. Вилка со вставленным кабелем

СОВЕТ

При отсутствии обжимного инструмента можно обжать вилку с помощью тонкой отвертки и плоскогубцев. Для начала очистите кабель от оболочки примерно на 2–3 см, разделите провода и расположите в соответствии с выбранной схемой. Не забудьте приблизительно на миллиметр очистить от изоляции извлеченные провода. Поместите подготовленный кабель в вилку и зафиксируйте его, утопив фиксатор вилки вниз с помощью широкой отвертки (иначе кабель может выскользнуть). В новом разъеме RJ-45 контакты немного выступают над корпусом. Утопите их с помощью отвертки или плоскогубцев до уровня корпуса. Далее с помощью тонкой отвертки погрузите каждый контакт еще на 0,5 мм, после чего операцию можно считать завершенной. Безусловно, этот способ не такой быстрый и простой, однако в случае одноразового применения вполне подойдет.

Патч-корд

Патч-корд (Patch cord) — это небольшой сегмент сетевого кабеля (не превышающий 5 м), обжатый с обоих концов вилками RJ-45. Он необходим для соединения компьютера с сетевой розеткой. Как правило, патч-корд производится из более гибкого и прочного кабеля, чем основной, чтобы уменьшить вероятность его перелома. Существуют патч-корды 3-й и 5-й категории. Они могут также различаться стандартами обжимки: 568A или 568B (см. ниже). Провод патч-корда несложно изготовить самому, установив на концы обрезка UTP-кабеля две вилки RJ-45.

Варианты заделки проводов для кабеля «витая пара» на вилку

Кабель должен быть симметричным, поэтому он разделывается одинаково с обеих сторон. Если в кабеле присутствуют лишь две пары (или ваша сеть работает на базе 100Base-TX), то он будет обжиматься в соответствии с табл. 2.14.

Таблица 2.14. Разделка кабеля с использованием двух пар провода

Одна сторона патч-корда	Цвет провода	Вторая сторона патч-корда
1	Бело-оранжевый	1
2	Оранжево-белый	2
3	Бело-синий	3
4	Сине-белый	4

В случае использования восьмижильного кабеля должны быть обжаты все четыре пары по двум вариантам заделки проводов — 568A или 568B. Сам вариант заделки не имеет принципиального значения, основное требование — он должен быть одинаковым для всей сети.

Вариант 568A представлен в табл. 2.15.

Таблица 2.15. Вариант разделки кабеля 568A

Одна сторона патч-корда	Цвет провода	Вторая сторона патч-корда
1	Бело-зеленый	1
2	Зелено-белый	2
3	Бело-оранжевый	3
4	Сине-белый	4
5	Бело-синий	5
6	Оранжево-белый	6
7	Бело-коричневый	7
8	Коричнево-белый	8

Вариант 568B представлен в табл. 2.16.

Таблица 2.16. Вариант разделки кабеля 568B

Одна сторона патч-корда	Цвет провода	Вторая сторона патч-корда
1	Бело-оранжевый	1
2	Оранжево-белый	2
3	Бело-зеленый	3
4	Сине-белый	4
5	Бело-синий	5
6	Зелено-белый	6
7	Бело-коричневый	7
8	Коричнево-белый	8

Сетевые розетки

Розетки (рис. 2.13) вмонтированы в сетевые карты, коммутаторы и прочие сетевые устройства. Разъем состоит из восьми пружинящих контактов и небольшой выем-

ки, которая предназначена для фиксатора вилки. Если рассматривать гнездо со стороны контактов, когда они находятся снизу, то отсчет будет идти справа налево.

Розетка является гнездом соединителя с любым приспособлением для фиксации кабеля и корпусом для упрощения процесса монтажа.

Существуют розетки различных категорий. В случае создания сети 100Base-TX нужно использовать исключительно пятую категорию розеток. Розетки данной категории также разделяются на подгруппы в зависимости от способа монтажа кабеля в этой розетке. Возможна реализация достаточно большого количества решений, как достаточно специфических, так и общепринятых — «тип 110», «тип KRONE» (название фирмы).

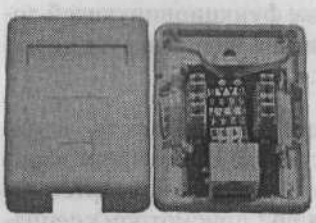


Рис. 2.13. Внешний вид розетки

На данном этапе производится большое количество разнообразных типов розеток, однако достаточно часто приходится использовать самые дешевые — внешние. Такая розетка представляет собой пластмассовый коробок, в комплекте с которым идет шуруп и двухсторонняя наклейка для того, чтобы закрепить розетку на стене. Если поверхность стены не позволяет использовать наклейку, то придется делать отверстие в стенке и прикручивать розетку с помощью шурупа. С одной стороны корпуса присутствует специальный разъем для подключения вилки RJ-45. Встречаются и розетки, имеющие в корпусе сразу два разъема — сетевой и телефонный, что позволяет несколько сэкономить пространство, которое отводится на рабочем месте под розетки.

Начинаем монтаж кабельной системы

При построении локальной сети в любом здании обычно возникает множество различных проблем. Одним из главных факторов их возникновения является высокая насыщенность зданий другими разнообразными сетями: телефонными, телевизионными, системами пожарной и охранной сигнализации, электропроводкой и т. д.

При создании локальной сети приходится сталкиваться со следующими проблемами:

- локальные сети, которые были установлены ранее, автономны и достаточно часто работают на ограниченных длинах кабельных коммуникаций;
- персонал, отвечающий за работу любой системы здания (электропроводка или пожарная сигнализация), убежден в том, что данная подсистема является основной, а потому ваши требования не стоит принимать к сведению;

- даже незначительные искажения архитектуры любой сети приводят к тратам не только на необходимые материалы, но и на доработку оставшейся части;
- установленные еще при строительстве здания коммуникации содержат множество различных кабелей, которые затруднительно использовать.

Как правило, локальная сеть монтируется в небольших офисах следующим способом. В определенном месте помещения устанавливается хаб или концентратор, который рассчитан на нужное количество портов (их может быть 8, 16 или 24). Если помещение достаточно большое, то допускается применение нескольких хабов или концентраторов. Хаб следует установить в центре всей сети, чтобы свести к минимуму использование кабеля. Кроме того, целесообразно разработать несколько вариантов монтажа локальных сетей в данном офисе: с двумя концентраторами в разных помещениях или этажах; соединение уже функционирующей локальной сети на коаксиальном кабеле с сетью, использующей витую пару, с целью дальнейшего увеличения количества пользователей и т. д.

Концентратор можно зафиксировать на стене или поставить в таком месте, где его никто не потревожит, — например, под каким-нибудь столом. Наилучшим вариантом является установка хаба в серверной комнате, где постоянно находится системный администратор. Если оборудование находится под присмотром специалиста, то риск его поломки или отключения сетевых кабелей сильно уменьшится.

После установки хабов и концентраторов их необходимо соединить между собой и проложить от них кабель к компьютерам пользователей. Иногда даже не нужно использовать настенные розетки, так как кабель от концентратора напрямую соединяется с сетевой платой компьютера. На этом этапе монтаж локальной сети завершается. Настоятельно рекомендую уложить кабель в специальные короба, иначе велик риск того, что о него кто-то споткнется и оборвет.

Желательно также отметить кабель, который приходит от рабочих станций пользователей к сетевому оборудованию. Такие отметки помогут вам разобраться с многочисленными проводами в процессе восстановления сети или же в случае ее модернизации.

Рекомендуется делать отметки не только в непосредственной близости от портов активных устройств, но и еще в некоторых местах.

Способов произведения такой отметки немало, однако многие из них несут в себе мало дополнительной информации. Между тем системному администратору необходимо знать как можно больше о сети — как минимум IP-адрес рабочей станции и имя пользователя. Разобраться в сплетении кабельных линий достаточно сложно, особенно если их прокладывал кто-то другой.

Достаточно удобными являются следующие варианты отметок.

- Бумажный ярлык. Может быть выполнен в виде флажка либо обыкновенной полоски, закрепленной на кабеле. В первом случае ярлык может мешать, если портов очень много, а во втором — прочтение может оказаться достаточно тяжелым занятием.

- Надпись на кабеле с помощью специального маркера (также крайне неудобно, однако широко распространено).
- Бирки, предназначенные специально для сетевого кабеля. Такие бирки представляют собой кусочек цветной пластмассы с бумажной вставкой. В случае смены параметров рабочей станции (например, IP) бумажку можно легко заменить. Кроме того, сами цвета бирок являются неплохими метками. Данный вариант является наилучшим, однако требует некоторых затрат.

После того как сеть смонтирована, можно приступить к настройке операционной системы компьютеров пользователей и сервера для того, чтобы локальная сеть заработала.

Если что-то не работает...

Как правило, использование локальных сетей не вызывает проблем, если все устройства правильно подключены, а компьютеры пользователей и серверы — настроены. Впрочем, иногда появляются различные неприятности. Нередко они проявляются не в сбоях и ошибках работы сети, а в снижении ее производительности.

Соответственно, важными элементами использования локальной сети являются тестирование, диагностика и профилактика.

Проблемы, возникающие при работе с сетью, можно разделить на четыре основные категории:

- неполадки в кабельной системе;
- перегрузка сети;
- некорректное функционирование сетевых протоколов;
- ошибки программного обеспечения.

Неполадки кабельной системы происходят из-за поломки какого-либо электрического или электронного сетевого оборудования. Перегрузки в сети происходят в результате того, что сетевое устройство не в состоянии справиться с удовлетворением запросов, которые к нему поступают. Ошибки сетевых протоколов влекут за собой невозможность взаимодействия сетевых устройств друг с другом из-за неправильной работы сетевых драйверов или отсутствия возможности обработки сетью пакетов определенного протокола. Ошибки в работе программного обеспечения могут появиться из-за неправильной настройки. Часто одни ошибки сети могут скрывать другие (даже более серьезные), поэтому их поиск и устранение иногда превращаются в очень сложную задачу.

Неисправности кабельной системы возникают в сетевом оборудовании (сетевые карты, коммутаторы и т. д.) или в самом кабеле и разъемах. К счастью, данную поломку несложно обнаружить. Неисправности, которые встречаются чаще всего, — отсутствие контакта в разъемах и короткое замыкание в кабеле. Найти такую неполадку помогут самые простые тестеры сети. Вид кабельного тестера изображен

на рис. 2.14. Данное устройство тестирует работу канала в одну сторону (например, от тестера к сетевой карте компьютера).

Рис. 2.14. Внешний вид кабельного тестера

Если возможно повреждение кабеля, то его можно обнаружить с использованием специального кабельного тестера. Намного сложнее определить плавающие ошибки, которые вызваны плохим контактом в соединителях. Однако и эти неполадки можно обнаружить с помощью кабельного тестера при должном внимании.

Сбои, возникающие в результате перегрузки сети и некорректной работы сетевых протоколов, самые сложные в плане обнаружения, так как носят нестабильный характер и появляются исключительно в моменты перегрузок.

Диагностировать подобные сбои можно, если проанализировать схему построения локальной сети на предмет наличия проблемных участков. Как правило, такими местами являются элементы сети со скоростью передачи 10 Мбит/с, некорректно отрегулированные маршрутизаторы и коммутаторы. Самый надежный способ нахождения состоит в последовательном отключении станций, концентраторов и кабельных трасс, а также внимательном изучении расположения линий заземления рабочих станций и серверов (особенно для сетей 10Base2).

Если ошибки в сети происходят в случайные моменты времени, которые не имеют отношения к работе пользователей, обратите внимание на уровень шума в кабеле, используя кабельный тестер. К тому же следует убедиться, что кабель не находится возле мощных источников электромагнитного излучения: высоковольтных кабелей, ламп, копиров.

Аппаратное тестирование происходит с помощью дорогостоящего оборудования — сетевых тестеров и анализаторов протоколов. Если необходим постоянный контроль за достаточно большой локальной сетью, то такие приборы необходимы.

Существуют также специальные сетевые тестеры, позволяющие обнаружить неполадку в сети. Внешний вид сетевого тестера представлен на рис. 2.15.

По количеству выполняемых функций сетевые тестеры являются промежуточным звеном между кабельными тестерами и анализаторами протоколов. Такие приборы могут измерять множество параметров, например пиковую и усредненную загруженность, долю широковещательного трафика, сбои в функционировании протоколов высших уровней. В сетях Ethernet некоторые сетевые тестеры могут вычислять число коллизий, определять адреса DLC-пакетов (с ошибками CRC, коротких и длинных), различать фрагменты пакетов, имеющих ошибки CRC и ко-

ротких пакетов. В сетях Token Ring тестеры подключаются к кольцу, внутри которого запущен процесс аварийной сигнализации, и могут диагностировать компьютер с перегруженным буфером приема, определить порядок компьютеров в кольце, засечь время прохождения маркера по сети и т. д.

Рис. 2.15. Внешний вид сетевого тестера

Определенные модели сетевых тестеров способны сохранять результаты проверки для последующего анализа с помощью специальных приложений. Для более полного анализа данные могут фильтроваться по некоторым параметрам (по протоколам и/или ошибкам).

Анализатором протоколов может быть компьютер, имеющий несколько сетевых карт и снабженный специализированным программным обеспечением. Такие машины перехватывают, расшифровывают и анализируют проходящие по сети пакеты и позволяют подробнее узнать о возможных проблемах локальной сети. С помощью специальных фильтров вы сможете узнать множество необходимой информации. Она может быть изучена для создания сводки о пакетах и получения подробного описания используемых в сети протоколов. Любой анализатор отмечает время прохождения пакета и отображает сетевые и физические адреса компьютера, который его отправил и получил. Некоторые анализаторы способны работать с протоколами, количество которых более 200.

Главный недостаток подобных устройств — дорогое программное обеспечение. Также нужны глубокие знания сетевых протоколов и достаточный опыт работы с анализаторами, так как в противном случае системный администратор будет не в состоянии разобраться с огромным объемом данных (в этом случае не всегда выручают даже фильтры) либо может некорректно понять данные, предоставленные анализатором. В случае неверной интерпретации данных можно лишь ухудшить ситуацию. Именно поэтому анализаторы протоколов используются как экспертные, если все другие возможности уже исчерпаны и не принесли ожидаемых результатов.

Портативные сетевые тестеры проще в освоении, но тоже требуют некоторого опыта работы с локальными сетями. На данном этапе их мощности достаточно, чтобы обеспечить нахождение большинства сетевых проблем.

Готовим систему для работы в локальной сети

Windows XP — одна их самых простых операционных систем с точки зрения настройки сети. Данная операционная система предоставляет возможность быстро и эффективно создавать локальные сети для дома или офиса. Она позволяет работать с сетью, просто настраивается и стабильна в работе. В самом начале конфигурирования убедитесь, что сетевая карта подключена и для нее установлены необходимые драйверы.

Как найти нужные параметры

Прежде всего рекомендуется поместить значок сетевого окружения на Рабочий стол. Для этого выполните команду Пуск ▸ Панель управления ▸ Экран ▸ Рабочий стол ▸ Настройка рабочего стола ▸ Значки рабочего стола.

Настроить сетевые параметры в Windows XP можно, используя Мастер установки сети.

Для запуска мастера нужно войти в Панель управления ▸ Сетевые подключения и нажать кнопку Установить домашнюю сеть или сеть малого офиса, после чего появится окно Мастер настройки сети (рис. 2.16).

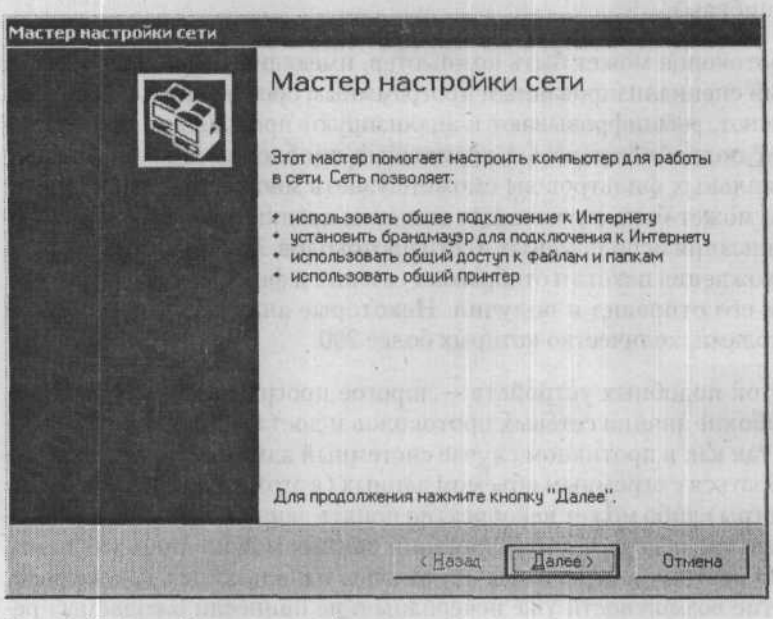


Рис. 2.16. Окно Мастер настройки сети

Нажмите кнопку Далее. На экране появятся инструкции по правильной установке сети (рис. 2.17). Тут же можно найти ссылку на справочное руководство, касающееся настройки сети.

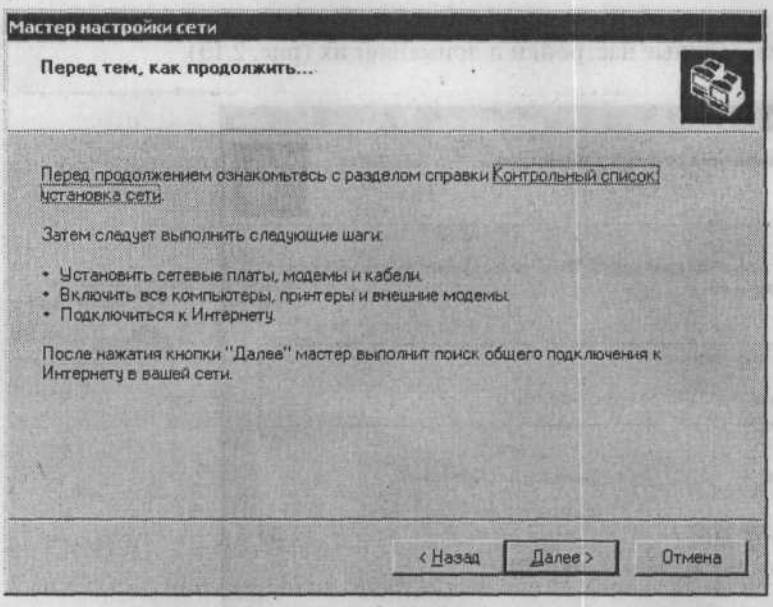


Рис. 2.17. Второе окно мастера

Теперь для всех компьютеров необходимо снять флажок Этот компьютер подключен к Интернету через другой компьютер в сети или через шлюз, после чего нажать кнопку Далее. В следующем окне можно будет ввести новое или изменить существующее название конкретного компьютера (рис. 2.18).

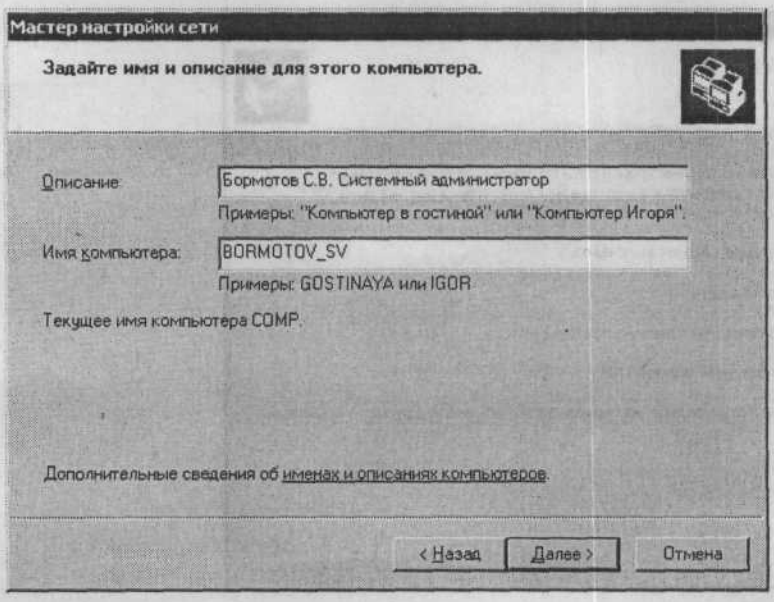


Рис. 2.18. Задаем имя и описание компьютера

Далее у вас будет возможность изменить имя рабочей группы. После этого мастер анализирует произведенные настройки и применяет их (рис. 2.19).

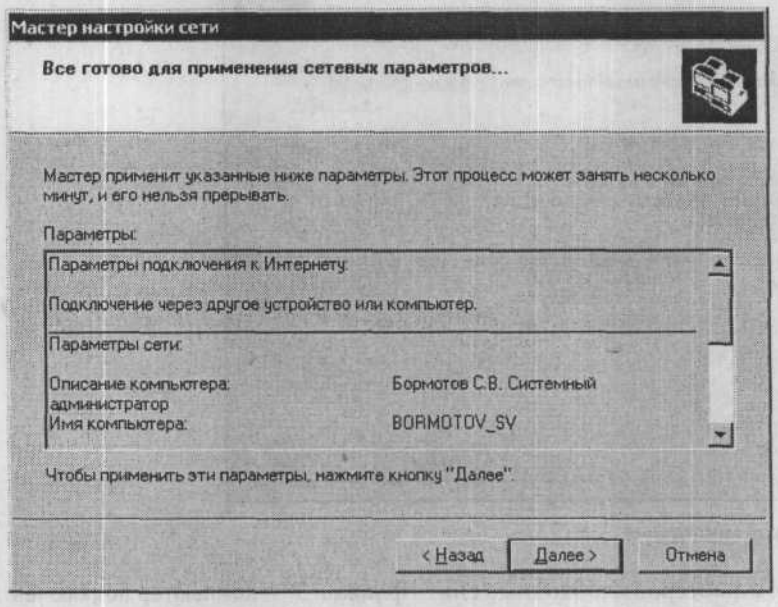


Рис. 2.19. Мастер резюмирует всё заданные настройки

В следующем окне можно создать диск установки сети (рис. 2.20).

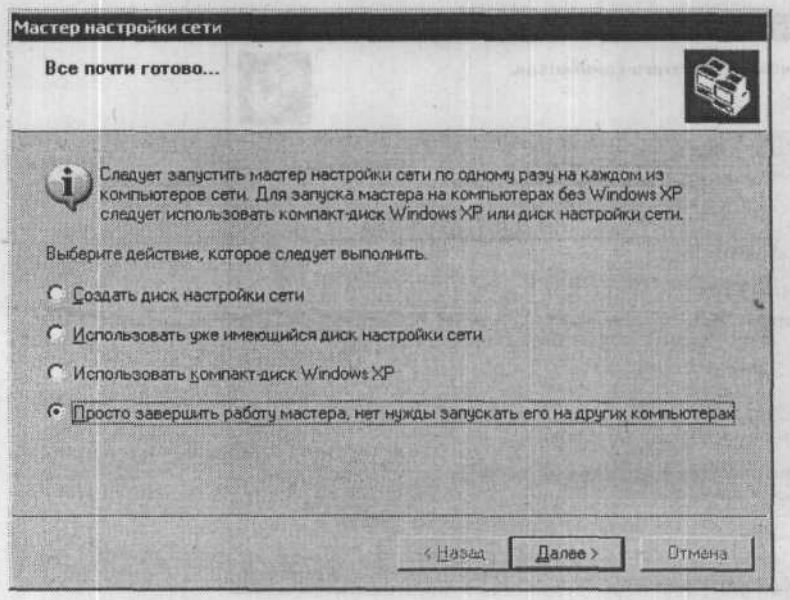


Рис. 2.20. Мастер предлагает создать диск настройки сети

Несмотря на такую возможность, лучше всего конфигурировать каждый компьютер вашей сети самостоятельно. При использовании диска иногда возникают некоторые проблемы.

Установите переключатель в положение Просто завершить работу мастера, нет нужды запускать его на других компьютерах.

Далее необходимо назначить IP-адреса каждой машине в вашей сети. Чтобы выполнить данную операцию, вам понадобится IP-адрес (Internet Protocol). IP-адрес — это индивидуальный уникальный номер каждого компьютера внутри сети. Данный адрес бывает статическим или динамическим. Динамические IP-адреса назначает DHCP-сервер данной сети, если он корректно функционирует. В небольших сетях более оправдана статическая адресация (IP-адреса заданы вручную). Данный способ более удобен, кроме того, вам не придется отдельно настраивать DHCP-сервер. Внутри локальной сети вы можете использовать IP-адреса класса C (диапазон от 192.168.0.1 до 192.168.0.254).

Первые две цифры IP-адресов компьютеров одной сети должны совпадать, третья цифра обычно равна 0 (кроме тех случаев, когда к сети подключено более 255 компьютеров), последняя цифра обозначает номер компьютера в сети. Маска подсети назначается автоматически. Если локальная сеть не имеет выхода в Интернет, то IP-адрес может быть произвольным, а главным условием будет его индивидуальность для каждого компьютера сети.

Примеры IP-адресов:

- 169.254.0.XXX;
- 128.128.0.XXX;
- 156.254.0.XXX.

Если через вашу сеть осуществляется совместный доступ к Интернету, можно будет использовать IP-адреса следующего формата: 192.168.0.XXX. Как правило, сервер получает адрес 192.168.0.1 (назначается по умолчанию).

ПРИМЕЧАНИЕ

Чтобы настраивать сетевые параметры в Windows XP, вы должны иметь права администратора.

Для присвоения IP-адреса выполните команду Пуск ▸ Панель управления ▸ Сетевые подключения. Теперь нажмите правой кнопкой мыши на значке Подключение по локальной сети и в контекстном меню выберите пункт Свойства (рис. 2.21).

В следующем окне выберите Протокол Интернета (TCP/IP) и нажмите кнопку Свойства. Сразу после этого появится окно, в котором можно настроить все нужные сетевые параметры (рис. 2.22).

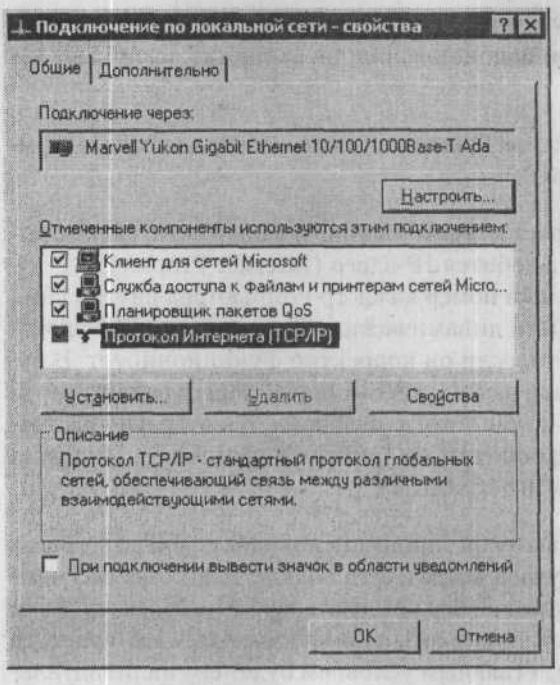


Рис. 2.21. Свойства сети

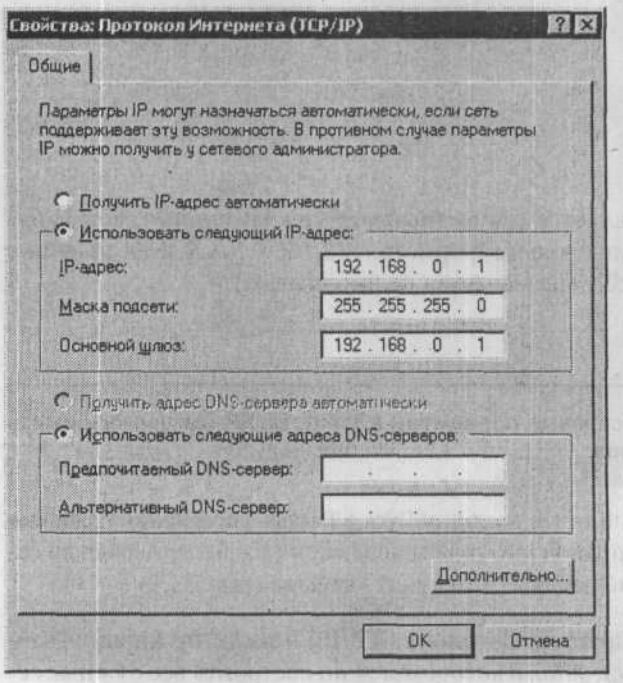


Рис. 2.22. Указываем сетевые параметры

На рис. 2.22 показана настройка IP-адреса для сервера. Теперь перейдем к настройке клиентских машин.

Настройка клиентских машин

Определите IP-адреса клиентских машин из диапазона 192.168.0.XXX. Как уже было сказано, IP-адреса внутри сети должны быть индивидуальными для каждого компьютера. Если какой-то IP-адрес будет дублироваться, операционная система уведомит вас об этом.

На рис. 2.23 видно, что одному из компьютеров, подключенных к сети, присвоен IP-адрес 192.168.0.11. Маска подсети задается автоматически, поэтому вам не придется делать это вручную.

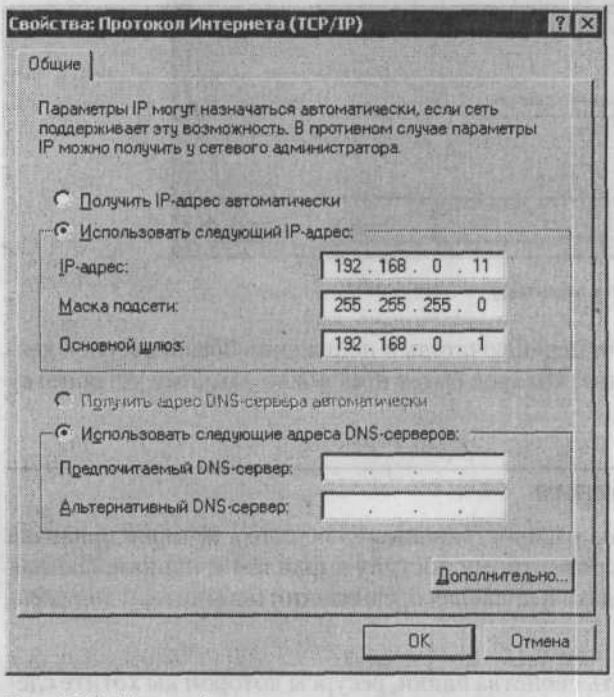


Рис. 2.23. Настройки сети на клиентских машинах

Один принтер на всех

После того как вы установите общий доступ в Интернет, можно заняться настройкой принтера для совместного использования. Сделав это, вы значительно сэкономите не только средства на покупку дополнительных принтеров, но и свое время. Установить принтер на ваш сервер можно с помощью команды Пуск ▸ Панель управления ▸ Принтеры и факсы. После того как вы установите данный принтер, щелкните на его значке правой кнопкой мыши и в контекстном меню выберите пункт Общий доступ (рис. 2.24).

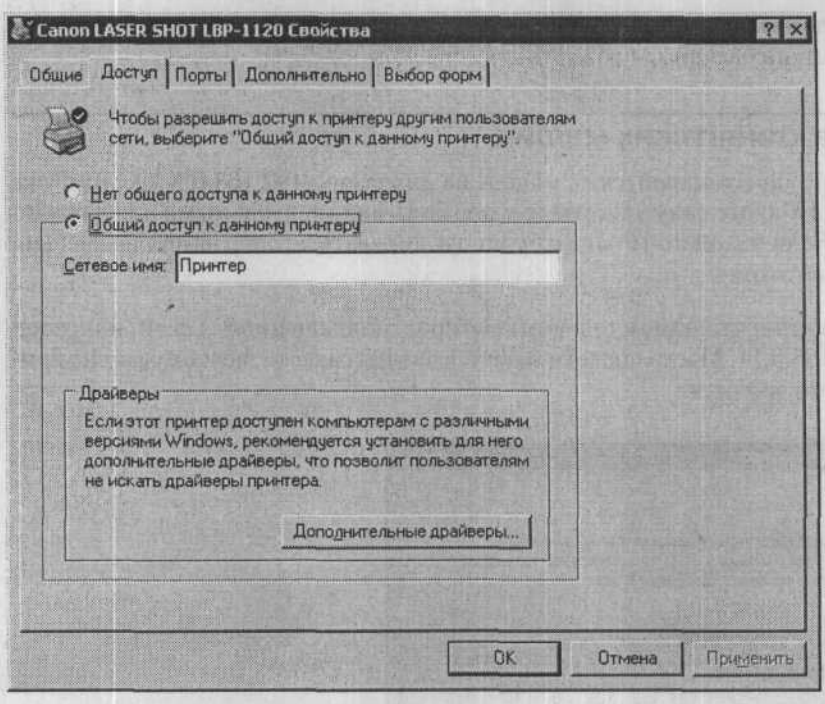


Рис. 2.24. Открываем общий доступ к принтеру

В появившемся окне установите переключатель в положение Общий доступ к данному принтеру и введите название, которое будет присвоено данному устройству в сети.

Файлы — общее достояние

Теперь пора перейти к наиболее распространенному заданию, которое призвана выполнять локальная сеть, — совместному доступу к файлам и папкам. Данная функция даст возможность создать в пределах организации библиотеку документов, шаблонов и т. д.

Прежде всего вам нужно выбрать свойства папки, ресурсы которой вы хотите сделать открытыми для пользователей сети, и перейти на вкладку, отвечающую за доступ. Внешний вид окна показан на рис. 2.25.

Здесь можно настроить следующие параметры.

- Открыть общий доступ к этой папке — дает право пользователям сети копировать файлы, однако изменить или удалить ваши файлы (а также записать свои) пользователи не смогут.
- Общий ресурс — устанавливает для папки сетевое имя, под которым она будет отображаться в сети. Обратите внимание на то, что сетевое имя не обязательно должно соответствовать реальному названию папки.

- Разрешить изменение файлов по сети — дает пользователям право копировать в эту папку свои файлы и изменять или удалять ваши. Не следует открывать полный доступ к системным папкам (Windows, Program Files) и папкам, которые содержат важные данные, так как кто-то из пользователей может случайно их удалить. Идеальный вариант — создать папку, специально предназначенную для передаваемых файлов, и открыть к ней полный доступ.

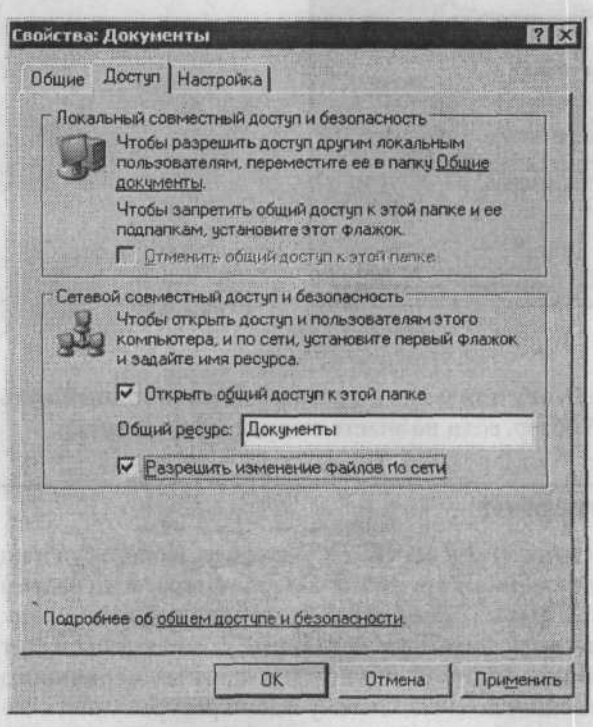


Рис. 2.25. Открываем общий доступ к файлам и папкам

В Windows XP используются два режима совместного доступа к папкам и файлам: простой и расширенный, который позволяет работать с паролями и некоторыми дополнительными функциями. Обычно для нормальной работы в малой сети полностью достаточно режима простого общего доступа к файлам и папкам, однако для более высокого уровня и контроля над доступом пользователей к информации следует включить расширенный общий доступ к файлам. Чтобы сделать это, вам следует в любом окне выбрать Сервис ▸ Свойства папки, перейти на вкладку Вид и снять флажок Использовать простой общий доступ к файлам.

Добавление сетевых дисков

Чтобы ускорить и упростить доступ к сетевым дискам, используемым наиболее часто, можно добавить их в Мой компьютер и обращаться к ним, как к обычным жестким дискам вашего компьютера. Чтобы сделать это, вам понадобится щелкнуть на значке сетевого окружения правой кнопкой мыши и в контекстном меню выбрать пункт Подключить сетевой диск (рис. 2.26).

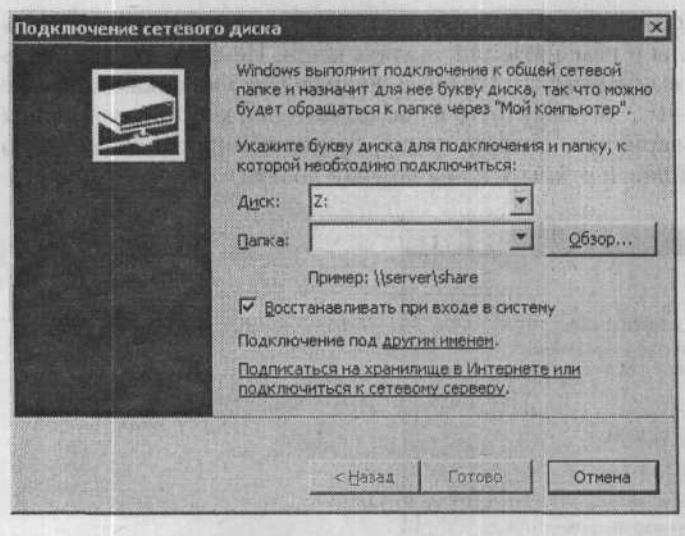


Рис. 2.26. Подключаем сетевой диск

В открывшемся окне назначьте букву для нового диска и укажите точный путь к нему (воспользуйтесь кнопкой Обзор, если не знаете точный сетевой путь).

Открываем доступ в Интернет

Теперь займемся организацией совместного доступа в Интернет. Используя наш пример, касающийся конфигурирования клиентского компьютера, мы создаем запрос к серверу с IP-адресом 192.168.0.1. Этот адрес будет использоваться как адрес шлюза (машины в сети, через которую все остальные компьютеры будут выходить в Интернет). Данный адрес следует указать и в качестве первичного DNS (DNS — это сервис, позволяющий по символьному имени ресурса узнать его реальный IP-адрес). После того как необходимые поля заполнены, нажмите кнопку OK и вернитесь в меню свойств сетевого соединения. Далее перейдите на вкладку Дополнительно. Для клиентских компьютеров флажок Защитить мое подключение к Интернету должен быть снят.

Когда компьютеры сети будут настроены, вам будет необходимо установить доступ в Интернет на сервере. После того как сервер будет успешно подключен, вам нужно зайти в папку Сетевые подключения и открыть окно редактирования свойств того подключения, которое вы хотите сделать общим. В окне Свойства нужно выбрать вкладку Дополнительно и установить флажок Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера (рис. 2.27).

Сразу после этого вы сможете настроить следующие параметры.

- Устанавливать вызов по требованию. Данный параметр касается модемных соединений. Если соответствующий флажок установлен, то пользователи сети получат возможность удаленно использовать модем для соединения с провайдером.

- Разрешить другим пользователям сети управление общим доступом к подключению к Интернету. Если данный флажок установлен, другие пользователи смогут корректировать свои права доступа к удаленным соединениям (что нежелательно).
- Параметры. Данный параметр содержит список протоколов, доступных удаленным пользователям при использовании данного соединения (например, исключительно отправка и получение электронной почты).

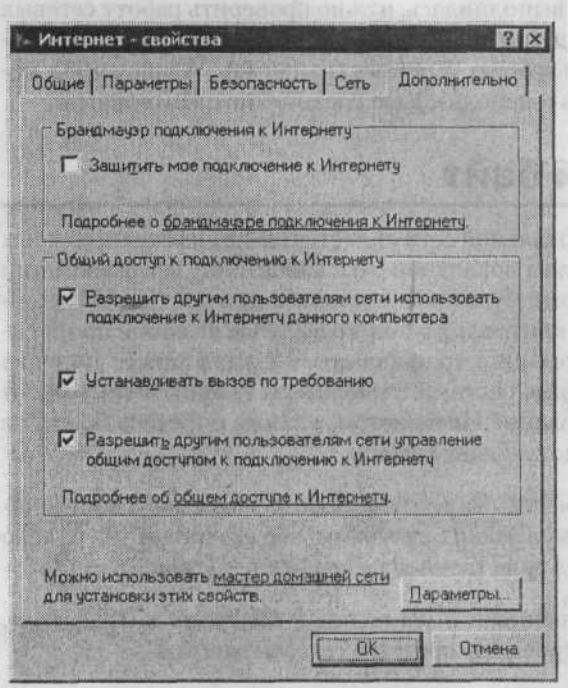


Рис. 2.27. Открываем общий доступ к Интернету

Обратите внимание на флажок Защитить мое подключение к Интернету. Его установка разрешит использование брандмауэра Windows, представляющего собой систему защиты в виде своеобразного барьера между внутренней и внешней сетями. Безусловно, мощность брандмауэра не может сравниваться со специальными аппаратными межсетевыми барьерами, однако и он способен защитить ваши данные от несанкционированного доступа.

Нажмите кнопку OK для сохранения всех сделанных изменений. После этого можно начинать проверку работы сети, войти в Интернет с сервера и клиентских компьютеров.

Если возникли проблемы

Если доступ к сети отсутствует, проверьте правильность соединения всех кабелей и наличие питания у концентратора или маршрутизатора. Если вы все сделаете правильно, то при подключении сетевого кабеля к сетевой карте на Панели задач

Windows появится уведомление о подключении сетевого кабеля на соответствующей скорости в 10 или 100 Мбит/с.

Если данное уведомление не отображается, нужно посмотреть, активна ли функция отображения индикатора в настройках сети, и проверить правильность подключения и состояние кабеля. После этого выполните команду Пуск ▸ Выполнить и в появившемся окне в соответствующее поле введите `ping 192.168.0.1`. Если команда по каким-то причинам не выполнилась, нужно проверить работу сетевых плат и концентратора. Одной из причин подобных неприятностей может быть инсталляция Windows XP на другую версию Windows (например, Windows 98), которая уже имела настроенную сеть и использовала соединение с Интернетом.

Сосчитаем каждый байт

Учет трафика (потока данных) в локальной сети является одним из самых важных заданий. Как правило, пользователям локальной сети какой-нибудь организации определяют лимит трафика, который будет расходоваться при доступе к Интернету. Если доступ к Интернету не контролируется, то в случае высокой пропускной способности сети и дорогостоящего трафика организация может понести колоссальные убытки. Разнообразные системы слежения за трафиком позволяют контролировать затраты на пользование Интернетом, а также определять, кто из пользователей наиболее активно потребляет трафик.

Программы, которые позволяют реализовать эту функцию, называются биллинговыми системами. На данный момент таких программ достаточно много, однако одной из самых лучших считается отечественная разработка — Traffic Inspector.

Программа Traffic Inspector обеспечивает полноценный контроль за трафиком, разграничивает доступ и имеет встроенные средства сетевой защиты.

Данная утилита не бесплатна, однако вы сможете бесплатно испытать ее в течение 30 дней. Ключ для пробной версии можно получить на сайте разработчиков.

Программа имеет несколько основных элементов: сервер, консоль управления и клиентский агент. Серверная часть (которую необходимо инсталлировать на сервер общего доступа в Интернет) работает только под управлением Windows 2000/XP/Server 2003, пользователи могут использовать любую операционную систему.

СОВЕТ

На компакт-диске, прилагаемом к книге, в папке ch02\Traffic Inspector v 1.1 находится последняя версия программы Traffic Inspector.

Следующий элемент программы — клиентский агент — необходимо установить на компьютеры клиентов. Его задача состоит в определении конкретного пользователя с помощью логина и пароля (используется шифрование данных). Кроме того, клиентский агент отображает лицевой счет данного пользователя и автоматически настраивает Internet Explorer.

Система достаточно просто инсталлируется, конфигурируется и управляется, в ней присутствует возможность удаленного управления. Для работы с этим приложением не требуется специалист: человек, способный установить Windows и настроить сеть, без затруднения сможет произвести конфигурирование данной программы.

Traffic Inspector включает достаточно функциональную систему биллинга, позволяющую не только создавать финансовый отчет по действиям конкретного клиента и разрабатывать различные тарифные планы, но и применять режимы блокировки, работы в кредит и произведения оплаты с помощью специальных карточек.

Единственное замечание, касающееся процесса инсталляции данной программы: когда вам предложат выбрать тип установки, укажите значение Сервер.

После завершения установки запустите консоль управления программой для произведения необходимых настроек. Окно консоли показано на рис. 2.28.

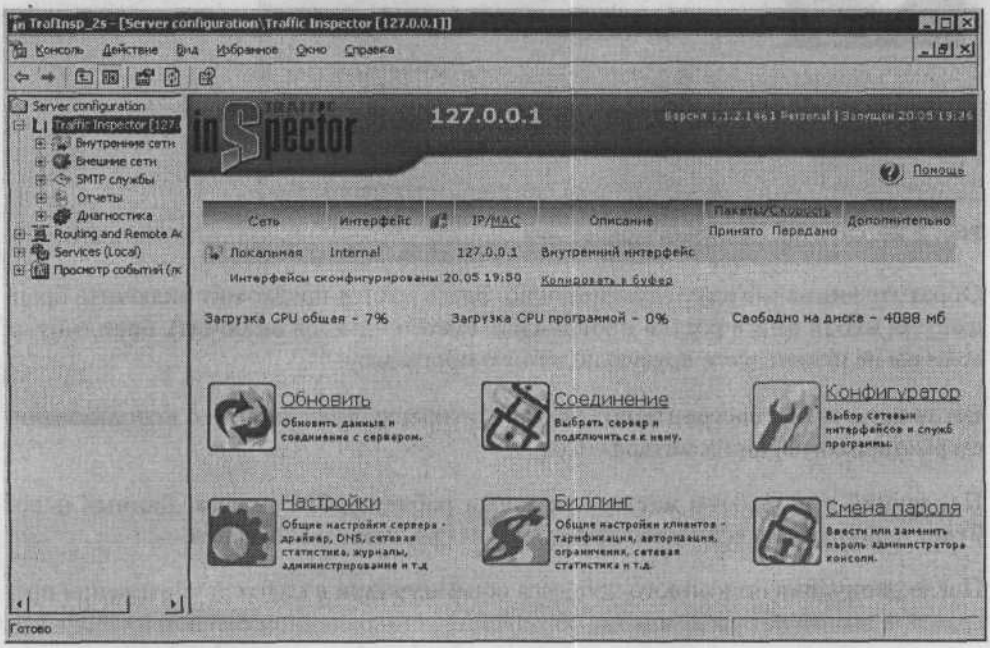


Рис. 2.28. Консоль управления программой

Чтобы произвести настройку сервера, нажмите кнопку Конфигуратор. Начнется работа соответствующего мастера (рис. 2.29).

Сначала мастер предложит указать топологию вашей сети. Исходя из того, что на сервере может быть использовано как внешнее, так и внутреннее соединение с сетью, вам нужно будет выбрать соответствующее значение.

Далее нужно указать внешнее сетевое подключение, которое будет использоваться для соединения с Интернетом. Следующий этап — конфигурирование

прокси-сервера, который создают программа и сервер статистики. Весь процесс будет состоять в том, что вам нужно будет указать перечень портов, с которыми они будут работать. Как правило, лучше оставить значения, предложенные по умолчанию.

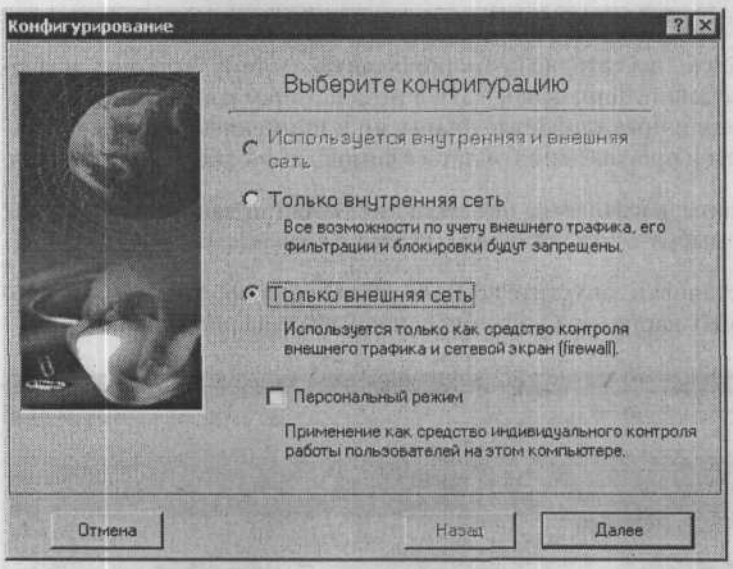


Рис. 2.29. Окно мастера конфигурирования

Обратите внимание на следующее окно. Здесь мастер предложит включить брандмауэр, входящий в состав программы. Рекомендуется включить брандмауэр, если вы не используете другую подобную программу.

Вы можете также настроить получение и отправку информации с использованием различных внешних интерфейсов.

Последний этап работы мастера включает работу SMTP-шлюза. Данный шлюз будет использован, если у вас присутствует свой почтовый сервер.

После окончания описанного процесса конфигурации в консоли управления программой возникнет уведомление об успешно установленном сетевом интерфейсе.

Далее можно заняться добавлением клиентов. Для этого откройте в меню консоли раздел Traffic Inspector, а в нем выберите пункт Внутренние сети. Шелкните на надписи Добавить клиента.

Здесь вы сможете осуществить различные настройки клиента: имя, процесс авторизации и аутентификации, ограничения по скорости и т. п. Данные настройки хорошо упорядочены, поэтому разобраться с ними сможет даже начинающий.

У вас будет возможность объединить клиентов в группы, чтобы применять сделанные изменения для всех пользователей, входящих в конкретную группу.

Программа разрешает выполнять аутентификацию исходя из IP- или MAC-адреса клиента, при этом нет необходимости устанавливать какие-либо дополнения на компьютер клиента. Однако существует другая проблема: пользователь может изменить свой IP, используя специально разработанные приложения, что позволит ему избежать учета трафика. В такой ситуации более надежной является аутентификация с использованием логина с паролем или же учетной записи домена. Предположим, что контроллер домена в нашем случае отсутствует, поэтому мы будем использовать первый вариант идентификации.

Любой пользователь может загрузить клиентскую часть приложения с локального сервера программы, который находится по адресу http.//192.168.0.1:8080.

Вы можете инсталлировать клиентские агенты самостоятельно или использовать специальную утилиту Traffic Inspector Client Remote Installer. После установки агента нужно указать адрес сервера в локальной сети, после чего агент сможет учитывать трафик, потребленный пользователями. Окно клиентского агента показано на рис. 2.30.

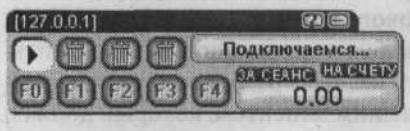


Рис. 2.30. Окно клиентского агента

Программа Traffic Inspector позволяет значительно ограничивать доступ к Интернету различных пользователей. Вы сможете ограничить доступ к некоторым сайтам или запретить выход в Интернет в определенные промежутки времени. Чтобы отдельный пользователь не занимал весь внешний канал, в программе можно ограничить скорость доступа для каждого клиента. Рекомендуется не предоставлять неограниченный доступ для рядовых пользователей. Не стоит исключать возможность заражения компьютера вирусом, который может стать причиной потребления огромных объемов трафика. Поэтому наилучшим вариантом будет выставление лимитов потребления трафика, после которых будет производиться автоотключение.

Удобно и то, что все управление происходит через консоль MMC с помощью профилей клиентов и их групп. Нужно обратить внимание на HTTP/SSL/FTP/SOCKS прокси-сервер, осуществляющий кэширование данных, что позволяет значительно сэкономить трафик. Кроме того, каждый клиент может сам устанавливать параметры использования кэширования и данных из кэша.

Программа действительно стоит того, чтобы быть приобретенной. Очень удобной является возможность удаленного управления сервером приложения с использованием встроенной консоли MMC. Такая функция позволит вам корректировать настройки и просматривать статистику потребления трафика с рабочего места администратора, не используя сервер.

Война со спамом

Спам — нежелательные сообщения (как правило, рекламного характера), приходящие на электронные почтовые ящики пользователей. Такая корреспонденция отнимает время и добавляет объем использованного трафика в вашей сети. Среди таких сообщений (а их может быть несколько сот в день) теряются важные письма. Кроме того, спам занимает в почтовых ящиках дополнительное место, которое часто ограничено.

Полностью избавиться от этой проблемы практически невозможно, однако использование специального программного обеспечения способно уменьшить объемы получаемого спама. Одной из лучших программ, борющихся с нежелательной корреспонденцией, считается SpamPal.

SpamPal — гроза для спама

Программа SpamPal представляет собой целую систему, задачей которой является сортировка почты для отделения спама от прочих сообщений. Программа помещает спам в специальную папку вашего почтового клиента, делая на подобных сообщениях пометку «спам». В дальнейшем у вас будет возможность ознакомиться с отфильтрованными сообщениями и удалить их. Программа является промежуточным звеном между почтовым сервером и вашим клиентом, который должен иметь возможность сортировать входящую почту по папкам.

ПРИМЕЧАНИЕ

Программу SpamPal можно свободно скачать на сайте производителя http://www.SpamPal.org.uk. Программа также находится на компакт-диске, прилагаемом к книге, в папке ch02\SpamPal. Там же можно найти руководство к программе на русском языке и несколько дополнительных модулей к программе.

Как работает программа

В процессе работы программа использует списки DNSBL (DNS Black Lists — «черные списки» Интернета) для сортировки электронных писем. Подобные списки состоят из набора адресов Интернета, которые очень популярны среди спам-рассылок.

Любое сообщение будет проанализировано на предмет принадлежности к спискам DNSBL. Если будет найдено соответствие, письмо получает метку, которая свидетельствует о возможной принадлежности данного сообщения к спаму. Почтовый клиент нужно настроить так, чтобы все письма с меткой отправлялись в специальную папку. Это позволит отделить нежелательные письма от нужной корреспонденции. Обратите внимание на то, что письма, получившие метку, не удаляются, так что вы можете впоследствии разобраться с ними подробнее.

Требования к оборудованию

Для установки программы необходимо следующее оборудование:

- установленная операционная система Windows 95/98/Me/NT/2000/XP;
- поддержка протокола POP3;
- стандартный почтовый клиент (Outlook Express, Microsoft Outlook, The Bat! или Eudora).

Установка

Инсталляция программы не отличается от установки большинства Windows-программ. Вам необходимо запустить программу инсталляции, согласиться с условиями лицензионного соглашения и нажимать кнопку Next до окончания установки. После установки SpamPal будет запущен, а его значок отобразится на Панели задач рядом с часами.

Далее вам потребуется настроить почтового клиента таким образом, чтобы он получал электронные письма из данной программы, а не с почтового сервера. Для этого вам нужно установить следующие значения настроек почтового клиента:

- Incoming Mail Server (Сервер входящей почты) или POP3 server (Сервер POP3);
- POP3 Username (Имя пользователя POP3) или Account Name (Имя почтового ящика).

Нужно добавить значение строки POP3 server к значению строки Username (после него), вставив между ними значок @. Например, если имя пользователя будет `sergey`, а адрес POP3-сервера — `pop3.mail.ru`, то необходимое значение будет таким:

```
sergey@pop3.mail.ru
```

Если имя POP3-сервера уже имеет символ @, поступайте точно так же, как в предыдущем случае, так как SpamPal умеет работать с именами, содержащими два знака @.

Если вы используете продукцию Netscape, то вместо символа @ вам нужно будет вставить символ % (например, `sergey%pop3.mail.ru`).

После этого измените значение поля POP3 server на localhost. Если почтовый клиент не разрешает назначить такое имя, вставьте IP-адрес «обратной петли» — 127.0.0.1.

ПРИМЕЧАНИЕ

Если ваш почтовый сервер использует отличный от стандартного (110) порт, вам следует добавить его в самый конец имени сервера (в поле Username, используя двоеточие). Например, в случае использования 8090 порта строчка примет такой вид: sergey@pop3.mail.ru:8090.

Попробуйте получить почту. Если никаких проблем не возникло, приступайте к настройке самого почтового клиента. Если вы получите уведомление об ошибке, то проверьте, указано ли в названии POP3-сервера имя `localhost` и правильно ли указан номер порта.

Далее вам следует создать и настроить почтовый фильтр, чтобы все сообщения, которые SpamPal считает спамом, перемещались в отдельную папку вашего клиента.

Для начала создайте папку, в которую будут перемещаться подозрительные сообщения.

Далее создайте новый фильтр входящей почты, который будет реагировать на специальный заголовок X-SpamPal: с содержимым SPAM. Настройте данный фильтр таким образом, чтобы подозрительные письма перемещались в папку, предназначенную для спама. Если ваша программа для работы с почтой не способна фильтровать служебные заголовки, то следует установить фильтрацию по полю Subject (Тема) на слово **SPAM**.

ПРИМЕЧАНИЕ

Некоторые антивирусы способны перехватывать почту для проверки на наличие вирусов таким же образом, как это делает SpamPal. Однако SpamPal способен корректно работать при наличии в системе такого антивируса, не конфликтуя с ним. Программа будет перехватывать почту раньше антивируса, проверять ее на признаки принадлежности к спаму и передавать антивирусной программе только те письма, которые прошли проверку.

Запускаем программу SpamPal

Сразу после успешной установки SpamPal помещает свой ярлык в автозагрузку и появляется на Панели задач в виде розового зонта, напоминая о своей работе.

Каждый раз при загрузке новой почты SpamPal будет проверять сообщения на предмет наличия спама, а фильтры почтовой программы поместят спам в определенную вами папку.

Если вдруг SpamPal отнесет к спаму нужное письмо, вы можете самостоятельно занести данный адрес в «белый список», который можно редактировать в параметрах программы. Для этого щелкните правой кнопкой мыши на значке программы, расположенной на Панели задач, и выберите пункт В Белый Список. После этого письма данного адресата будут беспрепятственно попадать в ваш компьютер.

Если щелкнуть на значке правой кнопкой мыши, то появится контекстное меню, состоящее из следующих пунктов: Помощь, В Белый Список, В Черный Список, Статус, Настройки, Выключить, Выход. Окно настроек показано на рис. 2.31.

Сначала вы обратите внимание на то, что получение новых сообщений происходит медленнее. Это происходит из-за того, что SpamPal должен сверять адрес отправителя со списками DNSBL на предмет наличия соответствий. Несмотря на это,

с помощью функции Авто-белый список SpamPal быстро развивается. Адресаты, с которыми вы регулярно обмениваетесь сообщениями, добавляются в Авто-Белый Список, и программа не сверяет адреса со списками DNSBL. Соответственно, скорость работы программы напрямую зависит от того, как долго она у вас установлена.

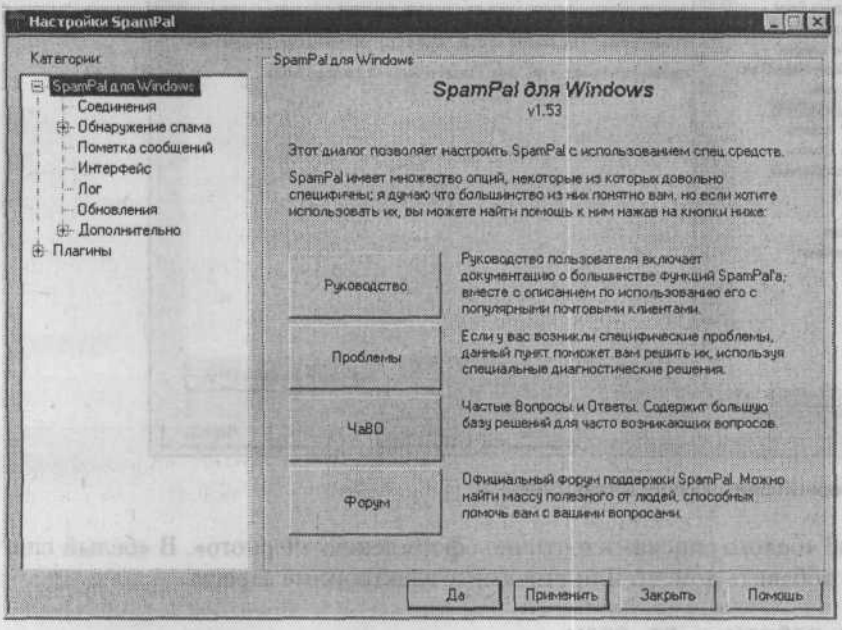


Рис. 2.31. Окно настроек программы

Настройка программы

Вы также можете занести определенный адрес в «черный список» (рис. 2.32).

Те письма, которые будут приходить с адресов, входящих в «черный список», будут считаться спамом в любом случае. В «черном списке» возможно наличие незаполненных строк. Строки, в начале которых расположен значок #, считаются комментарием и не учитываются при работе программы:

```
#Все эти адреса точно принадлежат спамерам!
spam@spammer.com
spam-robot@spammers.com
spammer@spam.edu
```

Чтобы установить адреса по маске, нужно вставить символ *:

```
#Все письма с этого домена — спам!
*@spam.com
```

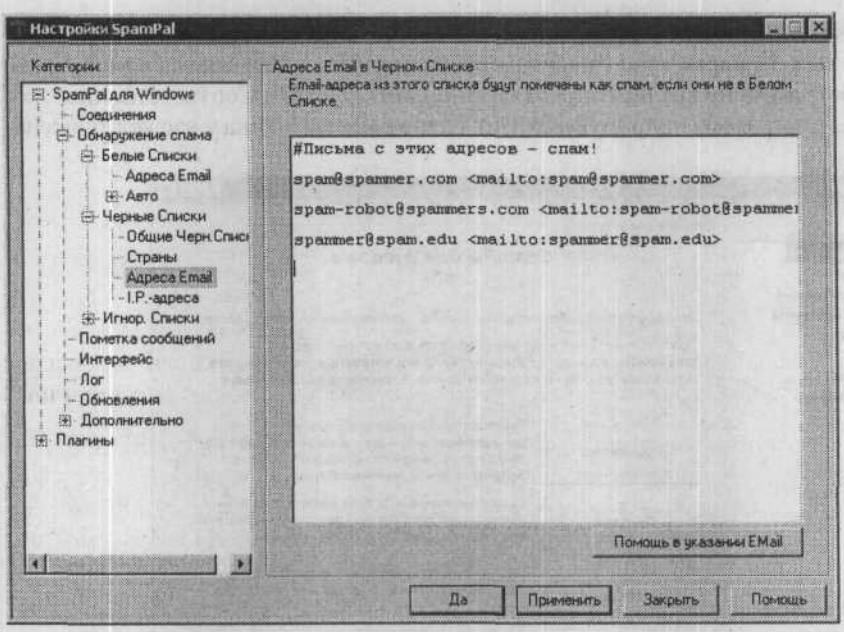


Рис. 2.32. «Черный список» программы SpamPal

Оформление «белого списка» идентично оформлению «черного». В «белый список» можно добавить домены или отдельные электронные адреса:

```
#Письма с работы - не спам

*@belgorodenergo.ru
```

Компоненты «белого списка» более важны, чем «черного». Это означает, что вы можете добавить в «черный список» весь домен `*@yahoo.com`, а в «белом» разрешить прием писем от некоторых клиентов данного домена.

Программа SpamPal способна автоматически составлять «белый список» адресов электронной почты, включая в него адреса, с которыми вы часто обмениваетесь письмами в течение определенного количества дней.

Обновление

Для правильной и эффективной работы программе SpamPal необходимо периодически обновлять списки DNSBL (наличие новых списков проверяется программой время от времени).

Служебный заголовок X-SpamPal

Ко всем сообщениям, которые прошли проверку, программа SpamPal добавляет заголовок X-SpamPal в самом окончании служебной зоны. В данной зоне заголовка сообщения прописаны адреса отправителя и получателя, все серверы, через кото-

рые прошло данное письмо в процессе транспортировки, дата отправки, тема и прочая информация. Как правило, данный заголовок расположен в начале письма. Строка X-SpamPal будет занимать в списке самое последнее место.

Для разрешенных сообщений заголовок примет следующий вид:

```
X-SpamPal: PASS
```

Письма, которые программа считает спамом, будут помечены так:

```
X-SpamPal: SPAM
```

Если вы хотите ознакомиться с заголовком X-SpamPal, нужно включить в вашем почтовом клиенте показ заголовков (служебной зоны) электронных сообщений.

В процессе настройки почтовой программы для совместной работы с SpamPal фильтр должен ориентироваться на строку SPAM в заголовке X-SpamPal. Как правило, такой фильтрации достаточно. Иногда происходят ситуации, когда нужно выяснить причину, по которой письмо было причислено к спаму. Далее рассмотрим некоторую дополнительную информацию о компонентах заголовка X-SpamPal.

Письма, которые признаны спамом, имеют следующий заголовок X-SpamPal:

```
X-SpamPal: SPAM <list code> <I.P. address>
```

Здесь `list code` — код списка DNSBL, с которым совпал адрес отправителя. `IP-адрес` — адрес, который нашелся в DNSBL. Как правило, данный адрес находится в служебной зоне заголовков письма в районе строк Received. Например, это может выглядеть следующим образом:

```
X-SpamPal: SPAM ORDB 174.22.36.2
```

Сообщения, которые отфильтрованы на основе «черного списка»:

```
X-SpamPal: SPAM BLIST FROM
```

Сообщения, адресаты которых относятся к «белому списку», получат следующую метку:

```
X-SpamPal: PASS WLIST FROM
```

Сообщения, допущенные в соответствии с «Авто-белым списком»:

```
X-SpamPal: PASS A-WLIST FROM
```

При невозможности определения статуса сообщения из-за превышения временного лимита запроса к службе DNSBL заголовок будет выглядеть так:

```
X-SpamPal: PASS TIME-OUT
```

Если такие превышения появляются часто, нужно увеличить интервал ожидания в параметрах приложения.

Параметры командной строки

Программа SpamPal сохраняет файлы со своими настройками в каталоге профиля пользователя Windows. Если профиль отсутствует, то конфигурационные файлы будут находиться в той директории, куда вы установили программу. У вас есть возможность изменить данные настройки, указав нужную папку с помощью командной строки, используя ключ `-configdir`. Если указанной папки не существует, то она будет создана. Например:

```
SpamPal.exe -configdir C:\config\SpamPalConfigDir
```

Если вам необходимо запустить на одном и том же компьютере две или более копии программы SpamPal (например, если нужно проверять сразу два разных порта с разными конфигурациями), то нужно применить следующий ключ — `allow_multiple_instances yes`:

```
SpamPal.exe -allow_multiple_instances yes
```

Если вам необходима только одна запущенная копия SpamPal, однако вы не желаете видеть уведомления об ошибках при попытке запуска еще одной копии, то нужно применить ключ `-suppress_multiple_instances_warning yes`:

```
SpamPal.exe -suppress_multiple_instances_warning yes
```

Это может быть использовано при написании сценариев для автоматического исполнения.

Вы можете убрать значок программы с Панели задач, используя ключ `-trayicon none`:

```
SpamPal.exe -trayicon none
```

Обратите внимание, что в этом случае вы не сможете изменять настройки программы. Данный ключ полезен, если вам нужно ограничить возможность пользователей изменять параметры работы программы. Чтобы возвратить возможность изменения настроек программы, следует завершить ее работу с помощью Диспетчера задач Windows, после чего запустить ее снова без использования указанного ключа.

ГЛАВА 3 Курс молодого администратора

- «Ящик с инструментами» для системного администратора
- Службы, с которыми вам предстоит познакомиться
- Реестр — сердце Windows
- Заставим Windows «летать»
- Безболезненное восстановление

Данная глава поможет изучить основные средства и приемы администрирования Windows. Вы узнаете о службах операционной системы Windows XP и научитесь управлять ими, а также работать с реестром и вносить в него необходимые изменения. Кроме того, вы познакомитесь с некоторыми приемами оптимизации работы операционной системы и ее «тонкой» настройки.

«Ящик с инструментами» для системного администратора

Администрирование сети в организации — непростая задача, отнимающая много сил и времени.

Администратору приходится решать проблему за проблемой, стараясь организовать корректную работу сервера и рабочих станций. Как правило, в больших организациях обслуживанием локальной сети и входящих в нее устройств занимаются несколько человек или даже специальный отдел IT. Несколько человек из такой службы специализируются на ремонте и установке «железа», один или два — на серверах и локальной сети, еще несколько устанавливают и конфигурируют программное обеспечение на клиентских компьютерах, а оставшиеся настраивают сетевые сервисы.

В небольших организациях все эти заботы ложатся на плечи одного человека, которому приходится разбираться и с операционными системами, и с прикладными программами, и с сетью. Кроме того, администратору приходится выполнять обслуживание оргтехники и мини-АТС, если она присутствует.

Администратор устраняет сбои в работе программного обеспечения, обновляет установленные программы и изменяет пароли, если пользователи вдруг их забудут. В такой ситуации просто не остается времени на то, чтобы разрабатывать новые схемы усовершенствования локальной сети и повышения ее производительности.

Если грамотно подобрать инструменты, которые предназначены для решения различных задач, связанных с сетевым администрированием, можно значительно упростить реализацию многих функций сетевого администратора, что позитивно скажется на работе всей сети. Например, определенные задачи администрирования можно передать конечным пользователям, а некоторые конфигурационные инструменты, входящие в операционную систему, позволяют автоматизировать большую часть процессов, связанных с управлением программным обеспечением и настройками системы, а также устранением разнообразных сбоев.

При работе с локальной сетью администратор решает следующие задачи:

- создание и изменение учетных записей пользователей, смена паролей;
- управление принтерами и обслуживание прочей оргтехники;
- обслуживание сетевого оборудования — концентраторов, маршрутизаторов, мостов и шлюзов;

- решение проблем, возникающих в процессе установки соединения между рабочими станциями и серверами сети;
- обеспечение комфортной работы удаленных пользователей и устранение возможных проблем, связанных с работой локальной сети;
- настройка рабочих станций локальной сети, установка и удаление необходимых программ;
- ремонт и обслуживание различных устройств, входящих в состав рабочих станций и серверов;
- конфигурирование общего доступа и настройка полномочий для доступа пользователей к файлам и службам сервера;
- обеспечение стабильной работы необходимых сетевых служб;
- просмотр, изучение и очистка журналов системного протоколирования.

Конечно, системный администратор не сможет обойтись без специальных утилит, позволяющих корректировать некоторые проблемы, возникающие в процессе работы Windows XP.

Прежде всего вам потребуются:

- установочные компакт-диски всех операционных систем, которые используются компьютерами сети;
- набор обновлений Windows, а также исправления всех критических ошибок;
- загрузочный диск (понадобится, если запустить операционную систему невозможно);
- разные полезные программы (например, приложения для работы с образами жестких дисков);
- программы, позволяющие обнаружить сбои в работе компьютера (диагностические утилиты, системные тесты).

Чтобы управлять дисками, службами и ресурсами локальной сети, в Windows XP присутствует набор программных средств администрирования, которые представлены в виде программных модулей, добавляющихся в консоль управления (Microsoft Management Console, MMC).

Еще одно их название — оснастки MMC. MMC является своеобразной оболочкой для запуска данных модулей (оснасток). Окно консоли управления показано на рис. 3.1.

Чтобы запустить консоли MMC, выполните команду Пуск ▸ Выполнить. В появившемся окне в соответствующее поле введите команду mmc и нажмите OK. Запустится консоль управления MMC.

У вас будет возможность создавать свои собственные консоли, в которые будут входить часто используемые средства администрирования. Более подробно на создании и использовании консолей мы остановимся несколько позднее.

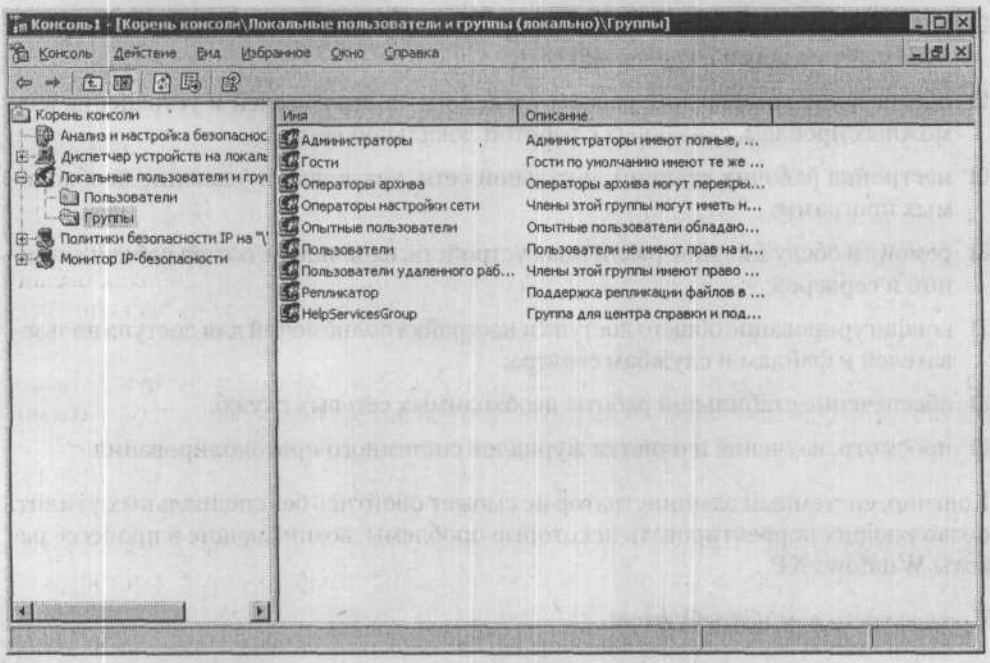


Рис. 3.1. Окно консоли MMC

Главное — составить план

Нередко системные администраторы сталкиваются с проблемами в процессе решения определенной задачи, вместо того чтобы заранее предусмотреть их появление и хорошо подготовиться, что позволило бы значительно сэкономить силы и время. К тому же, если приходится решать критические проблемы, времени на всевозможные эксперименты может просто не остаться.

Чтобы максимально ускорить процесс решения проблемы, нужно хорошо подготовиться еще до ее появления — провести анализ и планирование рабочей среды организации, разработать планы при необходимости экстренного устранения неполадок.

Необходимо заранее выяснить следующую информацию.

- Список оборудования, которое используется на рабочих станциях и серверах вашей сети, а также перечень установленного программного обеспечения. Обладая подобным описанием аппаратного и программного обеспечения вашей локальной сети, вы сможете достаточно оперативно решать разнообразные проблемы, предвидеть возможные отказы на конкретной конфигурации и возникновение сбоев.
- Подробное описание набора программного обеспечения, которое установлено на рабочих станциях пользователей. Чтобы упростить процесс администрирования, нужно составить несколько стандартных конфигураций компьютеров

сети, в соответствии с которыми будут настраиваться все компьютеры. Если вы будете разрабатывать стандартные конфигурации, то сможете сократить время, которое требуется на установку и конфигурирование новых компьютеров (значительно упрощается процесс клонирования операционной системы), обслуживание отдельных систем, замену комплектующих, обновление набора программ и драйверов.

- Составленный и заверенный руководством договор о допустимом уровне скорости работы основных служб сети, что позволит вам отвергать большинство претензий о невысокой скорости передачи данных. Если понадобится расширить сеть или увеличить ее пропускную способность, данное соглашение всегда можно изменить.
- План восстановления информации в случае сбоя. Прежде всего нужно выяснить порядок восстановления данных: что является первоочередным, а что может подождать. Достаточно часто администраторы разрабатывают план восстановления данных на сервере, однако упускают из виду рабочие станции, где часто хранится более важная информация.
- Результаты мониторинга производительности сервера и сетевых служб, а также общей производительности сети. Изучив эту информацию, вы сможете вовремя определить нехватку ресурсов сервера и обновить необходимое оборудование.
- План обучения дополнительного персонала, который занимается обслуживанием сети.
- Стратегический план, который будет объединять подробные данные из других планов. Данный план является долгосрочным и направлен на развитие и усовершенствование сети.

Создание стратегического плана является важным этапом в работе системного администратора. Если у вас будет стратегический план и данные наблюдения за производительностью сети и сервера, то вам будет значительно проще обосновать руководству необходимость дополнительных затрат на обновление оборудования. Хорошо составленный план восстановления информации в случае сбоя позволит сразу перейти к восстановлению работоспособности сети.

План наблюдения за локальной сетью — важный элемент любой надежной сетевой среды. В процессе составления такого плана нужно определить, какие именно сетевые службы и устройства наиболее важны для работы вашего предприятия. К этой группе нужно отнести устройства, службы и приложения, сбои в которых (или их недоступность) могут стать причиной нарушений в работе всей организации. Постоянный мониторинг подобных устройств и приложений позволит вовремя предупредить подобные дорогостоящие сбои.

Полученную статистику следует анализировать через призму бизнес-целей вашего предприятия. Например: «В прошлом году информация о продажах в системе "1С:Предприятие" была открыта для сотрудников предприятия в течении 99,7% рабочего времени, что позволило сократить затраты на обслуживание клиентов и повысить его качество». Такой вид представления отчетности будет более понятен руководству.

Несколько советов, к которым стоит прислушаться

Если вы не хотите значительную часть личного времени заниматься устранением неполадок, которые возникают в процессе эксплуатации локальной сети, то вам стоит обратить внимание на следующие советы.

- Регулярно производите обновления программного обеспечения и операционной системы. Не забывайте, что программа, в которой присутствует какая-то ошибка, является отличной лазейкой для хакера или вирусной атаки. Однако не стоит делать обновление самоцелью: производите его, только если это действительно необходимо (например, на сайте разработчика появилась информация, что новая версия исправляет очередную критическую ошибку).
- Отключайте ненужные службы и удаляйте неиспользуемое программное обеспечение. Кроме того, желательно закрыть все порты, которые не нужны для нормальной работы сети.
- Постарайтесь разобраться в работе операционной системы и ее сервисов. Вы должны понимать, что и как происходит в вашей системе — в какой момент запускаются определенные сервисы, как узнать, откуда данный сервис был запущен и почему он был запущен именно в этот момент. По возможности следует активировать протоколирование всех действий пользователей.
- Не пренебрегайте сетевыми средствами защиты. Самый эффективный способ борьбы с взломом — это его предупреждение. Именно поэтому использование брандмауэра (программного или аппаратного) является обязательным требованием! Предположим, что вы управляете веб-сервером. Запретите передачу данных со всех портов, кроме 80. Теперь даже если на вашем сервере окажется троянский конь, он не сможет отправить собранные данные, что значительно усложнит задачу потенциальному злоумышленнику. Кроме пассивной защиты — брандмауэра — существует и активная, которая основана на системах обнаружения атак, которые могут уведомить администратора о потенциальной атаке.
- Для управления группами пользователей нужно использовать групповую политику, чтобы контролировать сценарии подключения и отключения, настройки системы безопасности удаленных компьютеров и т. д. Желательно запретить пользователям изменение настроек групп.
- Для удаленных пользователей желательно предоставлять отключенные от сети сетевые каталоги.
- Мои документы и прочие папки с важной информацией нужно хранить в сети. В таком случае можно реализовать их общее резервное копирование и восстановление, если произойдет сбой или же данные папки кто-то случайно удалит.
- Никогда не предоставляйте пользователям дополнительных прав в сети, кроме тех, которые нужны для работы.
- Используйте консоли MMC для управления сетью. Создайте и настройте данные консоли для решения задач, с которыми вам приходится регулярно сталкиваться. Файлы консолей (MSC-файлы) храните на сетевом диске, чтобы они были доступны с любого компьютера в сети.

- Инсталлируйте и настройте на серверах и рабочих станциях сети программу удаленного администрирования — Remote Administrator. В этом случае у вас появится возможность реализовать удаленное администрирование сети, не снижая ее общий уровень защиты.

Есть ли жизнь в консоли?

Консоль управления Microsoft Management Console (MMC) — инструмент, предназначенный для создания, сохранения и восстановления средств администрирования (консолей MMC), которые способны управлять разнообразными устройствами, программными и сетевыми элементами операционной системы Windows. MMC способна работать с различными версиями операционной системы Windows.

MMC сама по себе не выполняет функций администрирования, однако в ней находятся инструменты, которые для этого предназначены. Основной тип инструментов, добавляемых на консоль, называется оснасткой. Кроме того, туда же могут быть добавлены элементы управления ActiveX, ссылки на разнообразные файлы в сети, папки, виды Панели задач и сами задачи.

Существует два способа использования возможностей консоли MMC: в пользовательском режиме (используя готовые консоли) или в авторском режиме (создавая новые или редактируя уже созданные).

Кроме того, используя консоли MMC, вы сможете создавать ваши личные инструменты, которые будут предназначены для выполнения необходимых вам задач.

Чтобы дать пользователю право на выполнение определенных административных задач, создайте новую консоль MMC, добавьте в нее все нужные инструменты, настройте ее конфигурацию, отрегулируйте права данного пользователя, после чего запишите созданную консоль на сменный носитель и передайте ее тому, кому она предназначалась. После запуска консоли пользователь получит все необходимые инструменты для выполнения конкретной задачи, что позволит ему сразу перейти к ее выполнению.

Чтобы создать нужную консоль, запустите из командной строки файл `mmc.exe`. После этого MMC начнет работу, а на экране отобразится новая консоль. С помощью командной строки вы также можете запустить уже созданную консоль.

ПРИМЕЧАНИЕ

Сохраненная консоль представлена файлом с расширением MSC.

Одна и та же консоль может сочетать в себе множество разнообразных инструментов, которые встраиваются в нее в виде отдельных модулей. Windows XP содержит множество таких модулей MMC, однако если ваша задача не может быть выполнена с их помощью, то можно попробовать добавить оснастки других разработчиков.

В консоли MMC вы можете создать окно, которое будет содержать значки, отвечающие за выполнение определенных задач или действий. Такие специальные окна называются Панелями задач.

В консолях MMC также возможно использование мастеров. Например, в случае использования оснастки Internet Information Services (IIS) пользователь может запустить Мастер разрешений.

Настройка и использование консолей

Чтобы запустить консоль, нажмите кнопку Пуск, выберите команду Выполнить, введите mmc и нажмите кнопку OK.

Оболочка MMC.EXE позволяет управлять любыми консолями вне зависимости от набора инструментов, которые в нее входят.

Интерфейс консоли напоминает Проводник Windows. Пункты меню Консоль позволят производить операции с консолями: открыть ранее созданную консоль, создать новую или же сохранить текущую консоль в файл. Кроме того, с помощью данного меню вы сможете добавить или удалить оснастку.

Пункты меню Действие позволят управлять удаленным компьютером (только если у вас есть права администратора на удаленном компьютере), а также управлять отображением консоли с помощью Мастера создания вида панели задач (кроме того, вы можете сделать это с помощью пункта меню Вид). Пункт меню Избранное напоминает аналогичное меню в Internet Explorer и позволяет быстро вызвать необходимые консоли.

С помощью пунктов меню Окно вы сможете быстро создавать новые окна консолей и контролировать их расположение.

Последнее меню — Справка. Нужно отметить, что справка написана достаточно подробно, поэтому вы найдете там ответы на большинство вопросов.

После этого можно добавлять необходимые инструменты. В меню Консоль нужно выбрать команду Добавить или удалить оснастку, после чего нажать кнопку Добавить (рис. 3.2).

В появившемся списке доступных оснасток двойным щелчком мышью выберите необходимый элемент, после чего выполните одно из следующих действий.

- Установите переключатель в режим управления локальным компьютером или же удаленным (в зависимости от поставленной задачи) и нажмите кнопку Готово.
- При появлении мастера следуйте его инструкциям.

Чтобы удалить ненужную оснастку, выполните следующее.

1. Выберите Добавить или удалить оснастку с помощью пункта меню консоль.
2. Выберите оснастку, которую нужно удалить, и нажмите кнопку Удалить.
3. Нажмите OK и вернитесь в главное меню.

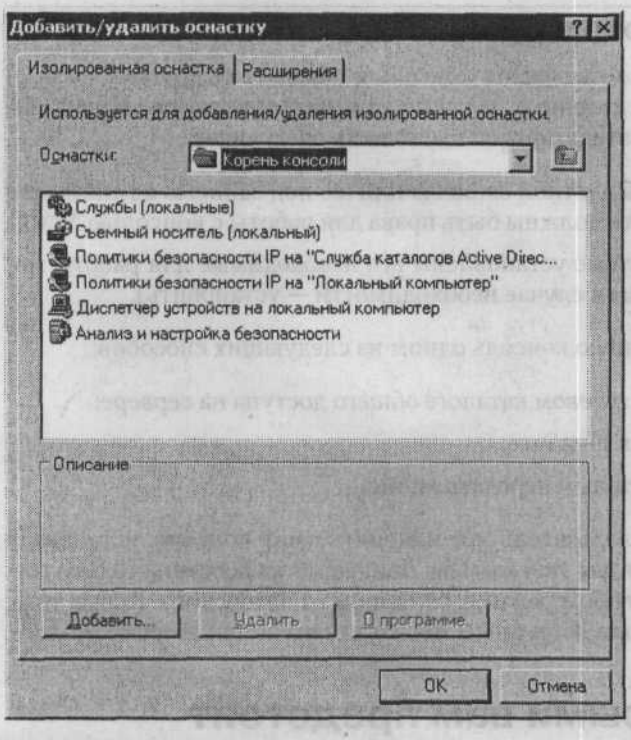


Рис. 3.2. Добавляем оснастку

Параметры командной строки MMC

С помощью командной строки MMC вы можете открыть ранее созданную консоль MMC, открыть MMC в режиме автора и выяснить разрядность открытой консоли (32-разрядная или 64-разрядная).

Команды должны быть введены в таком формате:

```
mmc путь\имя_файла.msc [/a] [/64] [/32]
```

Параметры, которые можно использовать при введении команды:

- `путь\имя_файла.msc` — загружает ранее созданную консоль. Учтите, что нужно вводить полный путь к файлу сохраненной консоли;
- `/a` — загрузит ранее сохраненную консоль в режиме автора. Данный режим позволяет вносить изменения в консоль;
- `/64` — загружает 64-битную версию MMC (MMC64). Данный параметр доступен только при использовании 64-битной версии ОС Windows;
- `/32` — загружает 32-битную версию MMC (MMC32). Данный параметр пригодится, если вы хотите использовать 32-битные оснастки под управлением 64-битной Windows;
- `/?` — справка.

Отдам консоль в хорошие руки...

Как уже упоминалось, вы можете создать консоль и передать ее другому пользователю для выполнения определенных задач по администрированию. При наличии нужной консоли пользователь должен выполнить следующее.

1. Войти в систему под своей учетной записью или же под записью администратора, однако при этом у него должны быть права для работы с консолью MMC.
2. Удостовериться, что в системе установлены все необходимые для работы модулей консоли библиотеки (в случае необходимости — установить).

Вы можете передать сохраненную консоль одним из следующих способов:

- разместить MSC-файлы в сетевом каталоге общего доступа на сервере;
- отправить в виде вложения по почте;
- записать на сменный носитель и передать лично.

Если вы не хотите, чтобы пользователь мог изменять вашу консоль, установите флажок Не сохранять изменения для этой консоли. Данная метка доступна только тогда, когда консоль открыта в любом режиме, отличном от авторского. Кроме того, вы можете сделать файл консоли доступным только для чтения в сетевом каталоге.

Службы, с которыми вам предстоит познакомиться

Во время работы Windows XP в фоновом режиме запущено множество служб (сервисов). Отличие служб от обычных приложений состоит в следующем.

- Службы можно запускать или останавливать, используя оснастку Службы, входящую в консоль Управление компьютером, или же с помощью команд `net start` и `net stop`. Если вы выполните команду `net start`, то сможете ознакомиться со списком активных на данный момент служб. Если вы знаете название нужной службы, то сможете управлять ею из командной строки.
- Многие службы взаимосвязаны, поэтому невозможность запуска одной из служб может привести к тому, что вы не сможете работать с зависимой от нее службой.
- Любая служба Windows XP может быть загружена автоматически с операционной системой или же запущена вручную (данная информация содержится в реестре).
- Некоторые службы могут быть запущены только в конкретной учетной записи. Устанавливать или снимать подобные ограничения может администратор данного компьютера.
- Все службы выполняются в фоновом режиме без участия пользователя, начиная свою работу при загрузке системы и заканчивая ее при перезагрузке или отключении питания компьютера.

Внешний вид оснастки Службы показан на рис. 3.3.

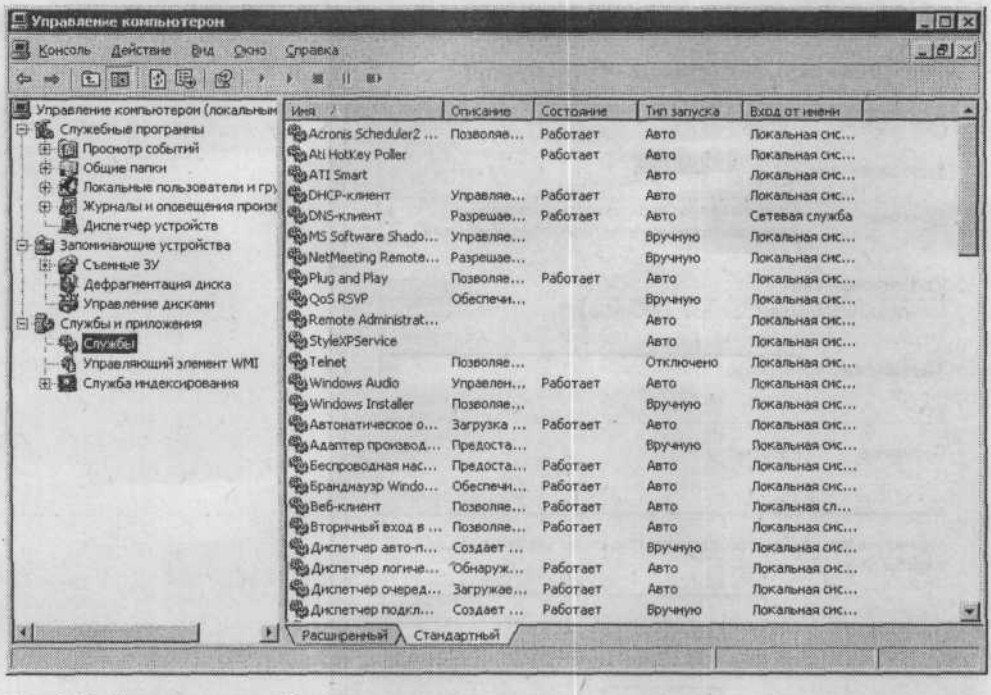


Рис. 3.3. Управление службами

Управлять запуском службы можно, если щелкнуть на названии нужной службы правой кнопкой мыши и выбрать в контекстном меню пункт Свойства. Окно установки свойств службы имеет четыре вкладки (рис. 3.4).

- Общие. Данная вкладка отвечает за запуск и остановку службы, а также позволяет назначить параметры запуска конкретной службы (вручную, автоматически, запрет на запуск).
- Вход в систему. Вкладка позволит вам указать, под какой учетной записью (или записями) можно использовать данную службу. Кроме того, здесь же вы сможете разрешить или запретить работу службы при использовании определенного профиля оборудования.
- Восстановление. Данная вкладка позволит назначить действия системы, когда служба не может запуститься. Вы можете дать указание системе отреагировать, если сбой службы произошел впервые, во второй раз или более чем два раза подряд. Действия, которые сможет выполнить система: перезапустить службу, перезагрузить компьютер или запустить указанную вами программу.
- Зависимости. На данной вкладке можно установить зависимости между двумя различными службами. Обратите внимание на то, что окно разделено на несколько частей. В первом разделе отображается список служб, от которых зависит редактируемая служба. Если хотя бы одна из них не будет запущена, зависимая служба также не будет работать. Во втором разделе содержится список служб, которые зависят от данной.

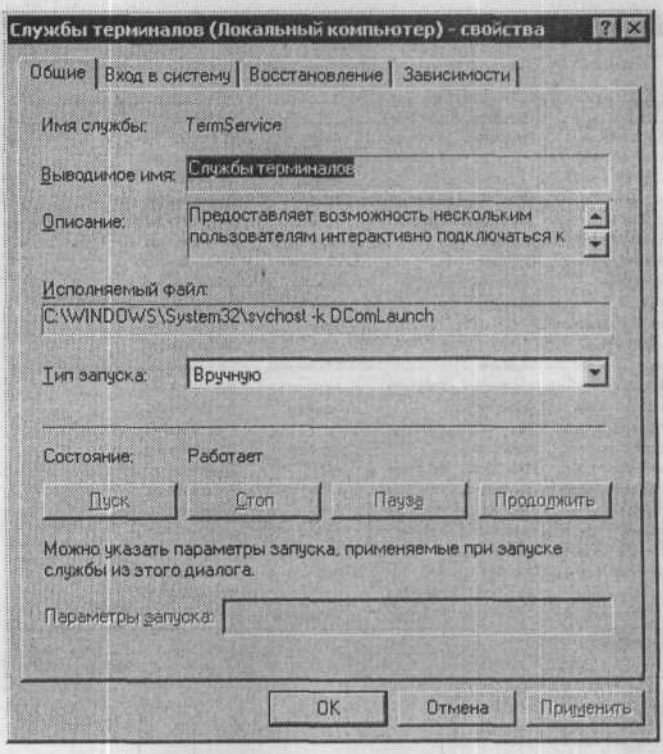


Рис. 3.4. Окно свойств службы

Обратите внимание на то, что список запущенных служб стоит отредактировать, отключив неиспользуемые сервисы. Если вы сделаете это, то сможете освободить часть ресурсов вашего компьютера.

Запуск, приостановка и остановка выполнения служб

Управление службами производится из оснастки Службы консоли Управление компьютером. Выберите из списка службу, которую нужно остановить или запустить, щелчком правой кнопкой мыши и выберите в контекстном меню соответствующий пункт — Пуск, Стоп, Пауза, Продолжить или Перезапустить.

- Пуск. Запускает службу (исполняемый файл или соответствующий программный поток).
- Стоп. Останавливает службу (при этом прекращается обслуживание всех запросов данной службой и разрываются все сетевые соединения, установленные ею).
- Пауза. Временная остановка работы службы.
- Продолжить. Продолжение работы службы (используется, если ранее была применена команда Пауза).
- Перезапустить. Останавливает службу и запускает ее снова.

Как уже упоминалось, управлять службами из командной строки позволяют команды `net start` и `net stop`. Например, если вы хотите запустить службу Telnet, введите в командной строке следующее:

```
net start telnet
```

Если в имени службы присутствуют пробелы или же имя написано русскими буквами, то его нужно взять в кавычки. Например, запуск службы Task scheduler произойдет по команде:

```
net start "task scheduler"
```

Какие службы вы сможете встретить в Windows XP

В табл. 3.1 приведены основные службы, имеющиеся в Windows XP.

Таблица 3.1. Службы в Windows XP

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Оповещатель	Отправляет выбранным пользователям и компьютерам оповещения от администратора	Автоматически	Svchost.exe (ShellHWDetection)
Управление приложениями	Обеспечивает службы установки программного обеспечения	Вручную	Svchost.exe
Сервер папки обмена	Предоставляет возможность просмотра страниц папок обмена удаленных компьютеров	Вручную	Clipsrv.exe (ClipSrv)
Система событий COM+	Автоматическое распространение событий подписавшимся компонентам COM	Автоматически	Svchost.exe (EventSystem)
Обозреватель компьютеров	Обслуживает список компьютеров в сети и выдает его программам по запросу	Можно отключить эту службу на всех компьютерах, кроме сервера локальной сети	Svchost.exe (Browser)
Сервер (Server)	Обеспечивает поддержку RPC и совместный доступ к файлам, папкам, принтерам и именованным каналам	Автоматически	Svchost.exe (lanmanserver)

Продолжение ⇩

Таблица 3.1. Службы в Windows XP (Продолжение)

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
DHCP-клиент	Управляет настройками сети с помощью регистрации и обновления IP-адресов и DNS-имен	Автоматически	Svchost.exe (Dhcp)
Клиент отслеживания изменившихся связей	Посылает уведомления о перемещении файлов между томами NTFS в сетевом домене	Если вы подключены к домену Win2k, установите Авто. Иначе — вручную	Svchost.exe (TrkWks)
Координатор распределенных транзакций	Координация транзакций, распределенных по нескольким базам данных, очередям сообщений, файловым системам или другим защищенным диспетчерам ресурсов транзакций	Вручную	Msdtc.exe (MSDTC)
DNS-клиент	Разрешает DNS-имена в адреса и размещает их в кэше	Автоматически	Svchost.exe (Dnscache)
Журнал событий	Записывает в журнал уведомления о событиях, которые предоставляют программы и операционная система	Автоматически	Services.exe (Eventlog)
Служба факсов	Позволяет отправлять и принимать факсимильные сообщения	Установите Авто, если у вас есть факс-модем и вы им пользуетесь для обмена факсами. Иначе — выключите совсем	Fxssvc.exe (Fax)
Служба индексирования	Индексирует содержимое документов для ускорения процесса поиска по их содержимому	Можно выключить совсем	Cisvc.exe (cisvc)
Общий доступ к подключению Интернета	Реализовывает поддержку служб трансляции адресов, адресации и разрешения имен в адреса для всех компьютеров домашней сети, подключенных через удаленное соединение	Автоматически	–

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Агент политики IPSEC	Управляет политикой IP-безопасности и запускает ISAKMP/Oakley (IKE) и драйвер IP-безопасности	Отключено	–
Диспетчер логических дисков	Обнаружение и мониторинг новых жестких дисков и передача данных о томах жестких дисков службе управления диспетчера логических дисков	Вручную	Svchost.exe (dmserver)
Служба администрирования диспетчера логических дисков	Служба администрирования для запросов, касающихся управления дисками	Вручную	Dmadmin.exe (dmadmin)
Служба сообщений	Отправляет и получает сообщения, переданные администраторами или службой оповещений операционной системы	Вручную	Svchost.exe (Messenger)
Сетевой вход в систему	Реализовывает сквозную идентификацию событий входа учетной записи для компьютеров домена	Вручную	Lsass.exe (Netlogon)
NetMeeting Remote Desktop Sharing	Позволяет указанным пользователям получать доступ к рабочему столу Windows с помощью NetMeeting	Отключено	Mnmsrvc.exe (mnmsrvc)
Планировщик заданий	Аналогична Task Scheduler в Windows 98. Позволяет запускать приложения по расписанию	Автоматически	Svchost.exe (Shedule)
Служба поддержки TCP/IP NetBIOS	Включает поддержку службы NetBIOS через TCP/IP (NetBT) и разрешения NetBIOS-имен в адреса. Служба предназначена для обеспечения работы сетевых служб от Microsoft: общего использования ресурсов, сетевой печати, аутентификации доступа	Автоматически	–

Продолжение ⇩

Таблица 3.1. Службы в Windows XP (Продолжение)

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Телефония	Реализует поддержку технологии Telephony API (TAPI) для программ, управляющих телефонным оборудованием и голосовыми IP-подключениями, а также через локальную сеть — на серверах, где запущена данная служба	Вручную	Svchost.exe (TapiSrv)
Telnet	Позволяет удаленному пользователю входить в систему и запускать приложения в ней, поддерживает различные клиенты TCP/IP Telnet	Если вы не пользуетесь Telnet, отключите ее в целях безопасности	TLntsvr.exe (TlntSvr)
Источник бесперебойного питания	Обеспечивает управление источниками бесперебойного питания (ИБП)	Включите автоматический запуск службы, если вы имеете источник бесперебойного питания и он подключен к компьютеру через управляющий им интерфейс (COM, USB). Если же у вас его нет — службу можно отключить	UPS.exe (UPS)
Диспетчер служебных программ	Обеспечивает запуск и настройку программ поддержки специальных возможностей	Отключено	–
Windows Installer	Устанавливает, удаляет или восстанавливает приложения в соответствии с процедурами, описанными в файле MSI	Автоматически	Msiexec.exe (MSIserver)
Служба времени Windows	Позволяет синхронизировать дату и время между рабочими станциями и сервером	Вручную	Svchost.exe (W32Time)

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Рабочая станция (Workstation)	Обеспечивает поддержку сетевых подключений и связь	Автоматически	–
Служба сетевого DDE	Реализует сетевой транспорт и безопасность для динамического обмена данными (DDE)	Автоматически	Netdde.exe (NetDDE)
Диспетчер сетевого DDE	Управляет разделяемыми объектами динамического обмена информацией и используется предыдущей службой	Автоматически	Netdde.exe (NetDDE)
Поставщик поддержки безопасности NT LM	Обеспечивает безопасность приложениям, которые используют удаленные вызовы процедур (RPC) через транспорты, отличные от именованных каналов	Вручную	Lsass.exe
Оповещения и журналы производительности	Управляет сбором информации о производительности вашего или удаленного компьютера и реализует запись данной информации в журналы или же производит оповещение компьютеров в сети	Автоматически	–
Plug and Play	Управляет автоматической установкой и настройкой устройств и уведомляет установленные приложения об изменениях конфигурации системы	Автоматически	Services.exe (PlugPlay)
Диспетчер очереди печати	Загружает в память файлы для последующей печати	Автоматически. Если у вас нет принтера, можно отключить	Spoolsv.exe (Spooler)
Защищенное хранилище	Обеспечивает защищенное хранение конфиденциальных данных	Автоматически (обязательно!)	Lsass.exe
QoS RSVP	Обеспечивает рассылку оповещений в сети и управление локальным трафиком для QoS-программ и управляющих программ	Отключено	Rsvp.exe (RSVP)

Продолжение ⇩

Таблица 3.1. Службы в Windows XP (Продолжение)

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Диспетчер авто-подключений удаленного доступа	Создает подключение к удаленной сети, когда программа обращается к удаленному DNS- или NetBIOS-имени или адресу	Автоматически	Svchost.exe (RasAuto)
Диспетчер подключений удаленного доступа	Создает сетевое подключение	Автоматически	Svchost.exe (RasMan)
Удаленный вызов процедур (RPC)	Обеспечивает сопоставление конечных точек и иных служб RPC	Автоматически (обязательно!)	Svchost.exe (RpcSs)
Локатор удаленного вызова процедур (RPC)	Управляет базой данных службы имен RPC	Автоматически	Locator.exe (RpcLocator)
Служба удаленного управления реестром	Позволяет выполнять удаленное управление реестром	Оставьте включенной, если вы занимаетесь редактированием реестра на удаленных компьютерах	Svchost.exe
Съемные ЗУ	Управляет съемными носителями, дисками и библиотеками	Автоматически	Svchost.exe (NtmsSvc)
Маршрутизация и удаленный доступ	Обеспечивает маршрутизацию в локальной и глобальной сетях	Автоматически	Svchost.exe (Remote Access)
Служба RunAs	Позволяет запускать процессы от имени другого пользователя	Автоматически	–
Диспетчер учетных записей безопасности	Хранит информацию о безопасности для учетной записи локального пользователя	Автоматически	Lsass.exe (SamSs)
Смарт-карты	Управляет и проверяет доступ к смарт-карте, вставленной в устройство чтения, подключенное к компьютеру	Оставьте включенной, если вы используете смарт-карты	Scardsvr.exe (SCardSvr)

Имя службы	Описание	Рекомендуемый тип запуска	Исполняемый файл (название службы)
Модуль поддержки смарт-карт	Поддерживает устройства чтения смарт-карт, не имеющих самонастройки	Аналогично предыдущей службе	Scardsvr.exe (SCardSvr)
Уведомление о системных событиях	Заносит в протокол системные события, такие как регистрация в Windows, в сети и изменения в подаче электропитания. Уведомляет подписчиков из разряда «'COM+ системное событие'», рассылая оповещения	Автоматически	Svchost.exe (SENS)

Если вы остановили какую-то службу, а компьютер не способен нормально работать (или вообще загружаться), вам следует запустить Редактор реестра, в ветви `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services` найти секцию, соответствующую отключенной службе, и в пункте `Start` ввести одно из трех значений:

- 4 — включает режим Отключено;
- 3 — включает режим Вручную;
- 2 — включает режим Авто.

Здесь приведены далеко не все службы, которые вы можете встретить, а лишь самые главные, на которые нужно было обратить ваше внимание. Перечисление всех служб заняло бы очень много места, кроме того, различные приложения способны добавлять в список свои собственные службы.

Реестр — сердце Windows

В операционной системе Windows сведения о параметрах и настройках устройств и приложений хранятся в глобальной базе данных, которая носит название реестр. В реестре находятся профили всех пользователей компьютера, сведения о конфигурации конкретного компьютера, параметры установленных программ и прочая важная информация. Windows использует эти сведения в процессе своей работы.

Реестр расположен в нескольких файлах, которые изменяются в процессе работы операционной системы Windows. Доступ к реестру защищен и контролируется редактором реестра.

Реестр является основой операционной системы, представляя собой большую базу функций и параметров системы и программного обеспечения, хранящуюся по адресу `%SystemRoot%\System32\Config` и в папке профилей пользователей компьютера (`Ntuser.dat`). Без реестра работа операционной системы невозможна.

Реестр связывает и координирует действия всех элементов операционной системы и отвечает за ее стабильную работу. Именно поэтому надо быть максимально осторожным при работе с ним.

Реестр Windows является:

- динамическим;
- иерархическим;
- защищенным.

Динамичность реестра проявляется в том, что Windows и программы во время работы постоянно изменяют его содержимое. Все изменения, которые были внесены в реестр, сразу же становятся доступными для всех остальных работающих приложений и утилит. В реестре сохраняются все настройки программного обеспечения и операционной системы, что позволяет не проводить повторного процесса конфигурации после перезагрузки системы.

Структура реестра является иерархической. Реестр делится на несколько основных разделов, которые носят название поддеревьев (Subtrees). Поддерево содержит множество различных ключей (Keys), каждый из которых способен содержать в себе несколько подключей (Subkeys). Каждый ключ или подключ может иметь несколько различных значений (Values).

Реестр содержит данные о приоритетах задач, процессов или устройств системы. Кроме того, в реестре находится информация о зависимости различных составляющих операционной системы друг от друга.

Определенные разделы реестра содержат информацию о порядке загрузки системы — порядок инициализации, запуска и конфигурирования драйверов, запуска сервисов и определения устройств, окончания загрузки и входа пользователя в систему.

Защищенность реестра означает, что у него присутствует собственная система безопасности, которая необходима для защиты от несанкционированного доступа и изменения, а также регулярной проверки целостности реестра.

То, что приложения помещают информацию о собственной конфигурации в реестр, имеет два аспекта: позитивный и негативный. Позитив состоит в том, что реестр позволяет эффективно хранить и использовать информацию. Негативный эффект проявляется в увеличении размеров реестра. По мере установки и удаления приложений в реестре накапливается множество ненужных ключей, что может значительно снизить производительность системы.

Что там, внутри реестра?

Научиться работать с реестром достаточно сложно, тем более что Microsoft не предоставляет официальной документации по его использованию. Однако если вы хотите подробно изучить возможности Windows и получить доступ к более гибкой настройке системы, то придется немного поработать.

Реестр Windows XP состоит из пяти основных поддеревьев, которые носят имена корневых разделов реестра. Вся информация, находящаяся в реестре, делится с помощью поддеревьев на несколько логических разделов.

ПРИМЕЧАНИЕ

Достаточно часто для обозначения ветвей реестра используется термин «куст». Как правило, кустом называют отдельный файл, в котором хранятся данные из конкретного поддерева.

Поддеревья реестра содержат огромное количество разделов (ключей). Реестр Windows XP содержит следующий перечень стандартных поддеревьев (табл. 3.2).

Таблица 3.2. Стандартные разделы реестра Windows XP

Раздел реестра	Назначение
HKEY_CLASSES_ROOT	Данный раздел содержит сведения о файловых расширениях и программы, которые этим расширениям соответствуют. Здесь также содержится информация, необходимая для работы технологий COM и OLE. Некоторые данные, связанные с названным выше, содержатся в ключе HKEY_LOCAL_MACHINE\Software\Classes
HKEY_CURRENT_USER	Здесь находится информация, которая касается активного на данный момент пользователя
HKEY_LOCAL_MACHINE	Раздел содержит информацию о конфигурации компьютера и о том, как будут обрабатываться запуск и остановка установленных в системе служб и оборудования. Здесь также содержится информация, которая относится к SAM (Security Accounts Manager) и политикам безопасности. Данная ветвь наиболее интенсивно используется приложениями
HKEY_USERS	Раздел содержит данные о пользователях компьютера. Каждому пользователю назначается определенная запись, название которой соответствует идентификатору SID данного пользователя
HKEY_CURRENT_CONFIG	Эта ветвь связана с подключами в HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current. Данный раздел содержит информацию, которая относится к аппаратному обеспечению и используется в процессе предварительной загрузки, чтобы разрешить взаимосвязи определенного аппаратного обеспечения

Что скрывается за значениями ключей реестра

Как уже было упомянуто, ключи реестра имеют одно или несколько значений разных типов. В зависимости от того, какой тип будет использован, значение ключа может быть двоичным, десятичным или шестнадцатеричным числом, текстом ASCII или же комбинацией из чисел и текста. Описание типов значений ключей реестра приведено в табл. 3.3.

Таблица 3.3. Описание типов значений ключей реестра

Тип значения ключа реестра	Описание
REG_BINARY	Двоичные данные, которые используются большинством аппаратных компонентов. Любой редактор реестра будет отображать данную информацию в шестнадцатеричном формате
REG_DWORD	В данном разделе различные данные представлены в виде значений, длина которых составляет всего 4 байта (такой тип сохранения данных используют многие драйверы). Редакторы реестра могут отображать эти данные в двоичном, шестнадцатеричном и десятичном формате
REG_EXPAND_SZ	Расширяемая строка данных. Такая строка содержит текст, в котором находится переменная (при вызове приложением может быть заменена)
REG_DWORD_BIG_ENDIAN	Данные этого типа являются 32-битными значениями, при этом старший байт располагается в первой позиции
REG_MULTI_SZ	Поле, которое содержит несколько строк. Строки разделены символом NULL и имеют удобный для восприятия человеком формат
REG_EXPAND_SZ	Строка данных с переменной длиной. Такая строка содержит имена переменных, которые могут замещаться приложением на фактические значения этих переменных. Значения такого типа используются, в частности, для поддержки переменных окружения
REG_SZ	Текстовая строка, удобная для восприятия. Значениям, представляющим собой описания компонентов, обычно присваивается именно этот тип данных
REG_LINK	Ссылка в формате Unicode
REG_FULL_RESOURCE_DESCRIPTOR	Информация, касающаяся аппаратных ресурсов вашей системы, таких как DMA, IRQ и диапазон адресов. Информация отображается в шестнадцатеричном виде и может редактироваться как отдельный байт, слово или двойное слово
REG_RESOURCE_LIST	Содержит необходимую информацию об аппаратных ресурсах — тип интерфейса и номер шины. Возможно расширение данной информации таким образом, чтобы отобразить тип REG_FULL_RESOURCE_DESCRIPTOR. Редактирование возможно только в шестнадцатеричном режиме
REG_NONE	Неопределенный тип, который используется, если Windows не способна идентифицировать полученные данные

Где находится реестр

Реестр операционной системы находится в нескольких файлах, имена и месторасположение которых приведены в табл. 3.4.

Таблица 3.4. Расположение ветвей реестра в файлах

Ветвь реестра	Имя файла	Путь к файлу
HKEY_LOCAL_MACHINE\Sam	Sam и Sam.log	Systemroot\System32\Config
HKEY_LOCAL_MACHINE\Security	Security и Security.log	Systemroot\System32\Config
HKEY_LOCAL_MACHINE\Software	Software и Software.log	Systemroot\System32\Config
HKEY_LOCAL_MACHINE\System	System и System.log	Systemroot\System32\Config
HKEY_CURRENT_CONFIG	System и System.log	Systemroot\System32\Config
HKEY_USERS\.DEFAULT	Default и Default.log	Systemroot\System32\Config
HKEY_CURRENT_USER	Ntuser.dat и Ntuser.log	Systemroot\Documents and Settings\Username\

ПРИМЕЧАНИЕ

Применяемая в таблице переменная %Systemroot% — это путь к папке Windows. Например, если Windows установлена в папку Windows на диске C:, значит, %Systemroot% — это C:\Windows.

Правка реестра — операция на сердце Windows

Для изменения каких-нибудь значений в реестре используются редакторы реестра. Чаще всего используется утилита regedit, входящая в состав операционной системы Windows. Для ее запуска нужно выполнить команду Пуск ▸ Выполнить и в появившемся окне набрать `regedit`. Главное окно программы представлено на рис. 3.5.

Используйте редактор реестра, только если вы точно знаете, что нужно сделать и к каким результатам это может привести. Помните, что редактор не проверяет правильность задания параметров, поэтому даже при опечатке любое изменение будет сохранено, что может привести к нежелательным последствиям. Сам по себе реестр не восстановится, и операционная система может отказаться загружаться.

Существуют определенные методы восстановления реестра из резервных копий, исправления ошибок реестра и удаления ненужных ключей, однако самый лучший способ — не редактировать реестр, если вы не знаете наверняка, что конкретно нужно делать.

Если вы изменяете реестр операционной системы при помощи редактора, то никто не сможет гарантировать, что Windows будет после этого корректно работать. По этой причине прежде всего сделайте резервную копию реестра или даже всего раздела с операционной системой.

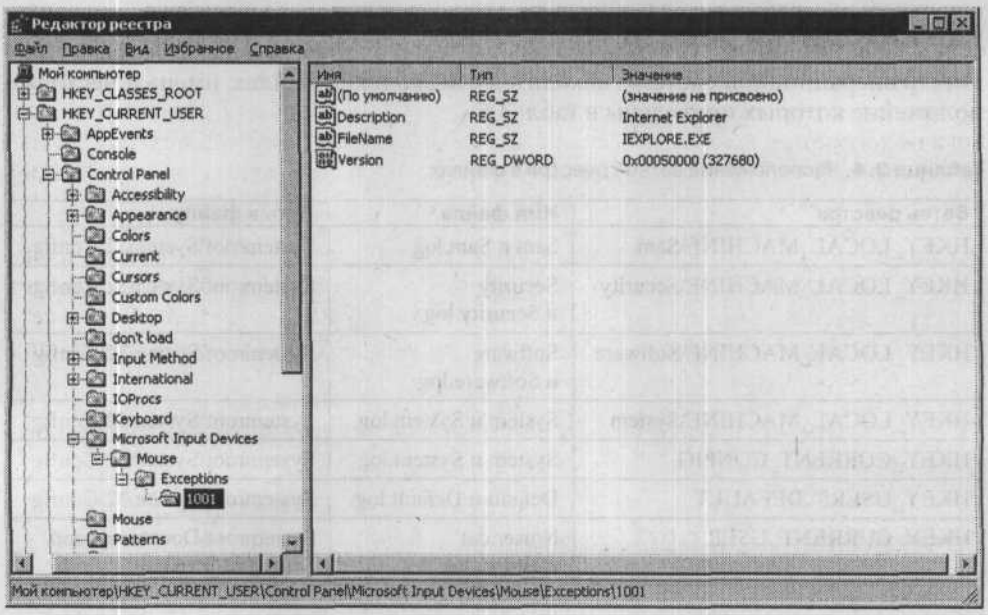


Рис. 3.5. Главное окно программы Regedit

Главное меню программы содержит следующие пункты: Файл, Правка, Вид, Избранное и Справка.

В пункте меню Файл можно экспортировать реестр в файл целиком или частично, загружать резервную копию реестра из файла, редактировать реестр на удаленной машине.

ПРИМЕЧАНИЕ

Чтобы изменять реестр удаленного компьютера, вы должны иметь права администратора как на локальном, так и на удаленном компьютере.

В пункте Правка можно производить поиск необходимых ключей и значений в реестре, создавать новые ключи и присваивать им значения, а также устанавливать доступ на редактирование реестра для пользователей.

В пункте меню Вид можно изменить внешний вид главного окна программы.

Пункт меню Избранное аналогичен такому же пункту в Internet Explorer. Сюда можно добавить наиболее часто используемые ветви реестра, чтобы потом быстро к ним обратиться.

Когда вы запускаете `regedit.exe`, перед вами появляется структура реестра, чем-то похожая на Проводник Windows. Слева будет отображено дерево разделов, а справа — список вложенных ключей и их значения. Все доступные разделы находятся в одном корневом разделе Мой компьютер в окне реестра.

Работа с отдельными ключами в редакторе схожа с работой в Проводнике, однако обратите внимание на то, что в правой части окна не появляются значки отдельных разделов. Если вы нажмете плюсик или же два раза щелкнете на значке отдельного раздела, то сможете последовательно разворачивать разделы реестра, пока не доберетесь до нужного вам ключа. Чтобы изменить имя раздела, щелкните на нем правой кнопкой мыши и в контекстном меню выберите соответствующий пункт (также можно просто нажать F2).

Вы можете экспортировать всю структуру реестра в специальный файл с расширением REG для последующего изучения или восстановления. Чтобы произвести такую операцию, выберите пункт Экспорт в подменю Файл редактора. Вы можете экспортировать как весь реестр, так и отдельный раздел (выбрав соответствующий параметр в процессе сохранения).

Учтите, что отменить любое ваше действие не получится, так что будьте осторожны в процессе редактирования.

Заглянем внутрь REG-файла

Файл реестра имеет стандартную структуру, отклонение от которой не допускается. В самом начале REG-файла находится строка `REGEDIT 4` или `Windows Registry Editor Version 5.00`. Если она отсутствует, то операционная система будет воспринимать файл как текстовый. Если такая строка есть, то вы можете импортировать значения, дважды щелкнув на файле.

ВНИМАНИЕ

Не стоит импортировать REG-файлы, если вы не знаете их предназначения. Например, некоторые приложения включают такие файлы в дистрибутив и используют их во время инсталляции для установки нужных параметров. При импорте такого файла все текущие установки будут заменены первоначальными без возможности восстановления.

После строки `Windows Registry Editor Version 5.00` (или `REGEDIT 4`) должен находиться пробел, после которого располагаются ключи, которые необходимо добавить в реестр. Имя отдельного раздела заключается в квадратные скобки. Для каждого имени раздела должна быть выделена отдельная строка в файле. Имена параметров расположены по одному в строчке, сразу за именем раздела, в кавычках, а рядом с ними должны быть расположены их значения. Значения параметров должны быть записаны в кавычках, значения параметров типа `Dword` — в виде шестнадцатеричной строки `dword:00000000`, значения двоичных параметров — в шестнадцатеричной системе в виде строки: `hex:14,00,00,00`.

Если в значении строкового параметра присутствует символ \, то при экспорте файла реестра он будет заменен парой таких символов. Данный символ нужен для установки переноса слишком длинных строк. Имя любого раздела или подраздела должно быть написано полностью и в отдельной строке. В промежутке между описаниями разделов и в конце файла (обратите на это внимание) должно

находиться по одной пустой строке. Символ @ означает использование параметра, установленного по умолчанию.

Чтобы удалить конкретный раздел или параметр, поставьте перед его названием знак –.

Заставим Windows «летать»

Windows XP — достаточно требовательная к ресурсам операционная система, однако существуют способы сокращения количества системных ресурсов, которые она будет использовать, как совершенно безопасные и незаметные, так и такие, которые несколько ограничивают ее функциональность.

Между тем, Windows XP способна к самооптимизации. В процессе своей работы вы запускаете определенное программное обеспечение, а Windows тем временем производит мониторинг поведения системы и сохраняет список часто запускаемых приложений в файле `layout.ini`. Раз в три дня операционная система изменяет физическое местоположение некоторых программ (перемещает их в начало диска, где процессы записи и чтения происходят несколько быстрее) для текущей оптимизации времени их загрузки.

В Windows XP присутствует специальная система предсказаний, которая направлена на ускорение процесса загрузки системы и оптимизацию ее запуска. Операционная система составляет список служб и приложений, начинающих работать после ее загрузки, чтобы ускорить их запуск. При загрузке отдельных приложений Windows XP следит за используемыми компонентами и файлами. Когда приложение будет запущено повторно, Windows XP предсказывает список файлов, которые ему понадобятся.

Предсказания используются ядром Windows XP и планировщиком задач. Ядро производит мониторинг страниц, к которым будет обращаться данный процесс сразу же после его создания. Данная служба составляет инструкции предсказания. Если приложение будет запущено повторно, то благодаря ранее созданным инструкциям можно будет значительно ускорить процесс загрузки.

Большинство советов по оптимизации, приведенных в этой главе, основано на редактировании реестра. Помните, что для этого вы должны обладать правами администратора. Перед изменением реестра желательно сделать его резервную копию, чтобы в случае неудачи можно было вернуться к исходной конфигурации.

Шаг 1. Уберем значки и фоновый рисунок Рабочего стола

Оптимизацию операционной системы стоит начать с Рабочего стола. Фоновые рисунки и расположенные на Рабочем столе файлы с рисунками способны значительно снижать производительность системы (особенно в процессе обновления экрана). Учтите, что значки и фоновый рисунок Рабочего стола постоянно находятся в оперативной памяти.

Впрочем, прирост производительности в случае отказа от использования фонового рисунка и значков будет совсем небольшим. Так что если у вас более 256 Мбайт оперативной памяти и процессор, тактовая частота которого превышает 1 ГГц, то волноваться не стоит. Однако владельцам более старых компьютеров стоит призадуматься над этой информацией.

Шаг 2. Уменьшим объем используемой памяти

В реестре Windows находится несколько ключей, позволяющих оптимизировать работу с памятью.

Вы можете ускорить запуск приложений и освободить некоторый объем оперативной памяти, если отключите отладчик Dr.Watson. Чтобы сделать это, установите значение ключа `Auto` равным `0` по адресу `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug`. Теперь в случае сбоя система поинтересуется, нужно ли закрыть приложение или же передать его программе Dr.Watson, которая запустится и создаст лог-файл. Если вы считаете такую возможность ненужной, удалите ветвь `AeDebug` из реестра.

Можно также поработать со значением ключа `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management`.

- `ClearPageFileAtShutdown` — активирует возможность стирать файл подкачки при выходе из Windows. По умолчанию данное значение равно `1`, однако вы можете изменить его на `0`, что ускорит работу компьютера при перезагрузке, однако снизит уровень безопасности.
- `DisablePagingExecutive` — запрещает записывать в файл подкачки код (драйверы и исполняемые файлы) и принудительно оставляет его в оперативной памяти. Значение этого ключа по умолчанию — `0`. Если у вас установлено более 256 Мбайт, то вы можете присвоить значение `1`, что значительно ускорит работу системы.

Если в системе установлено менее 128 Мбайт оперативной памяти, использование функции `Prefetch` может вызвать резкое снижение производительности системы, поэтому желательно ее отключить. Для этого вам нужно будет в ветке `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters` выбрать параметр `EnablePrefetcher` и присвоить ему значение `0`.

Кроме того, в процессе загрузки операционной системы запускается множество разнообразных служб, часть из которых можно отключить. На отключении неиспользуемых служб мы остановимся позднее.

Отключите неиспользуемую подсистему POSIX, что может несколько увеличить производительность. Для этого откройте ветвь `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems` и удалите строчки `Optional` и `Posix`.

Шаг 3. Настроим подкачку

Файл подкачки используется системой для увеличения объема доступной оперативной памяти. Когда в оперативной памяти не остается свободного места, часть данных оттуда перемещается в файл подкачки на жесткий диск. Если эта информация вновь понадобится, то она вернется в оперативную память.

Откройте свойства диска C:, щелкнув на его значке правой кнопкой мыши. Открыв вкладку Оборудование, нажмите кнопку Свойства. В открывшемся окне выберите вкладку Политика и убедитесь, что установлен флажок Разрешить кэширование записи на диск.

Возможно использование двух различных способов установки размера файла подкачки: фиксированный и динамический размер. В первом случае максимально возможный размер равен минимальному, что фиксирует размеры файла подкачки на установленном уровне. Такой подход уменьшает фрагментацию диска, однако может привести к разнообразным сбоям в процессе работы некоторых приложений, если памяти не будет хватать. Во втором случае максимальное значение должно быть в два раза больше, чем минимальное, что позволит размерам файла подкачки изменяться в указанных рамках. При этом будет происходить фрагментация диска и последующее снижение производительности. Следовательно, для файла подкачки следует установить фиксированный размер, который рассчитывается достаточно просто — размер оперативной памяти необходимо умножить на 2,5.

Файл подкачки следует располагать в первом разделе (что соответствует первому по порядку логическому диску), так как это позволит ускорить скорость доступа к нему.

Проверьте, включен ли режим DMA (Direct Memory Access, прямой доступ к памяти) для всех IDE-устройств системы. Для этого щелкните правой кнопкой мыши на ярлыке Мой компьютер, выполните команду Свойства ▸ Оборудование ▸ Диспетчер устройств ▸ IDE ATA/ATAPI контроллеры, в контекстном меню выберите Свойства вашего контроллера IDE. В открывшемся окне перейдите на вкладку Дополнительные параметры.

Параметр Тип устройства разрешает операционной системе автоматически определять подключенные устройства. Если к данному каналу ничего не подключено, установите значение Отсутствует, что позволит несколько ускорить процесс загрузки Windows.

ПРИМЕЧАНИЕ

Если жесткий диск или привод компакт-дисков используют режим PIO, это сильно нагружает процессор во время чтения или записи. Именно поэтому нужно использовать режим DMA.

Параметр Режим передачи Windows XP по умолчанию активирует максимально быстрый режим DMA, с которым способно работать устройство. Значение данного параметра должно быть DMA, если доступно.

Шаг 4. Уменьшим время загрузки приложений

В Windows XP присутствует возможность ускорения загрузки приложений. Чтобы ею воспользоваться, используйте ключ `/prefetch:1`.

Правой кнопкой мыши щелкните на ярлыке необходимого приложения и выберите в контекстном меню пункт `Свойства`. В поле `Объект` после указания пути к файлу добавьте `/prefetch:1` (пробел перед ключом обязателен).

Шаг 5. Снизим загрузку процессора

Чтобы снизить загрузку процессора, желательно отключить разнообразные графические эффекты, которых очень много в Windows XP. Выполните команду Панель управления ▸ Система ▸ Дополнительно ▸ Быстродействие ▸ Параметры. На экране появится список всех эффектов, которые используются операционной системой.

Отключив все ненужные эффекты, вы сможете несколько снизить нагрузку на процессор.

В окне Параметры быстродействия перейдите на вкладку Дополнительно и установите приоритет распределения ресурсов процессора и памяти на оптимизацию работы программ (приоритет использования служб и кэша понадобится для сервера сети).

Перейдем к меню Пуск. По умолчанию оно открывается с небольшой задержкой (400 мс), однако вы можете ее регулировать, изменяя в реестре значение ключа `MenuShowDelay`, который находится по адресу `HKEY_CURRENT_USER\ControlPanel\Desktop`. Если значение будет равно `0`, то меню будет появляться без задержки.

Кроме того, вы можете несколько ускорить работу интерфейса, поработав с параметром `MinAnimate`, который находится по адресу `HKEY_CURRENT_USER\ControlPanel\Desktop\WindowMetrics` и отвечает за анимацию при сворачивании окон. Значение `1` — эффект анимации включен, `0` — выключен. Если же данный ключ отсутствует, то создайте его (тип — `String`). Помните, что вам нужно перезагрузить компьютер, чтобы данные изменения вступили в силу.

Когда вы открываете в разделе, использующем NTFS, папки, содержащие большое количество файлов, этот процесс может происходить медленно, так как операционная система каждый раз обновляет метку последнего доступа к файлам. Чтобы отключить использование данной функции, создайте по адресу `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem` параметр типа `DWord`, назовите его `NtfsDisableLastAccessUpdate` и присвойте ему значение `1`.

Шаг 6. Оптимизируем поисковую систему

Служба индексирования предназначена для создания списков содержимого и параметров документов на жестком диске компьютера и на общих сетевых дисках.

Данная служба работает постоянно и использует значительное количество ресурсов процессора и некоторые объемы оперативной памяти. Если вы не используете контекстный поиск документов, то можете остановить работу этой функции. Для этого выполните команду Панель управления ▸ Установка и удаление программ ▸ Установка компонентов Windows. В появившемся списке нужно снять флажок Служба индексирования.

Windows XP может искать документы и в архивах. Вы можете отключить данную возможность, что значительно ускорит поиск. Для этого необходимо набрать в командной строке следующее:

```
regsvr32 c:\windows\\system32\zipfldr.dll /u
```

Если же вы снова хотите включить возможность поиска в архивах, наберите в командной строке следующее:

```
regsvr32 c:\windows\\system32\zipfldr.dll
```

Шаг 7. Настроим автоматически выполняемые программы

Одна из причин снижения производительности операционной системы — запуск большого количества приложений в процессе загрузки Windows.

Вы можете установить автоматический запуск конкретного приложения следующими способами.

- Добавление ярлыка, указывающего на исполняемый файл приложения, в папку Автозагрузка для текущего пользователя.
- Добавление ярлыка в папку Автозагрузка для всех пользователей компьютера.
- Добавление ярлыка в папку Планировщик заданий.
- Удаление или добавление записей в ключ реестра Run (системы). Ключ реестра `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.
- Удаление или добавление записей в ключ Run (пользователя) Ключ реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.
- В файле `Win.ini` можно отметить программы, предназначенные для 16-разрядных версий Windows. При этом добавятся строки типа Load= и Run= этого файла.
- Кроме того, существует группа ключей реестра, в которых содержится список программ, выполняющихся в процессе запуска системы. Эти ключи — RunOnce и RunOnceEx. Они могут иметь отношение к конкретным учетным записям: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`, `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx`, `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`, `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx`.

В состав Windows XP входит утилита `Msconfig.exe`, которая позволяет контролировать список автоматически загружаемых программ.

Шаг 8. Оставляем информацию об ошибках у себя

Каждый раз при возникновении ошибки в работе определенного приложения операционная система пытается отправить отчет о данной ошибке на сервер Microsoft. Чтобы отключить эту функцию, выполните команду Панель управления ▸ Система ▸ Дополнительно и нажмите кнопку Отчет об ошибках. Установите переключатель в положение Отключить отчет об ошибках, однако оставьте установленным флажок Но уведомлять о критических ошибках.

Порядок действий Windows в случае сбоя системы можно определить, выполнив команду Панель управления ▸ Система ▸ Дополнительно. В области Загрузка и восстановление нажмите кнопку Параметры. В области Отказ системы появившегося окна снимите флажок Выполнить автоматическую перезагрузку. Это позволит предотвратить неожиданные перезагрузки. В области Запись отладочной информации желательно выключить запись дампа памяти (часть кода программы и часть содержимого регистров, находившиеся в оперативной памяти во время сбоя).

Шаг 9. Ускоряем работу сети

Мало кто знает, что по умолчанию при работе в сети операционная система резервирует 20 % трафика для передачи критически важных данных. 20 % пропускной способности сети — слишком большое значение, поэтому такое резервирование стоит отключить.

Указанное ограничение контролируется групповой политикой, а резервированием занимается служба Диспетчер пакетов QoS. Если вы отключите данную службу, то ситуацию это не изменит. Эту проблему следует решать самостоятельно, изменяя групповую политику вручную.

Выполните в консоли команду `gpedit.msc`, что приведет к появлению консоли MMC с уже загруженной оснасткой Групповая политика.

Далее выберите раздел Конфигурация компьютера и в нем — Административные шаблоны ▸ Сеть ▸ Диспетчер пакетов QoS. Дважды щелкните мышью на пункте Ограничить резервируемую пропускную способность. В окне изменения параметров, которое появится после этого, установите переключатель в положение Включен и установите ограничение — 0 %. Если вы сделаете это, не забудьте установить в свойствах всех доступных сетевых подключений использование протокола Планировщик пакетов QoS.

Шаг 10. Контролируем автоматическое обновление

Windows является самой распространенной операционной системой, и это обеспечило наличие огромного количества вирусов, написанных специально под нее.

Windows XP способна самостоятельно следить за выходом исправлений ошибок (особенно критических), обновленных версий своих компонентов, решений проблем совместимости и прочих обновлений.

В состав операционной системы входит служба автоматического обновления, которая время от времени соединяется с сервером разработчика и при необходимости загружает доступные обновления.

Настроить параметры автоматического обновления (Automatic Updates) можно в окне Система Панели управления. Здесь можно указать, какие именно обновления загружать и устанавливать, можно задать Windows только проверять наличие обновлений (ничего не загружая) и дать вам знать при их появлении, а можно запретить ей делать что бы там ни было.

Шаг 11. Настраиваем файл boot.ini

`boot.ini` — это текстовый файл, содержащий основные настройки системы, который отвечает за загрузку Windows. Без данного файла операционная система не сможет загрузиться. Внося необходимые изменения в этот файл, вы сможете значительно ускорить загрузку Windows. Сам файл `boot.ini` выполняет следующие функции:

- координирует процесс загрузки Windows;
- устанавливает пункты меню выбора операционной системы;
- содержит некоторые настройки операционной системы.

Вы можете изменять этот файл, находящийся в корне системного раздела, с помощью любого текстового редактора.

Текст, находящийся в `boot.ini`, в самом тривиальном случае (использование одной ОС на компьютере Intel x86) выглядит следующим образом.

Листинг 3.1. Файл boot.ini

```
[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]

multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows
XP Professional RU" /noexecute=optin /fastdetect
```

Раздел `[boot loader]` служит для определения настроек загрузки операционной системы. Параметр `timeout` (по умолчанию его значение равно `30`) определяет время (в секундах), в течение которого пользователь выбирает один из пунктов загрузочного меню. Если значение `timeout` равно `0`, то данное меню не отображается, а при значении `-1` меню будет находиться на экране до того момента, пока не будет сделан выбор.

Параметр `default` указывает, где находится загружаемая по умолчанию операционная система. Раздел `[operation systems]` содержит данные об уже установленных операционных системах.

Если вы используете две операционные системы одновременно (например, Windows Me и Windows XP), содержимое файла будет выглядеть следующим образом.

Листинг 3.2. Файл boot.ini на компьютере с двумя операционными системами

```
[boot loader]

timeout=5

default=C:\

[operating systems]

C:\="Windows Millennium Edition"

multi(0)disk(0)rdisk(0)partition(2)\

WINNT="Windows XP Professional" /fastdetect
```

- `multi` — номер дискового адаптера, с которого производится загрузка; значение этого параметра всегда равно `0`;
- значение параметра `disk` для большинства моделей BIOS также равно `0`;
- параметр `rdisk(X)` определяет порядковый номер жесткого диска, с которого будет производиться загрузка ОС (возможные значения — от `0` до `3`);
- `partition(Y)` — порядковый номер логического диска (раздела), с которого будет загружаться ОС. Нумерация логических дисков начинается с единицы. Не нумеруются расширенные разделы MS-DOS (тип 5) и разделы типа 0 — неиспользуемые.

Чтобы восстановить файл `boot.ini`, воспользуйтесь командой `bootcfg`. Данная команда доступна из командной строки и может применяться для конфигурирования, извлечения, изменения или удаления параметров в файле `boot.ini`.

Формат команды `bootcfg`:

```
BOOTCFG /<операция> [<аргументы>]
```

Ключи командной строки программы:

- `/COPY` — копирует элемент списка загрузки в секции `[operating systems]`, куда после этого можно добавить параметры новой операционной системы;
- `/DELETE` — удаляет уже существующий фрагмент списка загрузки в секции `[operating systems]` файла `boot.ini`; вам потребуется указать номер элемента, который вы собираетесь удалить;
- `/QUERY` — отображает элементы списка загрузки и их настройки;
- `/RAW` — предоставляет возможность выбора любого переключаемого параметра, который будет добавлен для указанного элемента списка загрузки ОС;
- `/TIMEOUT` — устанавливает значение таймаута;

- /DEFAULT — устанавливает элемент списка загрузки, который будет использоваться по умолчанию;
- /EMS — позволяет устанавливать переключатель /redirect для указанного элемента списка загрузки;
- /DEBUG — позволяет установить порт и скорость для удаленной отладки определенного элемента списка загрузки;
- /ADDSW — добавляет определенные переключатели для указанного элемента списка загрузки;
- /RMSW — удаляет указанные пользователем переключатели указанного элемента списка загрузки;
- /DBG1394 — предоставляет возможность настройки отладки 1394 порта для определенного элемента списка загрузки;
- /? — справка.

Шаг 12. Не пренебрегаем специальными утилитами для настройки системы

Для быстрой настройки системы вы также можете обратиться к специальным утилитам — оптимизаторам. С их помощью вы сможете произвести настройку системы в целом, конфигурировать ее отдельные элементы, использовать некоторые скрытые возможности.

Одной из лучших программ в этом классе является XP Tweaker. Эта программа способна реализовать настройку и оптимизацию Windows XP. Кроме того, в нее дополнительно входят несколько параметров, специально разработанных для русских версий Windows XP.

Сайт разработчика данного XP Tweaker — http://www.xptweaker.net. Утилита распространяется бесплатно и имеет русскоязычный интерфейс. Она может сохранять все настройки в файле, чтобы в случае необходимости быстро настроить систему или же произвести аналогичные настройки системы на нескольких компьютерах.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch03\XP Tweaker v 1.53 вы найдете последнюю версию XP Tweaker.

Главное окно программы изображено на рис. 3.6.

Утилита способна настраивать большинство скрытых возможностей операционной системы и отображает подсказки по каждой из них.

Встроенная консоль XP Tweaker показывает список изменений, которые программа делает в реестре.

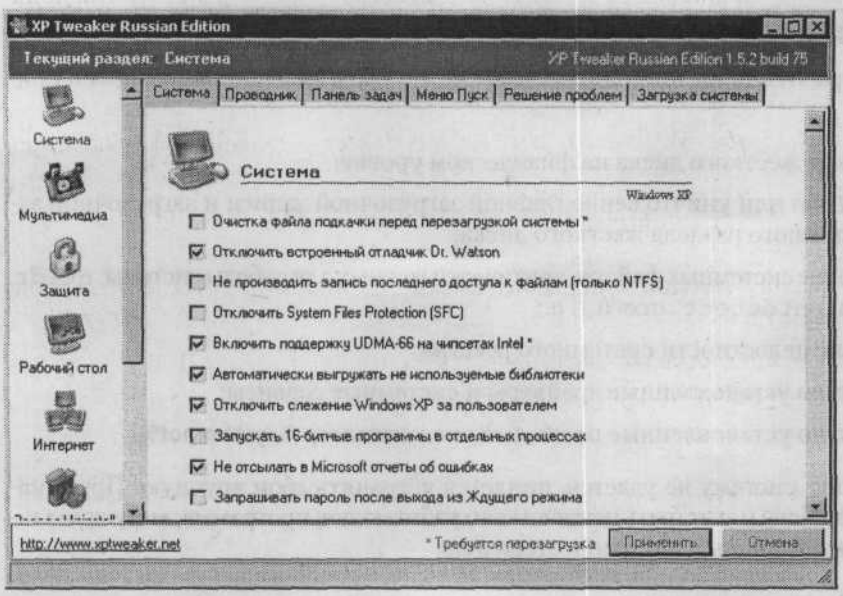


Рис. 3.6. Главное окно программы XP Tweaker

Программа тестировалась под следующими ОС:

- Windows XP Pro Rus;
- Windows XP Corporate Edition Eng + MUI;
- Windows Server 2003 Enterprise Edition Eng + MUI.

Вероятно, большинство функций будет работать в операционных системах Windows 2000 и Windows Longhorn, однако в этом случае вам нужно будет запустить программу с ключом `/nocheckver`. С операционными системами Windows 95/98/Me данная утилита работать не сможет.

ВНИМАНИЕ

Вы должны иметь права администратора, чтобы запустить эту утилиту (иначе большинство изменений сохранено не будет).

Безболезненное восстановление

Операционные системы Windows, принадлежащие к семейству NT (Windows NT/2000/XP/Server 2003), достаточно стабильны в работе. Причем чем меньше изменений внесено, тем надежнее функционирует операционная система. Однако в процессе работы некоторые изменения в конфигурацию вносить все же приходится (например, во время установки новых приложений), что может привести к нестабильной работе системы. Именно поэтому время от времени нужно делать резервные копии, которые позволят вам возвратиться к стабильному состоянию системы.

Почему система работает нестабильно

Нарушение работы операционной системы может быть вызвано следующими причинами:

- разрушение жесткого диска на физическом уровне;
- повреждение или уничтожение главной загрузочной записи и загрузочной записи системного раздела жесткого диска;
- повреждение системных файлов, критически важных для работы системы: `ntldr`, `boot.ini`, `ntdetect.com` и т. п.;
- нарушение целостности системного реестра;
- некорректно установленные драйверы и системные сервисы;
- некорректно установленные права доступа к каталогу %systemroot%.

Если загрузить систему не удается, придется устранять сбои вручную. Причинами подобных сбоев могут быть неправильно работающая программа, вирусная атака, ошибки в инициализации винчестера и др.

ПРИМЕЧАНИЕ

Обратите внимание, что по умолчанию Windows XP автоматически перезагружается при обнаружении серьезного сбоя в работе.

Остановимся подробнее на процессе загрузки операционной системы. Он состоит из следующих этапов.

1. Предварительная инициализация.
2. Работа загрузчика.
3. Загрузка ядра.
4. Загрузка системных служб.
5. Авторизация пользователя.

Проблема, возникшая на одном из этих этапов, может стать причиной того, что система не сможет загрузиться.

В состав Windows XP входят разнообразные средства восстановления работоспособности системы, среди которых безопасный режим, консоль восстановления и диск аварийного восстановления. Чтобы получить доступ к данным режимам, нужно удерживать клавишу F8 в процессе загрузки операционной системы.

Последняя удачная конфигурация

Если ошибки появились сразу после внесения пользователем каких-либо изменений (например, установки нового драйвера), можно использовать возможность загрузки операционной системы в режиме последней удачной конфигура-

ции. Этот режим позволит восстановить данные, находящиеся в реестре, и настройки драйвера, которые были установлены в последний раз, когда операционная система смогла нормально загрузиться. Обратите внимание, что данная функция восстанавливает только значения ветви `HKEY_LOCAL_MACHINE\System\CurrentControlSet`, а потому не способна решить проблемы с потерей системных файлов или повреждением разделов.

Если удалось загрузить Windows в режиме последней удачной конфигурации, то последние изменения, которые были сделаны в системе, скорее всего и были причиной, препятствующей корректному ее запуску.

Не бойтесь безопасного режима

Если вы выбрали способ загрузки Windows в безопасном режиме, то будут загружены только те службы и драйверы, которые необходимы для запуска системы. Этот режим может помочь, если загрузка становится невозможной в результате некорректной работы каких-либо драйверов или служб. В этом случае у вас будет возможность отключить их или же повторно настроить.

Прежде всего вам нужно проанализировать свои действия, которые могли привести к появлению сбоев (например, установка нового приложения). Если же вам не удалось выяснить причину сбоев таким способом, то придется остановиться на анализе состояния устройств и их драйверов (в этом поможет Диспетчер устройств), корректности работы системных сервисов, состояния файловой системы и реестра операционной системы. Помните, что если вам удалось загрузить систему в безопасном режиме, то, скорее всего, получится возобновить ее работоспособность.

Консоль восстановления: возьмите на заметку

Консоль восстановления представляет собой набор инструментов командной строки, которые способны исправить ситуацию даже тогда, когда система не может загрузиться и в безопасном режиме. Безусловно, возможности данной консоли ограничены и содержат лишь минимальный набор команд, однако часто и их оказывается достаточно, чтобы вернуть Windows к жизни.

Вы можете вызвать консоль восстановления, используя установочный диск Windows XP. Когда запустится программа установки, выберите режим восстановления (клавиша `R`), а в следующем окне — использование консоли (клавиша `C`).

ПРИМЕЧАНИЕ

Чтобы консоль восстановления обнаружила уже установленную операционную систему, системный реестр должен быть расположен в директории System32\Config. Если операционная система будет обнаружена, процесс восстановления продолжится (если систем несколько, то вам понадобится выбрать из списка нужную). Введите пароль администратора и начинайте работу с консолью.

Окно консоли восстановления показано на рис. 3.7.

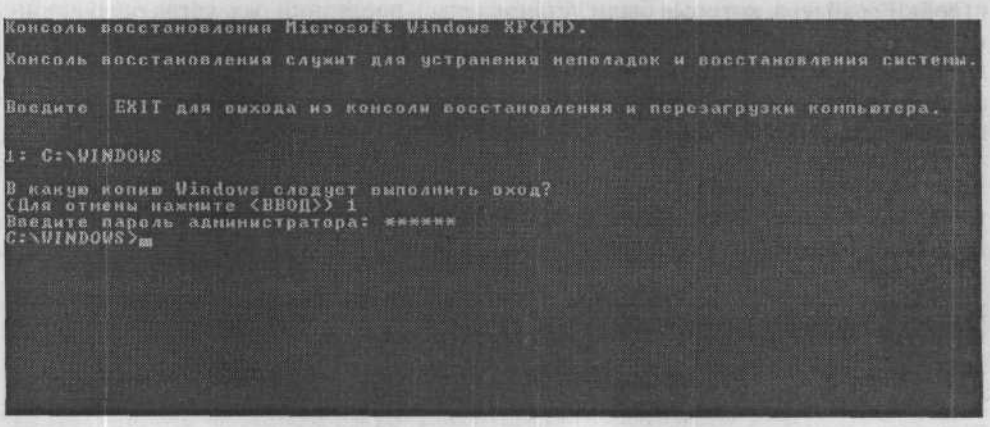


Рис. 3.7. Консоль восстановления

Введите в командной строке `help`, чтобы узнать перечень допустимых команд (или `help <command>` для получения справки по конкретной команде).

Используя консоль восстановления, вы можете:

- форматировать *логические разделы*;
- получить доступ к локальным дискам;
- запускать или останавливать работу драйверов или служб;
- совершать копирование файлов с установочного диска или прочих съемных носителей на жесткий диск (обратное копирование запрещено);
- создать или восстановить уже имеющийся загрузочный сектор и новую основную загрузочную запись (MBR).

В стандартном режиме консоль работает только с теми файлами, которые находятся в папке %systemroot%. Чтобы убрать данное ограничение, нужно воспользоваться локальной политикой безопасности. Выполните команду Пуск ▸ Панель управления ▸ Администрирование ▸ Локальная политика безопасности, затем Локальные политики ▸ Параметры безопасности. Теперь нужно включить один из параметров безопасности (рис. 3.8).

В своей работе консоль использует несколько важных переменных окружения:

- `AllowAllPath` (позволяет исполнить команду `CD` по всему диску);
- `AllowWildCards` (позволяет применять шаблоны имен файлов вместе с командами копирования и удаления);
- `AllowRemovableMedia` (позволяет копировать отдельные файлы со съемных носителей);
- `NoCopyPrompt` (позволяет перезаписывать файлы, которые уже находятся на жестком диске, без запроса разрешения пользователя).

Желательно активировать первые три переменные. Например, первую переменную активируют так:

```
set AllowAllPath = TRUE
```

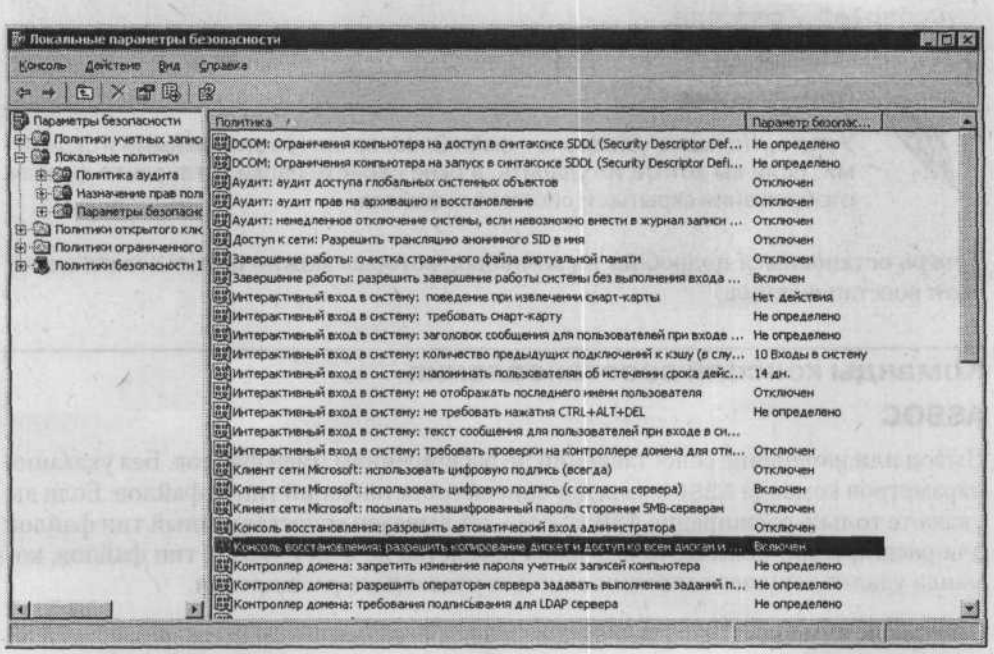


Рис. 3.8. Настраиваем консоль восстановления

Установка консоли восстановления на жесткий диск

Чтобы инсталлировать консоль восстановления на жесткий диск и установить в качестве одного из параметров меню загрузки, выполните следующие действия.

1. Войдите в Windows с правами администратора. Вставьте установочный диск Windows XP в привод компакт-дисков. Если вам будет предложено обновить операционную систему до Windows XP, откажитесь.
2. Используя командную строку, перейдите на установочный диск Windows XP. Введите команду: `\1386\winnt32.exe /cmdcons`.
3. Следуйте указаниям, которые будут появляться на экране.

Удаление консоли восстановления

Чтобы удалить консоль восстановления, проделайте следующее.

1. Удалите папку `\Cmdcons` и файл `Cmldr`, находящиеся в корне системного раздела.

2. Снимите флажок Только чтение для файла `boot.ini`, откройте данный файл с помощью Блокнота. Найдите и удалите строку, которая соответствует параметру запуска консоли управления. Например, данная строка может выглядеть так: `C:\cmdcons\bootsect.dat="Microsoft Windows 2000 Recovery Console" /cmdcons`.

ПРИМЕЧАНИЕ

Учтите, что папка \Cmdcons и файл Cmldr являются системными и скрытыми. Если вы хотите их удалить, в окне свойств папки установите флажок отображения скрытых и системных файлов.

Теперь остановимся подробнее на командах, которые можно использовать в консоли восстановления.

Команды консоли восстановления

ASSOC

Вывод или изменение сопоставлений по расширениям имен файлов. Без указания параметров команда `ASSOC` выведет список сопоставлений типов файлов. Если вы укажете только расширение файла, то будет выведен сопоставленный тип файлов для расширения. Если же после знака равенства не будет указан тип файлов, команда удалит текущее сопоставление для указанного расширения.

Синтаксис команды:

```
ASSOC [.ext[=[type]]]
```

- `ext` — расширение имени файла, которое сопоставляется с указанным типом файлов;
- `type` — тип файлов, который сопоставляется с расширениями имени файлов.

AT

Команда `AT` позволяет запускать команды и приложения по расписанию. Для использования данной команды нужно, чтобы была активна служба расписаний.

Синтаксис команды:

```
AT [\\имя_компьютера] [ [код] [/DELETE] | /DELETE [/YES]]

AT [\\имя_компьютера] время [/INTERACTIVE] [ /EVERY:день[,...]
| /NEXT:день[,...]] "команда"
```

- `\\имя_компьютера` — имя удаленного компьютера (если он не указан, будет использован локальный компьютер);
- `код` — порядковый номер задачи;
- `/delete` — отмена запланированной задачи (если код не указан, отменяются все запланированные задачи локального компьютера);

- /yes — отмена запроса на подтверждение при отмене всех запланированных задач;
- время — время запуска команды;
- /interactive — позволяет взаимодействие задачи и активного пользователя;
- /every:день[,...] — запуск задачи будет произведен по указанным дням недели или месяца (если значение опущено, будет использован текущий день месяца);
- /next:день[,...] — задача будет запущена в следующий указанный день недели (например, в следующую субботу); если значение указано не будет, то используется текущий день месяца;
- команда — команда Windows NT или имя пакетного файла.

CD

Вывод имени или смена текущего каталога. Данная команда необходима для перемещения по директориям жесткого диска.

Синтаксис команды:

```
CHDIR [/D] [диск:][путь]

CHDIR [..]

CD [/D] [диск:][путь]

CD [..]
```

- CHDIR — переход в родную директорию;
- /D — ключ, предназначенный для одновременной смены текущих диска и каталога.

Команда CD диск: выводит на экран имя текущего каталога данного диска. Команда CD без параметров отображает имена текущих диска и каталога.

COPY

Данная команда позволяет произвести копирование конкретного файла или папки.

Синтаксис команды:

```
COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/A | /B] источник [/A | /B]
[+ источник [/A | /B] [+ ...]] [результат [/A | /B]]
```

- источник — имя копируемого файла (файлов);
- /A — файл является текстовым файлом ASCII;
- /B — файл является двоичным файлом;
- /D — возможность создания зашифрованного файла;
- результат — папка, в которую производится копирование, а также конечные имена файлов в случае переименования;

- /V — контроль правильности копирования файлов;
- /N — использование коротких имен при копировании файлов, имена которых не соответствуют стандарту 8.3;
- /Y — утвердительный ответ на запрос подтверждения перезаписи существующего конечного файла;
- /-Y — обязательный запрос подтверждения на перезапись существующего конечного файла;
- /Z — копирование сетевых файлов с возобновлением.

Ключ /Y устанавливается с помощью переменной среды COPYCMD. Ключ /-Y командной строки переопределяет такую установку. По умолчанию понадобится подтверждение (исключение составляют случаи, когда команда COPY выполняется в пакетном файле).

СОВЕТ

Чтобы объединить фрагменты одного файла, укажите имя конечного и несколько исходных файлов, записывая команду в формате «файл1+файл2+файл3+...».

CHCP

Активирует определенную кодовую страницу.

Синтаксис команды:

```
CHCP [xxx]
```

xxx — номер кодовой страницы.

Если параметр не будет указан, то отобразится текущий номер кодовой страницы.

CHKDSK

Данная команда предназначена для выполнения теста файловой системы на жестком диске и отображения статистики.

Синтаксис команды:

```
CHKDSK [том:[[путь]имя_файла]] [/F] [/V] [/R] [/X] [/I] [/C] [/
L[:размер]]
```

- том — устанавливает имя тома или букву тестируемого диска с двоеточием;
- имя_файла — файлы, которые будут проверены на фрагментацию (только FAT);
- /F — исправление ошибок на диске;
- /V — отображение полного пути и имени каждого файла на этом диске (для FAT/FAT32), а для NTFS — также сообщений об очистке;

- /R — поиск поврежденных секторов жесткого диска и последующее восстановление данных из них (невозможно без использования ключа /F);
- /L:размер — используется только для NTFS: изменяет размер файла журнала до величины, которую указывает пользователь (в Кбайт);
- /X — предварительное отключение тома при необходимости. Все активные дескрипторы данного тома будут недействительны, необходим ключ /F;
- /I — только для NTFS: снижение уровня глубины проверки индексных элементов;
- /C — только для NTFS: принудительный отказ от тестирования циклов внутри структуры папок.

Последние два ключа способны ускорить процесс проверки.

CHKNTFS

Отображает или корректирует параметры проверки диска во время загрузки.

Синтаксис команды:

```
CHKNTFS том: [...]

CHKNTFS /D

CHKNTFS /T[:time]

CHKNTFS /X том: [...]

CHKNTFS /C том: [...]
```

- том — буква диска (с последующим двоеточием), точка подключения или имя тома;
- /T:time — изменяет обратный отсчет AUTOCHK на установленный пользователем отрезок времени (в секундах). Если значение не указано, отображает активную настройку;
- /X — принудительно отключает стандартную проверку диска в процессе загрузки. Информация, которая касается исключенных ранее дисков, не сохраняется;
- /D — все логические диски будут проверяться при загрузке, а CHKDSK будет запускаться при обнаружении ошибок;
- /C — посылает запрос на выполнение проверки диска при следующей загрузке. Если будут обнаружены ошибки, запускается CHKDSK.

СОВЕТ

Если вам не нужна задержка в 10 секунд перед проверкой дисков, то ключ chkntfs /t:0 избавит вас от этой проблемы.

CLS

Очищает содержимое экрана консоли (ключи не используются).

COLOR

Установка цветов для текста и фона консоли. Обратите внимание на то, что речь идет об установке цветов по умолчанию, а не о том, какие цвета будут применяться в текстовых окнах.

Синтаксис команды:

```
COLOR [цвет]
```

Параметр цвета назначается в виде двухзначного шестнадцатеричного числа, где первая цифра определяет цвет фона, а вторая устанавливает цвет текста. Любая цифра может иметь ряд значений, которые указаны в табл. 3.5.

Таблица 3.5. Коды цветов консоли

Цвет	Код цвета
Черный	0
Серый	8
Синий	1
Светло-синий	9
Зеленый	2
Светло-зеленый	A
Голубой	3
Светло-голубой	B
Красный	4
Светло-красный	C
Лиловый	5
Светло-лиловый	D
Желтый	6
Светло-желтый	E
Белый	7
Ярко-белый	F

Например, команда `COLOR 30` установит для фона голубой цвет, а для текста — черный. Если вы не указываете параметр, будут восстановлены значения, активные на момент запуска консоли.

ПРИМЕЧАНИЕ

Команда COLOR вернет значение ошибки ERRORLEVEL 1, если вы попытаетесь установить одинаковый цвет фона и текста.

COMPACT

Позволяет просматривать и изменять параметры сжатия файлов в разделах NTFS.

Синтаксис команды:

```
COMPACT [/C | /U] [/S[:dir]] [/A] [/I] [/F] [/Q] [file[...]]
```

- `/C` — сжатие указанных файлов. Папки получают пометку о сжатии, поэтому все файлы, помещенные в них, тоже будут сжаты;
- `/U` — распаковка выбранных сжатых файлов. С папок снимаются пометки о сжатии;
- `/S` — выполнение указанной операции во всех подпапках;
- `/A` — отображение файлов с атрибутами «скрытый» и «системный», которые пропускаются по умолчанию;
- `/I` — продолжение выполнения прерванной операции даже после сбоя;
- `/F` — принудительное сжатие всех указанных файлов, даже если некоторые из них уже сжаты;
- `/Q` — отображение только важных сведений;
- `file` — имя файла, имя директории или шаблон имен файлов.

В случае запуска без дополнительных параметров программа `COMPACT` отображает состояние сжатия текущей папки и каждого файла, который в ней присутствует. Возможен ввод нескольких файлов. Если указаны несколько параметров, они разделяются пробелами.

CONVERT

Данная утилита позволяет конвертировать FAT в NTFS.

Синтаксис команды:

```
CONVERT том: /FS:NTFS [/V]
```

- `том` — буква диска (с последующим двоеточием), точка подключения или имя тома;
- `/FS:NTFS` — файловая система, в которую происходит преобразование: NTFS;
- `/V` — включение режима отображения сообщений.

Процесс обратного конвертирования невозможен.

DEL

Удаление файлов.

Синтаксис команды:

```
DEL [/P] [/F] [/S] [/Q] [/A[[:]атрибуты]] имена

ERASE [/P] [/F] [/S] [/Q] [/A[[:]атрибуты]] имена
```

- имена — имена одного или нескольких файлов. Чтобы удалить несколько файлов, нужно использовать подстановочные знаки. Если будет указано имя директории, она будет удалена;
- /P — запрос на подтверждение удаления каждого файла;
- /F — принудительное удаление файлов, которые доступны только для чтения;
- /S — удаление указанных файлов из всех подпапок;
- /Q — отсутствие запроса на подтверждение при удалении файлов;
- /A — фильтр файлов для удаления по атрибутам.

Перечень атрибутов: S (системные файлы), R (доступные только для чтения), H (скрытые файлы), A (файлы для архивирования). Возможно также использование префикса -, который придаст команде противоположное значение (аналогичен логическому значению НЕ).

DISKCOMP

Сравнивает данные, которые хранятся на двух различных дискетах.

Синтаксис команды:

```
DISKCOMP [диск1: [диск2:]]
```

Буква первого диска может совпадать с буквой второго диска. Например, следующим образом: `DISKCOMP a: a:`

Для сравнения файлов существует команда FC (FileCompare).

FORMAT

Форматирование жесткого диска или его раздела.

Синтаксис команды:

```
FORMAT том: [/FS:система] [/V:метка] [/Q] [/A:размер] [/C] [/X]

FORMAT том: [/V:метка] [/Q] [/F:размер]

FORMAT тома: [/V:метка] [/Q] [/T:дорожки /N:секторы]

FORMAT тома: [/V:метка] [/Q] [/1] [/4]

FORMAT том [/Q] [/1] [/4] [/8]
```

- том — указывает букву диска (с последующим двоеточием), точку подключения или имя тома;
- /FS:filesystem — определяет тип файловой системы (FAT, FAT32 или NTFS), которая будет использоваться после форматирования;
- /V:метка — метка тома;
- /Q — быстрое форматирование;
- /C — использование сжатия для всех файлов, которые окажутся на новом томе;

- /X — отключает том в качестве первого действия, если это необходимо. Все активные дескрипторы тома будут неверны;
- /T:дорожки — число дорожек на каждой стороне диска;
- /N:секторы — число секторов на каждой дорожке;
- /1 — форматирование одной стороны дискеты;
- /8 — создание восьми секторов на каждой дорожке;
- /4 — форматирование 5,25I дискеты емкостью 360 Кбайт в приводе высокой плотности;
- /F:размер — устанавливает размер дискет, которые подлежат форматированию (160, 180, 320, 360, 640, 720, 1,2, 1,23, 1,44, 2,88 или 20,8);
- /A:размер — корректирует размер кластера по умолчанию.

Файловые системы поддерживают следующие размеры кластеров.

- NTFS — 512, 1024, 2048, 4096, 8192 байт, 16, 32, 64 Кбайт.
- FAT — 512, 1024, 2048, 4096, 8192 байт, 16, 32, 64 Кбайт, (128, 256 Кбайт для размера сектора больше 512 байт).
- FAT32 — 512, 1024, 2048, 4096, 8192 байт, 16, 32, 64 Кбайт, (128, 256 Кбайт для размера сектора больше 512 байт).

Учтите, что файловые системы FAT и FAT32 имеют следующие ограничения на количество кластеров тома:

- FAT — количество кластеров <= 65526;
- FAT32 — 65526 < количество кластеров < 268435446.

ВНИМАНИЕ

Тома NTFS с размером кластера более 4096 байт не подлежат сжатию.

FTYPE

Позволяет изменить командную строку открытия файлов. Если использовать данную команду без параметров, то будет выведен текущий список типов файлов, для которых назначены командные строки открытия. Эта функция команды FTYPE предоставляет возможность получить информацию о сопоставлениях типов. Обратите внимание, что те типы, которые были зарегистрированы с использованием OLE, здесь не отобразятся.

Синтаксис команды:

```
FTYPE [тип_файлов[=[командная_строка_открытия]]]
```

- тип_файлов — тип файлов для просмотра или редактирования;
- командная_строка_открытия — команда открытия, которая будет применяться при запуске файлов определенного типа.

RECOVER

Позволяет восстановить данные на поврежденном логическом (или физическом) диске.

Синтаксис данной команды:

```
RECOVER [диск:][путь]имя_файла
```

`[диск:][путь]имя_файла` — полный путь к файлу, который подлежит восстановлению.

Информация, которая находилась в поврежденных секторах, будет утеряна. Данная команда может быть использована для дискет, на которых размещен архив, включающий `Recovery Record`.

START

Позволяет запустить указанную пользователем программу (или команду) в индивидуальном окне.

Синтаксис команды:

```
START программа
```

`Программа` — команда или путь к исполняемому файлу.

SUBST

Позволяет сопоставить имя диска указанному пути (удобно для быстрого изменения буквы диска).

Синтаксис команды:

```
SUBST [диск1: [диск2:]путь]
```

```
SUBST диск1: /D
```

- `диск1` — виртуальный диск, который вы хотите сопоставить указанному пути;
- `[диск:]путь` — реальный диск и путь, которым вы собираетесь сопоставить виртуальный диск;
- `/D` — удаление существующего виртуального диска.

Данная команда, используемая без параметров, позволит ознакомиться со списком уже созданных жестких дисков.

TREE

Отображение дерева структуры папок или путей в графическом виде.

Синтаксис команды:

```
TREE [диск:][путь] [/F] [/A]
```

- /F — отображение имен файлов в каждой директории;
- /A — принудительное использование символов ASCII вместо символов локального алфавита.

VER

Отображает версию установленной операционной системы. Обратите внимание, что с помощью данной команды вы не сможете узнать версию установленного Service Pack. Для этого существует команда WINVER.

VERIFY

Включает или отключает режим контроля правильности записи информации на диск.

Синтаксис команды:

```
VERIFY [ON | OFF]
```

Ввод команды без параметров позволит узнать текущее состояние данного режима (включен или отключен).

MKDIR

Команда, позволяющая создать новую директорию.

Синтаксис команды:

```
MKDIR [диск:]путь

MD [диск:]путь
```

Команда MKDIR способна создать все необходимые поддиректории. Предположим, что каталога \a не существует. В таком случае команда `mkdir \a\b\c\d` даст такой же результат, как и следующий набор команд:

```
mkdir \a

chdir \a

mkdir b

chdir b

mkdir c

chdir c

mkdir d
```

Зная команды, используемые в Консоли восстановления, можно быстро восстановить работоспособность операционной системы, отказавшейся нормально функционировать. Количество этих команд невелико, однако они достаточно эффективны для борьбы с системными неполадками.

ГЛАВА 4 Полезные приемы установки и настройки Windows

- Драйвер без автомобиля
- Самоустанавливающаяся Windows — мечта администратора
- Откаты и резервные копии
- Администрируем локальную сеть, не покидая рабочего места
- Потеря файлов: что же делать?
- Ядерная инженерия

В этой главе остановимся на некоторых нужных и полезных приемах инсталляции и настройки Windows: работе с драйверами, создании автоматической установки и копировании Windows. Кроме того, подробно рассмотрим основные вопросы, касающиеся работы с программой Acronis TrueImage, которая позволяет выполнять резервное копирование ваших данных, и с программой Remote Administrator, позволяющей производить удаленное администрирование компьютеров в сети. Вы научитесь менять ядро Windows, адаптируя операционную систему к различным конфигурациям оборудования.

Драйвер без автомобиля

Драйвер — это вовсе не водитель, а модуль, который подключается к операционной системе и служит для ее корректного взаимодействия с физическим устройством. Драйверы прилагаются к большинству установленных устройств: видеокарте, звуковой карте, мультимедийной клавиатуре, монитору и т. д. Предположим, что операционной системе требуется получить данные, которые вводятся с клавиатуры. В этом случае система будет обращаться к драйверу, а не напрямую к устройству. Каждый драйвер содержит определенный набор команд, предназначенный именно для данного оборудования. Как правило, производители устройств сами разрабатывают драйверы для своих продуктов.

Подавляющее число оборудования укомплектовано дисками с «родными» драйверами, что связано с необходимостью непосредственного доступа к аппаратной части. Целью такой комплектации может быть оптимизация работы или обеспечение безопасного обмена информацией с устройством. Последний подход характерен для разработчиков антивирусного программного обеспечения. С помощью своих драйверов они могут получить необходимую информацию о размере исследуемых файлов, дате их изменения и прочих параметрах.

Любому пользователю приходится сталкиваться с драйверами в повседневной жизни, например при добавлении нового устройства или приполной переустановке системы. Далее мы подробнее остановимся на специальных программах, которые способны значительно упростить процесс работы с разнообразными драйверами.

Следует учесть, что Windows XP обладает возможностью сертификации драйверов в Windows Hardware Quality Labs (которая должна упразднить проблему с некорректно работающими драйверами), имеет объемную базу драйверов в дистрибутиве, способность возвращения ранее установленного драйвера в случае возникновения ошибок и множество других полезных функций. Это позволяет реализовать обновление или удаление драйверов и вручную, не используя дополнительных инструментов.

Однако при частой смене конфигурации вполне возможно появление разнообразных сбоев, так как некорректно работающие устройства являются повсеместно распространенной проблемой. Еще одна сложность возникает, если система не способна правильно распознать подключенное устройство.

Самые лучшие драйверы — «Мои драйверы» (My Drivers)

Основная задача программы My Drivers — обновление и резервное копирование всевозможных драйверов. Веб-страница разработчика — http://www.zhangduo.com. Впервые установив эту программу, вы можете использовать ее без ограничений в течение 15 дней, после чего программу следует приобрести (цена составляет $39). Окно программы My Drivers изображено на рис. 4.1.

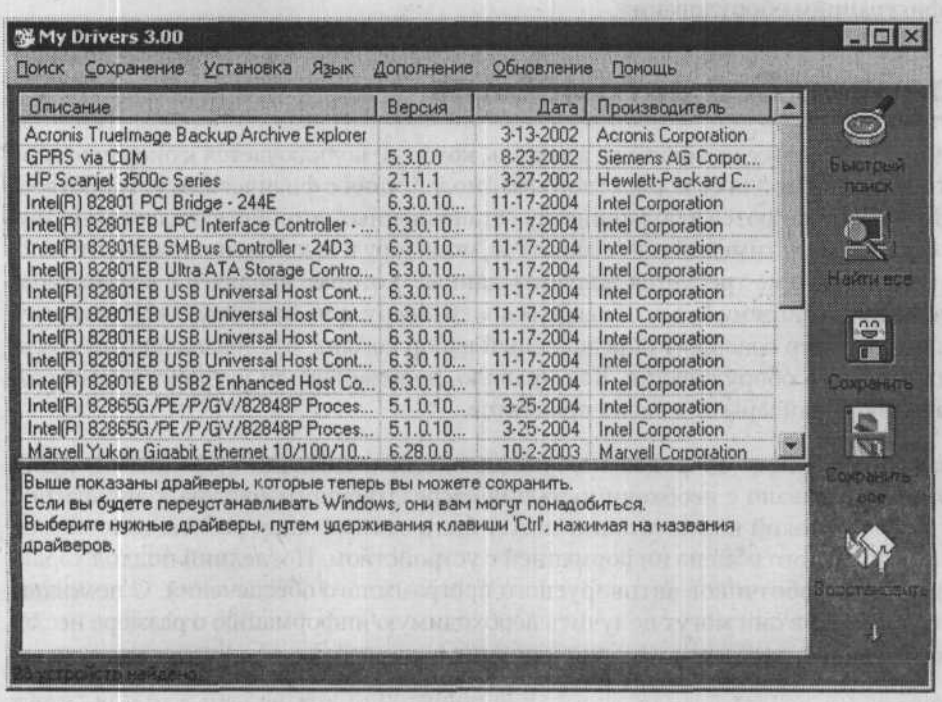


Рис. 4.1. Окно программы My Drivers

Одно из достоинств программы, которое сразу радует глаз, — поддержка русского языка. Программа My Drivers работает в двух основных режимах — определение драйверов оборудования и работа с драйверами, которые уже установлены. Работая в первом режиме, программа найдет все драйверы, которые используются вашей операционной системой, и упорядочит их в виде древовидного меню. Выбрав в данном меню конкретный драйвер, вы сможете ознакомиться с информацией о производителе и модели устройства.

Кроме того, вам будут доступны возможности перехода к сайту производителя или поисковой системе Google для поиска соответствующего драйвера. Во втором режиме работы можно проверить наличие обновлений для каждого установленного драйвера (или же для всех вместе). Сам процесс обновления выполнен более чем удобно: утилита загружает из Интернета небольшую базу и отображает список обновлений с указанием ресурса, откуда будут загружаться драйверы, и расчетным

процентом совместимости. Обязательно обратите внимание на дату создания драйвера, который предлагается для обновления, так как иногда случается, что программа пытается загрузить более старую версию имеющегося драйвера.

Программа способна сохранить указанные драйверы в CAB-архив или же в программу-инсталлятор. При этом полное резервное копирование драйверов отнимет всего несколько минут.

Восстановление драйверов из резервной копии тоже происходит достаточно быстро. Данная функция позволит вам значительно ускорить процесс переустановки системы, ведь теперь все необходимые драйверы будут установлены автоматически.

Программа умеет работать с подключаемыми модулями — плагинами. В дополнение к программе поставляются два плагина, которые производят резервное копирование базы Outlook и закладок Internet Explorer.

Корректно удаляем драйверы

Практика показывает, что чаще всего пользователи обновляют драйверы для видеоадаптеров. Если компания ATI каждый месяц выпускает официальные версии своего набора драйверов Catalyst, то новые Forceware от nVidia достаточно часто появляются на различных неофициальных сайтах и не всегда нормально функционируют.

Все производители рекомендуют удалять устаревшие версии драйверов, перед тем как устанавливать новые, для нормальной работы последних. Кроме того, достаточно часто драйверы при удалении оставляют множество записей в реестре, которые способны помешать нормальной работе новой версии драйверов.

Для удаления старых драйверов перед установкой новых версий или при смене оборудования была разработана небольшая программа Driver Cleaner. Домашняя страница разработчиков программы: www.drivercleaner.net.

Программа может удалить не только драйверы распространенных видеокарт ATI и nVidia, но и драйверы данных устройств от 3dfx, SiS, Intel, драйверы чипсета nForce, драйверы звуковых карт от Creative (в том числе KX), Realtek, Turtle Beach. Некоторым пользователям может пригодиться функция Cab Cleaner, которая позволяет удалить устаревшие версии драйверов из дистрибутива Windows. Любые изменения можно сохранить или же вернуться к предыдущей конфигурации при возникновении различных сбоев. Главное окно программы Driver Cleaner показано на рис. 4.2.

Чтобы удалить определенный драйвер, выполните команду Настройки ▸ Помощник и укажите тот драйвер, который собираетесь удалять, после чего нажмите кнопку Далее, а в следующем окне — Очистить. Как видите, процесс удаления максимально упрощен, однако со своими обязанностями программа справляется отлично.

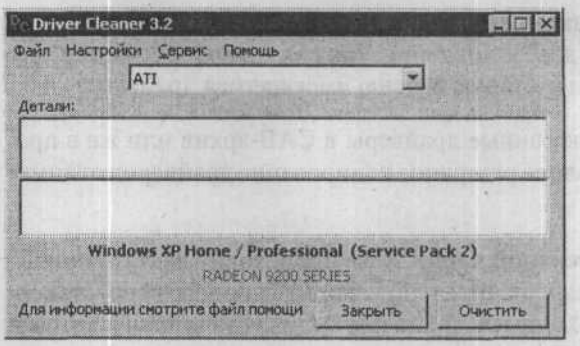


Рис. 4.2. Главное окно программы Driver Cleaner

Драйверы + Windows: тесная интеграция

После того как вы сохранили все самые последние версии нужных драйверов, стоит поместить их в дистрибутив Windows, чтобы при следующей переустановке система автоматически установила все драйверы. Чтобы сделать это, следует обратиться к такому способу установки, как создание файла ответов с помощью утилиты Setup manager, входящей в дистрибутив (находится по адресу `SUPPORT\TOOLS\Deploy.cab\setupmgr.exe`).

Запустите `setupmgr.exe` и выберите пункт Создать новый файл ответов в главном меню программы. Далее выберите пункт windows unattended installation (остальные настройки нас не интересуют). Следующий пункт — user interaction level — отвечает за автоматизацию процесса инсталляции. Устанавливаем значение fully automated (что позволит произвести установку автоматически) или Hide Pages (что позволит произвести более подробную настройку всего дальнейшего с выбором раздела для установки).

Далее следуйте инструкциям программы (рис. 4.3).

В самом конце вы получите файл с ответами. Вам следует открыть его в любом текстовом редакторе и несколько изменить. Для начала найдите раздел `[Unattended]`, с которым мы и продолжим работу. Обратите внимание, что здесь должен присутствовать параметр `OemPreinstall=Yes` (если его нет — создайте). В папке с дистрибутивом нужно создать директорию `$OEM$`, а в ней — папки `$$` и `$1`. В каталог `$OEM$\$1\Drivers\` поместите все необходимые для установки драйверы, а в каталог `$OEM$\$$\INR` — все нужные INF-файлы.

В файле ответов найдите параметр `OemPnPDriversPath=` и укажите после знака равенства пути к драйверам внутри каталога `$1` (например, `DriversVideo`) через точку с запятой. Чтобы Windows не уведомляла вас каждый раз об отсутствии подписей у используемых драйверов, в том же разделе нужно создать параметр `DriverSigningPolicy=Ignore`. После проделанной операции сохраняем файл ответа под именем `winnt.sif` и копируем его в папку `I386` дистрибутива Windows. Теперь в процессе инсталляции операционной системы все необходимые драйверы будут автоматически установлены.

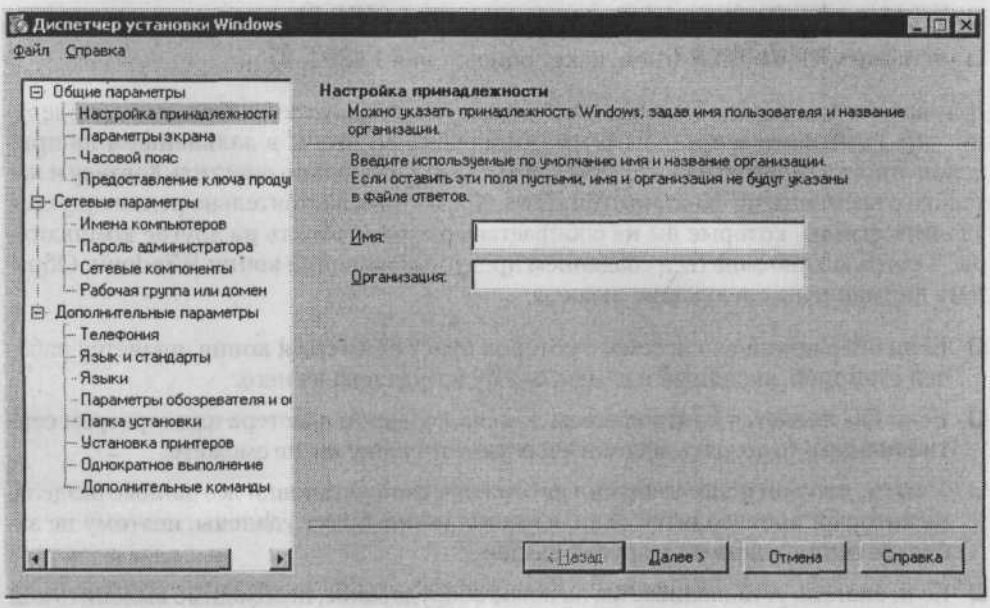


Рис. 4.3. Создаем файл ответов

Самоустанавливающаяся Windows — мечта администратора

При использовании больших локальных сетей может возникнуть потребность установить (или обновить) операционную систему сразу на всех компьютерах. Для решения подобной задачи существуют специальные приемы.

Как оказалось, у системного администратора есть возможность создания предустановленной копии дистрибутива Windows для последующей автоматической установки, а также полного копирования (клонирования) операционной системы Windows на любое количество компьютеров. Пригодится такая возможность и тем, кто хочет просто создать резервную копию операционной системы, чтобы достаточно быстро ее восстановить в случае полного краха.

Средства развертывания Windows дают возможность установить и настроить следующие операционные системы:

- Windows Server 2003, Standard Edition;
- Windows Server 2003, Enterprise Edition;
- Windows Server 2003, Datacenter Edition;
- Windows Server 2003, Web Edition;
- Windows XP 64-Bit Edition версия 2003;
- Windows XP Home Edition, пакет обновления 1 (SP1, 2);

- Windows XP Professional, пакет обновления 1 (SP1, 2);
- Windows XP 64-Bit Edition, пакет обновления 1 (SP1, 2).

Для начала вам понадобится операционная система с установленными драйверами, обновлениями и программным обеспечением, чтобы в дальнейшем не пришлось инсталлировать все это отдельно. Далее желательно очистить Корзину и каталоги с временными файлами Windows. Кроме того, настоятельно рекомендуется удалить файлы, которые вы не собираетесь распространять на другие компьютеры. Теперь можно заняться созданием предустановленной копии Windows. Обратите внимание на следующие нюансы.

- Если операционная система, с которой будет сниматься копия, является рабочей станцией, входящей в домен, она будет удалена из него.
- Если ОС является контроллером домена, сервером кластера или сервером сертификации, то создать автоматическую установку вы не сможете.
- Учтите, что при использовании автоматической установки все данные раздела, на который производится данная инсталляция, будут удалены, поэтому не забудьте скопировать их в другой раздел.
- Если система устанавливается на новое оборудование, необходимо выяснить вид HAL (Hardware Abstraction Layer — слой абстрагирования оборудования) — с поддержкой ACPI или без нее, APIC (Advanced Programmable Interrupt Controller) или PIC — так как исходная копия должна соответствовать указанным значениям (все необходимые данные можно посмотреть в `Power Management` вашей BIOS). В случае несовпадения нужно прописать правильный HAL в соответствующем разделе файла `sysprep.ini`.
- Раздел, на который будет устанавливаться система, должен быть не меньше того раздела, с которого снималась данная копия операционной системы.

Для начала создадим папку sysprep в корне системного раздела. Туда нужно скопировать файлы `sysprep.exe` и `setupcl.exe` из дистрибутива вашей ОС (находятся в архиве `\support\tools\deploy.cab`). По умолчанию утилита `sysprep.exe` изменяет Security ID (SID). Данное изменение нужно для корректной работы разных компьютеров в рабочей группе или домене. Если SID менять не следует (например, чтобы не возникло проблем с доменом при использовании старого NetBIOS-имени машины при переустановке операционной системы), запустите утилиту `sysprep.exe` с ключом `-nosidgen` (`sysprep.exe -nosidgen`).

Возможны два варианта автоматической установки Windows:

- полная автоматическая установка, проходящая в фоновом режиме без вашего участия;
- полуавтоматическая установка, предусматривающая ваши ответы на некоторые вопросы в процессе инсталляции (серийный номер, имя пользователя и т. д.).

Для того чтобы необходимые поля заполнялись автоматически, нужно создать файл `sysprep.ini` самостоятельно или с помощью утилиты `setupmgr.exe`, располо-

женной в том же архиве \support\tools\deploy.cab. Созданный файл необходимо поместить в одну папку с sysprep.exe и setupcl.exe.

Наиболее часто данный файл создается с помощью утилиты. Для этого запускаем setupmgr.exe, нажимаем кнопку Далее, выбираем пункт Создать и снова нажимаем кнопку Далее. В новом окне выбираем пункт Установка sysprep.

Далее следует выбрать устанавливаемую операционную систему. В утилитах, которые прилагаются к Windows 2000 и Windows XP/Server 2003, данные пункты несколько отличаются, однако общий принцип остается без изменений. После этого выберите значение Полностью автоматическая установка и нажмите кнопку Далее. В Windows XP/Server 2003 загрузится диспетчер установки с деревом значений слева. Пройдитесь по его разделам и заполните необходимые поля.

При использовании Windows 2000 мастер будет продолжать задавать вопросы. Большинство значений Windows 2000 и Windows XP/Server 2003 схожи, хотя небольшие отличия все-таки есть. Остановимся на этих пунктах подробнее.

- Имя и организация — реквизиты физического или юридического лица, на которое зарегистрирована данная копия операционной системы.
- Режим лицензирования (только для Windows 2000 Server) — сервер или рабочая станция.
- Имя компьютера — можно задать вручную, импортировать список имен или позволить системе самостоятельно сгенерировать имя.
- Пароль администратора — можно ввести самостоятельно или предоставить данную возможность пользователю (для этого нужно было ранее выбрать не Полностью автоматическая установка, а пункт Не отображать диалоговые окна), кроме того, можно после установки автоматически войти с правами администратора необходимое число раз (как правило, не более одного). В Windows 2000 пароль не шифруется, поэтому нужно быть аккуратнее с созданной копией (так как оттуда его совсем несложно достать), а вот в Windows XP/Server 2003 присутствует возможность шифрования пароля.
- Установки экрана — можно оставить значения по умолчанию или же выставить необходимые параметры.
- Сетевые параметры — зависят от вашей локальной сети.
- Рабочая группа или домен (если машина вводится в домен заново или же с новым SID, нужно указать логин и пароль вашей учетной записи).
- Часовой пояс — выберите нужный.

Дополнительные параметры можно настроить самостоятельно или разрешить сделать это операционной системе (берутся из текущей конфигурации):

- языковые настройки;
- удаленный доступ (с использованием модема);
- параметры обозревателя;

- каталог, в который установлена Windows (можно изменить);
- сетевые принтеры;
- можно задать запуск определенных приложений при первом входе пользователя в систему;
- можно указать папку с дистрибутивом, где расположены дополнительные компоненты или драйверы для установки (естественно, их нужно туда предварительно поместить);
- если в системе присутствуют нестандартные запоминающие устройства (SCSI, RAID), можно указать, где находятся драйверы к ним;
- при установке на компьютер, который имеет другой HAL, нужно указать его месторасположение (дистрибутив);
- фон и логотип, которые будут появляться при установке;
- дополнительные файлы и каталоги для копирования на компьютер, на который производится установка;
- место на жестком диске, куда следует сохранить файл установок.

Скопируйте дистрибутив в заранее созданную папку.

После того как вы выполнили описанные действия, запустите `sysprep.exe`, согласитесь с предупреждением и ждите отключения компьютера.

Теперь у вас есть предустановленная копия ОС в системном разделе. С данного раздела нужно снять образ с помощью любого специального приложения (Norton Ghost 2003, Acronis Migrate Easy из пакета Acronis Partition Expert и т. д.).

Образ не понадобится, если вы собираетесь автоматически устанавливать систему исключительно на своем компьютере, а вот если вы собираетесь клонировать Windows для установки на другие компьютеры, то без образа вам не обойтись.

Клонирование операционной системы заключается в копировании созданного образа на жесткий диск другого компьютера с дальнейшим восстановлением (при этом желательно, чтобы разделы, в пределах которых осуществляется клонирование, совпадали по размерам). Чистое клонирование (путем простого снятия образа) можно использовать для резервного копирования своей ОС или же для установки на другие компьютеры с идентичным оборудованием.

Оптимизируем образы автоматической установки

Чтобы оптимизировать процесс клонирования (уменьшить размер образа и сократить время, необходимое для установки), нужно придерживаться следующих правил.

- В случае возможной установки образа на компьютеры с различной конфигурацией постарайтесь подготовить универсальный набор, который будет подходить нескольким компьютерам одновременно.

- Сократите количество устройств в разделе [SysprepMassStorage] файла Sysprep.inf. Включение пустого раздела [SysprepMassStorage] в файл Sysprep.inf и указание значения параметра BuildMassStorageSection=Yes в разделе [Sysprep] приведет к тому, что программа Sysprep автоматически создаст записи в [SysprepMassStorage] на основе кодов оборудования Plug and Play из Machine.inf, Scsi.inf, Pnpscsi.inf и Mshdc.inf.
- Наиболее популярные приложения (например, Microsoft Office) нужно включить в образ, причем уже готовыми к работе.
- Перед созданием образа удалите из дистрибутива автоматической установки файлы Hiberfil.sys и Pagefile.sys (по своим размерам соответствует объему ОЗУ). Нужно удостовериться, что в разделе %SYSTEMDRIVE% компьютера, на который вы собираетесь копировать операционную систему, присутствует достаточно свободного места, чтобы поместить весь объем ОЗУ данной системы. Это нужно для корректного воссоздания файла Pagefile.sys в процессе автоматической установки. Чтобы удалить файл Hiberfil.sys, воспользуйтесь командой del /a:sh hiberfil.sys. При необходимости Windows восстановит оба файла самостоятельно.
- Кроме того, перед созданием образа нужно удалить все файлы, которые находятся в каталоге %WINDIR%\System32\Dllcache. Это нужно, чтобы защита операционной системы могла работать корректно. Если вы удалите папку %WINDIR%\System32\Dllcache, нужно указать значение параметра SourcePath в разделе [ComputerSettings] файла Winbom.ini, указывающее на папку i386 на компьютере конечного пользователя. Папка i386 должна быть расположена в каталоге %WINDIR%. Удаление файлов внутри образа возможно, только если у вас есть специальные утилиты для коррекции образа или доступ к диску для удаления данных файлов. В процессе установки Windows удаление файлов из инсталляционной копии Windows будет невозможным.

Как сделать раздел NTFS шире

Во время инсталляции Windows может понадобиться произвести расширение раздела диска на конечном компьютере. В случае добавления в раздел [Unattended] файла ответов Unattend.txt параметра ExtendOemPartition программа установки расширит раздел, в который производится инсталляция, используя неразмеченное дисковое пространство. Вы можете установить ограничение на увеличение раздела, присвоив параметру ExtendOemPartition значение, которое отличается от 1 (будет полезно, если нужно настроить несколько разделов).

ВНИМАНИЕ

Описанный параметр ExtendOemPartition можно использовать как в файле Unattend.txt, так и в Sysprep.inf. Когда он используется в файле Sysprep.inf, объем жесткого диска конечного компьютера, на который копируется образ, должен быть больше или равен объему жесткого диска компьютера, с которого снималась копия операционной системы.

Расширению поддаются только разделы жесткого диска, использующие NTFS. Если же расширяемый раздел использует файловую систему FAT или FAT32, его необходимо преобразовать в NTFS. Для этого присвойте параметру `FileSystem` в разделе `[Unattended]` файла `Unattend.txt` значение `ConvertNTFS`. Дело в том, что программа установки не способна расширять FAT32 и FAT-разделы, а утилита Sysprep не сможет самостоятельно преобразовать FAT32 или FAT в NTFS.

Откаты и резервные копии

Работа системного администратора тесно связана с настройкой операционной системы и разнообразных программ. Неправильная настройка может привести к потере работоспособности системы. Бывают такие ситуации, когда нужно серьезно изменять установки операционной системы (например, с целью повышения производительности). Само собой, существует риск того, что система даст сбой в результате каких-то неправильных действий. Именно поэтому стоит призадуматься о создании резервной копии операционной системы перед началом всевозможных экспериментов.

Решить подобную проблему поможет Acronis TrueImage. Данное приложение способно создавать образ жесткого диска (или его разделов) компьютера и позволяет сохранить данный образ в виде архива на винчестере или на сменном носителе (Iomega ZIP или Jaz, CD-R(W) или DVD-R(W)).

На сайте разработчика программы (`http://www.acronis.ru`) можно ознакомиться с документацией к Acronis TrueImage и скачать ее пробную версию. Демо-версия обладает одним существенным ограничением: не может сохранять изменения на жесткий диск. Чтобы получить возможность полноценной работы с программой, вам нужно будет приобрести лицензию ($49), однако помните, что зачастую потеря данных может обойтись дороже.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch04\Acronis TrueImage v 8 вы найдете демонстрационную версию Acronis TrueImage 8.

Когда у вас будет образ жесткого диска, вы легко сможете восстановить из него операционную систему в том виде, в каком она была на момент сохранения. Образ представляет собой архив, где содержатся данные жесткого диска или его раздела в зашифрованном виде. Файл архива способен вмещать образы нескольких дисков или разделов и может располагаться как на жестком диске, так и на другом носителе, который подключен к компьютеру на данный момент. Обратите внимание, что Acronis TrueImage способна извлекать из образа любой файл или каталог.

Одним из преимуществ Acronis TrueImage является посекторное (а не пофайловое, как у многих ее конкурентов) копирование, что предоставляет возможность использования программы для резервного копирования любых операционных систем. Кстати, с помощью Acronis TrueImage вы можете произвести процесс клонирования операционной системы и на несколько компьютеров.

После создания образа вы можете быть спокойны за сохранность вашей операционной системы и всех файлов данного раздела. При возникновении сбоя или вирусной атаки вы легко сможете восстановить всю необходимую информацию из образа. Acronis TrueImage может присоединить сохраненный образ в качестве временного раздела жесткого диска, чтобы вы могли скопировать с него все необходимые файлы.

Acronis TrueImage использует следующие средства для восстановления разделов жесткого диска (или всего диска целиком):

- создание загрузочной дискеты или компакт-диска, с которого будет происходить запуск Acronis TrueImage (необходимо, если запустить операционную систему невозможно);
- работа с дисками неограниченной емкости;
- возможность работы со сменными носителями, которые оснащены интерфейсом IDE, SCSI, USB или PCMCIA.

Кстати, программа позволяет восстанавливать разделы (кроме системных) на лету, без необходимости перезагрузки.

Программа работает под управлением операционных систем Windows следующих версий:

- Windows Server 2003;
- Windows XP;
- Windows 2000 Advanced Server;
- Windows 2000 Server;
- Windows 2000 Professional;
- Windows NT 4.0 Server Service Pack 6;
- Windows NT 4.0 Service Pack 6.

Используя утилиту Acronis TrueImage, можно создать загрузочный компакт-диск, содержащий программу, которая будет работать без загрузки операционной системы. Соответственно, такая возможность позволяет использовать утилиту на компьютере, использующем любую ОС.

Программа способна работать со всеми файловыми системами распространенных ОС, в том числе:

- MS-DOS всех версий;
- Windows 3.1 + MS-DOS;
- Windows 95/98/Me;
- Windows NT/2000/XP;
- Linux с файловыми системами Ext2, Ext3 и ReiserFS;
- FreeBSD;
- Solaris;

- SCO UNIX;
- OS/2;
- BeOS;
- QNX.

Системные требования для такой полезной программы очень скромные:

- PC-совместимый компьютер с процессором Pentium или выше;
- 32 Мбайт ОЗУ;
- дисковод или привод компакт-дисков;
- монитор VGA.

Производители Acronis TrueImage также рекомендуют иметь компьютерную мышь.

Создаем образ диска

Установка Acronis TrueImage достаточно стандартна: вам нужно лишь указать папку для инсталляции и ввести серийный номер. В самом конце установки вам будет предложено создать загрузочный компакт-диск или дискету (впрочем, вы сможете создать его и после установки).

Лучше не пренебрегать такой возможностью и создать загрузочный компакт-диск (дискета — ненадежный носитель, да и понадобится их немало): ведь в некоторых случаях вы сможете запустить систему только с загрузочного носителя. После установки программы следует перезагрузиться, после чего у вас в системе окажется новое устройство — Acronis TrueImage Backup Archive Explorer (рис. 4.4).

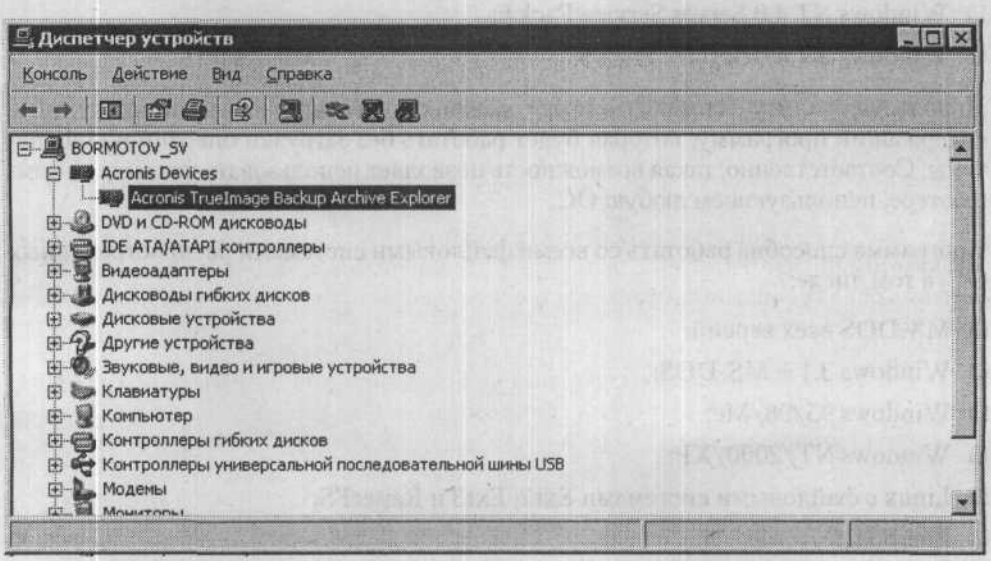


Рис. 4.4. Виртуальное устройство для резервного копирования

Главное окно программы изображено на рис. 4.5.

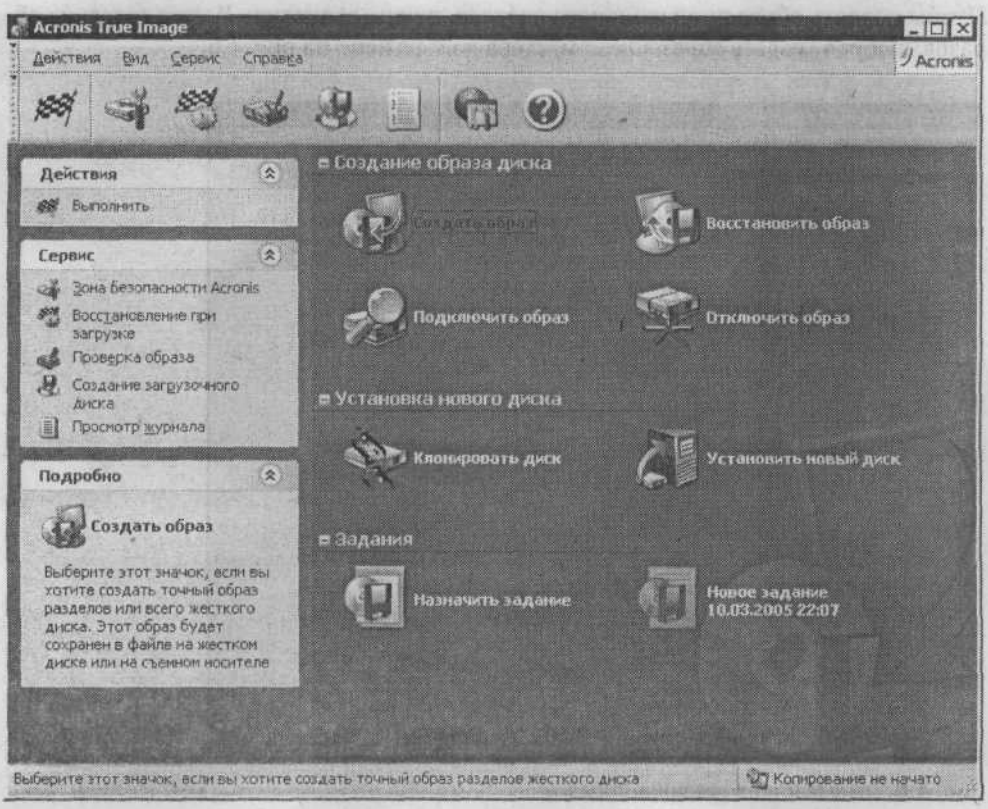


Рис. 4.5. Главное окно программы Acronis TrueImage

Здесь расположена строка меню, панель инструментов и основная область окна, разделенная на две части. В правой находятся значки операций, в левой — окна с описанием выбранной операции, набором основных действий для нее и списком доступных инструментов.

В группе Создание образа диска присутствуют все возможные операции, связанные с работой с образом диска: Создать образ, Восстановить образ, Подключить образ и Отключить образ. Образ подключается и отключается точно так же, как и произвольный логический диск.

В группе Установка нового диска находятся операции, которые совершаются в процессе установки в систему нового жесткого диска. Клонировать диск — полное дублирование информации, которая находилась на старом жестком диске, на новый диск. Установить новый диск — добавление нового жесткого диска.

В группе Задания по умолчанию содержится только операция Назначить задание, которая предназначена для создания образов дисков в определенное время по расписанию.

Создаем образ системного диска

Чтобы создать образ произвольного раздела, нужно запустить Мастер создания образов, выбрав Создать образ. Окно мастера изображено на рис. 4.6.

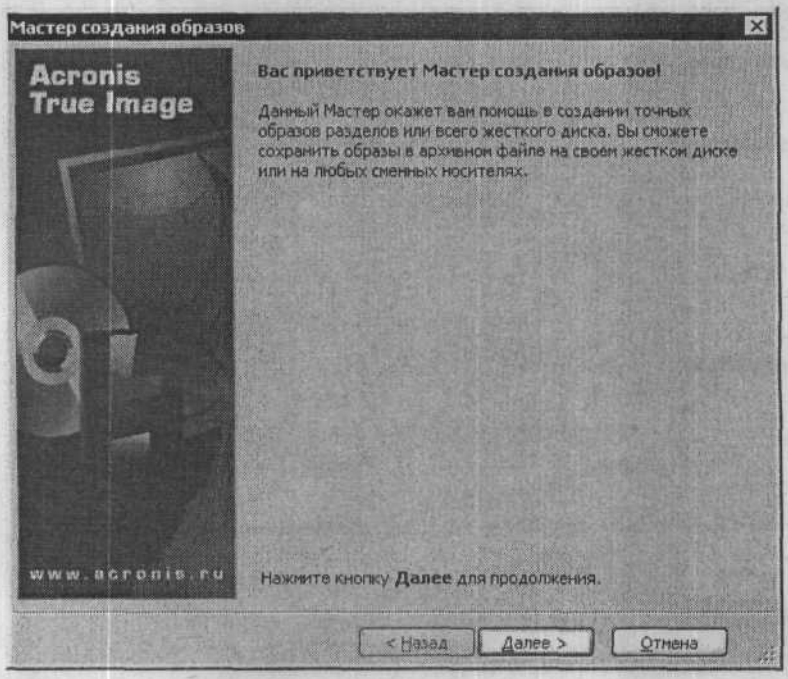


Рис. 4.6. Окно Мастера создания образов

В самом начале работы мастер поинтересуется, какие диски или разделы вы собираетесь использовать для создания образа (рис. 4.7). Выбрав необходимые значения, нажмите кнопку Далее.

Если в вашей системе присутствует всего один физический жесткий диск, для комфортной работы с программой его потребуется разбить как минимум на два логических раздела (если это не было сделано ранее). Если мастер используется впервые, программа подробно расскажет о ключевых моментах создания нового образа.

Далее вам нужно указать, куда следует сохранить образ. Обратите внимание на то, что образ не может быть помещен в тот же раздел, с которого был снят, а если вы хотите значительно ускорить этот процесс, то образ следует сохранить на другой жесткий диск. Кроме этого, у вас будет возможность сохранить образ на сетевой диск или на другой компьютер, подключенный к сети.

Далее нужно указать, хотите ли вы создать полный или инкрементный образ диска (рис. 4.8). Инкрементный образ содержит только те секторы диска, которые были изменены после создания полного или предыдущего инкрементного образа (что значительно ускоряет скорость его создания).

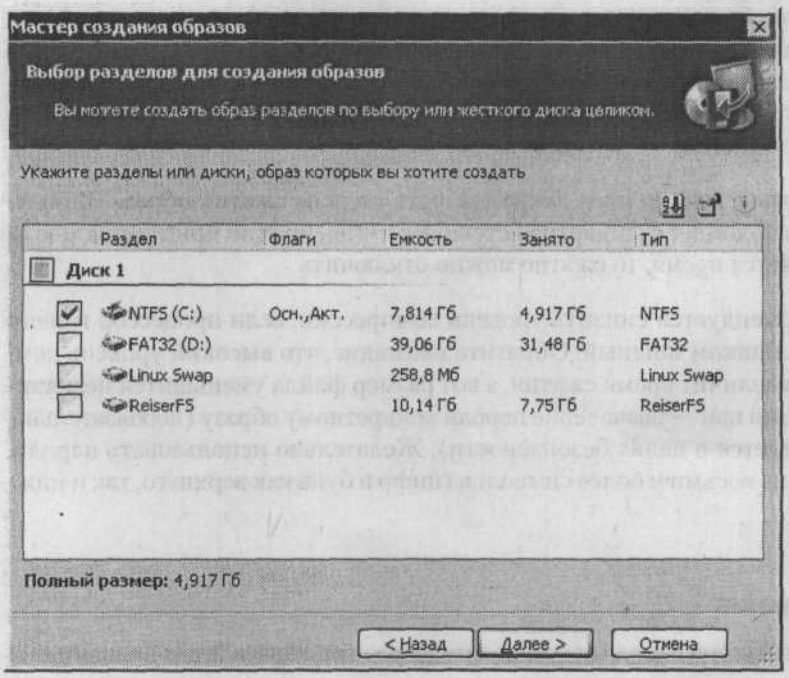


Рис. 4.7. Выбираем нужные диски

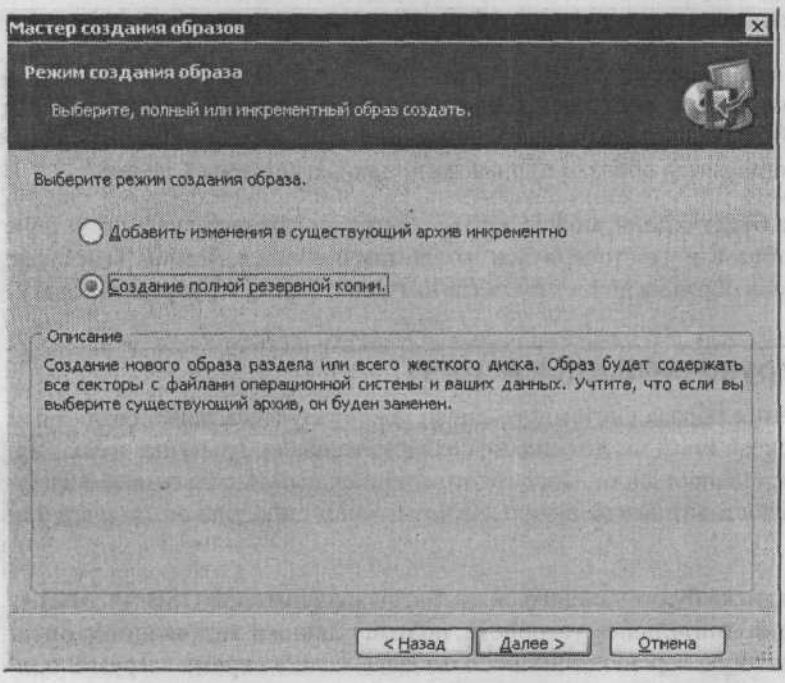


Рис. 4.8. Выбор режима создания образов

Если вы создаете образ впервые, то нужно установить переключатель в положение Создание полной резервной копии. Далее можно задать максимальный размер фрагментов образа. Например, если вы собираетесь записать образ на компакт-диски, то нужно указать максимальный размер, равный 700 Мбайт (объем стандартного компакт-диска).

На следующем этапе мастер предложит выбрать степень сжатия образа. В большинстве случаев подойдет стандартная степень сжатия, но если принципиальным параметром является время, то сжатие можно отключить.

Кроме того, рекомендуется снизить уровень компрессии, если процессор вашего компьютера не слишком мощный. Обратите внимание, что высокий уровень компрессии сильно увеличит время сжатия, а вот размер файла уменьшится незначительно. Следующий шаг — назначение пароля конкретному образу (необязательно, однако рекомендуется в целях безопасности). Желательно использовать пароли, которые состоят из восьми и более символов (цифр и букв как верхнего, так и нижнего регистра).

ВНИМАНИЕ

В случае утери пароля восстановить данные из образа будет невозможно!

Далее можно создать примечание к своему образу, которое поможет впоследствии его идентифицировать.

Последнее окно отобразит введенные ранее параметры. После нажатия кнопки Приступить программа начнет процесс создания образа. Как правило, данный процесс занимает 10–20 мин, однако эта величина во многом зависит от размеров раздела, с которого снимается образ, и производительности системы в целом.

Как только образ будет создан, можно зайти в папку, предварительно указанную для сохранения образа, и удостовериться, что он там появился. Acronis TrueImage способна проверять образ на целостность (пункт меню Сервис ▸ Проверить образ).

Создаем загрузочный диск Acronis

Для восстановления образа системного диска воспользуйтесь ранее созданным загрузочным диском. Если вы его еще не создали, то выберите пункт меню Сервис ▸ Создание загрузочного диска. После этого специальный Мастер создания загрузочных дисков предоставит вам на выбор два возможных типа дисков: полный или облегченный.

В полной версии диска будут находиться драйверы накопителей USB/PCMCIA/SCSI и прочих дополнительных устройств, поэтому данный тип является оптимальным. Облегченную версию стоит использовать, если во время загрузки полной версии появляются конфликты с устройствами компьютера.

СОВЕТ

Если вы используете USB-мышь или клавиатуру, выбирать лучше полную версию, так как облегченная версия не сможет работать с такими устройствами.

Далее мастер предложит выбрать тип носителя, на котором будут сохранены все данные, необходимые для загрузки. Как уже упоминалось, лучше всего использовать компакт-диск.

Предположим, что вы остановились именно на создании загрузочного компакт-диска. Теперь вам нужно вставить чистый компакт-диск в ваш пишущий привод и нажать на кнопку Приступить в окне мастера. Спустя несколько минут загрузочный диск Acronis будет готов.

Восстанавливаем сохраненные данные

После того, как загрузочный диск будет создан, вы легко сможете произвести загрузку с него. Когда система запустится, разрешение экрана изменится на 800 × 600 и откроется главное окно программы.

В данном окне следует выбрать Мастер восстановления образов. В окне мастера нужно указать расположение образа на жестком диске, компакт-диске или в локальной сети.

ПРИМЕЧАНИЕ

Программа способна корректно работать с жесткими дисками Serial ATA и файловой системой NTFS (для Windows 2000/Server 2003/XP), что позволяет и в этом случае беспрепятственно открыть образ. Если необходимо восстановить образ, который находится в локальной сети, то в меню Сервис ▸ Параметры вам понадобится указать адрес компьютера и маску сети.

Если в процессе создания образа был установлен пароль, то программа попросит ввести его. Если в одном образе находится несколько разделов, программа поинтересуется, нужно ли восстанавливать их все или же только некоторые из них.

Далее мастеру нужно указать раздел, на который будет производиться восстановление. Учтите, что ошибочный выбор раздела приведет к тому, что все данные на нем будут уничтожены. Кроме того, настоятельно рекомендуется переместить все папки, которые были изменены после создания образа, в другой раздел (например, Мои документы).

Когда вы укажете раздел для восстановления, нужно указать его тип. В случае восстановления системного раздела следует выбрать параметр Активный. Если восстанавливаются несколько разделов, мастер уточнит, какой именно раздел подлежит восстановлению (как вариант — какие разделы) и тип каждого их них.

В самом конце вам будет предоставлен отчет обо всех выбранных настройках восстановления. Нажмите кнопку Приступить, чтобы начать процесс восстановления образа.

Обычно восстановление образа происходит несколько быстрее, чем его создание. После восстановления образа нужно будет провести перезагрузку, далее перед вами появится операционная система в точно таком же виде, как на момент снятия образа. Если вы восстанавливаете обычный (не системный) раздел, то вам не понадобится загрузочный диск, так как такой процесс можно производить прямо в Windows, даже не перезагружая систему.

Безопасная зона

Вы можете автоматизировать процесс восстановления раздела, если создадите зону безопасности Acronis, чтобы получить возможность восстановления системного раздела прямо в процессе загрузки. Зона безопасности Acronis — это специальный логический диск, на котором программа будет хранить необходимые образы дисков или отдельных разделов. Доступ к данному диску из операционной системы по умолчанию закрыт, поэтому риск заражения вирусом или случайного удаления образов значительно уменьшается.

В случае использования зоны безопасности программа помещает свой загрузчик в MBR (Master Boot Record, загрузочная область диска). В процессе загрузки компьютера вы можете запустить Acronis TrueImage, нажав клавишу F11. Программа сможет запуститься даже тогда, когда основная операционная система не может быть загружена.

Чтобы создать зону безопасности, вам нужно будет предоставить программе неразмеченную область на диске или целый раздел, куда Acronis TrueImage поместит необходимые образы. Если вы предоставите программе уже существующий рабочий раздел, то программа разобьет его на несколько фрагментов. Предположим, что мы производим создание зоны безопасности в неразмеченной области диска.

Упростить данный процесс позволит Мастер управления зоной безопасности, который запускается из раздела Сервис.

Мастер позволит выбрать диск, на котором будет создаваться зона безопасности (рис. 4.9). Обратите внимание на то, что она может быть только одна.

После того как выбран жесткий диск, вам понадобится выбрать раздел, на котором будет создана зона безопасности. Если будет использовано неразмеченное пространство, достаточно нажать кнопку Далее, не делая выбора.

ПРИМЕЧАНИЕ

Для создания зоны безопасности нужно выделить все свободное неразмеченное место.

В следующем окне (рис. 4.10) мастер предоставит вам возможность разрешить функцию восстановления при загрузке.

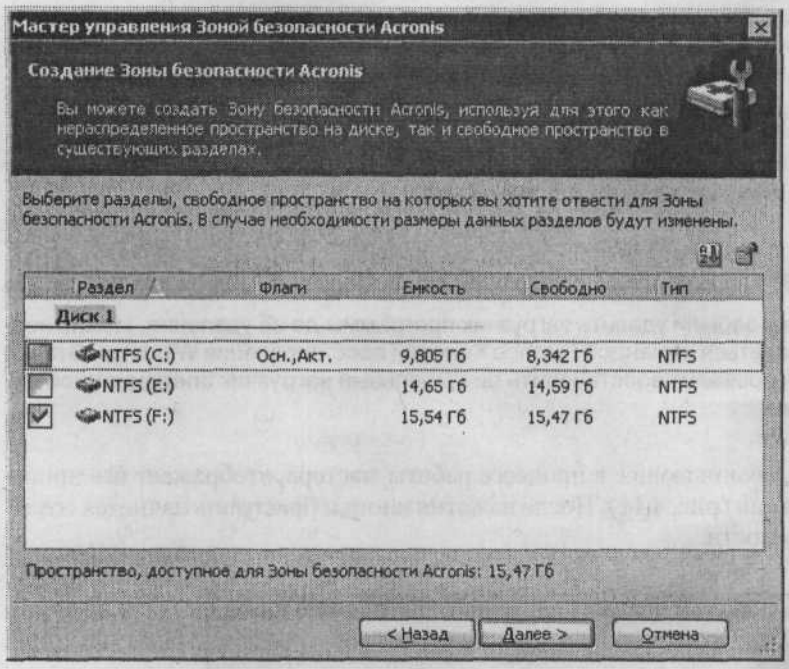


Рис. 4.9. Создаем зону безопасности Acronis

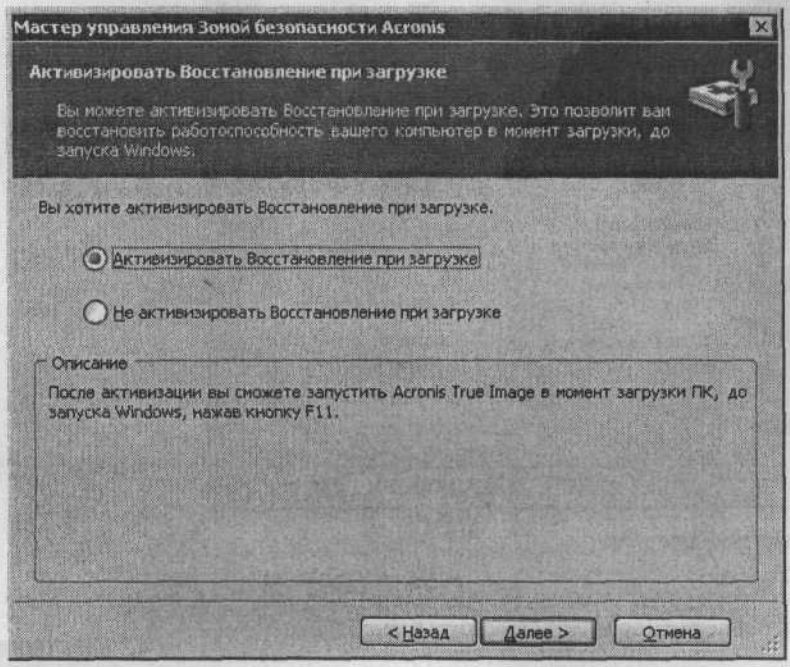


Рис. 4.10. Устанавливаем переключатель в положение Активизировать восстановление при загрузке

Данная возможность позволит запустить программу в момент загрузки компьютера, нажав клавишу F11 до того, как начнет загружаться Windows (загрузочный диск при этом не требуется). Активизировать данную функцию можно также в главном меню программы: Сервис ▸ Активизация при загрузке.

При необходимости вы можете удалить загрузчик Acronis из MBR. Данная функция пригодится в случае удаления программы.

СОВЕТ

Если вы забыли удалить загрузчик программы до ее удаления, можно воспользоваться командой fixmbr в Консоли восстановления Windows. Эта команда позволит восстановить оригинальный загрузчик операционной системы.

Последнее окно, возникающее в процессе работы мастера, отображает все произведенные изменения (рис. 4.11). После нажатия кнопки Приступить начнется создание зоны безопасности.

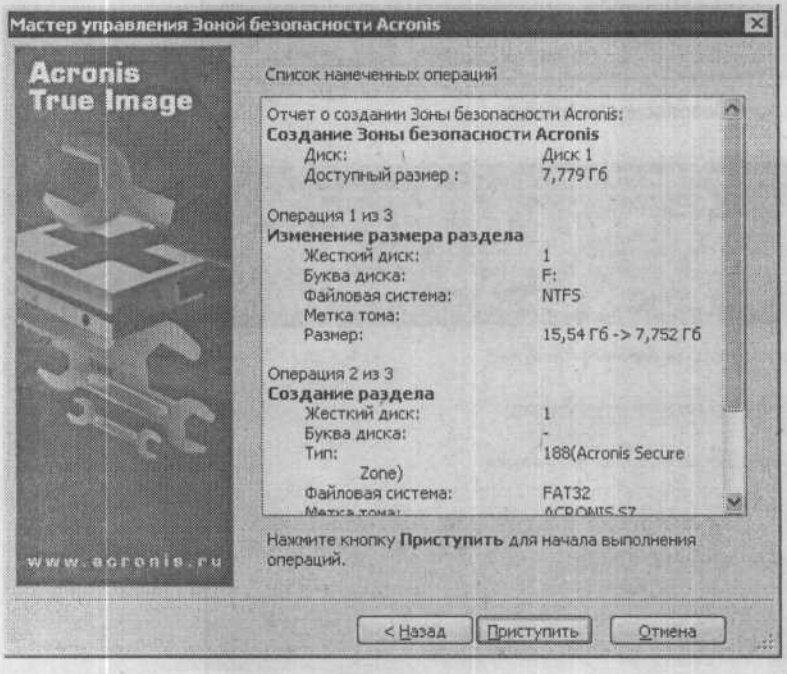


Рис. 4.11. Последнее окно мастера

Когда зона безопасности будет создана, можно посмотреть, как она выглядит, в Консоли управления, оснастка Управление дисками (рис. 4.12).

На рисунке можно заметить, что зона безопасности находится на дополнительном разделе, использующем FAT32. Данный раздел можно подключить к системе сред-

ствами оснастки Управление дисками и работать с ним, как с обычным логическим диском.

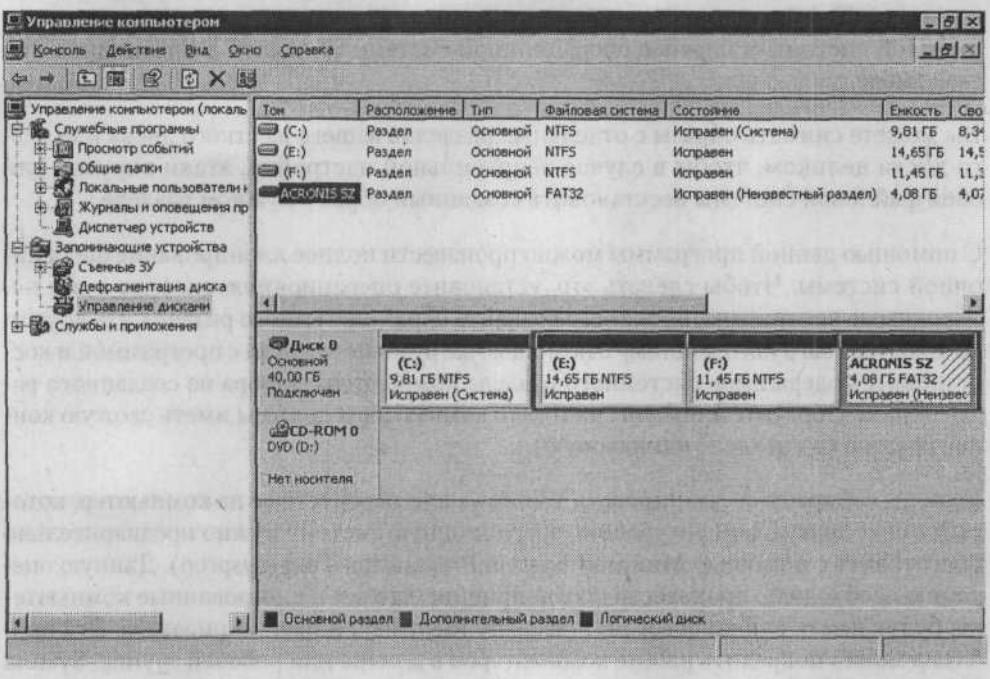


Рис. 4.12. Так выглядит зона безопасности в оснастке Управление дисками

Возможность подключения зоны безопасности к системе — ее серьезный недостаток, ведь в этом случае образы, находящиеся в ней, могут быть повреждены. Возможно, эта функция будет удалена в следующих версиях программы.

Исходя из этого лучше хранить резервные копии на компакт-дисках или DVD, где ваши данные будут в безопасности. Кроме того, это позволит сэкономить место на жестком диске.

Главное — все автоматизировать!

В программе существует возможность создания образа по расписанию, для составления которого можно использовать Мастер расписаний. Его отличие от Мастера создания образов состоит только в том, что на последних стадиях вам предложат задать время или регулярность создания образов. Например, вы можете создать еженедельное расписание резервирования на сетевой диск или удаленный компьютер сети, который выделен специально для этого. Использование расписания избавит вас от постоянной работы по созданию образов.

Когда расписание будет создано, мастер попросит ввести имя пользователя, в учетной записи которого будет производиться резервное копирование (учтите, что пользователь должен иметь права администратора).

Созданное задание отобразится в соответствующем разделе.

Существуют три основные задачи, для выполнения которых вам может пригодиться Acronis TrueImage: резервное копирование информации, клонирование операционной системы и перенос операционной системы на новый жесткий диск при его замене.

Вы можете снимать образы с отдельных разделов вашего жесткого диска или всего диска целиком, чтобы в случае неправильной настройки, атаки вирусов или сбоя файловой системы восстановить созданный образ в нужном разделе.

С помощью данной программы можно произвести полное клонирование операционной системы. Чтобы сделать это, установите операционную систему и все необходимые программы, после чего создайте образ системного раздела. На другом компьютере загрузите систему с помощью загрузочного диска с программой и восстановите содержимое системного раздела компьютера-донора из созданного ранее образа. Обратите внимание на то, что компьютеры должны иметь схожую конфигурацию (в идеале — одинаковую).

Если вы собираетесь клонировать Windows или перенести ее на компьютер, который имеет другую конфигурацию, операционную систему нужно предварительно подготовить с помощью Microsoft System Preparation Tool (sysprep). Данную операцию необходимо произвести по той причине, что все клонированные компьютеры будут иметь одинаковый SID (security identifier) и имя компьютера. Эта проблема может повредить работе компьютеров в домене или рабочей группе. System Preparation Tool (`Sysprep.exe`) способна удалить личные параметры компьютера (SID или имя).

Microsoft System Preparation для системы Windows XP можно загрузить по ссылке `http://www.microsoft.com/downloads/details.aspx?FamilyID=7a83123d-507b-4095-9d9d-0a195f7b5f69&DisplayLang=ru` (понадобится предварительная регистрация).

Рассмотрим некоторые моменты подготовки жесткого диска к клонированию.

1. Создайте загрузочный диск Acronis TrueImage (процедура его создания была описана выше).
2. Запустите `sysprep.exe`. Допустимо использование следующих ключей:
   - `nosidgen` — если вам необходимо удалить всю информацию со старого диска или же вы не будете использовать старый и новый жесткие диски одновременно;
   - `mini` — если вы собираетесь скопировать вашу операционную систему на компьютер, который имеет конфигурацию, отличную от вашей.
3. Загрузитесь с диска Acronis TrueImage. Создайте образ подготовленного жесткого диска.
4. Подключите новый жесткий диск к вашему компьютеру или разрешите доступ к образу для нового компьютера.

5. Еще раз загрузите систему с загрузочного диска, после чего восстановите образ на новый диск или компьютер.
6. Проведите повторную перезагрузку компьютера.

Если вы собираетесь заменить жесткий диск более быстрым, вы сможете сделать это без переустановки операционной системы. Для начала вам понадобится создать образ старого жесткого диска на произвольном носителе информации — другом жестком диске или компакт-диске. Подключите новый жесткий диск и, загрузившись с компакт-диска Acronis TrueImage, восстановите из образа содержимое старого диска, изменив при необходимости размер и расположение отдельных разделов диска, а также их тип и используемую файловую систему.

Как правило, вся описанная процедура занимает не больше часа.

Acronis TrueImage — одна из лучших программ в своем классе. Ее работа основана на использовании мастеров, которые призваны максимально упростить работу с образами. Программа имеет русскоязычный интерфейс и детальную документацию. Кроме того, в комплекте с компакт-диском присутствует печатная версия руководства пользователя, в котором подробно описаны все функции данной программы.

Администрируем локальную сеть, не покидая рабочего места

Закончив разбираться с проблемами резервного копирования, можно смело перейти к администрированию локальной сети и одному из инструментов, позволяющих осуществить данный процесс, — программе Remote Administrator (сокращенно Radmin).

Данная программа позволяет администрировать все рабочие станции и серверы вашей локальной сети прямо со своего рабочего места. Вы будете видеть экран администрируемого компьютера в окне на своем Рабочем столе или в полноэкранном режиме. Кроме того, вы сможете управлять данным компьютером с помощью своей клавиатуры и мыши (впрочем, вы можете просто наблюдать за действиями пользователя).

Radmin способна работать с соединениями по локальной сети, а также через коммутируемое соединение, так как высокая скорость соединения не является основным требованием программы. При использовании соединения через модем частота обновления экрана составит около 5–10 кадров в секунду, чего достаточно для работы. Если вы используете локальную сеть, то экран будет обновляться в реальном времени (около 100–500 кадров в секунду).

Данная программа предоставляет следующие возможности.

- Поддержку нескольких режимов просмотра экрана удаленного компьютера (оконный, полноэкранный, оконный масштабируемый).

- Radmin-сервер способен выступать в виде службы Windows NT/2000/XP и Windows 95/98/Me (таким образом, можно выйти и войти в систему удаленно).
- Radmin-сервер может устанавливать несколько соединений с удаленными компьютерами одновременно.
- Присутствует возможность передачи файлов удаленному компьютеру и наоборот.
- Доступна возможность управления питанием удаленного компьютера.
- Возможность использования TELNET-сервера.
- Реализована поддержка системы безопасности Windows NT. Возможно также предоставление прав на удаленное управление, слежение за информацией и обмен ею, TELNET-доступ определенным пользователям или группам пользователей Windows. Если конкретная рабочая станция входит в домен, то программа будет использовать активную учетную запись, чтобы организовать доступ к Radmin-серверу. Если же система безопасности Windows отключена, то на доступ будет установлен пароль с 128-битным ключом.
- 128-битное шифрование всех потоков данных.
- Применение специального IP-фильтра позволяет разрешать доступ к Radmin-серверу ограниченному количеству определенных IP-адресов и подсетей.

Remote Administrator состоит из клиентской и серверной частей.

- Серверная часть захватывает изображение на экране и передает его по сети клиентской части, а также исполняет инструкции, полученные от нее.
- Клиентская часть отображает экран удаленного компьютера и предоставляет возможность управления удаленным компьютером.

Системные требования для данной программы совсем невысокие: процессор не ниже 386, оперативная память не менее 8 Мбайт. Radmin является платной программой, поэтому вам потребуется приобрести лицензию (табл. 4.1). Обратите внимание на то, что наличие монитора и клавиатуры на сервере не является обязательным, главное — чтобы была правильно настроена сеть и активирована клиентская часть программы.

Таблица 4.1. Стоимость лицензий для программы Remote Administrator

Лицензия	Количество машин	Цена лицензии
Стандартная лицензия	На два компьютера	885 руб.
Пакет из 50 лицензий	На 100 компьютеров	29 500 руб.
Пакет из 100 лицензий	На 200 компьютеров	53 100 руб.
Пакет из 200 лицензий	На 400 компьютеров	94 400 руб.
Более 200 лицензий	Более 400 компьютеров	Цена договорная
Пакет привилегированной технической поддержки	На 1 год	5900 руб.

Более подробно о лицензиях вы сможете прочесть на сайте программы в Интернете www.radmin.ru. С этого же сайта вы можете загрузить демо-версию программы с 30-дневным сроком действия.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к этой книге, в папке по адресу ch04\Remote Administrator вы найдете демо-версию Remote Administrator 2.2 и beta-версию Radmin Viewer 3.0.

Установка программы

Установка программы ничем не отличается от процесса установки любого другого Windows-приложения. В конце программа-инсталлятор поинтересуется, что вы будете использовать для авторизации программы: пароль или систему авторизации Windows NT. Если в вашей локальной сети присутствует контроллер домена и все компьютеры входят в домен, то лучше использовать второй вариант. Если данный контроллер отсутствует, то для авторизации следует использовать пароль, длина которого должна быть не меньше восьми символов. После установки значок Radmin Server или Radmin Viewer (клиент) появится в меню Пуск.

Из меню Пуск также можно запустить элемент Настройки Remote Administrator Server, который позволит корректировать режим запуска Radmin Server, пароль для доступа и другие параметры программы.

Если ваша сеть защищена брандмауэром, то необходимо разрешить использование 4899 порта в его настройках, так как именно он используется в работе программы. Кроме того, вы можете изменить порт, который будет использовать программа, в ее настройках.

ВНИМАНИЕ

Для установки и работы с программой необходимо иметь права администратора в системе.

После того как Radmin установлен, запустите настройку сервера Radmin, выполнив команду Пуск ▸ Все программы ▸ Remote Administrator v2.2 ▸ Настройки Remote Administrator server. Окно настроек показано на рис. 4.13.

Прежде всего необходимо настроить параметры запуска Radmin Server на клиентских компьютерах. Чтобы сделать это, нажмите кнопку Тип запуска в главном окне настроек Remote Administrator Server. Вам будет предложено сделать выбор из двух вариантов.

- Автоматически служба Remote Administrator service будет загружена еще до входа пользователя в систему. Данное значение установлено по умолчанию, и изменять его не рекомендуется, так как только в этом режиме вы сможете подключиться к удаленному компьютеру еще на стадии авторизации.

- Вручную (Manual). В этом случае Remote Administrator запустится только после того, как на удаленном компьютере будет выполнена команда `r_server.exe /start` или же выбран аналогичный ярлык в меню Пуск.

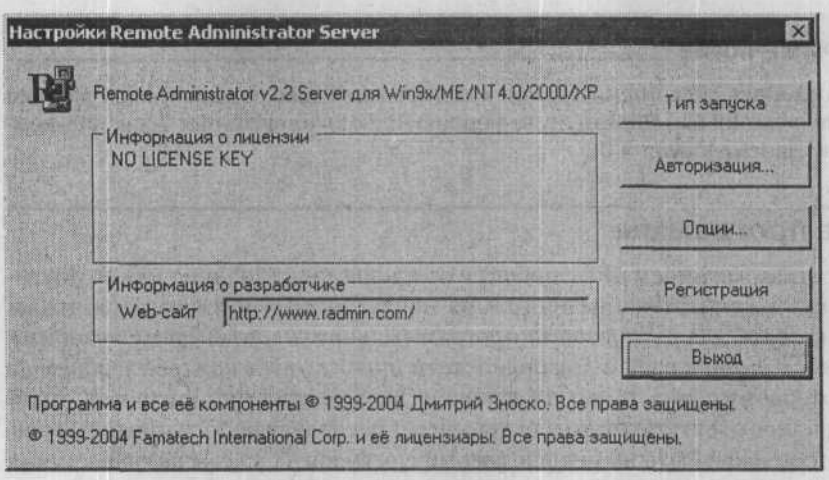


Рис. 4.13. Окно настроек программы Remote Administrator

После выбора режима запуска можно задать или изменить уже установленный пароль Radmin Server.

Если компьютер, оснащенный серверным модулем программы, работает под управлением Windows NT4.0/2000/XP/Server 2003, в диалоговом окне можно активировать параметр NT Security. Данный метод авторизации дает возможность администратору разделить права доступа к серверу между различными пользователями одного и того же компьютера. Возможна установка следующих вариантов доступа:

- полный контроль;
- только просмотр;
- TELNET-соединение;
- обмен файлами;
- переадресация.

Полный контроль!

Теперь приступим к тщательной проверке возможностей программы. Чтобы подключиться к удаленному компьютеру и контролировать его, необходимо, чтобы на нем был установлен и запущен Radmin Server. При запуске Radmin Server на Панели задач появится значок программы. Если вы подведете курсор к данному значку, то увидите подсказку, отображающую IP-адреса данной машины. Двойной щелчок на значке отобразит список подключений. Если вы в настройках Radmin Server установите флажок Не показывать значок, то значок не будет отображаться.

Далее вам нужно будет запустить Radmin Viewer на вашем компьютере. Для этого выберите пункт Соединения главного меню программы, затем пункт Подключиться к. В поле IP-адрес или DNS-имя укажите, соответственно, IP-адрес (например, `192.168.0.11`) или DNS-имя (например, `room1`) нужного удаленного компьютера (рис. 4.14).

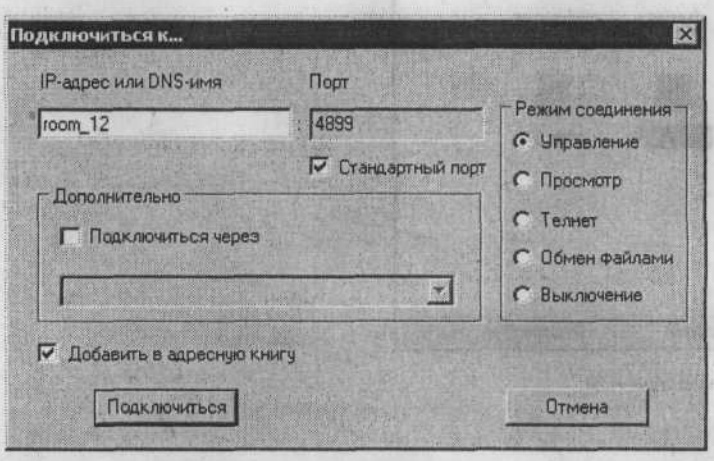


Рис. 4.14. Настраиваем подключение

Вам также нужно будет определить режим соединения, выбрав необходимый из числа доступных в списке. Будут предложены следующие варианты:

- управление;
- просмотр;
- телнет;
- обмен файлами;
- выключение.

Режим управления полностью соответствует своему названию: он предназначен для управления удаленным компьютером. Просмотр предоставит вам возможность следить за действиями пользователя на удаленном компьютере. Используя режим Телнет, вы сможете создать Telnet-соединение между вашим и удаленным компьютером. Режим Обмен файлами позволит загрузить файлы на удаленный компьютер или же получить необходимые данные с него. Выключение предоставит вам возможность выключить удаленный компьютер, выполнить его перезагрузку, приостановить работу или же завершать сеанс текущего пользователя.

Команда Подключиться к позволит настроить параметр Подключиться через, назначить номер порта, который отличается от стандартного, изменить тип подключения и т. п. Стоит также установить флажок Добавить в адресную книгу, так как в адресную книгу Radmin можно записать компьютеры, к которым приходится обращаться наиболее часто. После того как соответствующий компьютер будет внесен в адресную книгу, для доступа к нему достаточно будет щелкнуть на его значке (рис. 4.15).

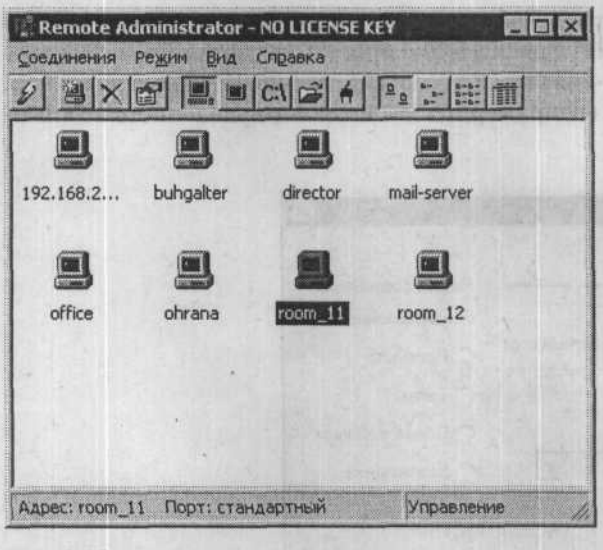


Рис. 4.15. Адресная книга программы

СОВЕТ

Адресная книга программы Radmin находится в системном реестре операционной системы. Чтобы транспортировать ее на другой компьютер или же восстановить после сбоя операционной системы, нужно запустить Редактор реестра (файл regedit.exe) и экспортировать все ключи раздела [HKEY_CURRENT_USER\Software\RAdmin\v2.0\Clients] в заданный файл (например, book.reg). Когда вы запустите данный файл на другом компьютере, адресная книга Radmin будет автоматически загружена. Для импорта файла выполните команду: regedit.exe /s settings.reg.

После того как произойдет подключение, перед вами появится Рабочий стол удаленного компьютера (рис. 4.16).

Теперь вы можете полноценно управлять данной машиной (однако не забывайте, что перед вами не ваш, а совершенно другой компьютер).

Переключение оконного, полноэкранного и масштабируемого видов отображения удаленного экрана производится с помощью клавиши F12.

СОВЕТ

Если вам нужно будет «нажать» данную клавишу на удаленном компьютере, воспользуйтесь командой Передать F12 в меню удаленного экрана.

Если разрешение экрана удаленного компьютера будет превышать ваше, то перемещение по экрану будет производиться с помощью появившихся полос прокрутки. В режиме полноэкранного просмотра для этого нужно подвести указатель

мыши к границе показанной части экрана. Еще один вариант, который можно использовать, — переключение в масштабируемый вид, когда окно отображает весь экран удаленного компьютера (вы можете выставить любой размер данного окна).

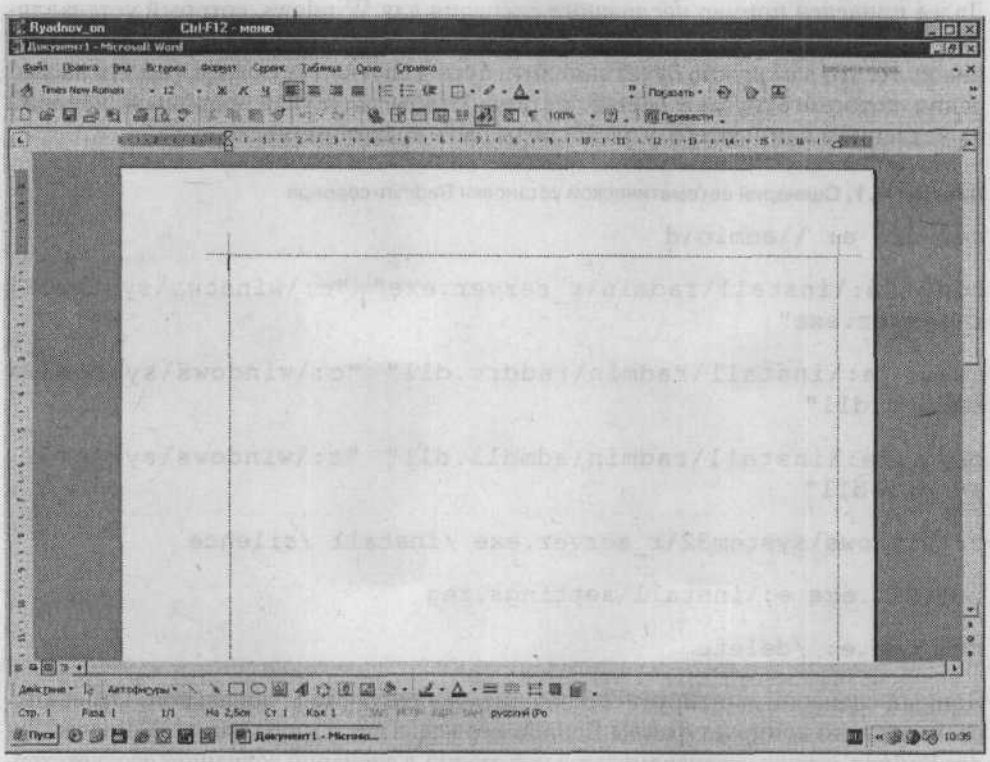


Рис. 4.16. Внешний вид Рабочего стола удаленного компьютера

Чтобы «нажать» на удаленном компьютере Ctrl+Alt+Delete, выберите команду Передать Ctrl+Alt+Delete в меню окна удаленного экрана. Обратите внимание, что данная команда доступна в режиме подключения Полный контроль. Кроме того, вы можете использовать комбинацию клавиш Ctrl+Alt+F12.

Если удаленная система сильно загружена, следует уменьшить значение параметра Максимальная частота обновления в диалоговом окне Параметры окна удаленного экрана.

При снижении скорости работы программы попробуйте отключить фоновый рисунок Рабочего стола на удаленном компьютере, что позволит значительно ускорить работу Radmin. Кроме того, повышению производительности будет способствовать снижение разрядности цвета передаваемого изображения путем переключения параметра Цветовой формат в режим 16 цветов в диалоговом окне Параметры окна удаленного экрана. Учтите, что при использовании модема физически невозможно достичь частоты обновления, превышающей 10 кадров в секунду.

Установка Radmin-клиента и сервера по сети

Установку сервера Remote Administrator на все удаленные компьютеры можно производить в автоматическом режиме с помощью сценариев.

Далее приведен пример несложного сценария для Windows, который устанавливает Radmin-сервер как сервис на любой удаленный компьютер. Обратите внимание на то, что вам нужно будет заменить пути к соответствующим файлам на значения, которые отвечают вашей системе. Чтобы запустить подобный сценарий на удаленном компьютере, у вас должны быть права администратора.

Листинг 4.1. Сценарий автоматической установки Radmin-сервера

```
net use e: \\admin\d

copy "e:\install\radmin\r_server.exe" "c:\windows\system32\
r_server.exe"

copy "e:\install\radmin\raddrv.dll" "c:\windows\system32\
raddrv.dll"

copy "e:\install\radmin\admdll.dll" "c:\windows\system32\
admdll.dll"

c:\windows\system32\r_server.exe /install /silence

regedit.exe e:\install\settings.reg

net use e: /delete
```

Данный сценарий монтирует сетевой диск в виде диска `E:` локального компьютера, после чего копирует файлы Radmin-сервера в системную папку Windows. Далее Radmin-сервер устанавливается как сервис, а сценарий сохраняет соответствующие параметры в реестре и отключает сетевой диск.

Данный сценарий позволит в короткие сроки установить Radmin на все компьютеры сети.

Настройки сервера (настройки значка, порт, настройки лог-файлов, IP-фильтрация, пароль) будут сохранены в реестре, так что вы можете переносить эти настройки с одного компьютера на другой.

Исходя из приведенного листинга, все настройки Radmin-сервера загружаются из файла `settings.reg`. В данном файле сохранены все значения ключей реестра Windows, где были определены настройки программы.

Чтобы создать такой файл, настройте Radmin-сервер на своем компьютере, после чего запустите `regedit.exe` и экспортируйте необходимые настройки в файл (`settings.reg`) для дальнейшего их восстановления.

В табл. 4.2 можно найти значения и расположение некоторых ключей в реестре.

Таблица 4.2. Расположение ключей программы в реестре

Значение ключа реестра	Путь к ключу в реестре
Настройки IP-фильтрации	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\FilterIp HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\iplist\
Подтверждение установки удаленного соединения со стороны пользователя	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\AskUser
Настройка диалога с пользователем	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\AskUser
Отключение отображения значка на Панели задач	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableTrayIcon
Настройки лог-файла	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\EnableLogFile HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\LogFilePath
Пароль для Radmin-сервера (шифрованный)	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\Parameter
Настройка номера порта	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\Port
Метка для включения поддержки NT системы безопасности	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\NTAuthEnabled
Перечень пользователей для NT	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Users\
Информация о регистрации	HKEY_LOCAL_MACHINE\Software\RAdmin\v1.01\ViewType\Data
Отключение звукового сигнала	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableBeep
Отключение режима полного контроля	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableRedirect HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableScreen
Отключает поддержку соответствующего типа соединения на сервере. Чтобы снова включить данный тип соединения, нужно создать ключ со значением binary 01 00 00 00	HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableView HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableTelnet HKEY_LOCAL_MACHINE\System\RAdmin\v2.0\Server\Parameters\DisableFile

Безопасность Remote Administrator

Когда вы используете полный доступ к удаленным компьютерам, то должны помнить о том, что это является потенциальной угрозой безопасности работы сети.

Программа Remote Administrator способна работать с системой безопасности операционных систем Windows NT/2000/XP/Server 2003. Таким образом, вы сможете

назначать права удаленного доступа определенному пользователю или же группе пользователей. Права на доступ к Radmin Server могут передаваться пользователям из доменов, с которыми установлены доверительные отношения (Trusted Domains), и из активных директорий (Active Directories).

Если вы не будете использовать систему безопасности Windows NT, то доступ к удаленному компьютеру будет производиться посредством проверки пароля. Radmin применяет аутентификацию с запросом и подтверждением. Этот метод напоминает тот, который используется в процессе авторизации в Windows NT, однако использует секретный ключ большей длины.

СОВЕТ

Пароль не должен быть осмысленным, так как в этом случае он может быть подобран с помощью специальных программ, которые используют большие базы популярных паролей.

Программа способна вести протокол собственной работы. Просматривая такой протокол, можно легко обнаружить любые несанкционированные действия, которые производились в сети с использованием Radmin.

В Radmin Server присутствует собственная таблица IP-фильтрации, с помощью которой можно ограничить доступ к Radmin Server определенных хостов и подсетей.

Учтите, что при использовании Windows NT/2000/XP/Server 2003 вы сможете установить Radmin Server исключительно в виде системной службы (возможность запуска данной программы как обычного приложения заблокирована в целях безопасности).

Потеря файлов: что же делать?

Пожалуй, самой ненадежной составляющей любого компьютера является жесткий диск. Именно поэтому все чаще на серверах и рабочих станциях, работающих с важной информацией, встречаются дисковые массивы RAID.

ПРИМЕЧАНИЕ

Более подробно дисковые массивы RAID мы рассмотрим в главе 6.

Выход винчестера из строя — это самое худшее, что может случиться, так как в этом случае теряются все данные, находящиеся на нем. Если вы не произвели до этого резервного копирования, убытки могут быть колоссальными.

Еще одной проблемой является ошибочное удаление важной информации. В локальных сетях это явление встречается достаточно часто — по ошибке пользователи удаляют нужные документы, отчеты и прочие важные файлы.

Все проблемы, связанные с винчестером, условно разбиваются на две группы: аппаратные и программные.

При механических повреждениях компьютер не сможет обнаружить жесткий диск, а сам винчестер может издавать непривычные звуки (например, стук головок).

Программные повреждения связаны с некорректной работой программного обеспечения. В таком случае винчестер может быть физически исправным, однако с него невозможно прочитать данные. Иногда операционная система по каким-то причинам не может увидеть логические диски.

Информация на жестком диске записана небольшими секторами по 512 байт каждый. Соответственно, в процессе записи или чтения данных жесткий диск обращается именно к секторам.

Следует помнить, что разным секторам назначаются различные роли в работе системы. Самый первый и наиболее важный сектор диска именуется главным загрузочным сектором (MBR). В нем находится таблица разделов, которая содержит необходимую информацию о логических дисках: номера начального и конечного секторов раздела, тип файловой системы и прочие данные. В первом секторе находится также программа загрузки, которая определяет в таблице активный раздел и начинает оттуда загрузку операционной системы. Первый сектор произвольного раздела содержит информацию об используемой файловой системе, а также загрузчик операционной системы.

Основных разделов диска не может быть более четырех, так как объем главного загрузочного сектора ограничен, а таблица разделов состоит из четырех ячеек. Подобное ограничение появилось с первыми винчестерами и все еще действительно (впрочем, используя технологию расширенных разделов, можно превысить установленный предел).

Расширенный раздел — это специальная структура, содержащая в себе описания неограниченного количества дополнительных разделов. Если расширенный раздел будет создан, то в таблицу разделов будет добавлена информация о нем. Основным недостатком такого раздела является отсутствие возможности загрузки с него операционной системы.

Разделы могут использовать файловую систему FAT, FAT32 или NTFS. FAT формирует специальную таблицу размещения файлов, которая содержит всю необходимую информацию о данных, расположенных в пределах конкретного раздела. В такой таблице отмечаются позиции отдельных файлов и их фрагментов на диске. Как правило, на диске находятся две одинаковых копии FAT, что должно повысить уровень безопасности хранения данных, однако на практике такой подход защищает только от случайных повреждений. Более надежной является файловая система NTFS, которая способна к самовосстановлению и значительно устойчивее к разрушению.

Восстановление удаленных файлов или поврежденной файловой системы абсолютно реально, так как, чтобы вся информация была уничтожена безвозвратно,

необходимо произвести полный цикл заполнения всего объема жесткого диска. Обычно возникающие сбои или вирус ограничиваются разрушением служебных программ. На практике этот процесс занимает достаточно продолжительное время. Как правило, атака вируса способна повредить область, которая не превышает нескольких процентов от общего объема диска. Чтобы сделать недоступными все разделы винчестера, нужно очистить всего один сектор. Повреждение структуры расширенного раздела лишит вас дополнительных разделов.

Перед тем как заняться восстановлением поврежденной файловой системы или отдельных файлов, нужно определить следующее:

- количество имеющихся логических дисков, их размеры и расположение;
- тип файловой системы, которая была использована;
- операционная система, которая использовалась;
- индивидуальные имена папок и файлов, которые находились в корне диска, имя директории с данными, которые необходимо восстановить в первую очередь, и имена подпапок и файлов, находящихся в данной директории.

Безусловно, для восстановления информации понадобится специальная программа. На данный момент таких программ существует немало, однако одной из лучших считается EasyRecovery компании OnTrack (www.ontrack.com).

ВНИМАНИЕ

Программа EasyRecovery способна копировать файлы и папки из поврежденного раздела, поэтому никаких изменений или исправлений в структуру раздела она вносить не будет. Чтобы восстановить данные, вам понадобится какой-нибудь исправный носитель — второй жесткий диск или же исправный раздел поврежденного диска. Ни в коем случае не пытайтесь переписать данные с поврежденного раздела на него же! После того как необходимая информация скопирована, можно смело форматировать поврежденный раздел.

Программа EasyRecovery может выполнять следующие действия:

- восстановление удаленных файлов;
- восстановление информации, находящейся на поврежденных носителях;
- восстановление информации с отформатированных разделов;
- выполнение SMART-диагностики жестких дисков;
- создание специальной загрузочной дискеты, которая позволит восстановить данные без участия операционной системы;
- восстановление файлов по расширению (например, DOC);
- восстановление почтовых архивов программ Outlook и Outlook Express;
- техническая поддержка со стороны разработчиков для зарегистрированных пользователей;
- автоматическое обновление программы.

Системные требования данной программы достаточно невысокие:

- Windows 98 SE/Me/NT4 (SP6)/2000/XP;
- браузер Internet Explorer 4.0 или выше;
- 16 Мбайт оперативной памяти;
- процессор 486 или лучше;
- 150 Мбайт свободного места на жестком диске.

Программа платная, однако вы можете использовать ее без регистрации с некоторыми ограничениями и без технической поддержки со стороны разработчиков.

ПРИМЕЧАНИЕ

Программу EasyRecovery Professional можно скачать на сайте производителя www.ontrack.com. Вы также найдете ее на компакт-диске, прилагаемом к книге, в папке ch04\EasyRecovery v 6.

К сожалению, программа не поддерживает русский язык, однако работа с ней трудностей вызвать не должна. Главное окно EasyRecovery изображено на рис. 4.17.

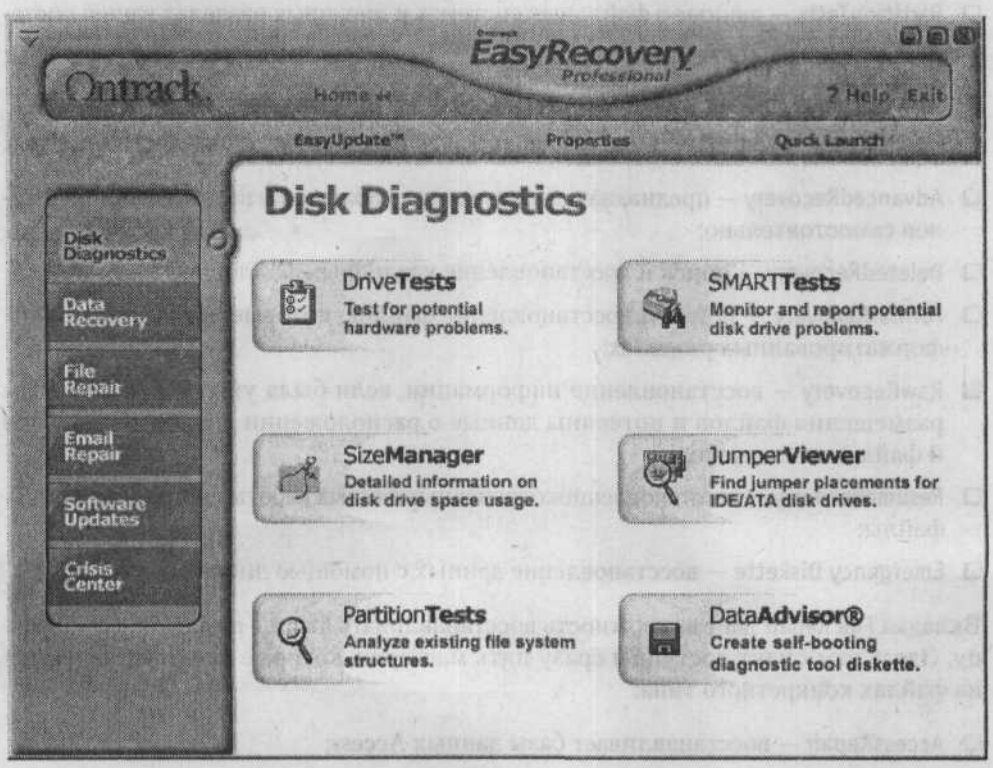


Рис. 4.17. Интерфейс программы EasyRecovery

Интерфейс программы основан на использовании мастеров. В главном окне программы расположены шесть вкладок:

- Disk Diagnostics;
- Data Recovery;
- File Repair;
- Email Repair;
- Software Updates;
- Crisis Center.

Первая вкладка (Disk Diagnostics) отвечает за диагностику винчестера и состоит из нескольких мастеров:

- DriveTests — тестирование винчестера на наличие потенциальных проблем;
- SMARTTests — SMART-тестирование жесткого диска;
- SizeManager — этот мастер предоставит вам подробные данные о размерах дисковых разделов;
- JumperViewer — показывает состояние джамперов на винчестерах вашей системы;
- PartitionTests — данные о файловых системах и дисковых разделах вашей системы;
- DataAdvisor — мастер по созданию загрузочной дискеты.

Вкладка Data Recovery позволяет восстанавливать файлы и состоит из шести мастеров:

- AdvancedRecovery — предназначен для задания параметров восстановления файлов самостоятельно;
- DeletedRecovery — поиск и восстановление удаленных файлов;
- FormatRecovery — поиск и восстановление файлов, которые находились на отформатированных разделах;
- RawRecovery — восстановление информации, если была уничтожена таблица размещения файлов и потеряны данные о расположении дисковых разделов и файловых системах;
- ResumeRecovery — восстановление сохраненных данных работы программы в DAT-файлы;
- Emergency Diskette — восстановление данных с помощью дискеты.

Вкладка File Repair дает возможность восстанавливать файлы по заданному образцу. Здесь вам будут доступны сразу пять мастеров, которые специализируются на файлах конкретного типа:

- AccessRepair — восстанавливает базы данных Access;
- ExcelRepair — восстанавливает файлы Excel;

- PowerPointRepair — восстанавливает файлы PowerPoint;
- WordRepair — восстанавливает документы Word;
- ZipRepair — восстанавливает ZIP-архивы.

Вкладка Email Repair содержит два мастера, восстанавливающих почтовые архивы Outlook и Outlook Express.

Вкладка Software Updates также содержит два мастера и предназначена для поиска обновлений на сайте производителя:

- ProductNews — проверка наличия обновлений;
- EasyUpdate — загрузка и установка обновлений.

Вкладка Crisis Center предназначена для получения консультации в подключенном режиме по вопросам восстановления данных и для получения адресов лабораторий, которые занимаются восстановлением информации.

Ядерная инженерия

Операционная система Windows считается закрытой системой, в которой сложно изменять какие-то компоненты. Это не совсем верно, так как существует способ безболезненной замены ее отдельных элементов, чтобы оптимизировать систему для использования на конкретном оборудовании.

Остановимся на процессе замены ядра Windows. Рассмотрим простой пример: первоначально на компьютере, работающем под управлением Windows, был установлен процессор Intel Celeron, после чего его место занял Pentium 4 с поддержкой технологии Hyper-Threading.

ПРИМЕЧАНИЕ

Технология Hyper-Threading позволяет одновременно обрабатывать два потока команд, создавая два виртуальных процессора на базе одного физического. Любая операционная система будет считать, что используется многопроцессорное решение.

Естественно, что Windows не захочет работать со вторым процессором, пока вы не произведете ее переустановку или не замените ядро операционной системы многопроцессорным (что значительно проще и быстрее).

Какие ядра предлагает Windows

В состав дистрибутива Windows входят сразу восемь вариантов различных ядер, которые предназначены для разных типов систем. Описание этих ядер приведено в табл. 4.3.

Таблица 4.3. Описание ядер Windows

Название ядра (русское/английское)	Описание
Многопроцессорный компьютер с ACPI (ACPI Multiprocessor PC)	ACPI-системы с многопроцессорной материнской платой и двумя или более установленными процессорами
Однопроцессорный компьютер с ACPI (ACPI Uniprocessor PC)	ACPI-системы с многопроцессорной материнской платой и одним установленным процессором
Компьютер с ACPI (Advanced Configuration and Power Interface (ACPI) PC)	ACPI-системы с однопроцессорной системной платой
Многопроцессорный компьютер с MPS (MPS Multiprocessor PC)	Не ACPI-системы с многопроцессорной материнской платой и двумя или более установленными процессорами
Однопроцессорный компьютер с MPS (MPS Uniprocessor PC)	Не ACPI-системы с многопроцессорной материнской платой и одним установленным процессором
Многопроцессорный Compaq SystemPro или 100 % совместимый (ACPI Compaq SystemPro Multiprocessor or 100 % compatible)	Компьютеры типа Compag SystemPro или полностью совместимые с ними
Стандартный компьютер (Standart PC)	Любой стандартный компьютер не ACPI с однопроцессорной системной платой (если плата поддерживает ACPI, то система ее заблокирует)
Стандартный компьютер I486 степпинг-C (Standard PC with C Step i486)	Однопроцессорные компьютеры с процессором 80486 Step C (степпинг-C, разновидность i486) или выше, без поддержки ACPI

ПРИМЕЧАНИЕ

Аббревиатура ACPI означает Advanced Configuration and Power Interface — менеджер питания устройств. Кроме того, он является и менеджером ресурсов системы. В ACPI-системах все устройства подключены к виртуальной шине ACPI-контроллера. Технология ACPI пришла на смену Plug and Play и берет на себя конфигурирование устройств в системе.

Как правило, программа-инсталлятор во время установки способна правильно определить необходимый тип ядра, а его смена нужна в случае серьезного изменения конфигурации компьютера или же при клонировании операционной системы на компьютеры с различным набором установленных устройств.

Выбираем ядро вручную

Для назначения необходимого ядра вручную во время установки операционной системы нажмите клавишу F5, когда будет происходить проверка конфигурации

и появится сообщение Press F6 if you need to install a third party SCSI or RAID driver/Нажмите F6, если вам необходимо загрузить SCSI или RAID драйвер стороннего производителя. Как видите, система не предлагает вам выбор ядра, однако клавишу F5 нужно нажать именно сейчас. После этого можно выбрать необходимое ядро из появившегося списка. Клавиша F7 отменит процесс тестирования и даст команду использовать ядро, установленное по умолчанию. Естественно, что выбранный тип ядра должен соответствовать установленному оборудованию.

Некоторые версии ядер можно заменять без переустановки системы. Для этого выполните команду Панель управления ▸ Система ▸ Оборудование ▸ Диспетчер устройств ▸ Компьютер. Щелкните правой кнопкой мыши на названии своего типа компьютера и в контекстном меню выберите Свойства. В появившемся окне откройте вкладку Драйвер и нажмите кнопку Обновить. В открывшемся окне Мастера обновления оборудования установите переключатель в положение Нет, не в этот раз, нажмите кнопку Далее. В следующем окне установите переключатель в положение Установка из указанного места, нажмите Далее. На следующем этапе мастера выберите Не выполнять поиск. Я сам выберу нужный драйвер и нажмите кнопку Далее. Система предоставит вам возможность выбрать необходимое ядро из перечня совместимых с вашей системой (рис. 4.18).

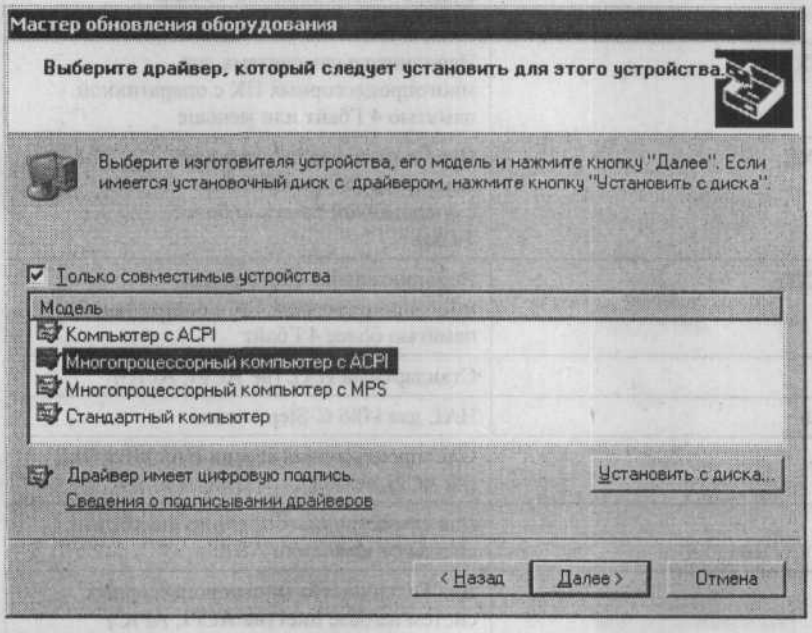


Рис. 4.18. Выбираем ядро

Выбранное ядро активируется после перезагрузки системы. Если обновление пройдет неудачно, операционная система может и не запуститься. Как правило, такое происходит в случае замены ACPI-ядра на стандартное и наоборот. Дело в том, что ACPI и не ACPI-ядра в своей работе по-разному строят деревья устройств и распределяют ресурсы системы.

В данном случае возвратиться к работоспособному состоянию системы проще с помощью меню последней удачной конфигурации. В процессе загрузки операционной системы нажмите и удерживайте клавишу F8, после чего на экране появится меню загрузки ОС. Если вы выберете пункт Последняя удачная конфигурация, то сможете вернуться к предыдущей конфигурации Windows.

Внутри ядра

Ядро состоит из двух файлов — библиотеки аппаратных абстракций (Hardware Abstraction Layer — HAL) и исполнительной системы, которая носит название KERNEL. В своей совокупности они образуют ядро системы, на котором основываются остальные компоненты.

Описание разных HAL и KERNEL приведено в табл. 4.4.

Таблица 4.4. Описание компонентов ядра

Компонент ядра	Описание
NTOSKRNL.EXE	Исполнительная система для однопроцессорных ПК с оперативной памятью 4 Гбайт или меньше
NTKRNLMP.EXE	Исполнительная система для многопроцессорных ПК с оперативной памятью 4 Гбайт или меньше
NTKRNLPA.EXE	Исполнительная система для однопроцессорных ПК с оперативной памятью более 4 Гбайт
NTKRPAMP.EX8E	Исполнительная система для многопроцессорных ПК с оперативной памятью более 4 Гбайт
HAL.DLL	Стандартный HAL (не ACPI, APIC)
HAL486C.DLL8	HAL для i486 C-Step систем
HALAPIC.DLL	Однопроцессорная версия HALMPS.DLL (не ACPI, APIC)
HALAST.DLL	Для симметричных многопроцессорных систем от компании AST
HALMPS.DLL	Для большинства многопроцессорных систем на базе Intel (не ACPI, APIC)
HALACPI.DLL	Однопроцессорная версия HAL с поддержкой ACPI, не APIC
HALAACPI.DLL8	Однопроцессорная версия HAL с поддержкой ACPI и APIC
HALMACPI.DLL	Многопроцессорная версия HAL с поддержкой ACPI и APIC

Данные файлы находятся по адресу `%systemroot%\Driver Cache\i386\` в файле `driver.cab`. Чтобы получить возможность их использования, скопируйте данные файлы в папку `%systemroot%\System32`.

ПРИМЕЧАНИЕ

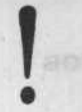
Аббревиатура APIC является сокращением от Advanced Programmable Interrupt Controller (усовершенствованный перепрограммируемый контроллер прерываний). Этот контроллер прерываний основан на микросхеме Intel 8259A или ее аналогах, способен работать с восемью линиями прерываний и функционирует лишь в однопроцессорных системах. В IBM PC всегда присутствуют два контроллера, причем второй подключен к первому, что увеличивает количество прерываний до 15. Новый модернизированный контроллер прерываний, который используется в многопроцессорных системах, способен работать с 256 прерываниями, которых, как правило, достаточно для работы всех устройств системы.

Чтобы предупредить сбои во время переключения ядер, нужно воспользоваться способом ручного переключения ядер, который предоставляет возможность использовать все доступные комбинации компонентов ядра, а также активировать многовариантную загрузку операционной системы. Для этого необходимо изменить файл `boot.ini`, который находится в корне системного раздела.

Откройте файл `boot.ini` в Блокноте и найдите там строку, подобную следующей:

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP
Professional RU" /fastdetect
```

Скопируйте данную строчку целиком и поместите ее в конец файла `boot.ini`, заменив название Windows XP Professional любым другим, например Secondary kernel, и допишите ключи `/KERNEL=` и `/HAL=`, написав имена выбранных файлов исполнительной системы ядра и уровня аппаратных абстракций (обратитесь к табл. 4.4).



ВНИМАНИЕ

Учтите, что в случае некорректного изменения данного файла система не сможет запуститься. Поэтому настоятельно рекомендуется сохранить его резервную копию на дискету, чтобы при необходимости boot.ini можно было легко восстановить.

Теперь при запуске операционной системы у вас появится возможность многовариантной загрузки, которая позволит переключаться между различными версиями ядра (что безопаснее процесса смены ядра в Диспетчере задач).

Смена ядра Windows значительно расширяет возможности по клонированию операционной системы на компьютеры с различной конфигурацией. В подавляющем большинстве случаев вам будет достаточно указать в файле `boot.ini` нужную версию KERNEL и HAL, и Windows будет корректно работать на новом оборудовании.

ГЛАВА 5 Защищаем информацию в нашей сети

- Кое-что об информационной безопасности
- Антивирусные мероприятия
- Защищаем систему от внешнего вторжения
- Проверяем свою сеть на защищенность
- Шифры для хранения секретов
- Сейф для файлов

В этой главе рассмотрим проблемы информационной безопасности сети. В настоящее время регулярно появляются новые вирусы и обнаруживаются критические недоработки в программном обеспечении. Кроме того, пугают масштабы хакерской активности. Вы узнаете о принципах организации антивирусной защиты, научитесь устанавливать и настраивать брандмауэр, научитесь определять уровень защищенности компьютеров в сети, используя сканеры безопасности. Кроме того, познакомитесь с программным обеспечением, позволяющим шифровать важную информацию.

Кое-что об информационной безопасности

Сегодня уже никому не приходится доказывать, что данные нужно защищать. В Интернете распространяется множество разнообразных вирусов, несанкционированный доступ становится своеобразным хобби среди молодежи, которая разбирается в технике, а большинство документации различных организаций приобретает электронную форму.

Мы все теснее и теснее связываем свою жизнь с компьютерными технологиями. Они помогают обрабатывать данные на работе, мы получаем деньги, используя пластиковые карточки, работаем и отдыхаем в Интернете.

Глобальная сеть — Интернет — постепенно превращается в продолжение реальной жизни. Некоторым людям Интернет необходим в работе, однако абсолютное большинство пользователей ищут в глобальной сети разнообразные развлечения — игры, общение и т. д.

Защита данных в настоящий момент является объективной необходимостью. Опыт показывает, что существует множество способов несанкционированного доступа к информации:

- стороннее подключение к локальной сети;
- перехват электромагнитного излучения;
- кража носителей информации, логинов и паролей;
- считывание данных из пользовательских массивов;
- чтение остаточных данных из памяти системы после выполнения основных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- применение программных ловушек;
- использование недоработок в операционных системах;
- использование вирусов, относящихся к подвиду троянский конь;
- намеренный вывод из строя механизмов, обеспечивающих защиту системы;
- умышленное и неумышленное заражение компьютерными вирусами.

Схожим является и список угроз конфиденциальности информации:

- перехват данных — эта угроза означает возможность злоумышленника подключаться к линии связи для получения информации, которая передается по данной линии, либо получать сведения на расстоянии с помощью побочного электромагнитного излучения, которое выделяется в процессе передачи информации;
- изучение трафика — обзор данных, которые касаются связи между клиентами (присутствие/отсутствие, частота, направление, тип, объем трафика и т. д.). В этом случае можно получить некоторый объем данных, основываясь на характеристиках трафика (непрерывность, присутствие или отсутствие информации);
- корректировка потока информации — внесение небольших искажений в поток данных, уничтожение отдельных сообщений или изменение порядка пакетов и сообщений в пределах потока;
- маскарад — попытка злоумышленника выдать себя за реально существующего пользователя, чтобы получить необходимые возможности и привилегии, или предоставление другому клиенту заведомо ложной информации;
- нарушение связи — искусственный обрыв связи или задержка передачи срочных сообщений.

Безусловно, идеальную защиту построить не удастся, однако существует набор правил, к которым стоит прислушаться любому администратору.

Простейшая защита сервера и рабочих станций

Сервер нужно поместить в отдельное помещение, доступ к которому ограничен. Лучше установить в данном помещении кондиционер для дополнительного охлаждения. Наилучшим вариантом будет организация отдельного помещения для мини-АТС, серверов и других сетевых устройств.

Сервер нужно обязательно опечатать, чтобы быть уверенным в том, что его в ваше отсутствие не разбирали. По возможности отключите дисководы и приводы компакт-дисков в BIOS или путем отсоединения кабелей (это нужно для того, чтобы никто не смог получить доступ к файловой системе с помощью этих носителей данных). Если сервер даст сбой и нужно будет загрузиться с дискеты или компакт-диска, их всегда можно будет вернуть в систему.

Точно так же, как и сервер, вам следует опечатать и компьютеры пользователей.

Если у клиентов отсутствует необходимость использования дискет, то отключите их приводы от материнской платы, оставив работающими приводы на нескольких компьютерах для того, чтобы там можно было произвести запись, если возникнет потребность. Отключите все неиспользуемые USB, COM и LPT-порты.

Установите пароль на BIOS и запретите возможность загрузки компьютера с дискет и компакт-дисков. Не давайте пользователям прав для сохранения файлов

на локальном диске, выделите для этого специальные сетевые диски. Таким образом, значительно проще настроить функцию резервного копирования. Через определенные промежутки времени уничтожайте всю лишнюю информацию с локальных дисков. Не следует открывать для общего доступа диски и принтеры рабочих станций.

Проводим работу с пользователями

Когда новый сотрудник устраивается на работу, крайне желательно указать в контракте, что он не должен придавать огласке информацию, которая касается локальной сети предприятия, а также свои логин и пароль.

Составьте инструкции, касающиеся работы в сети, с компьютером, периферией и прочей офисной техникой. В данной инструкции подробно опишите, что можно делать, а чего нельзя. Такая инструкция сэкономит массу времени.

Обязательно укажите, для каких целей пользователю выдается его логин и пароль, а также то, что запрещено пользоваться чужими паролями и разглашать кому бы то ни было свои собственные.

Антивирусные мероприятия

Возникновение вирусов относится к середине двадцатого века, когда активно начали проводиться первые разработки саморазмножающихся алгоритмов. Фон Нейман, Винер и некоторые другие авторы в своих работах дали определение и провели математическое исследование подобных алгоритмов, которые стали известны еще в 1940-х годах. Понятие компьютерного вируса появилось несколько позднее — считается, что впервые этот термин озвучил один из сотрудников Лехайского университета (США) Ф. Коэн в 1984 году во время доклада на седьмой конференции по безопасности данных.

В 1962 году инженеры компании Bell Telephone Laboratories — В. А. Высотский, Г. Д. Макилрой и Р. Моррис — разработали достаточно простую игру, получившую название Darvin. Данная игра представляла собой соревнование двух программ-соперников, способных к саморазмножению. Конечной целью данной игры был захват всех ресурсов компьютера или разрушение кода программы-оппонента. Для мониторинга процесса игры и определения победителя запускалась специальная программа-супервайзер, которая устанавливала правила данной схватки. Программы стали прообразами большинства компьютерных вирусов и обладали функциями исследования пространства, размножения и разрушения. Неудивительно, что Darvin имел колоссальный успех среди программистов и стал еще одной ступенькой в исследовании, развитии и создании компьютерных вирусов.

После этого начали появляться первые вирусы, напоминающие те, которые мы можем увидеть в наше время.

Какими бывают вирусы

В зависимости от проявления и дальнейшего поведения вредоносные программы можно условно разделить на следующие группы:

- «черви»;
- троянские кони;
- программы группы риска;
- непосредственно вирусы.

«Черви» рассылают свои копии по Сети (например, с помощью электронной почты). Название этого класса возникло из-за способности червей быстро размножаться, используя компьютерные сети: через системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN и т. д. «Черви» опасны прежде всего из-за того, что способны очень быстро распространяться. «Черви», попавшие в компьютер, определяют IP-адреса и адреса электронной почты других компьютеров, рассылают по ним копии своего кода. Достаточно часто представители этого семейства вирусов создают рабочие файлы на жестком диске, однако возможно и такое, когда они вообще не используют ресурсы компьютера, кроме оперативной памяти. Многие из «червей» существуют и рассылаются в виде файлов: добавление к электронному письму, ссылка на файл, пораженный вирусом, файл в каталоге обмена P2P и т. п.

Троянский конь — приложение, которое призвано незаметно и несанкционированно собирать данные и передавать их создателю вируса, разрушать или модифицировать важную информацию, создавать сбои в работе компьютера, использовать ресурсы компьютера для собственных целей. Троянские кони не распространяются сами, как это делают «черви». Как правило, их устанавливают или передают вручную, маскируя под необходимые пользователю программы и утилиты. Урон, который наносят троянские кони, может быть гораздо большим, чем при стандартной вирусной атаке, которая может быть успешно отбита специальным программным обеспечением.

Программы из группы риска — программное обеспечение, работа с которым несет в себе долю риска. Как пример можно привести браузер Internet Explorer. Всем известно, что в нем содержится большое количество ошибок, а потому работа с ним может стать причиной заражения вирусом или даже проникновения хакера.

Вирусами называются программы, которые способны заражать другие приложения, добавляя в них свой код, для получения управления в случае запуска зараженных файлов. Скорость размножения вирусов не такая высокая, как у «червей». Одна из ключевых особенностей компьютерных вирусов — способность изменять исполняемые файлы.

Вирусы классифицируются по следующим признакам:

- среда обитания;
- операционная система (ОС);

- алгоритм функционирования;
- способность к разрушению.

В зависимости от среды обитания вирусы можно разделить на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы способны дописывать свой код в исполняемые файлы (встречаются наиболее часто). Они могут создавать копии уже имеющихся файлов или используют слабые места самой файловой системы.

Загрузочные вирусы помещают свой код в загрузочный сектор диска (Boot-сектор) либо в сектор, в котором находится системный загрузчик жесткого диска (Master Boot Record).

Макровирусы способны поразить файлы текстовых документов и электронных таблиц.

Сетевые вирусы распространяют свои копии с помощью определенных протоколов или команд компьютерных сетей (а также электронной почты).

Кроме перечисленных, существует множество смешанных видов вирусов — например, вы можете встретить файлово-загрузочные вирусы, способные поразить загрузочные секторы дисков и файлы, находящиеся на жестком диске. Такие вирусы наиболее опасны.

Вирусы классифицируются в зависимости от операционной системы, в которой они работают. Любой вирус способен заразить файлы одной или нескольких операционных систем — Win98/XP, OS/2, Linux и т. д. Макровирусы заражают файлы Microsoft Word, Excel. Загрузочные вирусы также написаны для определенных форматов расположения системной информации в загрузочных секторах дисков.

Вот некоторые особенности работы различных вирусов:

- работа в резидентном режиме;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- нестандартные приемы в процессе работы.

Под работой в резидентном режиме понимается способность вирусов загружать свои копии в оперативную память, получать доступ к некоторым процессам (например, обращения к файлам или дискам) и заражать обнаруженные объекты (секторы жесткого диска или конкретные файлы). Резидентные вирусы работают не только в тот момент, когда запущено приложение, но и после того, как оно было закрыто. Данные вирусы будут оставаться в оперативной памяти до очередной

перезагрузки системы, даже если вы уничтожите все их копии на винчестере. Та же ситуация характерна и для вирусов, поражающих загрузочные сектора — форматирование диска в тот момент, когда в памяти находится резидентный вирус, не всегда способно избавить от него, поскольку некоторые резидентные вирусы способны заразить диск повторно после форматирования.

Резидентными в какой-то степени являются и макровирусы, так как они находятся в памяти компьютера в течение того времени, когда запущен соответствующий редактор. Данный редактор заменит вирусу операционную систему, и загрузкой для такого вируса станет выход из редактора.

Применение стелс-алгоритмов дает вирусам возможность частично или полностью скрыть от пользователя свое присутствие в процессе работы. Чаще всего встречается стелс-алгоритм, перехватывающий запросы ОС на чтение или запись зараженных объектов. Стелс-вирусы способны либо временно удалять из этих файлов свой код, либо предоставляют вместо себя незараженные сегменты информации. В случае с макровирусами самый популярный способ состоит в запрете вызова меню просмотра и редактирования макросов.

Самошифрование и полиморфичность — это способность вируса беспрерывно модифицировать свой код, что сильно затрудняет процесс его поиска и уничтожения. К полиморфичным вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок — участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами: шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Встречаются и достаточно экзотические примеры полиморфизма например Bomber, вирус под MS-DOS. Этот вирус не использует шифрование, однако набор команд, который отдает управление коду вируса, является абсолютно полиморфным.

Большинство нетривиальных приемов используются, чтобы как можно тщательнее спрятать вирус в системе, защитить от обнаружения его резидентную часть и максимально усложнить процесс лечения (например, записав свою копию в Flash-BIOS) и т. д.

В зависимости от разрушительных возможностей вирусы можно разделить на следующие группы:

- безвредные — не влияют на работу системы, кроме использования ресурсов компьютера для своей работы;
- неопасные — потребляют ресурсы компьютера и демонстрируют графические, звуковые и прочие эффекты;
- опасные — способны привести к серьезным проблемам в процессе работы компьютера;
- очень опасные — содержат в своем алгоритме процедуры, способные привести к уничтожению информации, сбоям в работе операционной системы и отдельных приложений.

Наиболее распространенной антивирусной программой в нашей стране является «Антивирус Касперского». Данное приложение (а точнее — целая система) установлено на 70 % компьютеров пользователей и является негласным стандартом в локальных сетях организаций.

«Антивирус Касперского Personal»

«Антивирус Касперского» считается одним из лучших антивирусных приложений на сегодняшний день. Сайт производителя — www.kaspersky.ru.

Программа способна находить и лечить объекты, которые заражены большинством известных вирусов. Антивирусные базы обновляются каждые три часа, а сама компания-разработчик обеспечивает круглосуточную поддержку пользователей по телефону и электронной почте.

«Антивирус Касперского» не бесплатный — лицензия стоит около $70, однако данная сумма совсем невелика по сравнению с теми убытками, которые организация может понести при заражении компьютеров вирусами.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch05\Kaspersky вы найдете дистрибутив программы «Антивирус Касперского Personal». Чтобы его использовать, необходимо купить ключ.

«Антивирус Касперского» выполняет следующие функции.

- Обеспечение непрерывной защиты файловой системы от вирусов в режиме мониторинга: перехват и исследование всех обращений к файловой системе конкретного компьютера и к сетевым дискам; лечение, удаление зараженных файлов или их извлечение для последующего анализа.
- Проверка заданной пользователем области.
- Проверка электронной почты в фоновом режиме: изучение всех запросов на получение и отправку электронных писем. Антивирус не позволяет зараженным сообщениям попадать на компьютер и запрещает отправку зараженных файлов получателям. Проверяется вся почта, отправляемая и принимаемая любой почтовой программой, использующей протоколы POP3 и SMTP.
- Защита офисных приложений, которые используют VBA-макросы: изучение макрокоманд перед тем, как выполнить их, предотвращение исполнения опасных макрокоманд.
- Проверка сценариев VBScript и JavaScript, которая производится перед выполнением сценария модулем обработки; запрет исполнения потенциально опасных сценариев.
- Изолирование подозрительных файлов: помещение их в специальную карантинную папку с целью их последующей отправки в Лабораторию Касперского

для исследования; восстановление файлов из карантинной директории по запросу администратора/пользователя.

- Создание копии зараженного файла в специальной папке перед лечением или удалением для того, чтобы данный объект можно было восстановить по первому требованию.
- Регулярное обновление антивирусных баз и системных модулей антивируса с серверов обновлений Лаборатории Касперского. Создание копии всех обновляемых файлов на тот случай, если понадобится отменить последнее сделанное обновление. Копирование файлов обновления на сетевой или локальный диск для дальнейшего использования всеми пользователями сети.

Аппаратные и программные требования к системе

«Антивирус Каперского» имеет следующие системные требования (в зависимости от используемой операционной системы).

- Microsoft Windows 98/Me/NT Workstations 4.0 с установленным Service Pack 6:
  - Intel Pentium 133 МГц или выше для Windows 98/NT;
  - Intel Pentium 150 МГц или выше для Windows Me;
  - 32 Мбайт свободной оперативной памяти;
  - 50 Мбайт свободного дискового пространства;
  - привод компакт-дисков.
- Microsoft Windows 2000 Professional с установленным Service Pack 2:
  - Intel Pentium 133 МГц или выше;
  - 64 Мбайт свободной оперативной памяти;
  - 50 Мбайт свободного дискового пространства;
  - привод компакт-дисков.
- Microsoft Windows XP Home Edition и XP Professional:
  - Intel Pentium 300 МГц или выше;
  - 128 Мбайт свободной оперативной памяти;
  - 50 Мбайт свободного дискового пространства;
  - привод компакт-дисков.

Инсталляция антивируса выполняется точно так же, как и установка большинства приложений Windows, поэтому проблем возникнуть не должно.

После окончания установки программа попросит провести перезагрузку компьютера. Выполнив это требование, вы сможете открыть главное окно антивируса (рис. 5.1), щелкнув на его значке на Панели задач.

Как видно на рисунке, программа обладает красивым и удобным интерфейсом.

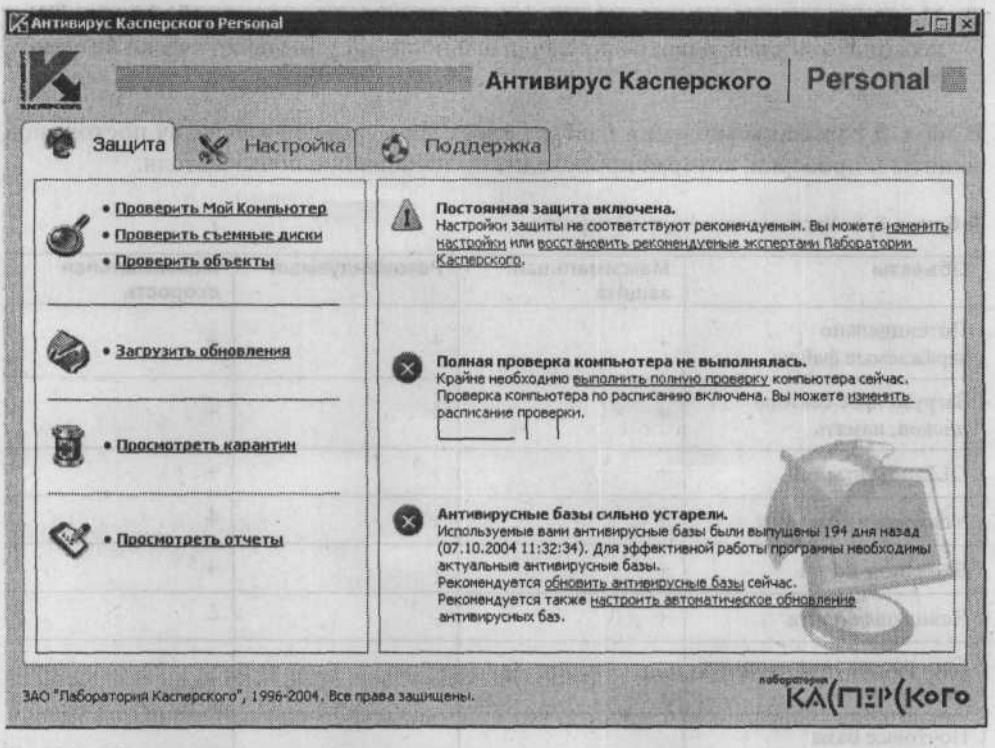


Рис. 5.1. Главное окно программы

Уровни антивирусной защиты

Для упрощения процесса настройки антивирусной защиты в программе существуют три уровня с определенным набором настроек. От того, какой уровень вы выберите, будет зависеть защита системы и скорость ее работы. Чем выше уровень, тем больше ресурсов вашего компьютера будет использовать антивирус (что может сказаться на производительности системы в целом).

Процесс поиска и анализа подозрительных файлов представляет собой сложную математическую задачу, которая основана на изучении структуры, подсчете контрольных сумм и математических преобразованиях информации. Поэтому основная нагрузка во время работы антивируса ложится именно на процессор. Каждый новый вирус, который появляется в антивирусной базе, увеличивает время антивирусной проверки.

Перечислим описанные уровни.

- Максимальная защита — максимально возможный уровень защиты, однако общая производительность системы может снизиться.
- Рекомендуемый — данный уровень обеспечивает баланс между глубиной проверки и общей производительностью системы.

- Максимальная скорость — в этом случае уровень антивирусной защиты будет несколько снижен, однако производительность системы практически не снижается.

В табл. 5.1 указаны значения настроек всех трех уровней для задач постоянной защиты и проверки, которая происходит по требованию пользователя.

Таблица 5.1. Уровни антивирусной защиты

Объекты	Максимальная защита	Рекомендуемый	Максимальная скорость
Потенциально заражаемые файлы	+	+	+
Загрузочные сектора дисков, память	+	+	+
OLE-объекты	+	+	+
Упакованные файлы	+	+	+
Входящая почта	+	+	+
Исходящая почта	+	–	–
Самораспаковывающиеся архивы	+	–	–
Почтовые базы и письма	–	–	–

Обновляться необходимо!

Постоянное обновление антивирусных баз — обязательное условие обеспечения безопасности вашей информации. Вам следует обновлять антивирусные базы как минимум раз в несколько дней. Если же на вашем компьютере присутствуют важные данные, то вам необходимо обновлять базы ежедневно.

Как уже упоминалось, «Антивирус Касперского» способен обновлять антивирусные базы со своих серверов в Интернете или из локального и сетевого каталога. Вы можете указать в настройках программы, откуда должно производиться обновление баз (рис. 5.2).

Возможность обновления из сетевого каталога будет полезна, если каждый компьютер вашей сети снабжен антивирусом. В этом случае вы можете загрузить обновленные базы и расположить их в общей сетевой папке, что позволит сэкономить трафик (ведь теперь остальные компьютеры будут обновлять базы из локальной сети, а не с сервера разработчика).

Описанный выше процесс можно автоматизировать. Сервер будет автоматически скачивать обновленные базы и сохранять их в папке, которая доступна каждой рабочей станции.

Вы можете настроить «Антивирус Касперского» так, чтобы он обновлял базы в определенное время. Если вы не используете эту функцию, то антивирус будет периодически уведомлять вас о том, что базы устарели.

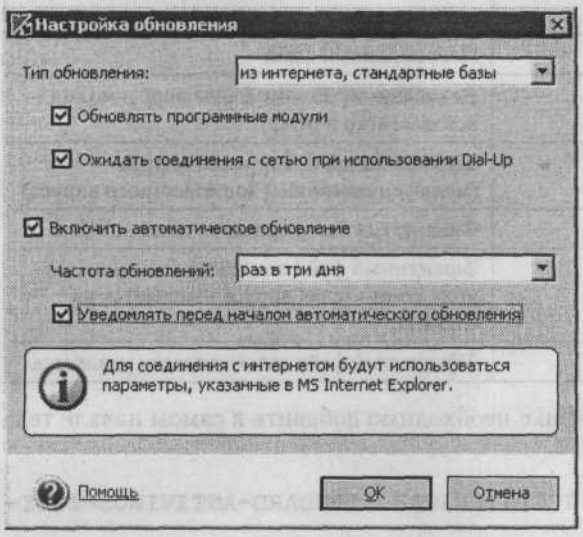


Рис. 5.2. Настройки автоматического обновления антивирусных баз

Проверим работу антивируса

После того как вы инсталлировали и настроили антивирус, можно проверить его работу, используя специальный тестовый вирус и несколько его видоизмененных версий. Данный имитатор вируса был создан организацией EICAR (The European Institute for Computer Antivirus Research) для тестирования работы антивирусных продуктов. Программа не содержит вредоносного кода, однако большинство антивирусов воспринимают ее как вирус.

Загрузить тестовый вирус можно с официального сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm. Если у вас нет доступа к Интернету, вы можете создать тестовый вирус самостоятельно. Для этого наберите в Блокноте следующую строку и сохраните документ в файле `eicar.com`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Созданный таким нехитрым способом файл содержит код тестового вируса. Антивирус воспримет его как вирус и проведет над ним все операции, которые вы назначили в настройках.

Чтобы проверить последовательность действий «Антивируса Касперского» при обнаружении других объектов, у вас есть возможность изменить тело тестового вируса, добавив в текст указанные ниже приставки (табл. 5.2).

Таблица 5.2. Варианты модификации тестового вируса EICAR

Префикс	Тип объекта
Префикс отсутствует, стандартный тест	Файл заражен. При попытке лечения объекта возникает ошибка; объект удаляется
CORR-	Поврежденный файл
SUSP-	Возможно заражение файла вирусом (код неизвестного вируса)
WARN-	Заражен одной из вариаций вируса (модифицированный код известного вируса)
ERRO-	Файл не мог быть проверен из-за ошибки
CURE-	Зараженный файл подлежит лечению, при этом текст «тела» вируса изменяется на CURED
DELE-	Зараженный файл автоматически удаляется

Указанный в первом столбце префикс необходимо добавить в самом начале тела вируса. Например:

```
DELE-X5O!P%@AP[4\PZX54(P^)7CC)7)$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Второй столбец таблицы подробно описывает те действия, которые должен выполнить антивирус в случае обнаружения тестового вируса, содержащего указанный префикс. Учтите, что порядок действий может корректироваться в настройках программы.

Создав тестовый вирус, можно начинать проверку (рис. 5.3).

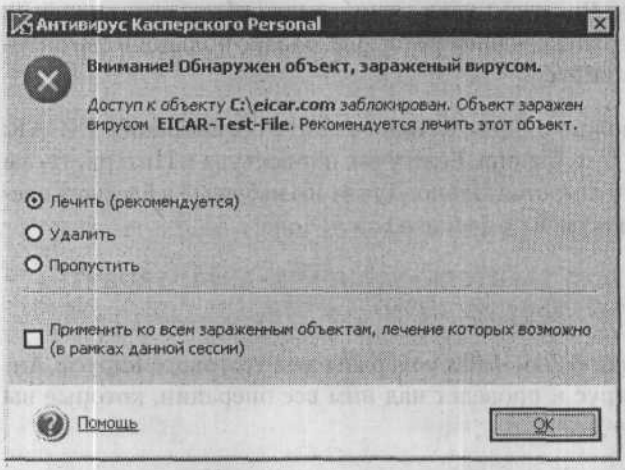


Рис. 5.3. Вирус обнаружен

Как видите, антивирус без труда обнаружил зараженный файл.

Защищаем систему от внешнего вторжения

Не забывайте, что установка антивируса не решает всех проблем сразу, ведь если ваша локальная сеть имеет выход в Интернет, то вам следует быть готовыми к хакерским атакам и борьбе с сетевыми червями.

Если вы считаете, что ваша сеть не может никого заинтересовать, то вы заблуждаетесь. Даже если в сети нет важной информации (списки логинов/паролей к различным ресурсам, номера кредиток, номера банковских счетов), хакеры могут взломать ее из просто так, из интереса. Подобные несанкционированные действия становятся популярными, поэтому достаточно велика вероятность атаки именно вашей сети.

Именно по этой причине, вам стоит своевременно позаботиться о безопасности и установить брандмауэр. Брандмауэр (firewall, англ. «огненная стена») — это программа или специальное устройство, которое пропускает через себя весь трафик. Эта программа входит в сеть и выходит из нее с целью фильтрации трафика. В процессе анализа и фильтрации потоков данных брандмауэр опирается на специально установленные системным администратором правила, блокируя пакеты с данными или же пропуская их. С помощью этой программы (или устройства) возможно не только защитить локальную сеть от внешней атаки, но и управлять ею. Например, можно ограничить доступ к некоторым сетевым ресурсам, заблокировать работу популярных клиентов IRC или ICQ, запретить загрузку рекламных баннеров с веб-страниц.

Если ваша сеть небольшая, то приобретение аппаратного брандмауэра вряд ли будет оправданным, поэтому вам следует остановиться на программной реализации этого устройства. На данный момент существуют самые разнообразные программные брандмауэры, которые отличаются набором функций, удобством в использовании и, конечно же, стоимостью. Одним из лучших брандмауэров считается Kaspersky Anti-Hacker, разработкой которого занимается Лаборатория Касперского.

Программа Kaspersky Anti-Hacker разработана для защиты компьютера от несанкционированного доступа к информации и атак хакеров из Интернета или локальной сети. Лицензионная копия Kaspersky Anti-Hacker стоит около $50, однако разработчики предлагают различные скидки.

Пользователи данной программы имеют право на круглосуточную поддержку по телефону и электронной почте. Если учесть ее невысокую стоимость, то Kaspersky Anti-Hacker идеально подходит для защиты небольших локальных сетей.

Программа выполняет следующие функции.

- Мониторинг сетевой активности (через протокол TCP/IP) всех программ, установленных на данном компьютере. Если будет замечена подозрительная активность какого-нибудь приложения, брандмауэр сообщит об этом и предоставит возможность заблокировать доступ для данного приложения. Например, если троянский конь будет пытаться направить собранные на вашем компьютере данные в Интернет, Kaspersky Anti-Hacker закроет для него доступ во всемирную сеть.

- Мониторинг сканирования портов вашего компьютера и блокирование дальнейшего взаимодействия с атакующим компьютером.
- Использование технологии SmartStealth значительно усложняет нахождение конкретного компьютера в сети, что приводит к потере объекта атаки. Кроме этого, данная технология способна защитить от любых DoS (Denial of Service — отказ в обслуживании) атак. Помните, что работа в невидимом режиме не мешает вашей работе в сети.
- Просмотр списков всех активных соединений, открытых портов и работающих сетевых программ (а также разрыв опасных соединений).
- Блокирует атаки хакеров, фильтруя входящий и исходящий трафик (существует возможность уведомления о попытке несанкционированного доступа).
- Позволяет использовать данное приложение, минуя сложный процесс конфигурирования. Kaspersky Anti-Hacker предусматривает упрощенное администрирование, используя пять режимов безопасности: Разрешить все, Низкий, Средний, Высокий и Запретить все. С самого начала включается режим Средний (способный обучаться), который изменяет настройки системы безопасности, опираясь на вашу реакцию на определенные события.
- Позволяет достаточно гибко настраивать систему защиты (настроить фильтрацию разрешенных и запрещенных сетевых операций, а также активировать детектор атак).
- Позволяет вносить определенные события в журнал. При необходимости можно изменять уровень подробности записи событий в журналы.

Установка программы достаточно стандартна, поэтому на ней мы подробно останавливаться не будем. Сразу после окончания процесса инсталляции приложение попросит совершить перезагрузку компьютера. После перезагрузки система безопасности начнет свою работу, отслеживая входящий и исходящий трафик. Внешний вид главного окна программы показан на рис. 5.4.

Теперь обратимся к настройкам. Программа позволяет установить один из пяти следующих режимов безопасности.

- Разрешить все — защита отключена, допускается любая активность.
- Низкий — приложение допускает сетевую активность всех программ, кроме тех, которые запрещены в правилах брандмауэра системным администратором.
- Средний — программа сообщает пользователю о каждом случае проявления сетевой активности приложений. При попытке программы выполнить сетевую операцию брандмауэр включит режим обучения. Вам будет предоставлена полная информация о данной сетевой активности, на основе которой вам нужно решить: разрешить или блокировать подобное событие только в этот раз, заблокировать любые попытки сетевой активности данной программы, разрешить активность программы или настроить дополнительные параметры для данного приложения. В зависимости от того, как вы себя поведете в данной ситуации, брандмауэр будет составлять правила сетевого доступа для данного приложения.
- Высокий — доступ разрешен только программам, перечисленным в правилах.

- Запретить все — брандмауэр полностью блокирует доступ каких-либо приложений к сети. Работу в данном режиме можно сравнить с физическим отключением кабеля.

Рис. 5.4. Главное окно программы

В режимах Высокий, Средний и Низкий возможно подключение дополнительного режима — Режима невидимости. В данном случае допускается только сетевая активность пользователя, все остальные подключения блокируются, если только какое-то из приложений не внесено в список правил, позволяющих доступ. Таким образом, компьютер становится «невидимым» в сети, и злоумышленники теряют объект для атаки. Мониторинг атак включен для всех режимов безопасности, кроме Разрешить все. При необходимости этот детектор можно отключить в настройках программы.

Для рабочих станций рекомендуется использовать режим безопасности Средний и заняться после этого обучением брандмауэра. Высокий уровень безопасности подойдет для сервера, однако при этом нужно вручную настроить разрешающие и запрещающие правила и активировать детектор атак.

Настройка может быть произведена с помощью создания правил фильтрации операций в сети. Часть фильтрации производится детектором атак автоматически путем обнаружения попыток сканирования портов, DoS-атак и тому подобных проблем (кроме того, может осуществляться блокировка атаки). Вы можете создать свои правила фильтрации, чтобы обеспечить наилучшую защиту компьютера.

Каждому виду сетевых операций в Kaspersky Anti-Hacker соответствуют специальные наборы правил.

Задаем правила для приложений

Если в главном окне программы вы выберете Сервис ▸ Правила для приложений, то сможете создавать, редактировать и изменять правила фильтрации программ, имеющих доступ к Интернету и локальной сети (рис. 5.5).

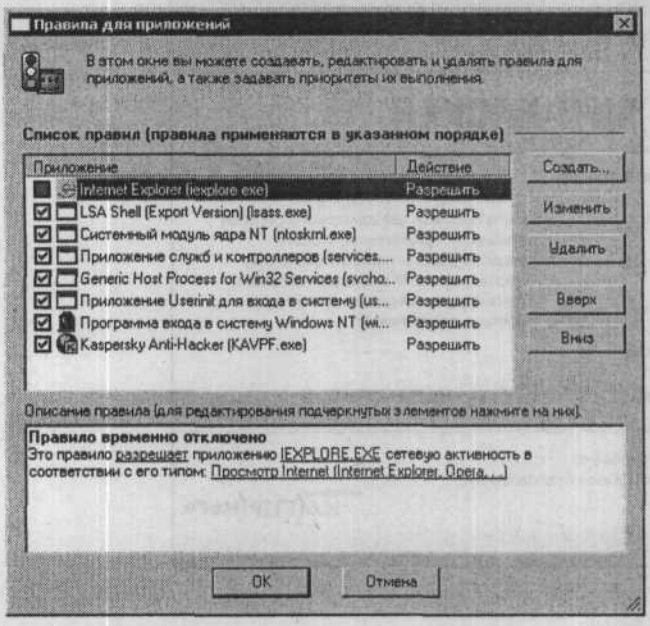


Рис. 5.5. Задаем правила для приложений

Каждому приложению можно разрешить специфический вид активности. В левой верхней части окна расположен список доступных правил. В столбце Приложение показан значок приложения, название и флажок, показывающий, активно ли данное правило сейчас. В столбце Действие находится краткое описание правила: Разрешить — разрешает, Запретить — наоборот, запрещает.

Правила отображены в порядке понижения приоритета их исполнения. При попытке любого приложения проявить сетевую активность список правил будет просмотрен сверху вниз, пока не найдется такое, которое разрешает или запрещает проводимую операцию, либо пока список не будет изучен полностью. Если необходимого правила не существует, выполняется действие, принятое по умолчанию. Если вы собираетесь заблокировать для приложения часть операций, нужно создать два правила. Одно — разрешающее часть операций (должно быть в списке выше), а другое — запрещающее все операции для данной программы. Если приложение попытается выполнить разрешенную операцию Kaspersky Anti-Hacker, то будет применено разрешающее правило (которое находится выше), а выполнение любой другой операции приведет к использованию запрещающего правила из нижней части списка. Если будет обнаружена операция, которая не отвечает вашим правилам, брандмауэр тут же уведомит вас об этом, чтобы можно было разрешить или заблокировать данную активность (при использовании режима Средний).

Устанавливаем правила фильтрации пакетов

Если выбрать в главном окне программы Сервис ▸ Правила фильтрации пакетов, то вы можете настроить список разрешенных и запрещенных портов (рис. 5.6).

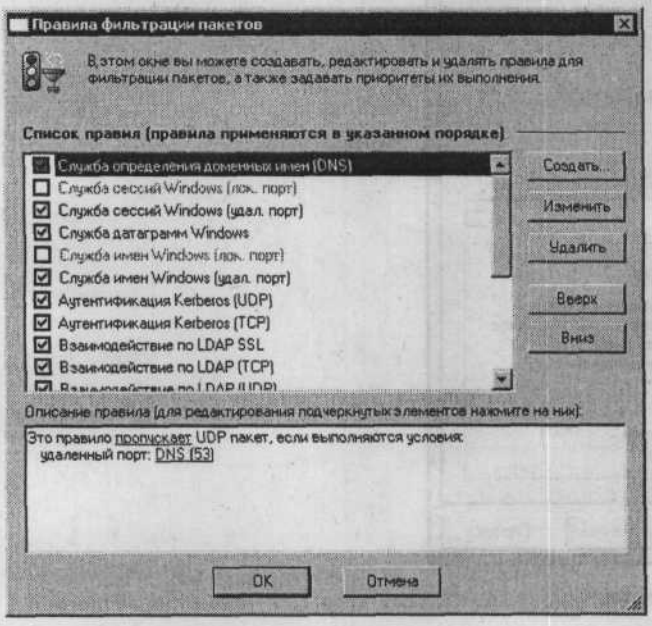


Рис. 5.6. Правила фильтрации пакетов

Например, если вы заблокируете порт 80, то доступ к веб-страницам будет закрыт, в то время как электронная почта, использующая другой порт, будет по-прежнему работать. Обратите внимание, что установленные правила фильтрации будут иметь более высокий приоритет, чем правила для приложений, следовательно, они обрабатываются и исполняются первыми.

Решение принимается с помощью заголовка пакета с данными: номеров используемых портов, протоколов, IP-адресов и др. Здесь вы можете установить целый набор правил, которые будут использованы для абсолютно всех приложений. Если вы таким образом заблокируете произвольный IP-адрес, то тем самым полностью запретите сетевые операции, которые исходят от него.

Отследим хакерскую атаку

Kaspersky Anti-Hacker может проводить мониторинг атак, которые осуществляются из сети Интернет. Он способен распознать большинство DoS-атак (SYN Flood, UDP Flood, ICMP Flood), атаки Ping of death, Land, Helkern, Lovesan и SmbDie, а также вовремя засечь сканирование портов, которое может производиться перед такой атакой.

Указать настройки мониторинга атак можно в окне Параметры, на вкладке Детектор атак (рис. 5.7).

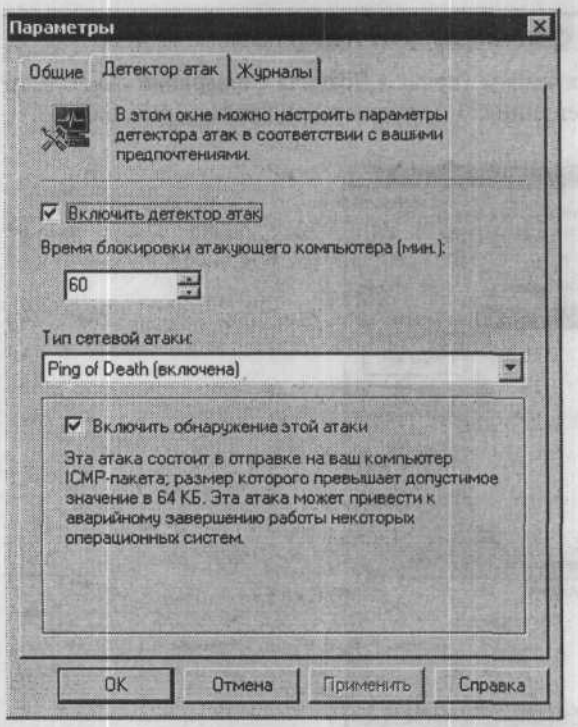


Рис. 5.7. Настраиваем детектор атак

Тут вы можете установить время, на которое будет блокирован атакующий компьютер, включить или отключить мониторинг различных видов атак.

Данный брандмауэр способен сохранять информацию обо всех своих действиях в специальный журнал. Всего возможно использование трех типов журналов.

- Журнал сетевых атак. Здесь содержится информация, которая касается атак, совершенных на ваш компьютер.
- Журнал активности сетевых приложений. Сюда будет заноситься информация, которую вы определили для протоколирования в процессе создания правил для программ и утилит.
- Журнал пакетной фильтрации. В этот журнал будет заноситься информация, которую вы определили для протоколирования в процессе настройки фильтрации пакетов с данными.

Для просмотра журналов и дальнейшей работы с ними существует специальное окно (окно журналов). Чтобы перейти к нему, выполните команду меню Вид ▸ Журналы и выберите нужный журнал.

Кроме того, вы можете ограничить максимальный размер любого журнала и задать режим его очистки при запуске. У вас также будет возможность сохранить любой журнал в виде файла на жестком диске.

Проверяем свою сеть на защищенность

Чтобы убедиться в том, что брандмауэр работает правильно, нужно использовать сканер безопасности. Сканер анализирует сеть и находит в ней все уязвимые места, обрабатывает полученные результаты и генерирует отчет на их основе. Достаточно часто найденное слабое место может быть устранено без вмешательства администратора. Рассмотрим перечень проблем, которые способны обнаружить системы сканирования:

- «люки» в приложениях (Back Door) и наличие троянских коней;
- непродуманные пароли, которые легко подобрать с помощью специального программного обеспечения;
- общая незащищенность системы и вероятность проникновения;
- неправильная настройка брандмауэра, веб-серверов и баз данных.

Для примера мы будем использовать приложение XSpider компании Positive Technologies (http://www.ptsecurity.ru). XSpider — программа, предназначенная для сканирования и удаленной диагностики компонентов сети на предмет обнаружения уязвимых мест. На сайте разработчика вы всегда можете скачать бесплатную демо-версию.

ПРЕМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch05\XSpider 7.0 находится дистрибутив демо-версии XSpider 7.

Основные отличия XSpider от подобных программ:

- многочисленные нововведения, которые используются в процессе сканирования;
- интеллектуальная идентификация сервисов;
- обработка всех RPC-сервисов с их полным определением;
- анализ структуры и интеллектуальная идентификация слабых мест веб-серверов.

Демонстрационная версия отличается следующими ограничениями:

- невозможно обновление из Интернета;
- отсутствуют возможность поиска DoS-уязвимостей;
- отсутствует набор проверок, которые опираются на эвристические механизмы;
- слабые места веб-приложений, такие как SQL-инъекции, XSS, HTTP Response Splitting, обнаруживаются, однако в отчете отсутствуют подробности;
- планировщик заданий не сохраняет созданные расписания;
- создаваемые отчеты содержат только часть текста;

- история проверок открывается только в режиме просмотра, потому использовать сохраненные результаты в дальнейших проверках невозможно.

XSpider значительно превосходит по своей функциональности многие стандартные сканеры, а его многооконный интерфейс и доступные средства автоматизации позволяют организовать логичный и упорядоченный процесс слежения за безопасностью. Внешний вид главного окна программы изображен на рис. 5.8.

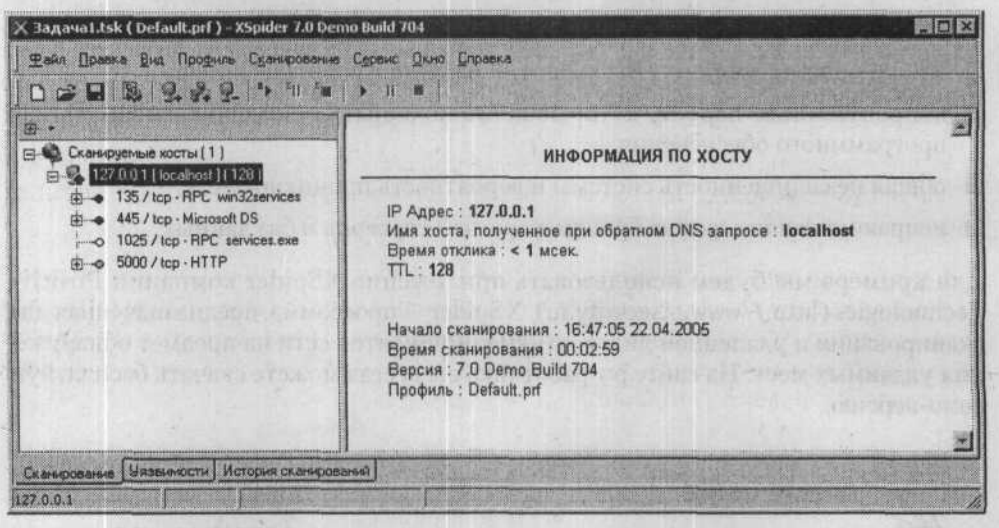


Рис. 5.8. Главное окно программы

Вся работа XSpider ориентирована на «задачу», которая включает в себя набор хостов, проверяющихся в процессе сканирования. В такую «задачу» стоит объединить те хосты, проверка которых будет производиться похожим образом. Как только «задача» будет создана, ей можно назначить определенный профиль — систему параметров, которые указывают, какие действия нужно выполнять в той или иной ситуации. Если вы не будете создавать новый профиль, будет применен профиль по умолчанию. Обратите внимание на то, что выполнение «задачи» может происходить в автоматическом режиме, достаточно будет создать расписание, согласно которому она будет выполняться. Для каждой существующей «задачи» будет создана история всех сканирований. Все сохраненные результаты можно загрузить и работать с ними, как с только что полученными (для анализа тенденций в работе).

Xspider 7 способен работать с несколькими «задачами» одновременно, причем любая из них может включать в себя множество хостов. Обратите внимание на то, что скорость и качество проверки может значительно снизиться, если канал, связывающий компьютеры в сети, перегружен, поэтому вам стоит следить за пропускной способностью сети в момент теста. XSpider создает достаточно небольшое количество трафика на один хост, поэтому перегрузка канала может появиться только при достаточно большом количестве (сотни) одновременно проверяемых хостов.

XSpider может сгенерировать отчет по результатам проверки, причем при использовании автоматического режима отчет придет к вам на указанный адрес элект-

ронной почты или же будет помещен на сетевой диск. Эта возможность очень удобна, поэтому вам стоит заняться подробной настройкой программы, чтобы далее все процессы происходили автоматически.

Так или иначе, большинство реальных слабых мест системы рано или поздно находятся, а ложных срабатываний сканера практически не происходит.

XSpider в процессе своей работы использует эвристические алгоритмы и занимается не только перебором слабых мест системы, которые прописаны в базе, но и дополнительно анализирует полученную информацию, ориентируясь на конкретную ситуацию. С помощью этого появляется возможность обнаружить даже те уязвимые места, которых нет в текущей базе.

Следует отметить, что база приложения обновляется каждый день и также может содержать обновленные программные модули с усовершенствованными механизмами сканирования.

Теперь можно заняться проверкой нашей сети. Проверке подлежат как подключенные к серверу компьютеры, так и сам сервер. Если вы хотите проверить свой компьютер, то нужно использовать адрес обратной петли (127.0.0.1). Добавляем новый хост, нажав клавишу Insert, и вводим его IP. После этого в меню Сканирование смело выбираем пункт Старт.

В процессе сканирования программа выведет IP-адрес удаленного компьютера, список его открытых портов, DNS-сервер, который используется, класс сети и прочую необходимую информацию.

Например, полученные данные могут указывать на некорректное использование файла виртуальной памяти, низкий уровень шифрования паролей и т. д. (рис. 5.9).

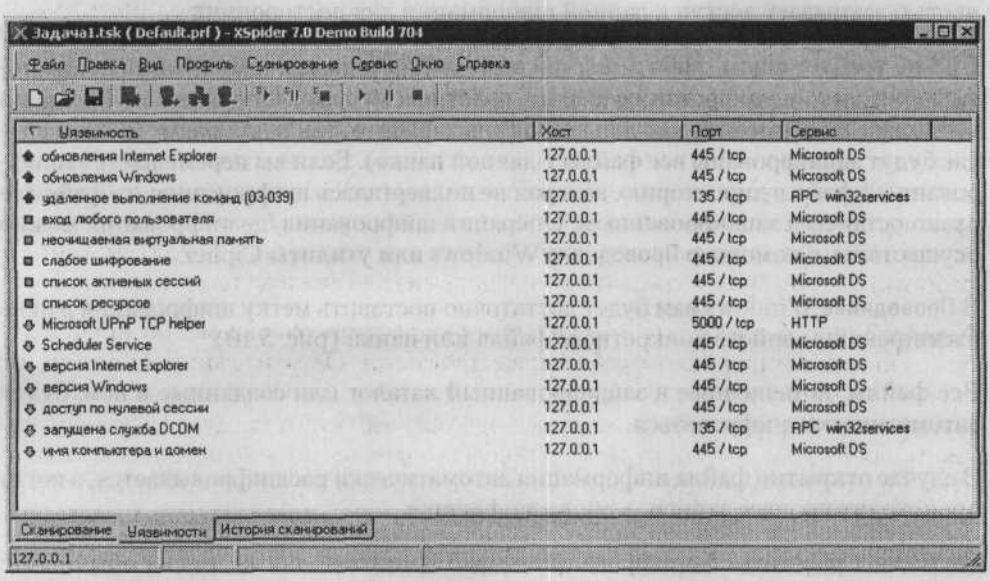


Рис. 5.9. Все уязвимости системы — как на ладони

В полученном отчете все уязвимые места будут различного цвета в зависимости от уровня их опасности для вашей системы. Что означает каждый из цветов, можно подробно узнать, нажав кнопку Легенда. Кроме того, отчет (который, кстати, может быть сохранен в виде HTML) отобразит возможные средства устранения найденных проблем. Теперь вам нужно дождаться окончания проверки и внимательно прочитать полученный отчет и устранить уязвимые места, следуя инструкциям программы.

Шифры для хранения секретов

Шифрующая файловая система — это специальная служба, расположенная в ядре операционной системы, которая тесно связана с файловой системой NTFS.

Данная служба защищает данные от несанкционированного использования с помощью шифрования всей информации на жестком диске. EFS (Encrypted File System — файловая система с шифрованием) основана на архитектуре Windows CryptoAPI, которая использует технологию шифрования с открытым ключом. Для шифрования произвольного файла генерируется уникальный ключ шифрования, который зависит от открытого (Public) и личного (Private) ключей пользователя.

Для шифрования файла в данном случае может быть использован любой симметричный алгоритм шифрования. Сейчас EFS применяет два алгоритма: DESX (модификация стандарта DES) и TribleDES (3DES), который также является наследником DES. Длина ключа составляет 56 бит.

Ключи шифрования EFS находятся в специальном пуле памяти, который не сохраняется на жестком диске (сама EFS расположена в ядре Windows XP), что полностью закрывает доступ к данной информации для посторонних.

EFS не требует каких-либо действий администратора, поэтому пользователи могут переходить к шифрованию файлов практически сразу. Операции шифрования возможно использовать как для конкретных файлов, так и для папок (в этом случае будут зашифрованы все файлы в данной папке). Если вы перемещаете зашифрованный файл в директорию, которая не подвергалась шифрованию, то файл все равно останется зашифрованным. Операции шифрования/дешифрования можно осуществить с помощью Проводника Windows или утилиты Cipher.

В Проводнике Windows вам будет достаточно поставить метку шифрования в окне расширенных свойств конкретного файла или папки (рис. 5.10).

Все файлы, помещенные в зашифрованный каталог или созданные в нем, будут автоматически шифроваться.

В случае открытия файла информация автоматически расшифровывается, а когда происходит процесс записи — снова шифруется.

Вы можете работать с зашифрованными файлами точно так же, как и с обычными: открывать, редактировать с помощью различных приложений или же удалять.

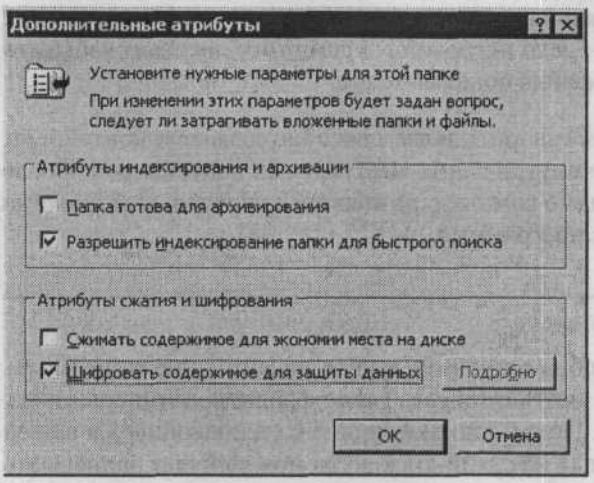


Рис. 5.10. Настраиваем атрибуты шифрования папки

Ни в коем случае не шифруйте файлы, которые используются при запуске системы, так как в этот момент ключи для дешифрования еще не будут доступны и система не сможет начать работу. В этом случае EFS применяет простую, но эффективную защиту: системные файлы просто не шифруются.

ВНИМАНИЕ

Если вы переустанавливаете операционную систему, то вам следует предварительно расшифровать все зашифрованные файлы, иначе не сможете работать с ними после переустановки.

Обратите внимание на то, что, если папка или файл сжаты, они не могут быть зашифрованы, а если они зашифрованы, то не могут быть сжаты.

Когда вам потребуется дешифровать данные, просто снимите метки шифрования в свойствах папки или файла.

Сейф для файлов

Не секрет, что иногда ценность информации может быть очень высокой (например, финансовая информация предприятия или переписка на высшем уровне).

Вы можете использовать для защиты шифрование файлов системой EFS, однако помните, что в ней присутствует специально сделанное уязвимое место, которое позволяет расшифровать зашифрованные файлы с помощью специальных инструментов.

На этом этапе нам нужно решить проблему сохранения важной информации от посторонних.

Использование архивов с установленным паролем не решает проблему, так как «вскрытие» подобного архива — дело несложное, кроме того, не стоит забывать о возможности удаления такого файла пользователем.

Приложение, о котором мы будем говорить далее, способно создавать контейнеры с файлами и шифровать данные внутри таких виртуальных контейнеров. После того как вы введете пароль, у вашего компьютера появится виртуальный диск (на который можно устанавливать и программы).

Работа с StrongDisk Pro

Программа StrongDisk Pro способна сохранять любую информацию в специальных файлах, расположенных на жестком диске. Такие файлы-контейнеры могут иметь любое имя и расширение. После подключения такого контейнера в вашей системе появится дополнительный жесткий диск, куда можно будет записывать необходимую информацию.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch05\StrongDisk Pro вы найдете дистрибутив демо-версии программы StrongDisk Pro и документацию к ней в PDF-формате.

Вы можете сохранять свои контейнеры на компакт-дисках и DVD или же пересылать их по электронной почте. Приложение способно использовать следующие алгоритмы шифрования: AES, Blowfish/Blowfish-448, SAFER, triple DES, CAST-128.

Кроме того, возможно использование внешних ключей, которые делятся на две группы: электронные ключи и файлы-ключи. Электронный ключ представляет собой специальное устройство, которое вставляется в USB или COM-порт компьютера и выполнено в виде брелока.

Файл-ключ — это файл, который записывается на сменный носитель. Чтобы подключить контейнер, вам потребуется вставить носитель с файлом-ключом в соответствующее устройство чтения. Вы можете установить проверку пароля вместе с использованием внешнего ключа, что позволит вам перестраховаться на тот случай, если ваш ключ будет похищен.

Установка программы проходит достаточно стандартно. После перезагрузки системы начнет свою работу мастер по созданию нового защищенного диска (рис. 5.11).

Вам нужно ввести все характеристики файла-контейнера: используемую файловую систему, расположение на винчестере и т. д. Вам будет предложено создавать защищенный диск указанного размера или такой защищенный диск, который будет увеличиваться по мере заполнения (его первоначальный размер будет совсем небольшим, так как там нет ничего, кроме служебного заголовка). Максимально

допустимый объем «резинового» диска нужно установить в поле Размер диска. Создание подобных дисков оправдано в том случае, если вы не знаете точного объема данных, которые на нем будут храниться.

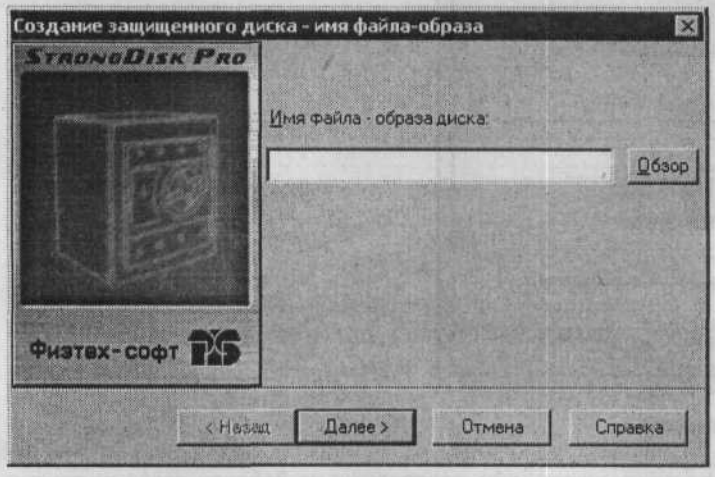


Рис. 5.11. Окно мастера создания защищенного диска

При использовании контейнера фиксированного размера неиспользуемый объем будет заполняться случайными данными. Такая операция не позволит узнать, сколько информации реально находится в контейнере. Далее нужно выбрать алгоритм кодирования заголовков и данных, а также алгоритм хэш-функции (можно оставить значения по умолчанию).

Программа не имеет ограничений, касающихся длины пароля, но желательно создать его не менее чем из восьми символов. Крайне не рекомендуется использовать пароли, которые легко подбираются (например, свое имя).

Также вы можете указать на необходимость использования файла-ключа, после чего вам понадобится указать, где он будет сохранен (дискета или компакт-диск). Теперь защищенный диск готов к использованию. Внешний вид главного окна программы показан на рис. 5.12.

Одной из полезных функций рассматриваемой программы является возможность шифровать и стирать после завершения работы файл подкачки. Это происходит потому, что большинство приложений создают во время работы временные файлы. В таких файлах может содержаться множество служебной информации и данных, с которыми программа работала на момент создания временного файла. Например, в процессе извлечения файлов из архива их копии первоначально записываются во временный каталог, и только после этого — в то место, которое было указано архиватору. Чаще всего файлы оказываются в Temp или Windows\Temp системного диска и могут там остаться в случае некорректного завершения работы архиватора.

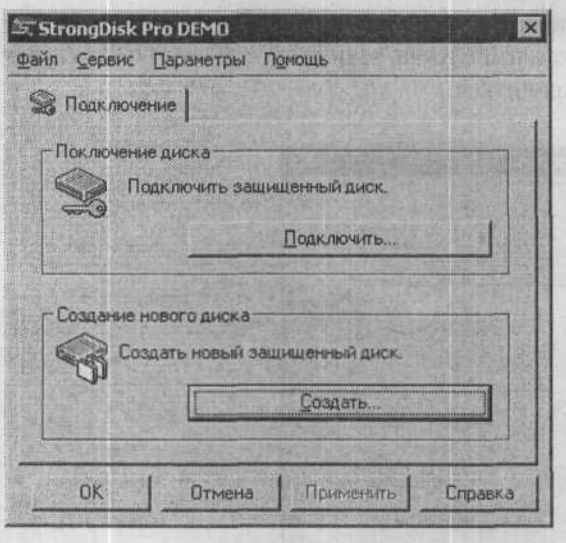


Рис. 5.12. Главное окно программы

Обратите внимание, что после установки программы на Рабочем столе появится ярлык Уничтожение данных (рис. 5.13).

Рис. 5.13. Ярлык Уничтожение данных

Если вы переместите на этот значок какой-то файл, StrongDisk Pro уничтожит его, проведя заполнение нулями всех кластеров, которые он занимал, что приведет к полной невозможности восстановления данных.

Кроме того, вы можете создать ложные жесткие диски, которые можно подключать вместо реальных после ввода специального пароля, указываемого в настройках. Также можно настроить полное уничтожение реальных контейнеров в случае подмены (если передача данных посторонним значительно хуже их потери).

После того как вы повторно подключите ложный диск, используя, однако, пароль реального, все вернется на свои места. Ложный и настоящий диски снова поменяются местами, а подключен будет настоящий (если он, конечно, не был уничтожен). У вас будет возможность убрать все упоминания о ложном диске даже в самой программе (чтобы злоумышленники точно не заметили подмены).

Все данные методы хороши, если злоумышленники не знакомы с принципами работы подобных программ, иначе обман может и не удаться. Однако функция экстренного уничтожения дисков может спасти положение, если компьютером не успели завладеть раньше.

ГЛАВА 6 Делаем систему более надежной и быстрой

- Как распознать сбой
- Предотвратить и распознать: тестирование системы
- Организуем RAID-массив

В этой главе мы сделаем Windows более надежной и безотказной, научимся предупреждать и диагностировать сбои, узнаем, как создать массив дисков RAID, увеличив производительность системы.

Как распознать сбой

Windows XP — довольно надежная и стабильная операционная система, однако и в ее работе иногда случаются ошибки и сбои. Большинство пользователей, использующих Windows, встречались с различными проблемами, связанными с оборудованием. Индикаторами таких проблем становятся автоматические перезагрузки, повреждение информации и потери данных, зависание системы — все это указывает на то, что система (пусть и только что установленная) работает с ошибками.

Под термином «сбой» подразумевают временный отказ в работе системы, который является скорее исключением, нежели правилом. Под отказом понимают неисправность, которая не может устраниться без постороннего вмешательства.

Сбои можно разделить на две группы: программные и аппаратные.

Аппаратные сбои

Любые аппаратные сбои, как правило, происходят по одной из следующих причин:

- неправильная установка оборудования;
- выход из строя какого-либо устройства или его части;
- неправильная работа драйвера;
- некорректная установка или настройка драйвера;
- ошибки BIOS.

Последние три причины вполне можно отнести к аппаратно-программным сбоям, так как кроме аппаратуры в сбое принимает участие и программное обеспечение (драйверы и BIOS).

Остановимся подробнее на первой причине возникновения сбоев — неправильной установке оборудования. Все современные устройства поддерживают технологию PnP: Plug and Play (включай и работай). Это означает, что чаще всего устройство достаточно подключить, а операционная система сама его настроит и установит все необходимые драйверы.

Именно поэтому распределение аппаратных ресурсов теперь производится автоматически BIOS, и вам не придется самостоятельно настраивать все необходимые параметры. Если же операционная система не в состоянии классифицировать и настроить устройство или найти для него необходимый драйвер, то нужно инсталлировать драйверы, которые распространяет производитель данного оборудо-

вания (на диске, который прилагается к устройству, или через Интернет). Устанавливать драйверы от производителя рекомендуется, даже если Windows настроила устройство автоматически. После установки фирменных драйверов вы, скорее всего, сможете использовать некоторые дополнительные функции вашего оборудования, которые были недоступны прежде. Для мониторов и большинства современных видеокарт установка драйверов производителя является необходимой, иначе вы рискуете испортить зрение при малой частоте обновления экрана (60 Гц).

Большинство проблем, которые могут возникнуть во время инсталляции драйвера или его работы, можно решить, внимательно прочитав документацию, которая прилагается к устройству или конкретному драйверу.

СОВЕТ

Неплохим вариантом будет обратиться в службу технической поддержки производителя вашего оборудования (с помощью электронной почты) или же попытаться разобраться с проблемой самостоятельно.

Существует также более серьезная проблема — выход устройства или его части из строя, что может послужить поводом для замены соответствующего оборудования.

Каким образом можно устранить аппаратный сбой? Для начала следует точно определить его причины. На самом деле таких причин может быть очень много: неправильное подключение устройства, конфликт прерываний и других ресурсов компьютера (особенно если у вас установлено старое оборудование).

Случается и так, что операционная система не может загрузиться на конкретной конфигурации (это может проявляться в периодическом зависании на первых стадиях загрузки). В этом случае следует отключить устройство, которое, по вашему мнению, может этот сбой вызвать, и попробовать загрузить Windows еще раз. Таким образом можно достаточно точно определить истинную причину зависания.

Когда вы выясните, какое устройство дает сбой, попробуйте подключить его к другому компьютеру. Еще можно подключить к своему компьютеру оборудование, аналогичное вашему. Идеальным вариантом будет выполнить оба действия: тем самым вы выясните, работает ли устройство и правильно ли сконфигурирована ваша система.

Программные сбои

В большинстве случаев программные сбои происходят по следующим причинам:

- ошибка в приложении;
- некорректная настройка;
- несовместимость в аппаратной части.

Как показывает практика, первая проблема является самой распространенной. В большинстве случаев она возникает из-за ошибок во время написания программы, и устранить ее сможет только разработчик.

Что касается конфликтов и несовместимости в аппаратной части, то сюда относятся любые сбои оборудования и нехватка оперативной памяти.

Кроме того, в эту группу проблем можно отнести невозможность работы некоторых программ с конкретным оборудованием (аппаратно-зависимые программы). Как правило, такое случается, если программа оптимизирована под конкретное оборудование (процессор, видеокарту и т. п.).

Главное — поставить диагноз

Здесь мы рассмотрим средства диагностики различных сбоев при работе системы.

Одним из самых первых средств диагностики проблем является BIOS. Процедура самотестирования системы (POST — Power On Self Test) запускается каждый раз, когда вы включаете свой компьютер. Если в процессе теста будет обнаружен какой-либо сбой, система выведет на экран предупреждение или издаст с помощью встроенного спикера определенную комбинацию сигналов. Проанализировав эту информацию, вы сможете решить, что делать дальше. Как правило, на компьютере будет установлена BIOS одного из трех известных разработчиков и производителей: AWARD, AMI или Phoenix. Вся сложность состоит в том, что BIOS различных производителей издают различные комбинации звуковых сигналов при одной и той же ошибке, поэтому вам необходимо точно установить производителя, прежде чем пытаться разобраться в сигналах. Начнем с AWARD. В этом случае возможны всего три звуковых сигнала для диагностики состояния системы. В табл. 6.1 представлены коды звуковых сигналов, которые сообщают о сбое.

Таблица 6.1. Коды звуковых сигналов AWARD BIOS

Сигнал	Ошибка
Один звуковой сигнал	Ошибок нет, запуск в нормальном режиме
Два звуковых сигнала	Небольшая неисправность. Если работают видеокарта и монитор, то на экране вы увидите уведомление о сбое или ошибке и приглашение нажать клавишу F1 для продолжения работы (Press F1 to continue)
Один длинный и два коротких сигнала	Проблемы с видеокартой. Скорее всего, плохо присоединен кабель, ведущий к монитору, или адаптер плохо вставлен в разъем на материнской плате. Извлеките и снова установите видеокарту в слот и удостоверьтесь, что кабель присоединен к монитору

AMI BIOS поддерживает большее количество комбинаций звуковых сигналов о неполадках (табл. 6.2).

Таблица 6.2. Коды звуковых сигналов AMI BIOS

Количество сигналов	Ошибка
1	Нормальный запуск
2	Если на мониторе нет изображения — это ошибка регенерации памяти. Как правило, такое происходит из-за плохого контакта, поэтому вам следует извлечь планки оперативной памяти и заново установить их. Если эта процедура не дает результатов, скорее всего, один из модулей просто вышел из строя
3	Ошибка контрольной суммы памяти. Это может свидетельствовать о неисправности одного из модулей памяти, однако контакты тоже следует проверить
4	Ошибка первых 64 Кбайт памяти. Причина та же, что и в предыдущем случае: плохой контакт или один из модулей вышел из строя
5	Неисправен первый системный таймер. Возможно, материнская плата неисправна
6	Ошибка процессора. На самом деле, это может быть и ошибкой материнской платы. Если ваш процессор работает на другом компьютере, значит, сбой действительно происходит из-за материнской платы
7	Невозможно перевести процессор в виртуальный режим (Gate A20 Failure). Для начала вам следует включить параметр Fast Gate A20 в SETUP. Если не помогло, то это может означать, что неисправна микросхема контроллера клавиатуры 8042 (данная проблема решается заменой материнской платы)
8	Особая ситуация процессора (Processor Exception Interrupt Error). Скорее всего, потребуется заменить процессор
9	Ваша видеокарта неисправна. Необходимо проверить ее контакты, кабель, присоединенный к монитору. Если возможно, попробуйте установить плату в другой слот
10	Неисправна микросхема BIOS. Возможен дефект адаптера с собственной BIOS
11	Неисправность в специальном регистре CMOS-памяти. Неисправна материнская плата

Предотвратить и распознать: тестирование системы

После того как вы определили вышедшее из строя устройство, его необходимо заменить. Правда, неисправности некоторых устройств (процессор, оперативная память, материнская плата) не всегда можно точно определить. Случается и такое, что при нормально работающем процессоре система периодически зависает и появляются самые разнообразные ошибки (особенно при больших нагрузках).

Даже если у вас нет никаких неприятностей, стоит время от времени проверять стабильность работы таких устройств. Таким способом вы сможете вовремя определить большинство проблем оборудования, приводящих к потере информации

в самый ответственный момент. Далее вам будет предложено несколько методов проверки надежности работы основных составляющих вашего компьютера.

Загрузка процессора

Если ваш компьютер периодически зависает или время от времени появляются всевозможные ошибки, то с самого начала вам следует проверить процессор. Большинство сбоев происходит из-за перегрева процессора, так что проверьте, хорошо ли работает кулер (вентилятор) и хватает ли его мощности для нормального охлаждения процессора. Большинство материнских плат снабжено средствами, которые отслеживают состояние системы. Если вы зайдете в настройки BIOS, то сможете увидеть текущую температуру процессора и материнской платы, скорости вращения вентиляторов и т. п. Также для мониторинга данных показателей можно использовать специально разработанные программы, с помощью которых вы можете наблюдать за большинством похожих параметров непосредственно во время работы.

Одной из лучших утилит считается Hardware Sensors Monitor. Эта программа может отслеживать большинство параметров — температуру процессора, чипсета материнской платы, жесткого диска, скорости вращения вентиляторов. С ее помощью вы сможете узнать необходимые данные о типе и параметрах процессора и BIOS в вашем компьютере. Утилита может предупреждать пользователя о том, что превышен максимально допустимый уровень температуры (устанавливается отдельно) и напряжений в вашей системе. Программа занимает совсем немного места в оперативной памяти, а потому может быть добавлена в автозагрузку для постоянного контроля над состоянием вашего компьютера.

СОВЕТ

Программу Hardware Sensors Monitor вы можете скачать на сайте разработчика http://www.hmonitor.com. Она также помещена на компакт-диске в папке ch06\Hardware Sensors Monitor.

Окно Hardware Sensors Monitor приведено на рис. 6.1.

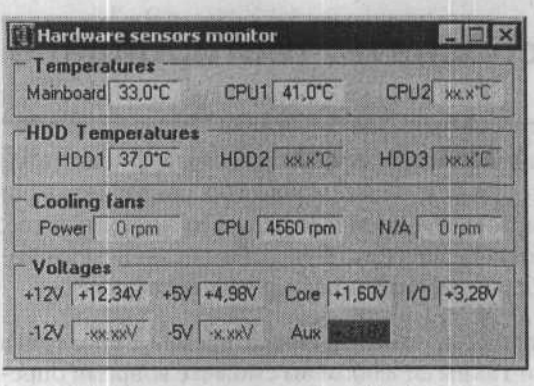


Рис. 6.1. Главное окно программы Hardware Sensors Monitor

Большинство слабых мест процессора можно найти, если дать ему какое-нибудь ресурсоемкое задание. Таким заданием могут стать современные 3D-игры, которые активно используют ресурсы процессора и видеокарты. Попробуйте поиграть в такую игру в течение двух-трех часов. Если за это время не произойдет никаких сбоев, а компьютер не будет самопроизвольно перезагружаться, то с процессором, скорее всего, все нормально.

ВНИМАНИЕ

Данный метод имеет одну недоработку — одновременно с процессором нагружается и видеокарта, которая также может стать причиной сбоев и ошибок, потому будет достаточно тяжело выяснить, что же стало истинной причиной нестабильной работы.

Как нам может помочь WinRAR

Проверить стабильность работы процессора можно и с помощью архиватора WinRAR, который весьма популярен и установлен на большинстве компьютеров.

Для проведения теста нужно создать большой архив (или даже несколько таковых) объемом 1–1,5 Гбайт. Архивировать нужно только те данные, которые хорошо поддаются сжатию. Например, можно заархивировать каталог с документами, программами, папку Program Files (неплохо сжимается).

Не стоит сжимать музыку в MP3-формате и фильмы, сжатые в MPEG-4. Они и так подвержены компрессии, поэтому сильно нагрузить процессор их сжатием у вас не выйдет. Даже если вы не имеете нужного объема данных, архивируйте одни и те же папки, изменяя их названия, ведь для теста важен только общий объем файлов. Архивация должна происходить с максимальным качеством компрессии.

После того как архив будет создан, следует запустить WinRAR и функцию Тест, предварительно выбрав свой архив. Таким способом мы протестируем архив на наличие ошибок. Дело в том, что во время компрессии файлов и тестирования архива очень сильно нагружаются процессор и оперативная память. Алгоритм сжатия информации, который использует WinRAR, построен таким образом, что любая нестабильность в работе компьютера вызовет ошибку в каком-то файле архива. На рис. 6.2 изображен процесс тестирования архива.

Конечно, вам нельзя ограничиться только одной-единственной проверкой архива — их следует сделать несколько раз подряд. Большинство новых процессоров пройдет тест такого объема за несколько минут.

СОВЕТ

Лучше всего протестировать процессор в течение нескольких часов (либо ограничиться 15–20 тестами). Если все они прошли без ошибок, ваш процессор в отличном состоянии. Обязательно следите за температурой в процессе ваших испытаний, так как перегрев в этой ситуации крайне нежелателен.

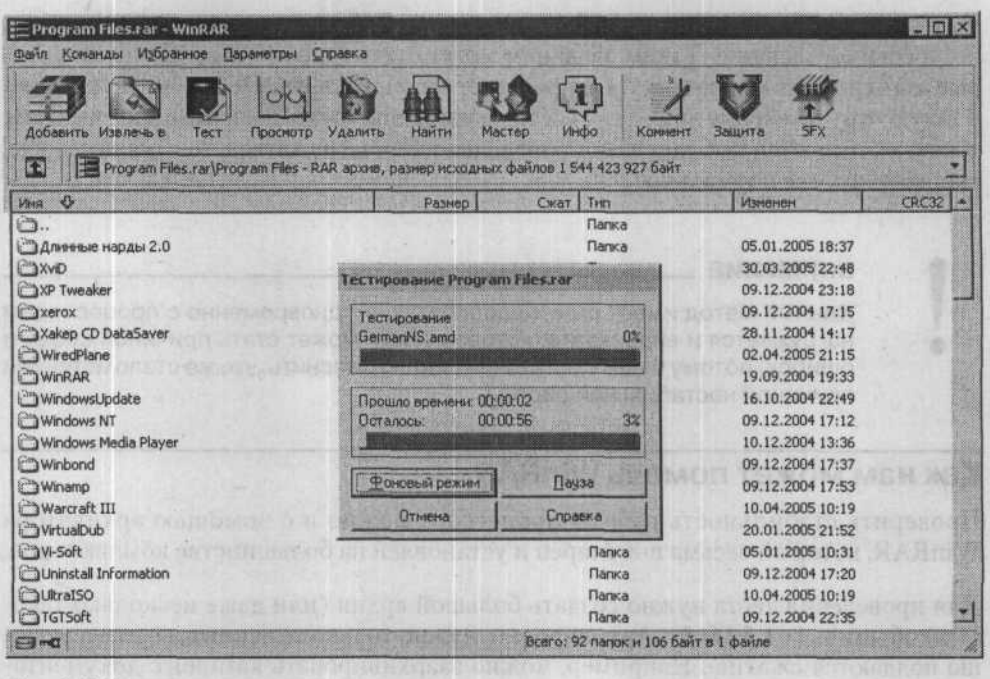


Рис. 6.2. Тестирование архива

Как вы уже догадались, точно так же можно проверить не только процессор, но и оперативную память, материнскую плату (одним словом — стабильность всей системы). Как уже было указано, алгоритм сжатия в WinRAR построен таким образом, что любая (даже незначительная) ошибка данных не останется без внимания и будет выведена на экран вашего монитора. Безусловно, достаточно проблематично заметить подобные ошибки в случае работы с малыми объемами информации, однако если архив измеряется гигабайтами, то точность такого теста сильно возрастает.

Проверка памяти: Memtest поможет

Как вы понимаете, кроме стабильно работающего процессора нужно иметь и хорошо работающие модули памяти. Некоторые пользователи уверены, что оперативная память не выходит из строя и не нуждается в проверке. Увы, это не так — некачественные модули памяти встречаются нередко, и за этим нужно следить. Другие думают, что если бы память была некачественной, то ее ошибки проявились бы еще во время загрузочного теста BIOS. Данное утверждение тоже не соответствует действительности, так как тест, который проводит BIOS, не проверяет всю оперативную память, поэтому обнаружить ошибки полностью не сможет.

Перечислим несколько признаков, которые могут указывать на некачественную оперативную память:

- если вы запускаете одновременно несколько приложений, некоторые из них закрываются с сообщением об ошибке;

- какой-либо файл при открытии оказывается поврежденным, однако через некоторое время тот же файл открывается без проблем;
- появляются ошибки при распаковывании архива, однако через некоторое время они исчезают сами собой.

Если вы сталкивались с подобными неприятностями, то ваша оперативная память может быть неисправной. Проверьте ее, используя метод, описанный ниже.

Как оказалось, существует неплохая программа для проверки оперативной памяти. Ее название — Memtest86+ (http://www.memtest.org/). Во время установки Memtest86+ создается загрузочная дискета или компакт-диск. Если вы загрузитесь с него, то можно начинать тестирование оперативной памяти. Проверка будет происходить циклически, а все тесты повторятся неограниченное количество раз (до тех пор, пока пользователь не отменит их вручную). Обычная проверка проходит за 20–30 мин, однако вы можете основательно протестировать память, запустив утилиту на несколько часов. Запомните: ошибок быть не должно!

Для начала закачайте образ диска по ссылке, которая приведена выше. После этого распакуйте архив и запишите образ на чистый компакт-диск, используя любую программу для записи дисков.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch06\Memtest находятся образы Memtest86+ для компакт-диска и дискеты, а также программа Memtest для Windows.

После того как образ будет записан, у вас на диске будет великолепный тестер оперативной памяти, всегда готовый к использованию. Наилучший способ использования этого теста — найти время, когда ваш компьютер не будет использоваться около шести часов подряд (а еще лучше — запустить тест на ночь).

Чтобы запустить данную утилиту, просто перезагрузите систему с использованием только что записанного компакт-диска. Сразу после загрузки программа начнет работать (рис. 6.3).

Практически все основные проблемы памяти (неработающие биты и т. п.) будут найдены в течение нескольких мгновений. Некоторые неисправности могут не определяться в течение нескольких часов, однако по прошествии определенного времени они все равно будут найдены. Если Memtest86+ найдет поврежденный бит, то внизу экрана появится сообщение, а проверка продолжится. Если после длительного многочасового теста никаких сообщений не появится, то это будет означать, ваша память в полном порядке. Если же вы увидели сообщения о найденных ошибках, вполне вероятно, что один из модулей нуждается в замене.

Если вам не повезло и тест обнаружил ошибки, то не расстраивайтесь — скорее всего, еще не все потеряно и кое-что можно исправить. Для начала внимательно просмотрите все настройки BIOS. В некоторых версиях BIOS присутствует функция,

касающаяся оперативной памяти, — Turbo Mode. Вам стоит ее отключить (если, конечно, она была включена до этого).

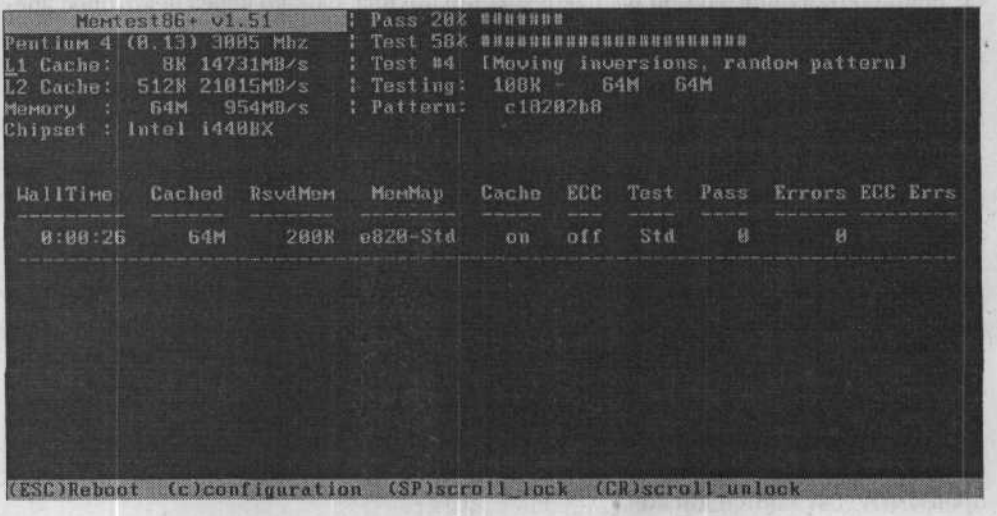


Рис. 6.3. Memtest86+ в работе

Еще одной причиной некорректной работы могут стать неправильно установленные тайминги — попробуйте изменить их значение (увеличив Refresh rate, снизив CAS setting), после чего перезапустите Memtest86+, чтобы узнать, не исчезла ли неполадка.

Если ошибки появляются и в этом случае, то нужно определить, какой именно модуль оперативной памяти является неисправным. Если у вас установлено два и более модулей памяти, то необходимо удалить один из них и снова запустить утилиту Memtest86+. Точно так же вам нужно проверить все доступные модули памяти, чтобы решить, какой из них нужно заменить.

Тестируем систему по всем параметрам

SiSoftware Sandra

SiSoftware Sandra (System Analyser, Diagnostic and Reporting Assistant) — одна из лучших утилит для сбора информации о системе и ее диагностики, написанных под Windows. Последняя версия на момент написания этой книги — 2004.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к этой книге, в папке ch06\SiSoftware Sandra вы найдете дистрибутив программы SiSoftware Sandra 2004.

Данная программа способна не только предоставлять информацию о системе, но и производить тестирование вашего компьютера по различным параметрам. Осо-

бенность такого тестирования заключается в экстремальности условий проведения. SiSoftware Sandra может собирать информацию о процессоре, чипсете, видеоадаптере, портах, принтерах, звуковой карте, памяти, сети, процессах Windows, AGP, связях ODBC, USB2, 1394/Firewire и прочих устройствах. Таким образом, утилита включает в себя 58 информационных, листинговых, тестовых и диагностических приложений, а также модулей, необходимых для тестирования производительности.

У данной программы есть следующие возможности:

- удаленное тестирование систем Pocket PC 2000, 2002, Windows Mobile 2003 и Smartphone 2002, 2003 (на базе Windows CE 3.0 и Windows .Net CE 4.2);
- тестирование съемных носителей и общий тест файловой системы;
- сравнительные результаты тестов различных платформ и конфигураций (например, Win32 x86, Win64 IA64, Pocket PC ARM);
- возможность работы с одно- и многопроцессорными системами на базе AMD Opteron/Athlon 64/Athlon FX-64 (процессоры AMD Athlon 64/Athlon FX-64; чипсеты SiS 755/760, VIA K8T800/M; южные мосты AMD 8111, SiS963/964; NUMA до 32/64 узлов; ACPI 2.0; SMBus 2.0);
- поддержка особенностей архитектуры Intel Pentium 4 2x400MHz (процессоры Intel Pentium 4 2.4-3.2GHz EE; чипсеты Intel 865FX, 848P, 855PM/DDR333, SiS 648FX, 655FX; южные мосты SiS 964);
- возможность работы с мобильной архитектурой Intel Pentium M (процессоры Intel Pentium M 1.2-1.8GHz; чипсеты Intel 855GM/DDR333);
- поддержка контроллеров USB 2.0 High-Speed (Enhanced HCI).

Данная утилита поставляется в двух модификациях: бесплатной и коммерческой. Бесплатная версия ограничена в своей функциональности, хотя модулей, которые в нее включены, вполне достаточно для тестирования всего доступного оборудования и общей диагностики системы. В бесплатной версии вам будут недоступны следующие элементы: Информация об OLE, Информация о модеме, Информация об интерфейсе SCSI, Мастер обновления утилит через Internet, а также все без исключения модули раздела Тестовые модули.

После установки программы на вашем Рабочем столе и в Панели управления появляется ярлык для SiSoftware Sandra. Двойной щелчок мышью на этом значке приведет к тому, что перед вами появится главное окно приложения. Оно представляет собой окно с набором пиктограмм, которые указывают на модули и утилиты, входящие в состав пакета.

Возможно использование следующих режимов отображения пиктограмм: Информационные утилиты, Утилиты оценки производительности, Просмотр системных файлов, Утилиты тестирования, Все утилиты. Для того чтобы выбрать какой-нибудь из этих режимов, нужно щелкнуть на соответствующем значке на линейке вверху окна оболочки. Первоначально в программе установлен режим отображения значков, которые соответствуют информационным утилитам (рис. 6.4).

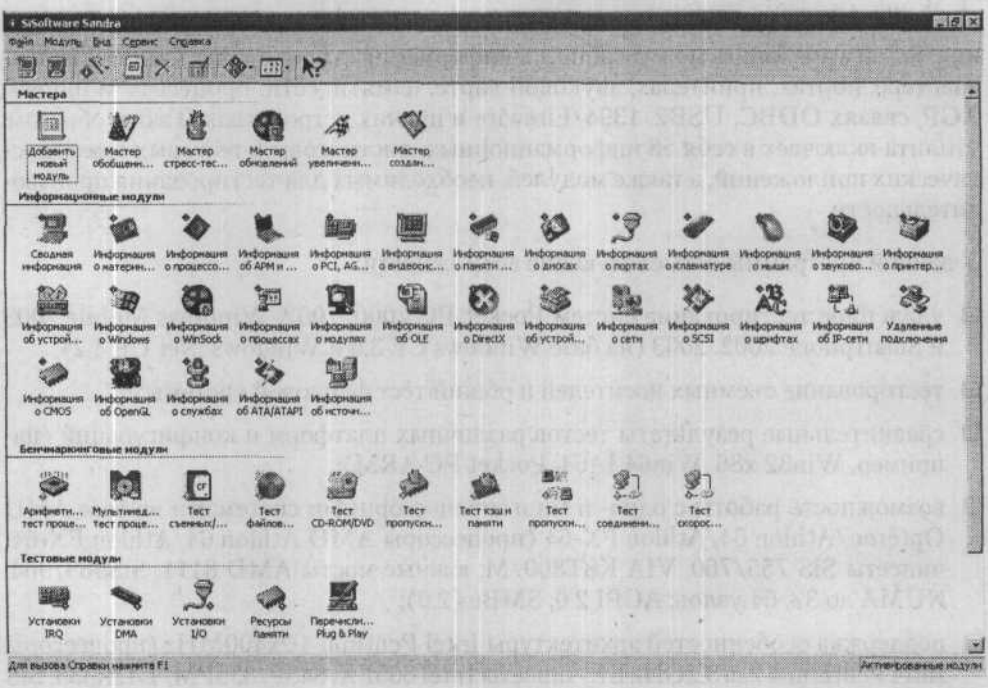


Рис. 6.4. Главное окно SiSoftware Sandra

Кроме того, данное приложение позволяет проверять производительность приводов компакт-дисков и DVD, проводить арифметический и мультимедийный тесты процессора, тестировать файловую систему, оперативную память, видеоадаптер и сетевую карту, съемные flash-диски.

PCMark 2004

Подобно предыдущей программе, тестовый пакет PCMark 2004 нужен для определения производительности компьютера. PCMark04 содержит 44 теста, десять из них нужны для определения общей производительности системы, остальные оценивают производительность различных компонентов вашего компьютера: процессора, оперативной памяти, 2D и 3D режимов видеокарты, жесткого диска, шины AGP. Программу можно загрузить с сайта разработчика – http://www.madonion.com. Системные требования, которые необходимы для нормальной работы программы, сравнительно невысокие:

- процессор не ниже AMD Athlon / Intel Pentium III 1 GHz;
- память не менее 128 Мбайт;
- свободное место на жестком диске не менее 130 Мбайт;
- видеокарта, совместимая с DirectX 7.

Кроме того, для работы всех тестов PCMark04 потребуется наличие установленных программ:

- Internet Explorer 6;
- Windows Media Player 9;
- Media Encoder 9;
- DirectX 9.0.

PCMark04 выпускается в двух вариантах: бесплатная версия PCMark04 Free и коммерческая версия — PCMark04 Professional/PCMark04 Business Edition.

Бесплатное издание позволяет выполнять:

- системные тесты с отображением конечного результата;
- отображение данных о характеристиках тестируемого компьютера;
- публикацию результатов теста в Интернете;
- отображение многих деталей итогов проверки.

Кроме перечисленных функций, профессиональная/бизнес-версия дополнительно способна:

- производить проверку оперативной памяти, жесткого диска и видеоадаптера;
- отображать дополненные результаты тестирования;
- получить дополненные данные о характеристиках тестируемого компьютера;
- создавать ваше личное собрание различных тестов в произвольном порядке неограниченное количество раз;
- использовать PCMark04 Pro ORB.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к этой книге, в папке ch06\PCMark находится свободная версия PCMark 2004.

Главное окно описываемого приложения состоит из 3 частей: Tests, System, Results (рис. 6.5).

В меню Tests вы можете выбрать необходимые тесты, которые будут использоваться в процессе проверки. Выбор пункта Advanced дает вам возможность создавать ваш собственный набор тестов в произвольном порядке и указывать, какое количество раз их нужно запускать. Пункт меню System не имеет никаких параметров и настроек, так как его функция заключается в отображении информации о вашем компьютере в XML-формате. Пункт меню Results содержит подменю Details, которое отображает результаты теста и три настройки: Online ResultBrowser (публикация результата теста на веб-сервере разработчика), Save As (сохранение вашего результата в специальный файл, который будет иметь расширение PSR), To Excel (сохранение результатов в виде стандартной таблицы Excel). Для измерения величины результатов служат специальные единицы — марки.

Кроме перечисленных функций, данное приложение может составить достаточно полный отчет о вашей системе в HTML-формате. Внешний вид отчета вы можете увидеть на рис. 6.6.

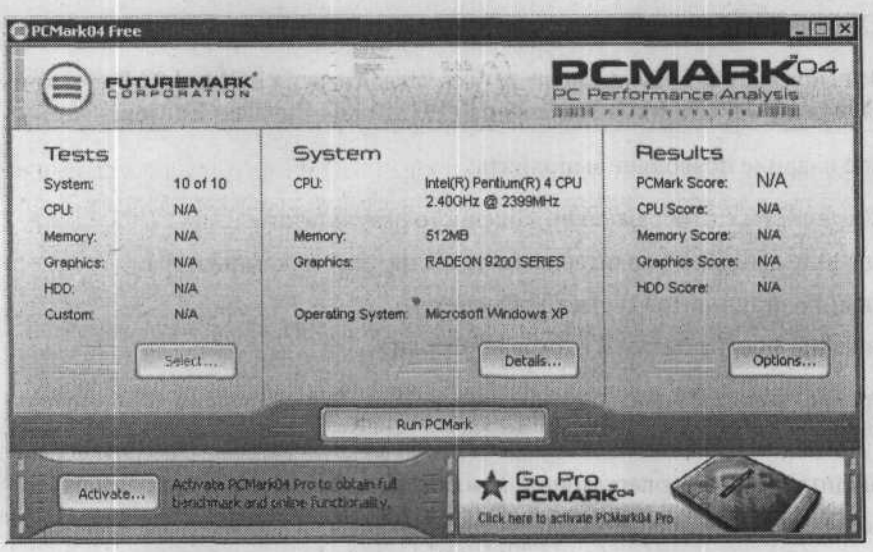


Рис. 6.5. Главное окно программы

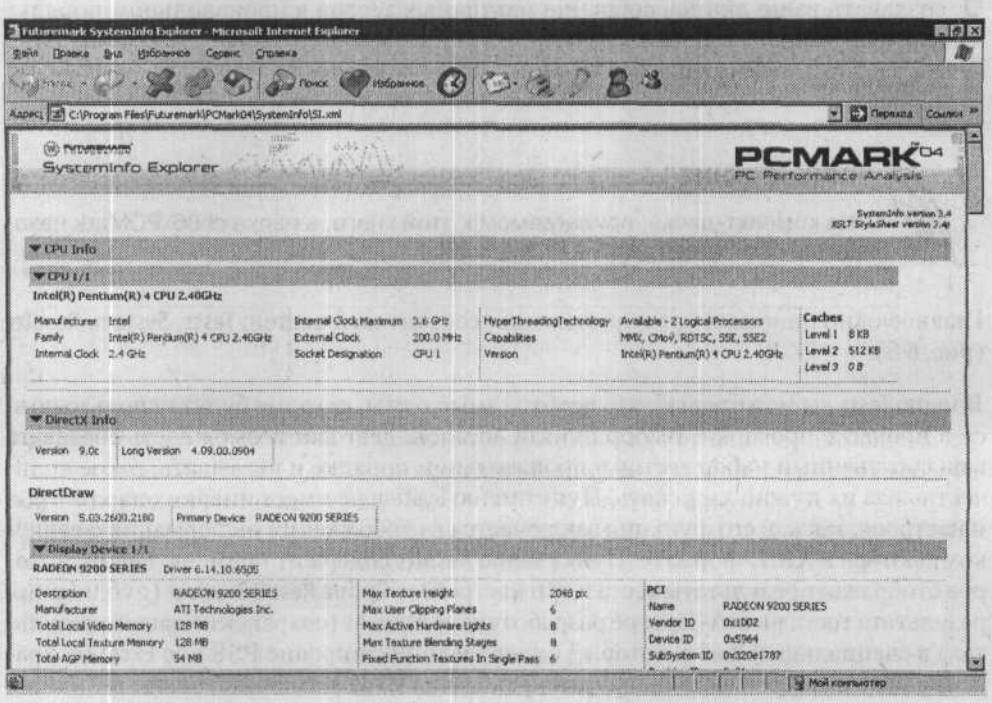


Рис. 6.6. Подробный отчет о комплектующих вашего компьютера

ПРИМЕЧАНИЕ

Тестирование компьютера при помощи PCMark04 достаточно полезно выполнять после обновления какой-либо составляющей части компьютера. Таким образом вы сможете узнать, насколько выросла производительность вашей системы.

Организуем RAID-массив

Системы хранения информации, которые основаны на магнитных дисках, выпускаются уже четыре десятилетия, однако масштабное производство систем, защищенных от сбоев, началось совсем недавно.

В 1987 году Паттерсон (Patterson), Гибсон (Gibson) и Катц (Katz) из калифорнийского университета Беркли напечатали совместную статью «Корпус для избыточных массивов из дешевых дисководов (RAID)» (A Case for Redundant Arrays of Inexpensive Disks (RAID)). Данная публикация была посвящена различным типам дисковых массивов, которые обозначались аббревиатурой RAID — Redundant Array of Inexpensive Disks (избыточный массив недорогих дисководов). Фундаментом RAID стала следующая идея: если объединить в массив некоторое количество небольших по объему и/или дешевых жестких дисков, вполне возможно получить систему, которая будет превосходить по своей вместительности, производительности и стабильности самые дорогие диски. Кроме того, такая система будет рассматриваться компьютером как единый жесткий диск.

В свое время с аббревиатурой RAID произошел интересный случай. Как оказалось, недорогими жесткими дисками на момент написания данной статьи назывались все диски, которые использовались в персональных компьютерах, в отличие от дорогих накопителей для универсальных вычислительных машин. Однако для использования в массивах RAID пришлось использовать дорогостоящее оборудование (по крайней мере, по сравнению с другими комплектующими ПК), поэтому RAID начали расшифровывать как Redundant Array of Independent Disks — избыточный массив независимых дисков.

Производители жестких дисков утверждают, что среднее время работы до отказа массива жестких дисков равняется среднему времени работы до отказа одиночного диска, деленному на число дисков в конкретном массиве. Из-за этого среднее время работы массива до отказа может оказаться слишком малым для многих ресурсоемких задач. Между тем, существует несколько методов, с помощью которых дисковый массив можно сделать устойчивым к отказу одного из входящих в него дисков.

Статья, о которой мы только что говорили, определяла пять уровней дисковых массивов: RAID-1, RAID-2 ... RAID-5. Каждый из данных уровней мог обеспечить устойчивость на отказ, а также другие преимущества перед одиночным жестким диском. Кроме уже названных уровней (типов) RAID-массивов, популярным также стал дисковый массив RAID-0, который не обладал избыточностью.

Уровни RAID

Как уже было отмечено, существует несколько уровней RAID, которые определяются различными способами объединения жестких дисков (табл. 6.3).

Таблица 6.3. Уровни RAID

Уровень RAID	Описание
0 (Non-Redundant Striped Array — неизбыточная матрица)	Способен реализовать распределение блоков данных по нескольким жестким дискам. Основное предназначение — хранение больших объемов информации, которые не способны поместиться на одном жестком диске. Данный уровень не обеспечивает избыточности, а при использовании этого массива жесткие диски просто объединяются в цепочку. Объем массива равен сумме объемов всех дисков, которые в него входят. Данный уровень можно использовать для работы с мультимедиа-информацией, так как в этом случае может понадобиться очень много дискового пространства. Таким образом, вы можете соединить несколько жестких дисков в массив RAID и использовать их как один винчестер. Не следует забывать о том, что при выходе из строя хотя бы одного из винчестеров, входящих в массив, восстановить данные не получится
1 (Mirrored Arrays — зеркальная матрица)	Данный уровень обеспечивает зеркальное копирование (то есть диски данного массива дублируют друг друга). Исходя из этого суммарный объем массива равен объему наименьшего из дисков. В такой массив должно входить минимум два жестких диска. Данный уровень рекомендуется использовать, если вам необходима высокая скорость работы, а данные, которые вы обрабатываете, некритичны
2 (Parallel Array with ECC — параллельный массив с коррекцией ошибок)	Запись на различные диски, входящие в массив, производится методом битового чередования малых блоков данных с добавлением кодов исправления ошибок (ECC — Error Correction Code), которые хранятся на одном диске, а данные — на другом диске (или дисках). Для исправления возможных ошибок обычно используется кодирование Хэмминга (Hamming). Подобные системы крайне избыточны и вследствие этого — дорогостоящи
3 (Parallel Array with Parity — параллельный массив с контролем четности)	Практически аналогичен RAID-2, однако контрольные коды будут записываться на отдельный жесткий диск. В данном случае вам понадобится как минимум три жестких диска. Массивы уровня RAID-3 обеспечивают максимальную производительность, если вы работаете с большими объемами данных
4 (Striped Array with Parity — полосный массив с контролем четности)	Является целой совокупностью связанных между собой данных, которые записываются на один диск, а контрольные коды — на другой. Однако массивы RAID-4 не производят одновременную запись на разные диски

Уровень RAID	Описание
5 (Striping Array with Rotating Parity — смешанная четность)	На данном уровне используются контрольные суммы, а информация записывается «вперемешку» на все жесткие диски, входящие в массив. В случае выхода из строя одного диска вся потерянная информация будет восстановлена с помощью контрольной суммы. Общий объем подобного массива можно рассчитать по формуле min_size*(n-1), где min_size — объем наименьшего из жестких дисков, входящих в массив, а n — количество дисков в массиве (минимум три)
6 (Independent Data Disk with Two Independent Distributed Party Schemes — независимые диски с данными с двумя независимыми схемами четности)	Данный уровень был предложен учеными из института Беркли. Система RAID-6 представляет собой модернизированную версию системы RAID-5. Главное отличие RAID-6 от RAID-5 состоит в том, что он вычисляет сразу две контрольные суммы для каждой отдельной единицы информации и хранит их на разных жестких дисках массива. Такие системы очень надежны, ведь даже при одновременном выходе из строя двух дисков массива существует возможность восстановления утерянной информации. Несмотря на свои преимущества, массивы RAID-6 не стали популярными из-за достаточно высокой стоимости

Наиболее часто используются массивы уровней 0, 1 и 5. Иногда можно встретить и комбинации этих массивов, например 5 + 1. Наиболее надежным и стабильным является уровень 5. Безусловно, мы теряем часть емкости любого массива за счет сохранения кодов избыточности, однако в случае ошибки можно заменить один из жестких дисков без ущерба быстродействию и потерь важной информации, а если позволяет оборудование, то и без перезагрузки системы.

Организуем RAID-массив

Существует два способа организации дискового массива: программный или аппаратный. С программной реализаций способны работать операционные системы Windows NT 4.0 Server, под управлением которой возможна программная реализация массивов RAID-0, RAID-1 и даже RAID-5 (обратите внимание, что Windows NT 4.0 Workstation работает только с RAID-0 и RAID-1), Windows 2000 Server, Windows XP Professional и Windows Server 2003.

В случае программной реализации RAID все действия по поддержке массива выполняет центральный процессор, что снижает быстродействие и стабильность работы системы. Именно поэтому в данной реализации практически нет каких-либо сервисных функций, и все операции по замене нестабильно работающего диска, добавлению нового диска, модификации уровня RAID приводят к полной потере информации и отключению выполнения каких-либо других операций. Основным преимуществом программной реализации RAID является ее минимальная стоимость. Таким образом, программную реализацию массива стоит использовать исключительно на домашних компьютерах и серверах небольших локальных сетей, когда нагрузка на сервер не слишком большая.

Куда большие возможности предоставляет аппаратная реализация RAID с помощью специализированных RAID-контроллеров.

- Данный контроллер берет на себя основные операции с RAID, освобождая центральный процессор, причем с повышением уровня сложности RAID эффективность работы контроллера становится все заметнее.
- Достаточно часто контроллеры снабжены драйверами, которые дают возможность реализовать RAID практически для любой ОС.
- Интегрированный BIOS контроллера и дополнительные программы управления позволяют администратору системы без усилий подключать, отключать или заменять жесткие диски, которые входят в массив, создавать несколько RAID-массивов одновременно (даже разных уровней), совершать контроль над состоянием массива и т. д. Большинство контроллеров позволяет выполнять перечисленные операции на лету (не выключая системный блок). Многие операции будут выполняться в фоновом режиме, не прерывая работы пользователя и даже с другого рабочего места.
- Внешние контроллеры имеют буферную память, в которой сохраняются несколько последних блоков информации, что позволяет увеличить быстродействие дисковой системы при частом обращении к одним и тем же файлам.

Недостаток аппаратной реализации RAID-массивов лишь один — высокая стоимость. В последнее время цена RAID-контроллеров снижается, кроме того, в некоторых материнских платах часто можно увидеть интегрированный RAID-контроллер с вполне достаточным набором возможностей, что позволяет создавать RAID-системы не только на серверах, но и на домашних компьютерах.

При разработке RAID-массива нужно уделить внимание электропитанию. Каждый жесткий диск массива будет потреблять порядка 40 Вт при условии нормального режима работы. В тот момент, когда жесткий диск включается и его шпиндель начинает раскручиваться, потребляемая мощность на некоторое время может увеличиться до 60–70 Вт. Учитывая, что жестких дисков в массиве минимум два, при включении нагрузка на блок питания сильно возрастет, что может привести к повреждению всего массива. Именно поэтому для массива необходимо использовать отдельный блок питания. Наилучшим вариантом будет организация питания массива от двух спаренных источников питания (с возможностью их замены в ходе работы).

Выяснить, какой мощности необходим блок питания, можно с помощью программы Power Supply Calculator, которую написал Александр Леменков. Скачать ее можно с сайта разработчика по адресу http://people.overclockers.ru/awl/files.

ПРИМЕЧАНИЕ

Программа Power Supply Calculator находится на диске, прилагаемом к книге, в папке ch06\Power Supply Calculator.

Используя данное приложение, вы сможете проверить надежность и сбалансированность своей системы и восполнить нехватку мощности путем замены комплектующих либо с помощью установки более мощного блока питания. Внешний вид программы представлен на рис. 6.7.

Рис. 6.7. Главное окно программы Power Supply Calculator

В главном окне приложения вам необходимо установить тип и тактовую частоту вашего процессора, видеоадаптер, количество жестких дисков и модулей оперативной памяти. Исходя из этих параметров будет рассчитано энергопотребление компьютера в целом.

Кроме того, вы можете выбрать ту модель блока питания, которая у вас установлена, из большого списка и выяснить, будет ли достаточно его мощности для питания системы. Используя эту программу, можно провести тестирование своей системы. Тестирование начнется сразу после нажатия кнопки Тест напряжений. Процесс проверки заключается в измерении напряжений в режиме отсутствия активности системы и в случае сильной нагрузки на процессор. Стандартом на блоки питания ATX12V допускается следующий разброс значений напряжений (табл. 6.4).

Таблица 6.4. Допустимый разброс напряжений

Суммарная мощность	Минимальное значение	Максимальное значение	Допустимое отклонение
+12V	+11,4	+12,6	+/–5 %
+5V	+4,75	+5,25	+/–5 %

Изменение напряжения более чем на 5 % может вызвать ошибки и сбои в работе с возможной порчей комплектующих, так что в этом случае стоит подумать о приобретении нового блока питания.

Важным элементом стабильной работы системы является и охлаждение. Жесткие диски сильно нагреваются, а потому нуждаются в отдаче тепла, иначе перегрев может привести к выходу из строя контроллера или дисков. Для охлаждения

могут использоваться дополнительные кулеры (вентиляторы), часть которых направлена на обдув дисков, часть на выведение горячего воздуха, а часть на приток холодного.

Как выбрать модель RAID-контроллера

Существует несколько типов RAID-контроллеров в зависимости от их возможностей, архитектуры и стоимости.

- Контроллеры дисков с функциями RAID. Это обыкновенный дисковый контроллер, который способен объединять диски в RAID-массив уровня 0, 1 или 0 + 1.
- RAID-контроллеры, которые работают вместе с имеющимся дисковым контроллером. Такие RAID-контроллеры предназначены для работы с материнскими платами, имеющими встроенный дисковый контроллер. По этой причине на плате контроллера будет находиться только «логическая» часть RAID-контроллера, а функции обмена информацией с дисками ложатся на дисковый контроллер, который встроен в системную плату. Такие усеченные контроллеры зачастую поддерживают большинство функций полноценных RAID-контроллеров, однако стоят намного дешевле. Безусловно, данное решение имеет и ряд недостатков. Основной недостаток состоит в том, что каждый урезанный контроллер привязан к определенному виду микросхем дискового контроллера и будет работать только на тех системных платах, которые интегрированы с точно такой микросхемой.
- Полноценные RAID-контроллеры. Они содержат все необходимое для нормальной работы с высокопроизводительными системами: BIOS, которая дает возможность конфигурировать и форматировать RAID любого уровня вне зависимости от используемой ОС; RISC-процессор для моментального вычисления контрольных сумм и исправления ошибок; кэш-память для хранения часто используемой информации; до трех канальных контроллеров, работающих независимо друг от друга и поддерживающих до 15 дисков. Подобные RAID-контроллеры производятся в виде отдельной платы для установки в PCI-слот.

Внешние RAID-контроллеры

Описанные выше RAID-контроллеры показывают великолепные результаты в работе, однако все они имеют достаточно серьезный недостаток, который основан на их конструкции. Данные контроллеры выполнены в виде PCI-схемы и получают энергию от системной платы (именно поэтому они и называются внутренними). Таким образом, сбои и ошибки материнской платы могут привести к повреждению или потере информации в RAID-массиве. Этот недостаток был исправлен во внешних RAID-контроллерах, которые поставляются в отдельном корпусе и имеют свой независимый блок питания. Управление такими контроллерами происходит через внешний канал SCSI-контроллера, который подключен к материнской плате.

Компьютер работает с внешним RAID-контроллером точно так же, как и с одним SCSI-диском. Внешний RAID-контроллер представляет собой отдельный корпус

модульной конструкции, который содержит дисковый массив. На передней панели внешнего RAID-контроллера может располагаться индикатор, отображающий текущее состояние и настройки контроллера, и клавиши, предназначенные для управления и конфигурирования. Модульная конструкция позволяет расширять дисковый массив с помощью установки дополнительных схем и жестких дисков.

Различные модели дополнительных схем могут содержать разные типы каналов — Ultra Wide SCSI, LVD SCSI или FC-AL. Кроме того, все эти каналы могут оказаться двунаправленными. Внешние RAID-контроллеры имеют намного большую стоимость, чем их внутренние аналоги, однако такая разница оправдана их более широкими возможностями.

Использование двунаправленных каналов и собственный корпус с блоком питания позволяет создавать кластерные дисковые системы, имеющие высокий уровень безотказности и надежности. В подобных системах несколько серверов соединяются одновременно с несколькими RAID-контроллерами, которые контролируют несколько общих массивов, причем выход из строя любой части такой системы (сервера, RAID-контроллера, диска, блока питания, кабеля и т. д.) не приведет к краху всей системы, а просто несколько снизит скорость ее работы.

Hot Swap: горячая замена диска, вышедшего из строя

Если даже недолгий перерыв в работе системы или ее перезагрузка недопустимы, нужно воспользоваться технологией Hot Swap, которая делает возможной замену жестких дисков без выключения системы. Данную технологию поддерживает большинство профессиональных моделей RAID-контроллеров. Hot Swap позволяет быстро заменить вышедший из строя жесткий диск. В случае использования RAID-массива любого уровня, кроме 0, система сможет продолжить работу, так как благодаря избыточности информации RAID-контроллер восстановит данные, которые хранились на жестком диске, вышедшем из строя.

Данный режим работы не является защищенным (сбой или отказ любого жесткого диска приведет к потере информации), и администратору придется остановить систему, чтобы заменить неисправный винчестер.

Для использования технологии замены одного из жестких дисков без остановки системы необходимы RAID-контроллер, который поддерживает функцию Hot Swap (данный режим нужно включить в настройках контроллера), и специальный модуль, позволяющий менять диски, не вскрывая корпуса. Данный модуль носит имя mobile-rack. Он представляет собой специальный корпус, внутри которого находится 3,5" HDD, который вставляется в П-образную рамку, закрепленную в стандартном 5,25"-разъеме корпуса системного блока. На рамке находятся блок управления питанием диска и замок с ключом, которые необходимы для того, чтобы запереть или открыть привод диска, включить или выключить напряжение, которое подается на диск, один или несколько вентиляторов, необходимых для охлаждения жесткого диска и индикатор, отображающий активности HDD. Как правило, mobile-rack делают совместимым с интерфейсами IDE или Serial-ATA, однако существуют модели, поддерживающие интерфейс SCSI.

К преимуществам данной технологии можно причислить удобный корпус, безопасную для системы процедуру замены диска, наличие индикаторов и дополнительных вентиляторов. Существуют и определенные недостатки: высокая цена (от $50 до $150 за диск), дополнительные разъемы и платы, которые также могут давать сбои.

Hot Spare: резервный диск на случай сбоя

Еще одну технологию — Hot Spare — рассматривают как замену уже знакомой Hot Swap, хотя это не совсем так. Для функционирования Hot Spare нужно следующее:

- RAID-контроллер, который поддерживает режим Hot Spare;
- как минимум один дополнительный жесткий диск, к которому подключены питающий и сигнальный кабель.

В процессе инициализации RAID-массива этот дополнительный диск подключается в состав RAID, но не как активный, а как резервный. Если один из активных дисков выйдет из строя, RAID-контроллер отключает неисправный диск и подключает резервный. Перенос (восстановление) данных произойдет в фоновом режиме без прерывания работы системы.

Преимущество этой технологии состоит в том, что время, в течение которого RAID-массив находится в незащищенном режиме, минимально. Говоря о недостатках, нужно помнить о том, что для реализации данной технологии потребуется дополнительный жесткий диск, который большую часть времени не будет использоваться. Кроме того, после выхода из строя какого-либо жесткого диска вам все равно придется через какое-то время остановить систему, чтобы добавить очередной резервный диск.

Наилучший результат достигается в случае совместного использования технологий Hot Swap и Hot Spare. Если один жесткий диск вышел из строя, система введет в работу резервный диск, а неисправный вы сможете заменить, не останавливая систему.

ГЛАВА 7 Виртуальные машины — полигон для системного администратора

- Что нужно знать о виртуальных машинах
- Виртуальная платформа VMware
- Virtual PC: еще один виртуальный знакомый

В этой главе вы познакомитесь с технологией создания и использования виртуальных машин и программами для их создания — VMware и VirtualPC. Кроме того, вы узнаете, как организовать виртуальную локальную сеть между «реальными» и виртуальными машинами.

Что нужно знать о виртуальных машинах

В настоящий момент активно развиваются разнообразные информационные технологии. Постепенно растет тактовая частота процессоров, объемы оперативной памяти и жестких дисков. Еще несколько лет назад 1 Гбайт оперативной памяти казался огромным и совершенно ненужным, а сейчас этот объем является практически необходимым для современной машины. В компьютерах домашних пользователей появляется поддержка технологий, ранее использовавшихся только на серверах: многопроцессорность, массивы жестких дисков RAID, большие объемы оперативной памяти.

Основным стимулятором увеличения производительности современных компьютеров являются игры. А как может распорядиться огромными вычислительными ресурсами системный администратор? Одна из новых интересных возможностей — запуск и эмулирование нескольких операционных систем на одном компьютере.

Одной из привычных проблем системного администрирования является расширение локальной сети, инсталляция и настройка новых утилит и приложений, дополнительных сетевых сервисов. Предположим, что вам необходимо установить на базе функционирующего прокси-сервера организации почтовый сервер или контроллер домена. Очевидно, что в процессе установки всех необходимых сервисов вам придется изменять конфигурацию, перезагружать систему, определять и анализировать причины сбоев и неполадок, искать ошибки в настройках, снова перезагружаться... Вполне возможно, что, если вы не имеете опыта в настройке данной системы, пройдет достаточно продолжительный период времени, прежде чем система нормально заработает. В процессе ваших экспериментов пользователи, подключенные к серверу, будут испытывать различные трудности с доступом к Интернету — ведь по условию задачки на вашем сервере установлен прокси.

Однако выход из данной ситуации есть: вы можете использовать для настройки виртуальную машину. У вас появляется возможность настроить любой сервер, испытать его в работе, найти все ошибки, проверить его работу внутри локальной сети. И только после этого, отработав на подобном тренажере основные принципы установки и настройки дополнительных приложений, их можно инсталлировать на реальный сервер, значительно ускорив процесс инсталляции.

Собственно говоря, вы можете использовать для этих целей еще один компьютер. Проблема заключается лишь в том, что не всегда есть такая возможность, ведь свободного для экспериментов компьютера может и не оказаться. В таких случаях на помощь спешит виртуальная машина.

Виртуальная машина — это приложение, которое эмулирует настоящий компьютер таким образом, что на него можно будет инсталлировать операционную систему и необходимые программы, которые будут работать точно так же, как и на ре-

альном, «физическом» компьютере. Виртуальная машина способна имитировать различные аппаратные конфигурации (с некоторыми ограничениями), так что вы можете легко установить, сколько оперативной памяти она сможет использовать. Программа эмуляции и работающая внутри нее операционная система называются виртуальной машиной, а ваша основная операционная система и физический компьютер получат статус хост-системы. Любая операционная система, которая будет запущена внутри виртуальной машины, будет называться гостевой.

Все ресурсы вашего компьютера (оперативная память, вычислительные мощности), необходимые виртуальной машине для работы, будут распределяться между хост-системой и виртуальной машиной.

Одними из самых популярных программ эмуляции под Windows являются программы VMware и VirtualPC. Используя их, вы сможете эмулировать любую операционную систему серии Windows (включая Windows XP/Server 2003 и даже не вышедший пока Longhorn), MS-DOS, все популярные дистрибутивы Linux, FreeBSD, OS/2. По большому счету, можно использовать можно любую ОС, если она способна работать на архитектуре Intel и не работает с аппаратной частью, используя недокументированные возможности. Если нужная ОС соответствует этим требованиям, то она, скорее всего, будет работать на вашей виртуальной машине.

Следует отметить, что программы эмуляции способны реализовать полноценную сетевую поддержку. Они будут работать в локальной сети, как настоящие серверы и клиенты. Обмен данными между гостевой операционной системой и хост-системой может происходить через локальную сеть или с помощью общих папок на жестком диске.

Операционная система, которая запущена на виртуальной машине, и приложения, выполняющиеся под ее управлением, полностью независимы от хост-системы. Любые ошибки, неполадки, вирусное заражение гостевой операционной не нанесут вреда хост-системе.

Разумеется, никакая установка операционной системы не может обойтись без жесткого диска. В процессе создания новой виртуальной машины программа устанавливает виртуальный винчестер, после чего вы сможете создать еще несколько таких дисков.

Созданный диск может быть привязан к произвольному каналу IDE или SCSI — однако если вы решите изменить эти параметры, то вам следует сделать это до установки нужной операционной системы, так как после инсталляции далеко не каждая система способна правильно понять перевод жесткого диска с одного канала на другой.

С виртуальными жесткими дисками связано несколько основных возможностей. Прежде всего, файл жесткого диска можно сохранить, перенести на другую систему, воссоздав там такую же виртуальную машину в первоначальном виде.

Еще одна интересная возможность — настройка отката изменений на диске. Как правило, все ваши изменения хранятся на диске точно так же, как это происходит на вашем «физическом» компьютере. Режим отката дает пользователю возможность

работать с системой, однако после перезагрузки все изменения, которые произошли в течение сеанса работы, будут утеряны (в том числе и установленные программы). Возможен и такой вариант, когда при выключении виртуальной машины вам будет задан вопрос о том, желаете ли вы сохранить изменения.

Третья возможность, о которой пойдет речь, — не создавать в процессе установки виртуальный диск в файле, а выделить под данный диск физический раздел. Данный способ несколько трудоемок и, к тому же, не слишком эффективен. Однако он пригодится, если вам необходимо инсталлировать виртуальную машину, настроить параметры системы в виртуальном режиме, после чего перенести свой жесткий диск на другой компьютер и запустить на нем систему с собственными настройками.

Виртуальные машины используются во всем мире для разработки и тестирования программ и операционных систем, отладки кода приложений, ознакомления с сетевыми возможностями нового программного обеспечения. Одним из немногих недостатков виртуальных машин является несколько большая, чем у реальных компьютеров, потребность в системных ресурсах (наибольшие требования касаются объема оперативной памяти).

Список системных требований к оперативной памяти и объемам жесткого диска в зависимости от устанавливаемой на виртуальный компьютер операционной системы представлен в табл. 7.1.

Таблица 7.1. Объемы оперативной памяти и жесткого диска, требуемые виртуальными машинами

Гостевая операционная система	Требуемый объем дискового пространства	Требуемый объем оперативной памяти
MS-DOS	0,05 Гбайт	32 Мбайт
Windows 3.1	0,1 Гбайт	32 Мбайт
Windows 95	0,5 Гбайт	32 Мбайт
Windows NT 4.0 Workstation	1,0 Гбайт	64 Мбайт
Windows NT 4.0 Enterprise	2,0 Гбайт	192 Мбайт
Windows NT 4.0 Server	1,0 Гбайт	128 Мбайт
Windows 98	0,5 Гбайт	64 Мбайт
Windows Me	2,0 Гбайт	96 Мбайт
Windows 2000 Professional	2,0 Гбайт	128 Мбайт
Windows 2000 Server	2,0 Гбайт	192 Мбайт
Windows 2000 Advanced Server	2,0 Гбайт	256 Мбайт
Windows 2003 Server Enterprise	2,0 Гбайт	256 Мбайт
Windows XP Professional	2,0 Гбайт	128 Мбайт
Windows XP Home	2,0 Гбайт	128 Мбайт
OS/2	не менее 0,5 Гбайт	не менее 64 Мбайт
Novell NetWare 6.0	2,0 Гбайт	196 Мбайт
Linux	не менее 2,0 Гбайт	не менее 64 Мбайт

Безусловно, представленные требования достаточно условны и напрямую зависят от задач, которые вы собираетесь решать с помощью виртуальной машины. Вы можете самостоятельно установить объем оперативной памяти, который будет выделяться виртуальной системе.

Всем известно, что несколько приложений одновременно будут работать медленнее (иногда значительно), чем по отдельности. Если вы используете виртуальную машину, то процесс усложняется тем, что все программы на реальной и виртуальной машинах будут использовать один процессор. Так как виртуальная машина не использует специальных средств для искусственного разделения процессорного времени, кроме системных диспетчеров операционной системы, и общие расходы современных диспетчеров не превышают 1–2 %, то для расчета быстродействия можно использовать описанную ниже схему.

Рассмотрим наглядный пример: для полноценной работы виртуальной машины с установленной операционной системой Windows 2000 нужен процессор Pentium II или III 600 МГц и 128 Мбайт оперативной памяти. Для комфортной работы с хост-системой Windows XP необходим процессор с тактовой частотой в 1 ГГц и 256 Мбайт ОЗУ.

Сложив данные числа, вы получите тактовую частоту процессора равную, 1,6 ГГц и 384 Мбайт оперативной памяти. При условии наличия таких ресурсов компьютера обе системы будут поддерживать производительность на прежнем уровне.

Виртуальная платформа VMware

Программа VMware (VMware Virtual Platform), разработанная компанией VMware Inc. (http://www.vmware.com/), позволяет запускать на одном компьютере одновременно несколько различных операционных систем и переходить из одной ОС в другую, просто переключаясь между окнами без необходимости перезагрузки системы. Последняя на момент написания книги версия программы — пятая. Скачать ее можно с сайта разработчика, размер дистрибутива 54 Мбайт.

Стоимость программы составляет около $300, однако у вас есть возможность бесплатно получить регистрационный ключ на 30 дней, заполнив регистрационную форму на сайте разработчика. Как видите, вы абсолютно официально получаете в свое распоряжение на целый месяц полнофункциональную версию данной программы.

Для этого зайдите на сайт www.vmware.com, найдите ссылку Download и зарегистрируйтесь. После непродолжительной регистрации вы получите сообщение, что лицензионный код отправлен на ваш электронный ящик. Через несколько минут придет письмо, содержащее серийный номер для программы.

Вы можете получать новые тестовые лицензии неограниченное количество раз, но только при условии заказа на разные почтовые ящики. Исходя из этого вы можете использовать VMware Workstation, не нарушая закона, в течение любого промежутка времени. Подобная лояльность компании VMware Inc. достойна искреннего уважения. Вы можете получать ключи и использовать программу совершенно бесплатно каждый месяц.

Список основных возможностей:

- возможность запускать несколько различных операционных систем одновременно;
- возможность работы с виртуальными машинами как в оконном, так и в полноэкранном режиме. Для переключения между виртуальными машинами будут использоваться специально назначенные клавиши;
- возможность запуска уже установленных на компьютере операционных систем без их переустановки или дополнительной настройки;
- создание виртуальных машин без предварительной переразбивки дисков;
- проверка работоспособности приложений сразу в нескольких операционных системах;
- возможность совместного использования файлов и программ различными виртуальными машинами с помощью виртуальной сети;
- возможность одновременного запуска клиент-серверных и веб-приложений на одном компьютере, установив серверную часть на одном виртуальном компьютере, а клиентскую — на другом;
- возможность запуска на одном компьютере нескольких виртуальных машин и имитации работы локальной сети.

Безусловно, мы упомянули далеко не все возможности этой великолепной программы. Для использования их в полном масштабе понадобится достаточно мощная система. Минимальный объем оперативной памяти, который вам понадобится, — 256 Мбайт, а комфортно работать можно лишь при 512 Мбайт. В этом случае хост-системе и гостевой ОС можно выделить по 256 Мбайт. Идеальный вариант — если у вас установлен 1 Гбайт оперативной памяти. Это позволит вам запускать одновременно несколько виртуальных машин, не ощущая приостановок.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к этой книге, в папке ch07\VMware 5 вы найдете дистрибутив VMware. Для использования программы вам остается только заказать ключ на сайте производителя.

Для установки VMware у вас должны быть права администратора в хост-системе. Процесс установки программы достаточно прост и не должен вызвать никаких вопросов. Обратите внимание на то, что в самом конце установки начнется инсталляция драйверов для виртуальных устройств. Данные драйверы не имеют электронной подписи Microsoft, поэтому вам будет необходимо разрешить их установку в окне, которое появится.

После того как все компоненты программы будут установлены, вам потребуется лицензионный ключ. Введите комбинацию из букв и цифр, которые вы ранее получили в электронном письме от разработчиков, после чего процесс установки завершится.

Создаем виртуальную машину

Программа VMware установлена. После ее запуска перед вами появится главное окно программы (рис. 7.1).

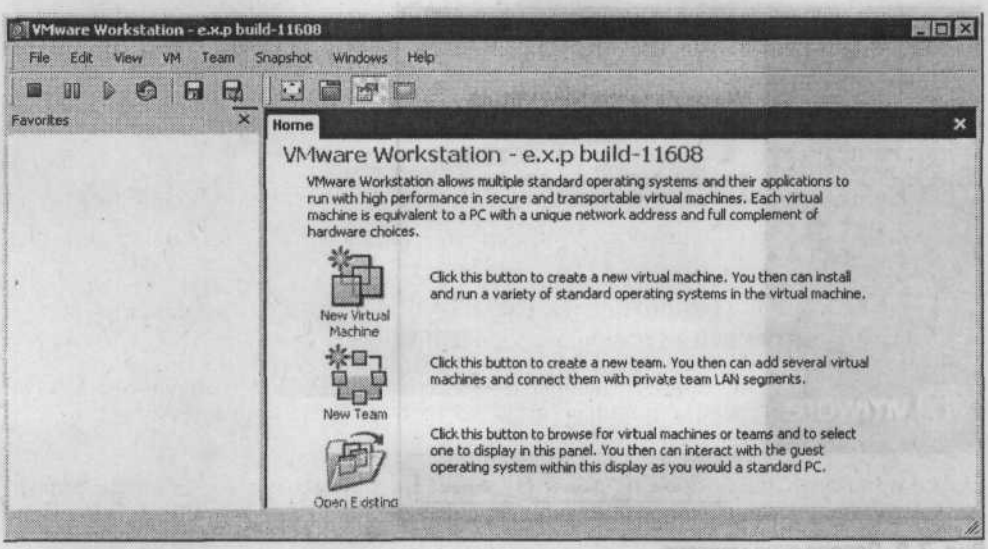


Рис. 7.1. Главное окно программы

Для начала вам потребуется создать новую виртуальную машину. Разработчики утверждают, что «процесс создания виртуальной машины подобен сборке реального компьютера».

Впрочем, на процесс сборки реального компьютера это ничуть не похоже. Список эмулированного оборудования совсем небольшой, кроме того, создать новую виртуальную машину нам поможет New Virtual Machine Wizard (мастер создания новой виртуальной машины).

Данный мастер запускается нажатием кнопки New Virtual Machine. Прежде всего, вам нужно решить, будет ли новая машина использовать виртуальный жесткий диск (является обыкновенным файлом) или будет работать непосредственно с физическим жестким диском.

Если вы остановитесь на первом варианте, то придется заново устанавливать операционную систему на виртуальный диск. Данный вариант намного проще и безопаснее. В этом случае вы не сможете нанести вреда хостовой операционной системе, что подойдет всем начинающим пользователям программы VMware.

Выбрав второй вариант, вы сможете заново установить ОС на физический диск (если ее там до этого не было) либо запустить на виртуальной машине ОС, которая была предварительно установлена на данный жесткий диск. Такая возможность пригодится тем пользователям, у которых уже было установлено несколько ОС, и была задействована многовариантная загрузка. Разработчики рекомендуют

устанавливать операционную систему на физический диск только тем пользователям, которые уже имеют достаточный опыт.

В окне мастера нажмем Далее (рис. 7.2).

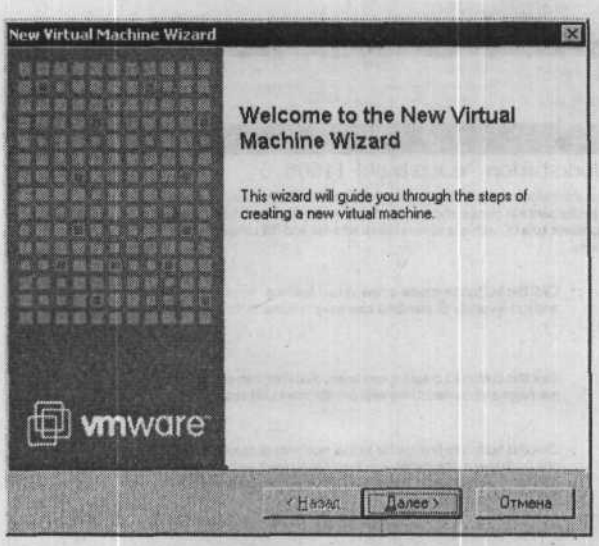


Рис. 7.2. Первое окно мастера

После этого мастер задаст вопрос о том, нужно ли использовать стандартную конфигурацию для новой виртуальной машины или предоставить возможность задать все параметры вручную (рис. 7.3). Подробнее остановимся на втором варианте, чтобы лучше понять, как настраивается виртуальная машина.

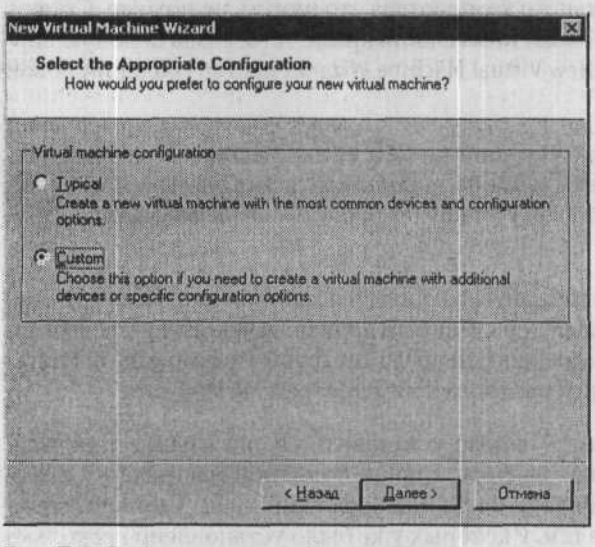


Рис. 7.3. Выбор режима конфигурирования

В следующем окне (рис. 7.4) можно выбрать устанавливаемую операционную систему. Выбрав ОС (мы рассмотрим конкретный случай, когда устанавливается Windows Server 2003), снова нажмем Далее.

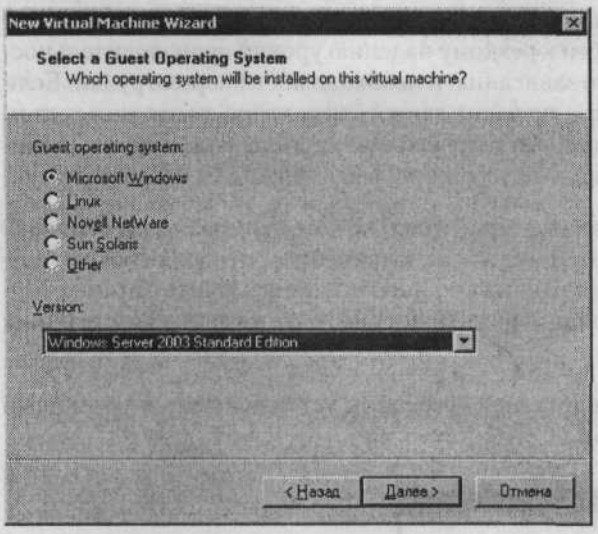


Рис. 7.4. Выбираем операционную систему

В следующем окне вам следует выбрать папку, в которой будут храниться все необходимые файлы созданного виртуального компьютера, и название вашей виртуальной машины. Обратите внимание, что для каждого нового виртуального компьютера нужно создать отдельный каталог с файлами настроек. По умолчанию вам предлагается создать такую папку в каталоге Мои документы.

Следующее окно позволяет вам установить, какой объем оперативной памяти будет присутствовать в вашей виртуальной машине. Данная настройка очень важна, так как именно она сильно влияет на скорость работы как виртуальной машины, так и системы в целом. Значение этого параметра должно быть не меньше минимальных системных требований ОС.

Оптимальный объем оперативной памяти, который выделяется виртуальной машине, будет опираться на несколько факторов:

- тип приложений, которые вы будете запускать на виртуальной машине;
- собираетесь ли вы использовать одновременно несколько виртуальных машин;
- какие программы вы будете запускать на хост-системе вместе с виртуальной машиной.

Следует помнить, что общий объем памяти, который выделяется для всех виртуальных компьютеров, запущенных одновременно, не может быть больше объема физической оперативной памяти, который остается после запуска хост-ОС и запущенных в ней программ.

Если вы собираетесь использовать только одну виртуальную машину, вам следует отдать ей половину физической оперативной памяти вашего компьютера. Нарушать данное правило могут лишь достаточно опытные пользователи, так как неправильная установка данного параметра может сильно повлиять на быстродействие как хоста, так и виртуального компьютера. Слишком большое значение данного параметра может привести к резкому падению уровня производительности базового компьютера или к его зависанию и необходимости перезагрузки. Если вы установите слишком маленькое значение данного параметра, то это может привести к снижению производительности виртуальной машины и ограничить количество виртуальных компьютеров, которые могут быть запущены одновременно.

VMware самостоятельно устанавливает максимально допустимое количество виртуальных машин, которые можно запустить одновременно, определяя объем имеющейся и необходимой оперативной памяти. При попытке включить питание виртуальной машины, когда оперативной памяти нет, VMware не даст такой машине запуститься.

Объем оперативной памяти для виртуальной машины устанавливается с помощью специального ползунка (рис. 7.5).

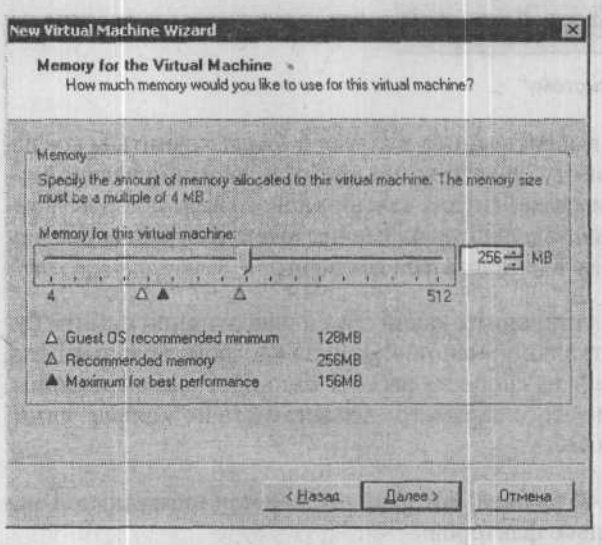


Рис. 7.5. Выбираем объем оперативной памяти для виртуальной машины

Далее вам нужно указать тип подключения виртуальной машины к локальной сети (рис. 7.6).

Всего возможны три основных режима подключения виртуального компьютера к сети: Bridged networking, Network address translation (NAT) и Host-only networking.

Режим Bridged networking предоставляет виртуальной машине прямой доступ к внешнему интерфейсу хост-машины. С помощью этого виртуальный компьютер автоматически устанавливает или получает через DHCP собственные сетевые пара-

метры — IP-адрес, маршрутизатор по умолчанию и т. п. Данный вариант подключения необходимо использовать, если внутри виртуальной машины вы будете устанавливать серверы, имеющие определенные сетевые адреса.

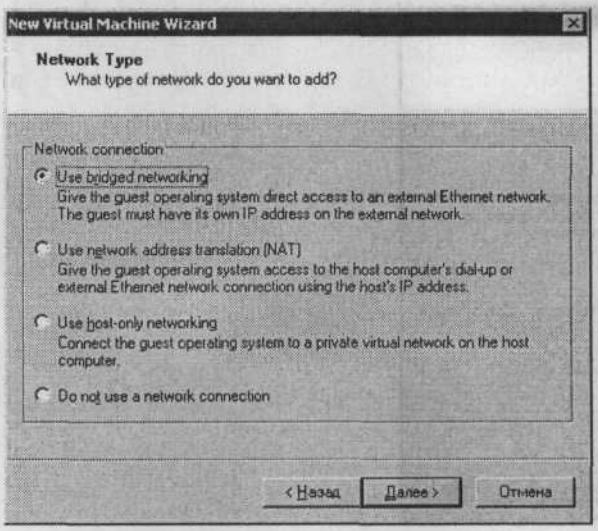


Рис. 7.6. Выбор режима доступа к сети

Режим Network address translation (NAT) применяет трансляцию адресов исходящих потоков данных. Адрес виртуальной машины, полученный с помощью интегрированной в NAT DHCP, в момент отправки на внешний протокол заменяется на адрес хост-машины. Одновременно с этим запрос помещается в таблицу запросов. Все ответы, которые будут получены от удаленных компьютеров, сверяются с этой таблицей на предмет нахождения соответствий. При передаче в VMware адрес снова заменяется, чтобы программа, которая запрашивала данные, получила все пакеты на свой порт и адрес. По этому принципу пересылаются запросы и в серверные приложения (например, DNS).

Режим Host-only networking устанавливает на хост-машине еще одну виртуальную сетевую карту, к которой и будет подключен виртуальный компьютер, создавая с хост-машиной небольшую подсеть. С помощью этой функции вы сможете установить сеть на одном компьютере. При этом хост-машина может выступать своеобразным мостом между подсетями и переадресовывать пакеты на другой интерфейс (например, модем).

Для работы с сетью можно использовать первый и третий режимы. Если ваш компьютер физически не подключен к локальной сети, то вам следует использовать режим Host-only networking.

После выбора нужного режима нажмите кнопку Далее.

На следующем этапе вам предложат изменить драйвер применяемого адаптера SCSI, однако лучше это значение не изменять.

Далее необходимо указать, нужно ли создавать новый виртуальный диск для виртуального компьютера или использовать уже созданный (как вариант — физический) диск (рис. 7.7).

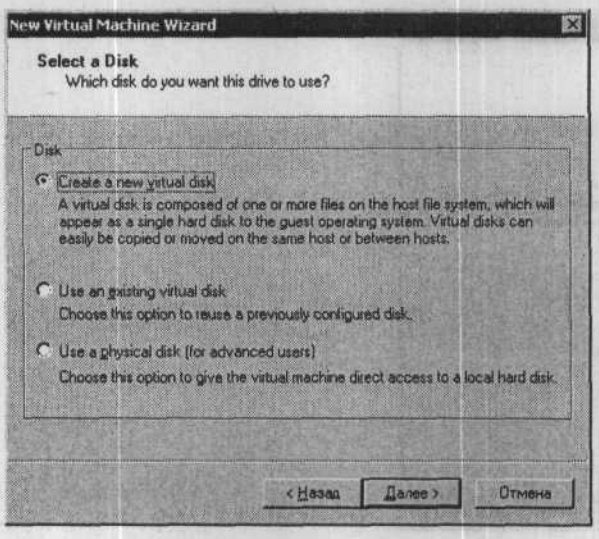


Рис. 7.7. Выбор используемого виртуального диска

В следующем окне необходимо выбрать тип виртуального диска — IDE или SCSI (можно оставить по умолчанию — рис. 7.8).

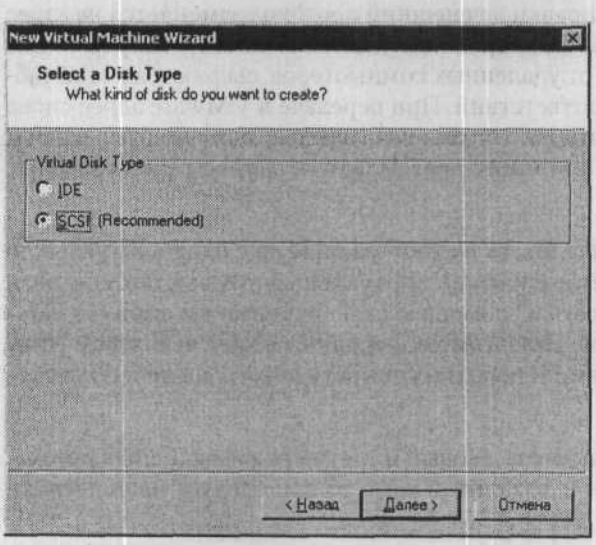


Рис. 7.8. Выбор типа диска

Далее вам придется настроить виртуальный жесткий диск. Для этого укажите его максимальную емкость (рис. 7.9).

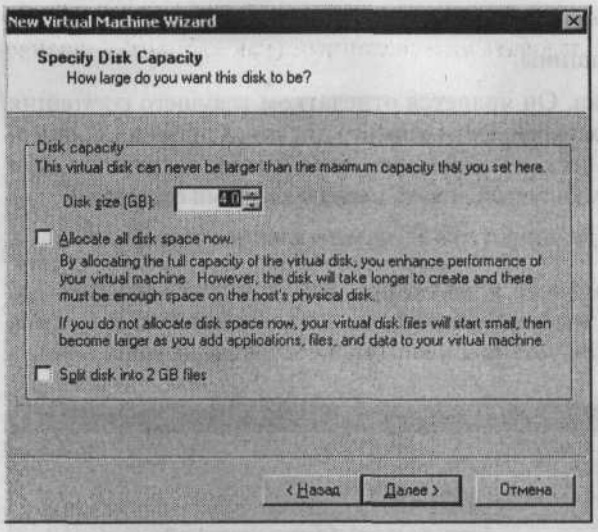


Рис. 7.9. Выбираем размер виртуального диска

Кстати, вы можете сделать этот диск «резиновым», то есть увеличивающимся по мере необходимости (должен быть снят флажок Allocate all disk space now) или же сразу принимающим свой максимальный объем. Лучше всего сразу сделать «резиновый» диск, чтобы сэкономить дисковое пространство. Обратите внимание на то, что если вы создадите диск максимального объема, то производительность виртуальной машины будет несколько выше.

После того как будут установлены ключевые параметры диска, вам предложат указать, где он будет расположен на реальном жестком диске. Все! Виртуальный компьютер успешно создан.

Запускаем!

Теперь вашу виртуальную машину можно включить и установить на нее операционную систему. Для управления питанием виртуального компьютера на Панели инструментов приложения присутствуют шесть кнопок (рис. 7.10).

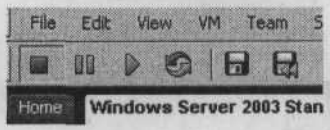


Рис. 7.10. Кнопки на Панели инструментов программы

Опишем функции, которые данные кнопки выполняют (слева направо).

- Выключение виртуальной машины.
- «Заморозка» виртуального компьютера (содержимое оперативной памяти и текущее состояние устройств будет сохранено в специальном файле).

- Включение и запуск виртуального компьютера.
- Перезагрузка виртуальной машины.
- Снятие моментального снимка. Он является отпечатком текущего состояния виртуальной машины — ее настроек, содержимого дисков и прочего. С помощью моментального снимка всегда можно вернуться к тому состоянию, при котором он был сделан (рекомендуется делать перед опасными опытами).
- Восстановление системы из сделанного ранее моментального снимка.

Перед первым запуском виртуального компьютера рекомендуется изучить его установки. Для этого щелкните в поле Commands на надписи Edit Virtual Machine Settings. Перед вами появится окно установок виртуальной машины (рис. 7.11).

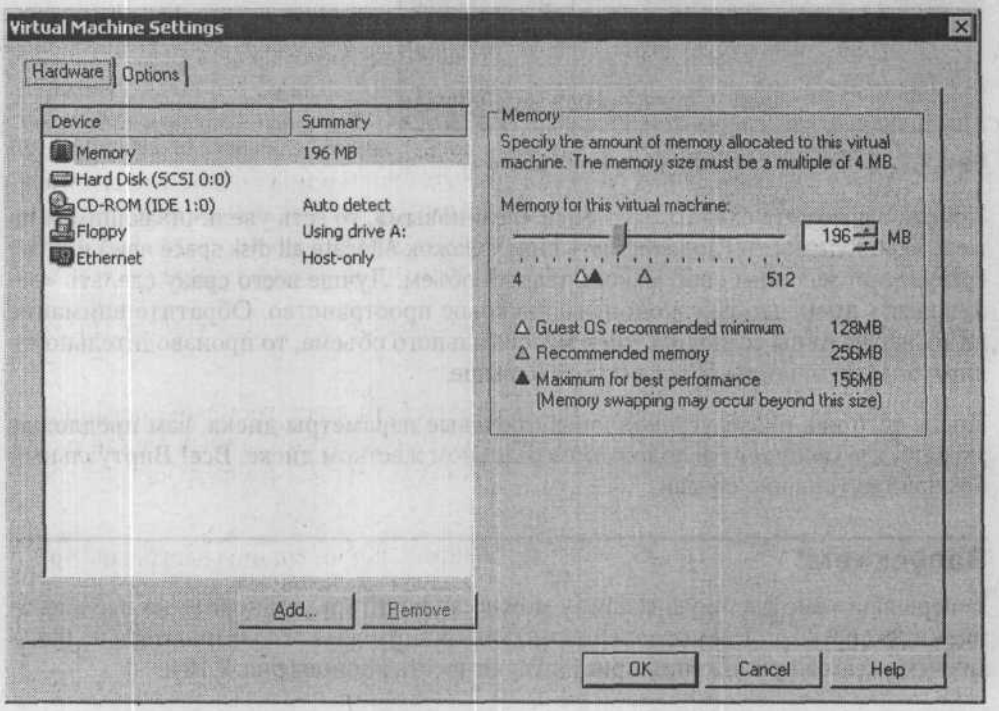


Рис. 7.11. Окно свойств виртуальной машины

Любой виртуальный компьютер состоит из целого набора виртуальных устройств:

- виртуальный привод компакт-дисков;
- виртуальные IDE и SCSI жесткие диски;
- стандартный PCI видеоадаптер;
- стандартный дисковод;
- IDE-контроллер Intel 82371 (включает первичный и вторичный IDE-контроллеры);

- адаптер жестких дисков SCSI BusLogic BT-958-совместимый;
- стандартная 101/102-клавишная клавиатура;
- PS/2-совместимая мышь;
- адаптер Ethernet AMD PCNET (PCI-ISA);
- последовательные порты COM1-COM4;
- параллельные порты LPT1-LPT2;
- звуковая карта, совместимая с Sound Blaster 16.

Данное собрание виртуальных устройств может отличаться от набора устройств, установленных на вашем компьютере, и не зависит от реальной конфигурации последнего.

В окне настроек можно изменить объем оперативной памяти виртуальной машины, установить или удалить лишнее виртуальной оборудование, провести дефрагментацию виртуального жесткого диска и т. п. Для виртуального привода компакт-дисков желательно указать ссылку на ваш реальный привод и установить флажок Legacy emulation, иначе виртуальный компьютер может и не увидеть ваш привод. Вместо ссылки на реальный привод компакт-дисков можно использовать ISO-образ компакт-диска. Данная возможность полезна, если вы располагаете только ISO-образом установочного диска необходимой операционной системы.

То же самое относится и к виртуальному дисководу: вам следует указать ссылку на реальный дисковод или на образ дискеты.

Кроме того, вы можете настроить режим работы сети и тип гостевой операционной системы. Очень важно установить правильные значения данных параметров, если вы не хотите иметь в дальнейшем проблем, связанных с работой виртуального компьютера.

После того как вы убедитесь, что параметры виртуальной машины настроены правильно, вставьте в привод компакт-диска загрузочный компакт-диск с операционной системой, которую вы собираетесь устанавливать, после чего смело запускайте виртуальную машину.

ПРИМЕЧАНИЕ

После того как виртуальная машина будет создана, вам придется отформатировать ее жесткий диск с помощью загрузочной дискеты или компакт-диска.

После включения виртуальной машины начнется загрузка виртуальной BIOS (эмулируется AMI BIOS). Если в этот момент нажать клавишу F2, то вы окажетесь в BIOS-меню. Здесь нужно будет установить загрузку с компакт-диска или дискеты (в зависимости от того, с какого носителя вы собираетесь загрузиться), после чего можете покинуть данное меню, сохранив изменения. Как выглядит BIOS виртуальной машины, можно увидеть на рис. 7.12.

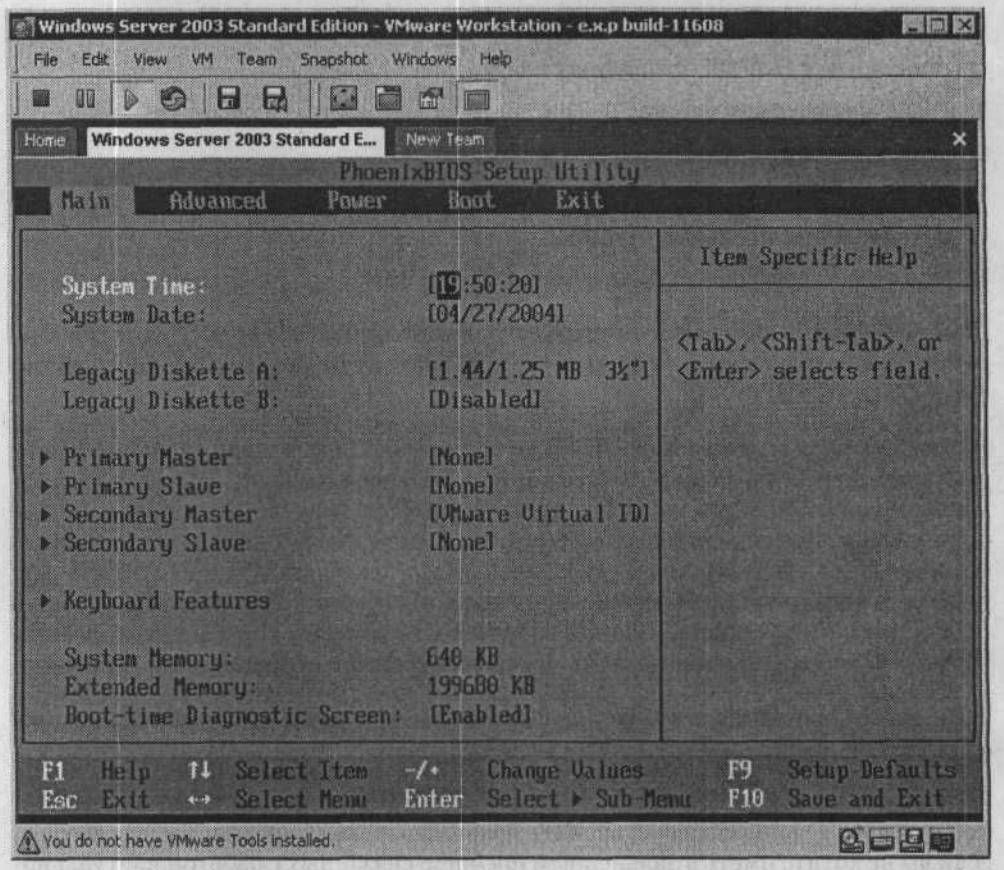


Рис. 7.12. BIOS виртуальной машины

Дальнейшие ваши действия будут точно такими же, как при обычной инсталляции операционной системы: форматирование жесткого диска и установка операционной системы. На данном этапе работа виртуального компьютера ничем не будет отличаться от работы реальной системы.

1. Вставьте в привод компакт-диск или дискету с дистрибутивом операционной системы.
2. Запустите виртуальную машину, щелкнув мышью на кнопке Power On, которая находится на Панели инструментов программы.
3. Внимательно читайте и выполняйте инструкции, которые будет отображать программа инсталляции.

Более подробные рекомендации по установке некоторых операционных систем вы всегда сможете найти на сайте VMware.

Первоначально виртуальная машина будет запускаться в оконном режиме. Чтобы перейти в полноэкранный режим, нажмите кнопку Enter Full Screen Mode, располо-

женную на Панели инструментов программы. Для возврата в оконный режим необходимо нажать сочетание клавиш Ctrl+Alt. Обратите внимание на то, что VMware захватывает курсор, если щелкнуть мышкой внутри окна виртуальной машины. Чтобы его освободить, используйте уже знакомую комбинацию клавиш Ctrl+Alt. Как выглядит окно VMware с установленной гостевой системой Windows XP, показано на рис. 7.13.

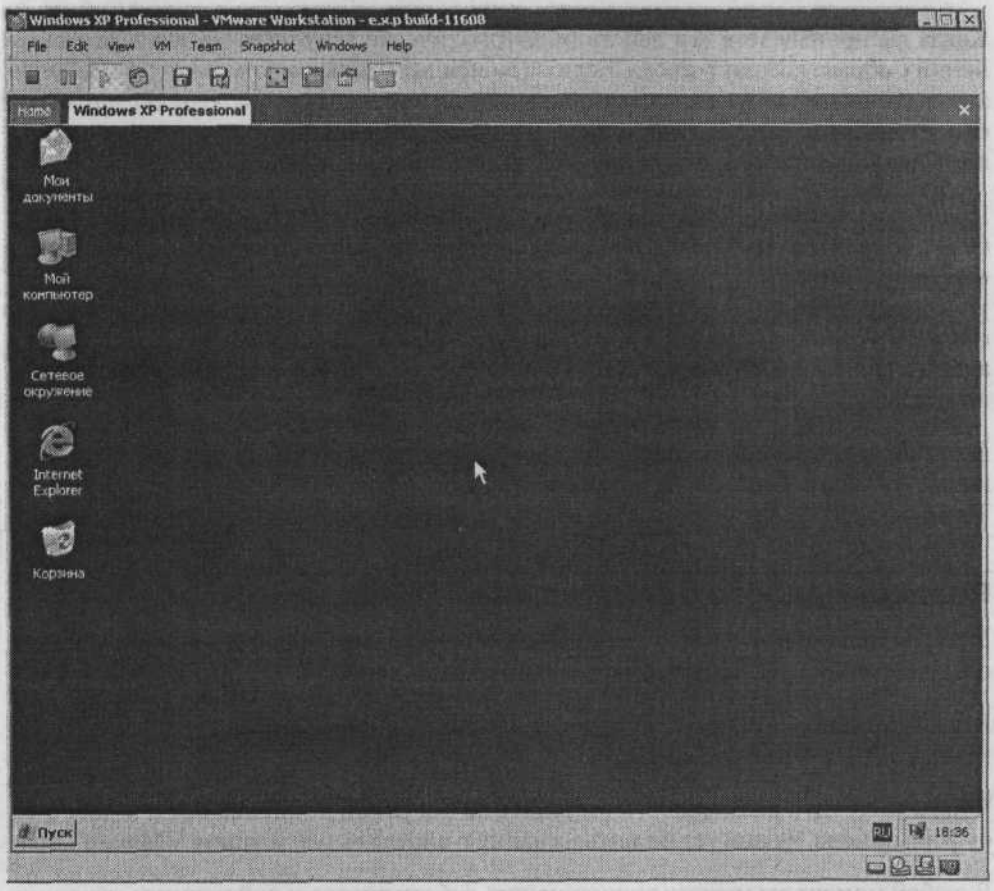


Рис. 7.13. Windows XP в виртуальной машине

Дополнительные инструменты VMware Tools

После установки операционной системы вы сразу же обратите внимание на невозможность установки разрешения экрана больше 640 × 480. Это происходит из-за того, что программа VMware эмулирует VGA-видеоадаптер без предварительной инсталляции VMware Tools. После того как они будут установлены, у вас появится возможность использовать любые видеорежимы, поддерживаемые вашим видеоадаптером. Вы также сможете переносить в буфере обмена данные между гостевой и хостовой ОС, несколько упростится работа с указателем мыши.

Для установки VMware Tools необходимо настроить виртуальную машину таким образом, чтобы можно было использовать образ привода компакт-дисков, который содержит установочные файлы VMware Tools. Чтобы сделать это, выберите пункт меню программы VM ▸ Install VMware Tools. Приложение выдаст сообщение о том, что временно изменены настройки вашего виртуального компьютера (вместо физического привода компакт-дисков был подключен его образ, на котором находятся необходимые для установки VMware Tools файлы).

Когда вы произведете эти действия, автоматически запустится установка дополнений с образа компакт-диска. Если на вашем виртуальном компьютере отключен автоматический запуск компакт-диска, утилиту установки нужно будет запустить самостоятельно (открыв Мой компьютер и дважды щелкнув на значке привода компакт-дисков, а после этого на значке с названием этой программы).

После того как запустится программа установки, следуйте инструкциям, которые будут появляться на экране. Инсталляция не должна вызвать никаких вопросов — вам понадобится просто нажать кнопку Next несколько раз. Когда вы закончите установку VMware Tools, перезагрузите свою виртуальную машину. Теперь вы сможете установить желаемое разрешение экрана. Проверьте, что используется адаптер монитора VMware SVGA(FIFO). Как видите, скорость работы значительно возросла.

В любой виртуальной машине с установленной гостевой ОС Windows после установки VMware Tools for Windows на Панели задач появляется значок VMware Tools.

Реальная работа с виртуальными машинами

Установка дополнительных программ в середине виртуальной машины VMware осуществляется так же, как и на реальном компьютере.

Включите вашу виртуальную машину. Проверьте, имеет ли она доступ к приводу компакт-дисков или дисководу.

Чтобы получить возможность выполнения операции копирования и вставки из буфера обмена, нужно установить на данную виртуальную машину VMware Tools.

В любой момент вы можете приостановить работу виртуальной машины, сохранив текущее состояние. Через некоторое время продолжите работу с виртуальной машиной с того самого места, на котором вы остановились в прошлый раз (включая запущенные программы и открытые документы).

Ранее в программе VMware состояние виртуальной машины сохранялось в оперативную память и терялось после перезагрузки реального компьютера. В более новых версиях состояние виртуальной машины сохраняется на жесткий диск, однако только если на нем достаточно свободного места для проведения этой операции (впрочем, вы можете вручную задать сохранение текущего состояния в оперативную память). Скорость сохранения и загрузки состояния виртуальной машины зависит, в первую очередь, от количества изменений, которые были сделаны в те-

чение последнего сеанса работы. Как бы там ни было, но самое первое сохранение длится дольше, чем остальные.

Чтобы сохранить текущее состояние виртуальной машины, выполните следующее.

1. В случае работы в полноэкранном режиме необходимо вернуться в оконный режим, нажав сочетание клавиш Ctrl+Alt.
2. Нажмите кнопку Suspend, которая расположена на Панели инструментов VMware.
3. После этого необходимо безопасно выйти из приложения с помощью команды File ▸ Exit.

Чтобы вернуться к сохраненному состоянию, нужно выполнить следующее.

1. Загрузите VMware и выберите тот виртуальный компьютер, работу которого вы ранее приостановили.
2. Нажмите кнопку Resume на панели VMware.

Взаимодействие с хостовой операционной системой

Существует всего три вида взаимодействия гостевой и хостовой операционных систем:

- наличие общего жесткого диска;
- виртуальная локальная сеть;
- использование совместных папок (Shared Folders).

Если вы выбрали первый вариант, то сможете использовать физический жесткий диск вашей хост-операционной системы; однако помните, что все изменения будут отражаться и на виртуальном диске.

Взаимодействие с виртуальным компьютером возможно и с помощью эмулируемой программы локальной сети. После установки программы в хостовой операционной системе должен появиться виртуальный сетевой адаптер VMware Network Adapter, который предназначен для связи с виртуальным компьютером (принцип работы такого адаптера соответствует реальному).

Когда вы настроите адаптер, в сетевом окружении появится еще один элемент — виртуальная машина VMware. Принцип работы с таким компьютером точно такой же, как с любой машиной в реальной локальной сети. В случае одновременного запуска нескольких операционных систем в сетевом окружении появится такое же количество новых элементов.

Настройка сети гостевой ОС производится достаточно стандартно: делается установка необходимых протоколов, IP-адреса и маски подсети. У вас есть возможность дополнительно настроить сеть с помощью встроенных средств самого виртуального компьютера VMware. Таким образом, вы сможете произвести более точную настройку Network Address Translation (NAT), Dynamic Host Configuration

Protocol (DHCP), виртуальных сетевых карт и мостов, которые их соединяют. Эта возможность пригодится в случае необходимости тестирования сетевых адаптеров: вы можете создать несколько виртуальных компьютеров и настроить эмуляцию локальной сети. Единственный минус данного способа — высокие требования к хост-компьютеру, так как придется одновременно запускать несколько гостевых операционных систем.

Самый простой способ обмена данными с виртуальным компьютером — создание общих каталогов (Shared Folders). Вам будет необходимо указать произвольную папку на физическом жестком диске и разрешить доступ к ее содержимому виртуальной машине.

Путь к общей папке нужно указать в окне настроек виртуального компьютера. Для этого щелкните в поле Commands на ссылке Edit virtual machine settings, после чего выберите вкладку Options. Войдя в пункт Shared Folders, нажмите кнопку Add. Это приведет к запуску Add Shared Folder Wizard (мастера создания общих папок). Вам будет достаточно указать полный путь к папке и режим доступа к ней (только для чтения, чтение и запись).

В виртуальном компьютере папки, к которым открыт общий доступ, подключаются, как новые сетевые диски. Чтобы подключить общую папку, необходимо выполнить команду Мой компьютер ▸ Сервис ▸ Подключить сетевой диск и из раскрывающегося списка выбрать предварительно установленную папку.

Virtual PC: еще один виртуальный знакомый

Данная программа для создания виртуальной системы издается и разрабатывается компанией Microsoft. Первоначально разработчиком Virtual PC была фирма Connectix, однако несколько лет назад проект был куплен Microsoft. Стоимость лицензионной копии программы составляет $129, а в отсутствие регистрации программа будет работать 45 дней. Для комфортной работы с программой вам понадобится компьютер с достаточно большим объемом оперативной памяти.

ПРИМЕЧАНИЕ

На компакт-диске, прилагаемом к книге, в папке ch07\VirtualPC вы найдете демонстрационную версию Microsoft VirtualPC 2004.

Установка программы не должна вызвать вопросов, главное — не забыть перезагрузиться по ее окончании.

Окно программы показано на рис. 7.14.

Принцип создания виртуального компьютера и работа с ним в VirtualPC очень напоминает аналогичные процессы в программе от VMware. Отличия незначительны, и на них мы остановимся отдельно. Подробно будут описаны только раз-

личия в работе рассматриваемых программ. VirtualPC позволяет устанавливать следующие операционные системы:

- все версии MS-DOS;
- Windows 95;
- Windows 98;
- Windows Me;
- Windows NT;
- Windows 2000;
- Windows XP;
- Windows Server 2003;
- OS/2.

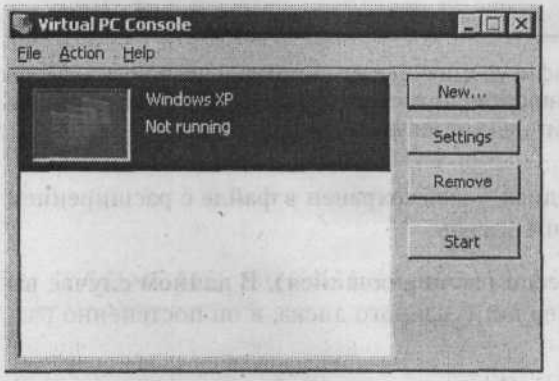


Рис. 7.14. Главное окно программы VirtualPC

Корректная работа других операционных систем также возможна, однако не гарантируется разработчиком.

Основное окно программы (VirtualPC Console) имеет несколько кнопок:

- New — создание новой виртуальной машины;
- Settings — настройки уже созданной виртуальной машины;
- Remove — удаление виртуальной машины;
- Start — запуск виртуальной машины.

New Virtual Machine Wizard — мастер, который поможет вам создать новую виртуальную машину. Сразу после установки он предложит создать новый виртуальный компьютер или воспользоваться уже существующим. Мастеру достаточно указать, какую операционную систему вы собираетесь инсталлировать на виртуальную машину, определить объем оперативной памяти, который ей требуется выделить, и создать новый виртуальный жесткий диск (если вы не используете уже созданный).

В разделе Settings главного окна можно произвести настройку всего оборудования, которое эмулируется: названия, дисплея, мыши, оперативной памяти, портов последовательных и параллельных. Также вы можете создать дополнительные жесткие диски для виртуального компьютера, настроить привод компакт-дисков, сетевую и звуковую карты (табл. 7.2).

Таблица 7.2. Типы эмулируемых устройств

Тип устройства	Эмулируемое устройство
BIOS	AMI BIOS
Чипсет материнской платы	Intel 440BX
Звуковая карта	Creative Labs Sound Blaster 16 ISA
Сетевая карта	DEC 21140A 10/1000
Видеокарта	S3 Trio 32/64 PCI с 8 Мбайт памяти

СОВЕТ

Не стоит добавлять в конфигурацию вашего виртуального компьютера звуковую карту, если вы не собираетесь ее использовать, так как такая эмуляция требует дополнительных ресурсов.

Созданный виртуальный жесткий диск будет сохранен в файле с расширением VHD. Вам доступны следующие типы дисков.

- Dynamically expanding (динамически расширяющийся). В данном случае вы указываете максимальный размер виртуального диска, и он постепенно разрастается.
- Fixed size (фиксированный размер). Сразу создается файл виртуального диска, объем которого будет соответствовать указанному.
- Differencing (различающий или дифференцирующий). Данный вариант означает привязку нового виртуального диска к уже существующему. При работе система видит оба диска, однако изменения, которые вы записываете, сохраняются только на дифференцирующий диск. Предположим, что у нас есть диск с Windows. Мы добавляем к нему дифференцирующий диск, после чего инсталлируем Internet Explorer 5. Все изменения сохранились. Затем мы устанавливаем новый дифференцирующий диск и инсталлируем Internet Explorer более поздней версии. После этой операции на каждом диске у нас будут видны и Windows, и разные версии Internet Explorer.
- Linked to a physical hard disk (связанный с физическим диском). Вместо виртуального используется физический жесткий диск. Учтите, что в этом режиме вы можете как добавить, так и удалить файлы на своем физическом диске, так что используйте данный режим только при необходимости.

Для установки операционной системы запустите виртуальную машину, войдите в ее BIOS (эмулируется AMI BIOS), нажав клавишу Delete в самом начале заг-

рузки виртуального компьютера, и установите загрузку системы с компакт-диска или дискеты (в зависимости от того, с какого носителя будет происходить загрузка).

СОВЕТ

VirtualPC захватывает указатель мыши при щелчке на его окне. Чтобы освободить курсор, нажмите правый Alt.

Процесс установки операционной системы на VirtualPC ничем не отличается от процесса установки ОС на реальный компьютер (форматирование диска, копирование файлов и т. д.).

Пять важных значков

В нижнем левом углу окна виртуального компьютера размещено пять значков (рис. 7.15). Вам придется достаточно часто с ними работать.

Рис. 7.15. Важные значки устройств

Первый значок представляет собой индикатор жестких дисков виртуальной машины. Зеленая отметка на индикаторе свидетельствует о чтении с диска, красная — о записи на диск. Если щелкнуть на этом значке правой кнопкой мыши, то появится контекстное меню, в котором можно настроить основные параметры виртуальных жестких дисков.

Второй значок является индикатором привода компакт-дисков. Щелчок правой кнопкой мыши вызывает меню, в котором можно изменить настройки виртуального привода, дать ему инструкцию работать с физическим диском (Use Physical Drive <буква диска>) или с ISO-образом (Capture ISO Image). Чтобы отказаться от использования ISO-образа, используется пункт Release.

Третий значок представляет собой индикатор виртуального дисковода. Параметры аналогичны параметрам виртуального привода компакт-дисков: Control Physical Drive <буква диска> (работа с физическим устройством), Capture Floppy Disk Image и Release Disk (монтирование и демонтирование образа дискеты).

Четвертый значок необходим для настройки работы общих папок. В VirtualPC возможно создание общих папок для обмена данными между хостовой и гостевой операционными системами. Двойной щелчок на этом значке позволит вам добавить и настроить общие папки.

Чтобы у вас была возможность работать на вашем виртуальном компьютере с общими папками, необходимо установить дополнение к VirtualPC — Virtual Machine Additions (далее — VMA).

В гостевой операционной системе после установки VMA появится возможность работы с общими папками, перетаскивания файлов прямо в окно виртуального компьютера, добавится поддержка общего буфера обмена. Следует отметить, что установка дополнений существенно повысит уровень быстродействия виртуальной машины и позволит устанавливать желаемое разрешение экрана на гостевой операционной системе с помощью изменения размеров окна.

Для инсталляции VMA достаточно выбрать Action ▸ Install of Update Virtual Machine Additions в окне виртуальной машины. После того как VMA будет установлена, у вас появится возможность добавлять общие папки в настройках параметров виртуальной машины.

Пятый значок — индикатор активности сетевой карты. Двойной щелчок на этом значке позволит указать параметры доступа к локальной сети виртуального компьютера.

Сеть настраивается во вкладке Networking в окне настроек виртуального компьютера. В этом же окне вы сможете выбрать нужное количество сетевых адаптеров и настроить их конфигурацию. Основных вариантов четыре (практически аналогичны режимам доступа в VMware):

- Not connected — без сети;
- Local only — сеть доступна только между гостевой и хостовой компьютерами;
- Shared Networking — этот режим позволяет виртуальной машине получать доступ ко всем сетевым ресурсам, к которым подключена хостовая операционная система;
- Network adapter on the physical computer — виртуальная машина будет вести себя как физический компьютер в сети, используя настройки данной сети.

Для полноценного доступа к сети рекомендуется использовать последние два варианта.

VMware и VirtualPC: что лучше?

Данные программы достаточно схожи, однако самое главное отличие VirtualPC от VMware состоит в том, что VirtualPC (даже без установки дополнений) эмулирует видеоадаптер S3 Trio 32/64 PCI, который работает с большинством операционных систем. VMware без установленных VMware Tools может работать исключительно в ограниченных графических режимах VGA. Поэтому какая-нибудь не слишком распространенная ОС с большей вероятностью будет работать под VirtualPC.

Одним из преимуществ VMware является то, что она практически бесплатна для некоммерческого использования (однако вам нужно будет время от времени заказывать ключи на сайте производителя). VirtualPC без регистрации будет работать в течение 45 дней, а для дальнейшего ее использования вам придется купить лицензию.

Следует отметить и тот факт, что VMware поддерживает большее количество операционных систем, нежели VirtualPC.

В любом случае вам следует взвесить все преимущества и недостатки этих очень похожих программ перед тем, как сделать выбор. Достаточно часто VMware показывает отличные результаты, однако если возникают ошибки при установке какой-нибудь малораспространенной операционной системы, то стоит попробовать VirtualPC — вполне возможно, что она осилит эту проблему.

Как вы уже поняли, виртуальная машина практически незаменима в работе системного администратора или разработчика программного обеспечения. Автору книги с ее помощью удалось опробовать множество сетевых технологий (включая Windows Remote Desktop, Windows Terminal Services, Windows Home Network, Distribute File System, Routing, NAT, DHCP и другие расширенные сетевые настройки) на своем домашнем компьютере. Однако помните, что для полноценного использования виртуальной машины вам потребуется достаточно мощный компьютер.

Заключение

Приемы и трюки системного администрирования, перечисленные в этой книге, не являются исчерпывающим материалом по настройке и системному администрированию сетей на базе операционной системы Windows XP, однако я надеюсь, что они смогут помочь вам в этом нелегком процессе.

Главное — читать больше документации и разбираться в составе операционной системы, ее сервисах и сервисах используемого прикладного программного обеспечения. Тогда ответы на возникающие вопросы будут находиться быстро, а системное администрирование из нудной рутины превратится в увлекательное занятие.

Надеюсь, эта книга поможет вам.

Приложение. Содержимое компакт-диска

На компакт-диске, который вы получили вместе с этой книгой, расположены все упомянутые в ней программы. Программное обеспечение располагается в папках, рассортированных по главам книги. Например, чтобы найти программное обеспечение, рассматриваемое в третьей главе, нужно открыть папку ch03 на компакт-диске.

Кроме того, в папке utils в корневом каталоге компакт-диска расположены утилиты и программы, полезные системному администратору, описание которых не вошло в эту книгу.

Содержимое папки ch02

Папка SpamPal:

- программа SpamPal.

Папка Traffic Inspector v 1.1:

- Traffic Inspector v 1.1.

Содержимое папки ch03

Папка XP Tweaker v 1.53:

- программа XP Tweaker v 1.53.

Содержимое папки ch04

Папка Acronis TrueImage v 8:

- программа Acronis TrueImage v 8.

Папка Driver Cleaner v 3.3:

- программа Driver Cleaner v 3.3.

Папка EasyRecovery v 6:

- программа EasyRecovery v 6.

Папка Remote Administrator:

- программа Remote Administrator v 2.2;
- программа Radmin Viewer v 3.0 beta.

Содержимое папки ch05

Папка Kaspersky:

- программа Kaspersky Anti-Haker v 1.7;
- программа Kaspersky Anti-Virus v 5.0.

Папка StrongDisk Pro:

- программа StrongDisk Pro 3.0;
- документация к программе StrongDisk Pro в формате PDF.

Папка XSpider 7.0:

- программа XSpider 7.0 Demo.

Содержимое папки ch06

Папка Hardware Sensors Monitor:

- программа Hardware Sensors Monitor.

Папка Memtest:

- образы программы Memtest86+ v 1.4 для компакт-диска и дискет;
- программа Memtest v 3.0 для Windows.

Папка PCMark:

- программа PCMark 2004.

Папка Power Supply Calculator:

- программа Power Supply Calculator.

Папка SiSoftware Sandra:

- программа SiSoftware Sandra 2004.

Содержимое папки ch07

Папка VirtualPC:

- ознакомительная версия программы Microsoft VirtualPC 2004.

Папка VMware 5:

- программа VMware 5.

Содержимое папки utils

Эта папка содержит различные утилиты и программы, которые могут быть полезны системному администратору.

Папка Anti-Spammer v 2.0.4 Light:

- Anti-Spammer v 2.0.4 Light — программа для борьбы с нежелательной корреспонденцией.

Папка Awatch v 1.0:

- Awatch v 1.0 — утилита для тестирования сетевых карт. Интерфейс английский.

Папка Diskeeper v 9.0:

- Diskeeper v 9.0 — ознакомительная версия программы для восстановления данных.

Папка Drive Rescue v 1.9:

- Drive Rescue v 1.9 — утилита для восстановления удаленных по ошибке данных или восстановления случайно отформатированного жесткого диска (работает с FAT12/16/32 и частично с NTFS). Конечно, есть профессиональные программы аналогичного назначения, но Drive Rescue, в отличие от них, является бесплатной.

Папка Far v 1.7:

- Far v 1.7 — популярный файловый менеджер.

Папка Firefox v 1.0.3:

- программа Firefox v 1.0.3 — облегченная версия браузера Mozilla.

Папка Folder Locker v 1.1:

- Folder Locker v 1.1 — ознакомительная версия утилиты для блокирования доступа к отдельным папкам вашего компьютера.

Папка Recover My Files v 3.25:

- Recover My Files v 3.25 — программа для восстановления удаленных файлов.

Папка Systerac XP Tools 3.0b:

- Systerac XP Tools 3.0b — это десять инструментов для оптимизации, диагностики, предотвращения сбоев и исправления ошибок в Windows XP.

Папка Total Commander 6.52:

- Total Commander 6.52 — один из лучших файловых менеджеров. Настоящая находка для системного администратора.

Папка TweakMASTER PRO 2.04 build 764:

- TweakMASTER PRO 2.04 build 764 — отличается от подобных программ прежде всего узкой направленностью. Если другие оптимизаторы часто включают в себя самые разнообразные утилиты, от чистильщика реестра до средств резервного копирования данных, то TweakMASTER содержит только средства для настройки интернет-соединения независимо от его типа — модем, кабель, спутник и т. д.

Папка Tweak-XP Pro 4.05:

- Tweak-XP Pro 4.05 — это программный комплекс из 22 утилит, позволяющий оптимизировать производительность операционной системы Windows XP. Утилиты позволяют настроить скрытые установки операционной системы. С их помощью можно получать доступ к скрытым настройкам производительности системы, устанавливать блокировку баннеров и всплывающих окон Internet Explorer, настраивать безопасность Outlook, восстанавливать поврежденные ZIP-архивы, создавать виртуальные диски, оптимизировать соединение с Интернетом. С помощью Tweak-XP Pro 4.05 вы также сможете скрыть любую папку от просмотра, поиска и удаления «мусора» на диске.

Папка WinRAR 3.11:

- WinRAR 3.11 RUS — один из лучших архиваторов.

[на 100 %]

Системное администрирование

В книге, которую вы держите в руках, рассмотрены все аспекты системного администрирования: от настройки и управления учетными записями до устранения неисправностей и резервного копирования.

Издание выполняет сразу несколько функций: опытные системные администраторы могут использовать его в качестве наиболее полного справочника, начинающие — в качестве учебника, все категории читателей — в качестве практического руководства по системному администрированию. С помощью изложенных приемов и методик вы не только обеспечите бесперебойную работу ваших компьютеров, но и заметно увеличите их производительность.

Все программы, описанные на страницах книги, находятся на прилагаемом компакт-диске. Там же можно найти множество дополнительных утилит, которые будут полезны системному администратору.

ПИТЕР®

Заказ книг:

197198, Санкт-Петербург, а/я 619
тел.: (812) 703-73-74, postbook@piter.com

61093, Харьков-93, а/я 9130
тел.: (057) 712-27-05, piter@kharkov.piter.com

www.piter.com — вся информация о книгах и веб-магазин

ISBN 5-469-01220-4

9 785469 012207